A Letters Journal Exploring the Frontiers of Physics

October 2008

EPL, **84** (2008) 20013
doi: 10.1209/0295-5075/84/20013

www.epljournal.org

Quantum direct communication with continuous variables

S. Pirandola[1(a)], S. L. Braunstein[2], S. Mancini[3] and S. Lloyd[1,4]

[1] *MIT - Research Laboratory of Electronics - Cambridge MA 02139, USA*
[2] *Computer Science, University of York - YO10 5DD York, UK, EU*
[3] *CNISM and Dipartimento di Fisica, Università di Camerino - I-62032 Camerino, Italy, EU*
[4] *MIT - Department of Mechanical Engineering - Cambridge MA 02139, USA*

received 5 February 2008; accepted in final form 12 September 2008
published online 14 October 2008

PACS 03.67.Dd – Quantum cryptography and communication security
PACS 03.67.Hk – Quantum communication
PACS 42.50.-p – Quantum optics

Abstract – We show how continuous-variable systems can allow the direct communication of messages with an acceptable degree of privacy. This is possible by combining a suitable phase-space encoding of the plain message with real-time checks of the quantum communication channel. The resulting protocol works properly when a small amount of noise affects the quantum channel. If this noise is non-tolerable, the protocol stops leaving a limited amount of information to a potential eavesdropper.

Introduction. – In recent years, quantum communication protocols have been extended to the domain of continuous-variable (CV) systems, *i.e.*, quantum systems, like the bosonic modes of the radiation field, which are characterized by infinite dimensional Hilbert spaces [1]. In particular, it has been understood how a sender (Alice) can exploit bosonic modes in order to send analog signals to a receiver (Bob) and then extract a secret binary key from these signals [2,3]. Beyond the possibility of such a continuous-variable quantum key distribution (QKD), here we show how to use these systems in order to perform a (quasi)confidential quantum direct communication (QDC) [4], *i.e.*, the (quasi)private communication of a message from Alice to Bob which is directly encoded in CV systems.

The ideal situation for QDC trivially occurs when Alice and Bob are connected by a noiseless channel. However, in general, this is not the case and the honest users must randomly switch their confidential communication with real-time checks on the channel. As soon as they detect the presence of a non-tolerable noise, they promptly stop the communication. The maximum noise that can be tolerated is connected to the maximum amount of information that they are willing to give up to an eavesdropper. In other words, a good QDC protocol should enable Alice and Bob to communicate all the message when the noise is suitably low, while losing a small amount of information when it is not.

(a) E-mail: pirs@mit.edu

Let us consider a bosonic mode described by quadrature operators $\hat{q}$ and $\hat{p}$, satisfying $[\hat{q},\hat{p}]=i$. An arbitrary state of the system (density operator ρ) must fulfill the uncertainty principle $V(\hat{q})V(\hat{p})\geqslant 1/4$, where $V(\hat{x})=\mathrm{Tr}(\rho\hat{\mathrm{x}}^2)-[\mathrm{Tr}(\rho\hat{\mathrm{x}})]^2$ denotes the variance of the arbitrary quadrature $\hat{x}=\hat{q}$ or $\hat{p}$. In particular, coherent states satisfy $V(\hat{q})=V(\hat{p}):=\Delta$, where $\Delta=1/2$ represents the quantum shot-noise. This is the fundamental noise that affects *disjoint* measurements of the quadratures $\hat{q}$ and $\hat{p}$ (homodyne detection), and it is doubled to $\Delta=1$ when the two quadratures are *jointly* measured (heterodyne detection). A density operator ρ may be faithfully represented by the Wigner quasi-probability distribution $W(q,p)$, whose continuous variables q and p are the eigenvalues of the quadratures. In this phase-space representation, states with Gaussian Wigner functions are called *Gaussian states*. This is the case of a coherent state $|\bar{\alpha}\rangle$, whose Gaussian Wigner function is centered at $\bar{\alpha}=2^{-1/2}(\bar{q}+i\bar{p})$. For coherent states the detection of an arbitrary quadrature $\hat{x}$ provides outcomes x following the marginal distribution

$$G_{\Delta}(x-\bar{x})=\frac{1}{\sqrt{2\pi\Delta}}\exp\left[-\frac{(x-\bar{x})^2}{2\Delta}\right], \qquad (1)$$

where $\Delta=1/2$ for homodyne and $\Delta=1$ for heterodyne.

The protocol. – Let us show how Alice can transmit message bits by using the phase-space of a bosonic mode. We discretize the phase-space via a square lattice of half-step size Ω. Then, an arbitrary cell specifies the values

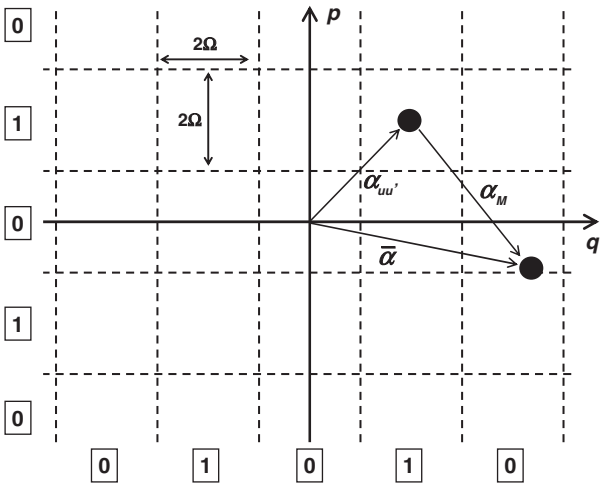

Fig. 1: Square lattice in phase-space with unit cell of size 2Ω. Each cell specifies the values of a pair of bits (u, u').

of two bits (u, u') which are given by the parity of its address along the q and p axes (see fig. 1). In a simple lattice encoding, Alice embeds two bits (u, u') by *randomly* choosing a target cell with parities (u, u') or, equivalently, by constructing the message amplitude $\alpha_{uu'}$ pointing at the center of that target cell. Then, in a first naive protocol, Alice directly prepares the coherent state $|\alpha_{uu'}\rangle$ from the message amplitude $\alpha_{uu'}$. Such a state is sent to Bob, who performs a heterodyne detection for extracting $\alpha_{uu'}$ and, therefore, the pair (u, u'). Notice that, even in the presence of a noiseless channel, Bob's decoding cannot be perfect since the Gaussian shape of the coherent state spreads over the whole phase-space and this leads to an *intrinsic error*. It is easy to check that the probability of an intrinsic error (per transmitted bit) is

$$\varepsilon(\Omega, \Delta) = 2 \sum_{j=0}^{\infty} \int_{(4j+1)\Omega}^{(4j+3)\Omega} \mathrm{d}x \; G_{\Delta}(x). \tag{2}$$

In particular, here we fix $\Omega \simeq 2.57$ in order to have the reasonable low value of $\varepsilon = 1\%$. On the one hand, such a choice for Ω enables Bob to approach an error-free decoding when the communication channel is noiseless. On the other hand, it makes the protocol fragile to eavesdropping since Eve can optimize her attack to the structure of the lattice, *e.g.*, by using non-universal quantum cloning machines.

Fortunately, we can preclude these strategies by adding a simple classical (*masking*) step to the above procedure. In fact, after having computed the message amplitude $\alpha_{uu'}$, Alice can add a *mask* amplitude α_M, in such a way that the total *signal* amplitude $\bar{\alpha} := \alpha_M + \alpha_{uu'}$ is continuously distributed in phase-space according to a spread Gaussian (see fig. 1). Then, in a second refined protocol, Alice prepares the message $\alpha_{uu'}$, the mask α_M and the signal state $|\bar{\alpha}\rangle$ (see fig. 2). As a first step, Alice sends the signal state $|\bar{\alpha}\rangle$ to Bob, who heterodynes it with outcome

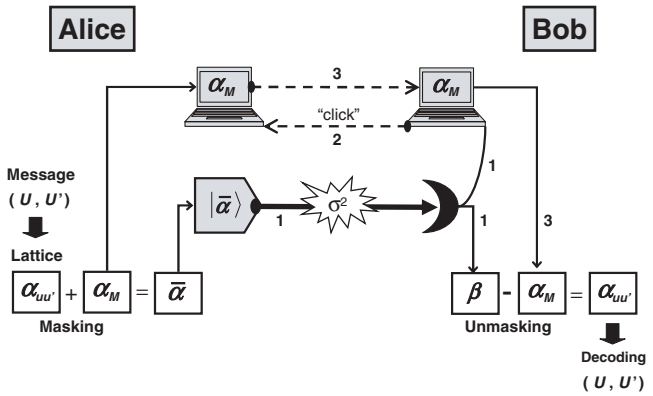

Fig. 2: Message mode (MM). From the message bits (u, u'), Alice computes the message amplitude $\alpha_{uu'}$ (lattice encoding) and then adds the mask α_M achieving the signal amplitude $\bar{\alpha}$. Then, Alice prepares and sends to Bob the signal state $|\bar{\alpha}\rangle$, that Bob heterodynes with outcome β (step 1 in the picture). After detection, Bob classically informs Alice (step 2) and, then, Alice classically communicates the mask α_M (step 3). At that point, Bob is able to unmask the signal $(\beta - \alpha_M)$, thus reconstructing $\alpha_{uu'}$ and, therefore, (u, u').

$\beta \simeq \bar{\alpha}$. Then, after Bob's confirmation of detection, Alice classically communicates the mask α_M. As a consequence of these steps, Bob gets the pair (β, α_M) from his detection and Alice's communication. Then, Bob is able to *unmask* the signal by computing $\beta - \alpha_M \simeq \bar{\alpha} - \alpha_M = \alpha_{uu'}$ and, therefore, retrieves the message bits (u, u') via lattice decoding. The key point here is that Eve must choose the probing interaction before knowing the value of the mask. Since the continuous signal $\bar{\alpha}$ is highly modulated, the best choice is to adopt a universal interaction which does not privilege any particular portion of the phase-space. Here, we consider for Eve the usage of a universal Gaussian quantum cloning machine (UGQCM) [5]. Such a machine maps the signal state $|\bar{\alpha}\rangle$ into a pair of output clones ρ_B (sent to Bob) and ρ_E (taken by Eve), equal to a Gaussian modulation of $|\bar{\alpha}\rangle\langle\bar{\alpha}|$ with cloning variances $\sigma_B^2 := \sigma^2$ and $\sigma_E^2 = (4\sigma^2)^{-1}$. This means that the arbitrary quadrature $\hat{x}$ of the clone $K = B, E$ has a marginal distribution equal to $G^K_{\Delta+\sigma_K^2}(x - \bar{x})$.

The above procedure of directly communicating message bits is called the *message mode* (MM) of the protocol. However, Alice and Bob have to also perform real-time controls of the added noise σ^2 on the channel. This is possible if Alice randomly switches from message mode instances to suitable instances of *control mode* (CM) (see fig. 3) [6]. In control mode, Alice does not process any text message but only prepares and sends the signal state $|\bar{\alpha}\rangle$. Then, after Bob's detection (outcome β), Alice communicates the value $\bar{\alpha}$ of the signal amplitude. At that point, Bob extracts from $(\beta, \bar{\alpha})$ the actual value of the *test variable* $\tau := \beta - \bar{\alpha}$ which is then used to infer the total noise $\Delta_B = 1 + \sigma^2$ affecting the signal. As soon as they recognize a non-tolerable noise, *i.e.*, $\sigma^2 > \tilde{\sigma}^2$ for

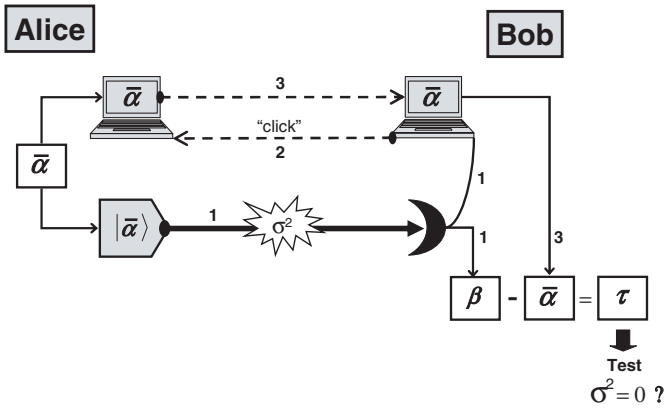

Fig. 3: Control mode (CM). Alice picks up a Gaussian amplitude $\bar{\alpha}$ and prepares a signal coherent state $|\bar{\alpha}\rangle$. Such a state is sent to Bob, who heterodynes it with outcome β (step 1 in the picture). Then, Bob classically informs Alice (step 2) and Alice communicates the value of the signal $\bar{\alpha}$ (step 3). At that point, Bob computes the test variable $\tau := \beta - \bar{\alpha}$ and tests the noise of the channel.

some threshold noise $\tilde{\sigma}^2$, they stop the communication. Hereafter, we assume a zero-tolerance protocol where no added noise is tolerated on the channel, *i.e.*, $\tilde{\sigma}^2 = 0$. We shall see that the QDC protocol can be applied in realistic situations even with such a strict condition[1].

Let us show how the real-time check works in detail. For each control mode, Bob collects the two quadratures $x = q, p$ of the test variable τ. Then, after M control modes, he has collected $2M$ quadratures values $\{x_1, x_2, \cdots, x_{2M-1}, x_{2M}\}$ which give the estimator $v = \sum_{l=1}^{2M} x_l^2$. By using this estimator, Bob must distinguish the two hypotheses

$$H_0 = \text{no Eve} \Leftrightarrow \sigma^2 = 0, \qquad H_1 = \text{yes Eve} \Leftrightarrow \sigma^2 \neq 0. \quad (3)$$

Let us fix the confidence level r (*i.e.*, the probability to reject H_0 though true) to a reasonably low value (*e.g.*, $r = 5 \times 10^{-7}$). Then, the hypothesis H_0 is accepted if and only if

$$v < \mathcal{V}_{2M,1-r}, \quad (4)$$

where $\mathcal{V}_{i,j}$ is the j-th quantile of the χ^2 distribution with i degrees of freedom. In other words, Alice and Bob continue their direct communication in MM as long as the condition of eq. (4) is satisfied in CM.

Let us explicitly analyze what happens when the channel is subject to eavesdropping. In an individual UGQCM attack, Eve clones the signal input and, then, heterodynes her output to estimate the signal amplitude $\bar{\alpha}$. After the release of the mask's value α_M, Eve infers the message amplitude $\alpha_{uu'}$ and, therefore, the input bits (u, u'). In this process, Eve introduces an added noise σ^2 on the Alice-Bob channel, while her output is affected by a total noise equal to $\Delta_E = 1 + (4\sigma^2)^{-1}$. On the one hand, we must compute the probability $\Pi_M(\sigma^2)$ that Eve evades M control modes while introducing noise $\sigma^2 \neq 0$. After some algebra we get

$$\Pi_M(\sigma^2) = \left[\Gamma(M,0) - \Gamma\left(M, \frac{\mathcal{V}_{2M,1-r}}{2(1+\sigma^2)}\right)\right] \Big/ (M-1)!, \quad (5)$$

where $\Gamma(z,a) := \int_a^{+\infty} \mathrm{d}t\, t^{z-1} e^{-t}$ is the incomplete gamma function. On the other hand, we must evaluate the amount of information she can steal during her undetected life on the channel. Let us assume that every input bit is a bit of information. As a consequence, the stolen information per MM is equal to $I_{AE} = 2[1 - H(p)]$, where $H(p) := -p \log p - (1-p)\log(1-p)$ and $p = \varepsilon(\Omega, \Delta_E)$ can be computed from eq. (2). By combining Π_M and I_{AE}, we can derive Eve's survival probability as a function of the stolen information. Let c be the probability of a control mode, so that N runs of the protocol are composed by cN control modes and $(1-c)N$ message modes, on average. As a consequence, the survival probability will be $P := \Pi_{cN}(\sigma^2)$ and the average number of stolen bits will be $I := (1-c)N I_{AE}(\sigma^2)$. Then, for every value of c and σ^2, we can determine the function $P = P(I)$. Let us fix $c = 69/70$ so that the protocol has efficiency

$$\mathcal{E} := \frac{\#\text{bits}}{\#\text{systems}} = \frac{1}{35}. \quad (6)$$

In fig. 4, we have numerically plotted $P = P(I)$ for several values of the added noise σ^2. If the noise is low, *e.g.*, $\sigma^2 = 0.01$, Eve steals very little information ($\simeq 1$ bit) while Alice and Bob complete an almost noiseless QDC. In particular, Alice is able to transmit $\simeq 1.5 \times 10^4$ bits of information by using $N \simeq 5 \times 10^5$ systems. Notice that the maximum length of the QDC is roughly bounded by the verification of r^{-1} hypothesis tests and, therefore, it is limited to about $4(1-c)(cr)^{-1}$ bits (*i.e.*, $\simeq 1.2 \times 10^5$ bits or $\simeq 4 \times 10^6$ systems using the above parameters). If the attack is more noisy (*e.g.*, $\sigma^2 = 1$), Eve again steals little information ($\simeq 1$ bit). In such a case, in fact, Eve is promptly detected by the honest parties who, however, are prevented from exchanging information (denial of service). According to fig. 4, Eve's best strategy corresponds to use a UGQCM with $\sigma^2 \simeq 1/20$, so that she can steal $\simeq 80$ bits before being revealed (for a cut-off of $P = 1\%$). In such a case, Alice transmits $\simeq 630$ bits by using $N \simeq 2.2 \times 10^4$ systems.

How can we decrease the maximal amount of stolen information? One possible solution is to increase further the control mode probability c, so that the eventual presence of Eve is detected before sending too many bits. However, this approach affects the efficiency $\mathcal{E}$. An alternative and better solution consists of making the decoding more sensitive to the presence of added noise. Such an approach is possible by introducing classical error correcting codes.

[1] A zero-tolerance protocol does not promptly stop in realistic situations (where $\sigma^2 \neq 0$) because the confidence level r cannot be equal to zero.

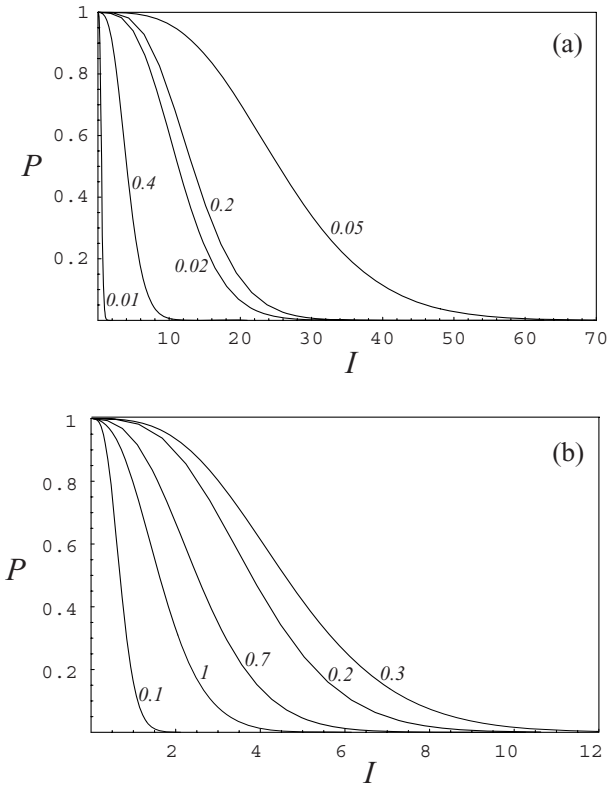

Fig. 4: Survival probability P *vs.* the number of stolen bits I. In (a) no codes are used while in (b) a repetition code with $n=35$ is used. The curves refer to UGQCM attacks with different values of added noise σ^2.

Improving QDC via repetition codes. – In the basic scheme of QDC with continuous variables, noiseless communication is possible up to an intrinsic error probability ε depending on Ω. In particular, such a probability decreases for increasing Ω. An alternative way for decreasing ε consists of leaving Ω unchanged while introducing a classical error correcting code. Such procedures are essentially equivalent for a noiseless channel, since ε is sufficiently small and the codes work very well in that case. However, the scenario is different as the channel becomes noisier. In such a case, in fact, the correcting codes have a non-linear behavior which makes their performance rapidly deteriorate. Such a non-linear effect can be exploited to critically split the correction capabilities, and therefore the information gains, between the Alice-Bob channel and the Alice-Eve channel.

For the simplest case of an n-bit repetition code, an input bit $U=\{0,1\}$ is encoded into a logical bit $\bar{U}=\{\bar{0},\bar{1}\}$ of n physical bits via the codewords

$$\bar{0}=\underbrace{00\cdots0}_{n},\qquad \bar{1}=\underbrace{11\cdots1}_{n}. \tag{7}$$

By choosing an odd $n=2m+1$ (with $m=1,2,\cdots$), we can apply a non-ambiguous majority voting criterion. This means that every bit-flip error of weight $t<m+1$ is correctable, while every bit-flip error of weight $t\geqslant m+1$ is not. Let us now consider a memoryless channel, where each physical bit is perturbed independently with the same bit-flip probability p (as happens in the case of individual attacks). Then, the probability of an uncorrectable error is given by

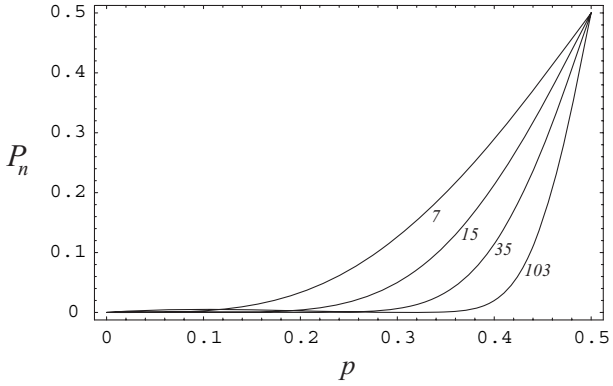

Fig. 5: Probability of an uncorrectable error P_n *vs.* the single bit-flip probability p. Here, we consider repetition codes with $n=7;\ 15;\ 35;\ 103$.

$$P_n(p)=\sum_{k=m+1}^{n}\binom{n}{k}p^k(1-p)^{n-k}. \tag{8}$$

For a sufficiently large n, the curve $P_n(p)$ displays a critical point after which the correction capability suddenly starts to deteriorate very quickly (see, *e.g.*, fig. 5, showing $\tilde{p}\simeq 0.3$ for $n=35$ and $\tilde{p}\simeq 0.4$ for $n=103$). Exactly these critical points enable one to improve the QDC by transforming the communication protocol into a threshold process, where the sensitivity to added noise is remarkably amplified.

Let us choose a critical lattice's half-step $\tilde{\Omega}$, *i.e.*, leading to a critical intrinsic error probability $\varepsilon=\tilde{p}$. On the one hand, when the channel is noiseless, Bob is able to recover the codewords and reconstruct the logical bit with a very low error probability $P_B=P_n(\tilde{p})$ (that we call the *logical* intrinsic error probability). On the other hand, when the channel is noisy, Alice's information is split into two sub-channels: the Alice-Bob channel, with added noise $\sigma_B^2=\sigma^2$, and the Alice-Eve channel, with added noise $\sigma_E^2=(4\sigma^2)^{-1}$. The corresponding error probabilities are, respectively, given by

$$P_B=P_n(\tilde{p}+p_B),\qquad P_E=P_n(\tilde{p}+p_E), \tag{9}$$

where $p_B=p_B(\sigma_B^2)$ and $p_E=p_E(\sigma_E^2)$ are monotonic functions of the added noises (and are therefore linked by the uncertainty principle). Now, if Eve tries to hide herself by perturbing the Alice-Bob channel with a relatively small p_B, then her dual p_E will always be big enough to perturb $\tilde{p}$ into the non-linear region. As a consequence, Eve will tend to experience $P_E\simeq 1/2$, gaining her negligible information.

Let us explicitly show how to use an n-bit repetition code for encoding/decoding. This is possible by

simply adding pre-encoding and post-decoding classical steps to the basic protocol. The message bits (U, U') are pre-encoded into a pair of logical bits

$$\bar{U} = U_1 U_2 \cdots U_n, \qquad \bar{U}' = U'_1 U'_2 \cdots U'_n, \tag{10}$$

via the n-bit repetition code. Each pair of physical bits (U_k, U'_k) is then subject to the same encoding as before, *i.e.*, lattice encoding $(U_k,\ U'_k) \to \alpha_{u_k u'_k} := \alpha_k$, masking $\alpha_k \to \alpha_k + \alpha_M = \bar{\alpha}$ and quantum preparation $\bar{\alpha} \to |\bar{\alpha}\rangle$. Then, after n message modes, Bob will have collected perturbed versions of the n pairs $(U_1, U'_1), \cdots, (U_n, U'_n)$. By applying standard error recovery (majority voting), he will then perform the post-decoding of (U, U'). In the same way as before, these instances of MM (each one carrying a single physical bit of a codeword) must be randomly switched with instances of CM, where Alice skips encoding and simply sends Gaussian signals $\bar{\alpha}$ for testing the channel (exactly as in fig. 3).

Let us choose a repetition code with $n = 35$. Then, consider a critical half-step $\tilde{\Omega} = 1$. Such a choice implies $\tilde{p} \simeq 32\%$ which leads to $\tilde{\varepsilon} \simeq 1\%$ for the logical bits (U, U'). Then, let us also choose $c = 1/2$, so that we again achieve an efficiency $\mathcal{E} = 1/35$. Let us then analyze the effect of a UGQCM attack. On every cloned system (with noise σ^2_E), Eve detects the complex amplitude via heterodyne detection, therefore, estimating Alice's signal amplitude $\bar{\alpha}$ up to a total noise $\Delta_E = 1 + \sigma^2_E$. After Alice's declaration of the mask α_M, Eve derives the message amplitude and, therefore, a pair of physical bits (U_k, U'_k). Each physical bit will be affected by an error probability $p(\Delta_E)$. After n eavesdropped message modes, Eve will be able to decode Alice's logical bit by majority voting up to an error probability $P_E = P_n[p(\Delta_E)]$. For each logical bit, the acquired information is simply equal to $1 - H(P_E)$. As a consequence, for each message mode, Eve acquires on average

$$I_{AE}(\sigma^2) = 2\left[1 - H(P_E)\right]/n, \tag{11}$$

bits of information (simply because 2 logical bits are sent via n physical systems).

Let us then consider the probability of Eve to evade M control modes. Since the control mode is implemented exactly as before, we have again $\Pi_M(\sigma^2)$ as in eq. (5). Such a quantity can be again combined with the one of eq. (11). After N runs of the protocol, we have an average of cN control modes and $(1-c)N$ message modes, so that Eve's survival probability is again $\Pi_{cN}(\sigma^2) := P$ and the stolen information is equal to $(1-c)N I_{AE}(\sigma^2) := I$. Then, for every σ^2, we can again evaluate the curve $P = P(I)$. According to fig. 4, the best choice for Eve is a UGQCM with $\sigma^2 \simeq 0.3$, which enables her to steal only 10 bits of information before being detected (for $P = 1\%$). Such a result is a strong improvement with respect to the basic protocol, where 80 bits were left to Eve. Notice that, for a low value of the noise like $\sigma^2 = 0.1$, Eve gets $\simeq 1$ bit while Alice transmits $\simeq 320$ bits of information by using $N \simeq 1.1 \times 10^4$ systems. The maximal length of QDC is here bounded by $4(1-c)(ncr)^{-1} \simeq 3500$ bits, *i.e.*, $N \simeq 1.2 \times 10^5$ quantum systems.

Conclusion and discussion. – We have considered Alice and Bob confidentially communicating without resorting to QKD. Such a task is in general risky and very demanding. However, here we have shown how to construct a QDC protocol which uses the same quantum resources as standard QKD, even if they are exploited with a different logic. Such a protocol is sufficiently confidential since it combines real-time checks of the channel and a suitable masking of the secret information. In particular, the maximum stolen information (*i.e.*, the lack of complete secrecy) can always be decreased by increasing the number of controls at the expense of efficiency. As an alternative approach we have also suggested the use of error correcting codes, in such a way as to amplify the difference of information between the eavesdropper and the honest user.

As a natural consequence of a demanding task like QDC, our protocol allows an effective communication only when a small amount of noise affects the quantum channel, thus restricting its application to relatively short distances. Despite this restriction, there are non-trivial situations where it can be used in a profitable way. One of the possible applications concerns entity authentication [7], where one of the users (*e.g.*, Bob) identifies the other (Alice) by comparing the bits of a pre-distributed and secret *authentication key* $K_{\rm aut}$. Using the QDC protocol, the honest users have the chance to perform this task without wasting too many quantum resources. For instance, let us consider the case where Eve does not perturb the quantum channel but impersonates Alice. Such a quantum impersonation attack [8] is promptly revealed by a small QDC session, where Bob receives directly the bits of $K_{\rm aut}$ and, therefore, performs an immediate comparison with his secret data. By contrast, in actual QKD protocols, such an attack can be revealed only after the generation of the encryption key $K_{\rm enc}$ (to be used in the private comparison of $K_{\rm aut}$). This clearly requires the distribution and detection of many quantum states (ideally infinite) and, therefore, the useless manipulation of a huge amount of quantum resources (especially when entity authentication is mutual). In general, since our QDC scheme adopts the same quantum hardware as the standard coherent state QKD, one can also consider random switching between QDC (for authentication) and QKD (for key generation).

As a final remark notice that our security analysis concerns the case of individual attacks (where Eve does not exploit any quantum memory). In future work it would be interesting to investigate the performance of the protocol in the presence of collective attacks, where Eve exploits a quantum memory to store all her output probes and performs an optimal coherent measurement. It would be also interesting to extend the security analysis to other forms of Gaussian interactions

(*i.e.*, not referable to a UGQCM) and even to non-Gaussian interactions, that may play a role against the usage of repetition codes.

* * *

The research of SP was supported by a Marie Curie Outgoing International Fellowship within the 6th European Community Framework Programme. SL was supported by the W. M. Keck Foundation Center for Extreme Quantum Information Theory (xQIT).

REFERENCES

[1] Braunstein S. L. and Pati A. K., *Quantum Information Theory with Continuous Variables* (Kluwer Academic, Dordrecht) 2003; Braunstein S. L. and van Loock P., *Rev. Mod. Phys.*, **77** (2005) 513.

[2] Grosshans F. and Grangier Ph. *et al.*, *Phys. Rev. Lett.*, **88** (2002) 057902; Grosshans F. *et al.*, *Nature*, **421** (2003) 238.

[3] Weedbrook C. *et al.*, *Phys. Rev. Lett.*, **93** (2004) 170504; Lance A. M. *et al.*, *Phys. Rev. Lett.*, **95** (2005) 180503.

[4] Shimizu K. and Imoto N., *Phys. Rev. A*, **60** (1999) 157; **62** 054303 (2000); Beige A. *et al.*, *J. Phys. A*, **35** (2002) L407; *Acta Phys. Pol.*, **101** (2002) 357.

[5] Cerf N. J. *et al.*, *Phys. Rev. Lett.*, **85** (2000) 1754.

[6] Boström K. and Felbinger T., *Phys. Rev. Lett.*, **89** (2002) 187902; Lucamarini M. and Mancini S., *Phys. Rev. Lett.*, **94** (2005) 140501.

[7] Menezes A. J., van Oorschot P. C. and Vanstone S. A., *Handbook of Applied Cryptography* (CRC Press) 1997.

[8] Dušek M. *et al.*, *Phys. Rev. A*, **60** (1999) 149.