Confidential Direct Communications: A Quantum Approach Using Continuous Variables

Citation: Pirandola, S. et al. "Confidential Direct Communications: A Quantum Approach Using Continuous Variables." Selected Topics in Quantum Electronics, IEEE Journal of 15.6 (2009): 1570-1580. © 2009 Institute of Electrical and Electronics Engineers.

As Published: http://dx.doi.org/10.1109/jstqe.2009.2021147

Publisher: Institute of Electrical and Electronics Engineers

Persistent URL: http://hdl.handle.net/1721.1/54818

Version: Final published version: final published article, as it appeared in a journal, conference proceedings, or other formally published context

Confidential Direct Communications: A Quantum Approach Using Continuous Variables

Stefano Pirandola, Samuel L. Braunstein, *Senior Member, IEEE*, Seth Lloyd, and Stefano Mancini

(Invited Paper)

***Abstract*—We consider the problem of privacy in direct communications, showing how quantum mechanics can be useful to guarantee a certain level of confidentiality. In particular, we review a continuous variable approach recently proposed by us [Pirandola *et al.*, *Europhys. Lett.*, vol. 84, pp. 20013-1–20013-6, 2008]. Here, we analyze the degree of privacy of this technique against a broader class of attacks, which includes non-Gaussian eavesdropping.**

***Index Terms*—Cloning, continuous variables, error correction, Gaussian states, non-Gaussian attacks, quantum communication, security.**

I. Introduction

QUANTUM mechanics provides a nice solution to an old cryptographic problem, i.e., the key distribution problem [1], [2]. Going further, we consider whether or not quantum mechanics could profitably be exploited even for direct confidential communication, without resorting to the use of predistributed private keys. Since many quantum communication protocols like quantum key distribution (QKD) [1], [2] and quantum teleportation [3] have been extended to continuous variable systems [4]–[11], i.e., quantum systems associated with infinite-dimensional Hilbert spaces [12], [13], we find it rather natural to address the problem of direct communication in this framework. Here, an important role has been played by the bosonic modes of the radiation field and Gaussian states. In particular, coherent states of the radiation have become the most appealing choice for implementing many quantum information tasks. Along this line, we have shown [14] how a sender (Alice) can exploit coherent states of a bosonic mode in order to send confidential messages to a receiver (Bob), with an acceptable degree of privacy. This is the first proof of principle of a (quasi) confidential quantum direct communication (QDC) in the framework of continuous variable systems. In particular, this QDC can be implemented in an easy way, since it exploits the same "quantum hardware" of the standard continuous variable QKD, even if this is done via a completely different logic of classical operations and communications.[1] The price one pays in order to have a simple technique of QDC is that a notion of "degree of privacy" must replace the one of unconditional security (used in QKD). This means that we allow a potential eavesdropper (Eve) to access a limited fraction of the information, even if this fraction can be evaluated in advance and also made very small.

The ideal situation for a QDC occurs when Alice and Bob are connected by a noiseless channel, so that the unique noise they have to correct is due to the continuous structure of quantum phase space.[2] However, in general, this is not the case, and the honest users must randomly switch instances of direct communication with instances of statistical checks on the quantum channel. As soon as they detect the presence of a *nontolerable 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 the entire message when the noise is suitably low, while losing a small amount of information when it is not. According to [14], the maximum information that Eve can steal can be made small at will, but at the expense of the efficiency of the protocol, corresponding to the ratio of the number of communicated bits to the number of quantum systems used. An alternative approach consists of the use of classical error-correcting codes, which makes Eve's perturbation more evident to Alice and Bob's statistical checks. This approach enables the honest users to reduce the number of stolen bits while keeping the efficiency of the protocol fixed. This improvement is proven assuming the model of eavesdropping is also taken fixed, i.e., Eve is restricted to a Gaussian attack given by a universal Gaussian cloner.

In this paper, we thoroughly review the results of [14], giving a more detailed description of the various protocols for QDC, together with the basic ideas that are behind them. Furthermore, we provide a deeper analysis of the possible eavesdropping strategies. In particular, we consider new kinds of attacks that are non-Gaussian and consist of the intermittent use of Gaussian

Manuscript received February 1, 2009; revised March 22, 2009. First published July 28, 2009; current version published December 3, 2009. The work of S. Pirandola was supported by the European Community under Marie Curie Fellowship (Contract MOIF-CT-2006-039703). The work of S. Lloyd was supported by the W. M. Keck Center for Extreme Quantum Information Theory (xQIT).

S. Pirandola is with the Research Laboratory of Electronics and the Center for Extreme Quantum Information Theory (xQIT), Massachusetts Institute of Technology, Cambridge, MA 02139 USA, and also with the Department of Computer Science, University of York, York YO10 5DD, U.K. (e-mail: pirs@mit.edu).

S. L. Braunstein is with the Department of Computer Science, University of York, York YO10 5DD, U.K.

S. Lloyd is with the Research Laboratory of Electronics and the Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, MA 02139 USA.

S. Mancini is with the Department of Physics, University of Camerino, Camerino 62032, Italy.

Digital Object Identifier 10.1109/JSTQE.2009.2021147

[1]These classical steps are *very cheap* since they involve just classical computers and standard communication lines (like telephone lines).

[2]Note that, in a realistic experimental setting, such an intrinsic noise could include some "trusted" environmental noise that is not referable to Eve.

cloners. These *intermittent attacks* are proven to be more powerful in the eavesdropping of QDC when it is aided by classical error correction. As a result, the improvement given by the classical codes is no longer clear if Eve is also allowed to optimize her strategy. Despite this open problem, the new concepts and the basic schemes for QDC still have great potentialities to be explored.

The paper is organized as follows. In Section II, we review the basic protocol for QDC together with its Gaussian eavesdropping. In Section III, we review QDC with repetition codes. Its security analysis is performed in Section III-C for Gaussian eavesdropping and in Section III-D for a non-Gaussian generalization. Finally, the conclusions are given in Section IV. A discussion of possible variants for QDC is given in Appendixes I–III.

II. Basic Protocol for QDC

A. Continuous Variables of a Bosonic Mode

Let us consider a bosonic mode with Hilbert space $\mathcal{H}$ and ladder operators $\hat{a}, \hat{a}^\dagger$ satisfying $[\hat{a}, \hat{a}^\dagger] = 1$. Equivalently, this system can be described by a pair of quadrature operators

$$\hat{q} = \frac{\hat{a} + \hat{a}^\dagger}{\sqrt{2}} \qquad \hat{p} = \frac{\hat{a} - \hat{a}^\dagger}{i\sqrt{2}} \tag{1}$$

satisfying the dimensionless canonical commutation relation (CCR) $[\hat{q}, \hat{p}] = i$. From the previous CCR, we see that an arbitrary state of the system ρ must fulfill the uncertainty principle

$$V(\hat{q})V(\hat{p}) \geq \frac{1}{4} \tag{2}$$

where $V(\hat{x}) := \mathrm{Tr}(\rho\hat{x}^2) - [\mathrm{Tr}(\rho\hat{x})]^2$ denotes the variance of an arbitrary quadrature $\hat{x} = \hat{q}$ or $\hat{p}$. In particular, an arbitrary coherent state $|\bar{\alpha}\rangle$ saturates (2) symmetrically, i.e., $V(\hat{q}) = V(\hat{p}) := \Delta = 1/2$, where the value 1/2 quantifies the so-called quantum shot noise. This is the fundamental noise that affects the *disjoint* measurements of the quadratures $\hat{q}$ and $\hat{p}$ of a coherent state (via homodyne detection [15]). Such a noise is instead doubled to $\Delta = 1$ when the two quadratures are measured *jointly* (via heterodyne detection [15]).

According to the Wigner representation, an arbitrary density operator ρ is equivalent to a characteristic function $\chi(\lambda) := \mathrm{Tr}[\rho\hat{D}(\lambda)]$, where $\hat{D}(\lambda) := \exp(\lambda\hat{a}^\dagger - \lambda^*\hat{a})$ is the *displacement operator*. Equivalently, ρ can be described by a Wigner function, which is a quasi-probability distribution defined by the Fourier transform

$$W(\alpha) := \int_{\mathbb{C}} \frac{d^2\lambda}{\pi^2} \exp\left(\lambda^*\alpha - \lambda\alpha^*\right) \chi(\lambda). \tag{3}$$

In (3), the Cartesian decomposition of the complex variable $\alpha = (q + ip)/\sqrt{2}$ provides the real eigenvalues q and p of the quadrature operators of (1). Such variables span the phase space $\mathcal{K} = \{q, p\}$ of the system, and therefore represent its fundamental *continuous variables*. For a coherent state $|\bar{\alpha}\rangle$, the Wigner function takes the form

$$W_{|\bar{\alpha}\rangle}(\alpha) = \mathcal{G}_{1/2}(\alpha - \bar{\alpha}) \tag{4}$$

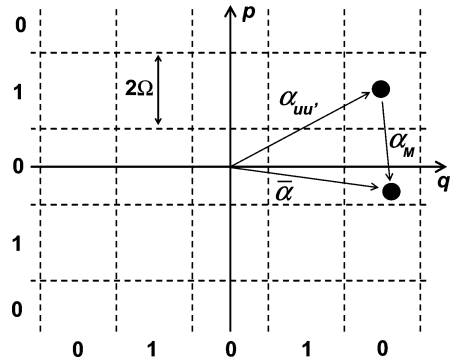

Fig. 1. Square lattice of step size 2Ω in phase space. The center of each cell is specified by an amplitude $\alpha_{u\,u'}$, where (u, u') is a pair of integers representing the address of the cell. Each address (u, u') is associated with a pair of bits (U, U') given by the parities of u and u' (see the binary digits at the border of the figure). The picture also shows the masking procedure that adds a mask α_M to the amplitude $\alpha_{u\,u'}$ in order to create a continuous and Gaussian signal $\bar{\alpha}$.

where

$$\mathcal{G}_V(\alpha - \bar{\alpha}) := \frac{1}{\pi V} \exp\left(-\frac{|\alpha - \bar{\alpha}|^2}{V}\right) \tag{5}$$

is a complex Gaussian function with mean $\bar{\alpha}$ and variance V. As a consequence, the measurement of the arbitrary quadrature $\hat{x}$ provides outcomes x, which are distributed according to the real Gaussian

$$G_\Delta(x - \bar{x}) = \frac{1}{\sqrt{2\pi\Delta}} \exp\left[-\frac{(x - \bar{x})^2}{2\Delta}\right] \tag{6}$$

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

B. Phase-Space Lattice Encoding

Let us discretize the phase space $\mathcal{K}$ by introducing a square lattice whose unit cell has size equal to 2Ω (see Fig. 1). An arbitrary cell can be addressed by a pair of integer indices (u, u') and its center specified by the coordinates

$$q_u = 2\Omega u \qquad p_{u'} = 2\Omega u' \tag{7}$$

or equivalently, by the complex amplitude

$$\alpha_{u\,u'} = \frac{q_u + ip_{u'}}{\sqrt{2}}. \tag{8}$$

Due to the introduction of this discrete structure, two bits of information may be simply encoded in quantum phase space. In fact, an arbitrary cell of address (u, u') can be associated with a pair of bits (U, U'), representing the parities of the indices u and u'. In this approach, Alice encodes two classical bits (U, U') by choosing a cell whose address (u, u') is randomly selected according to the relations

$$u = 2m + U \qquad u' = 2m' + U' \tag{9}$$

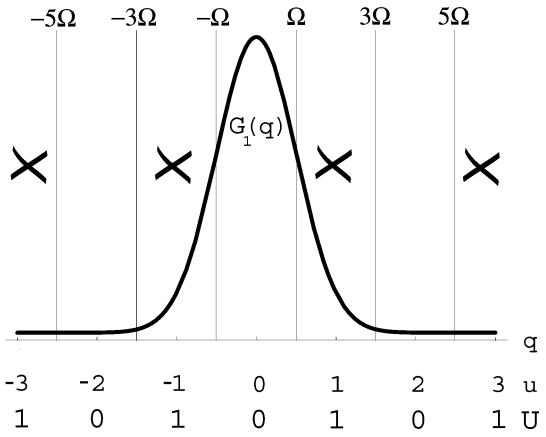

Fig. 2. Intrinsic error probability $\varepsilon(\Omega)$ in the decoding of Alice's bit U from the q-quadrature of the coherent state.

where m and m' are random integers.[3] Then, she considers the complex amplitude $\alpha_{uu'}$ pointing at the center of that cell and prepares a corresponding coherent state $|\alpha_{uu'}\rangle$. Such a state is finally sent to Bob, who performs a heterodyne detection in order to estimate the amplitude $\alpha_{uu'}$, and therefore the encoded information (U, U'). It is clear that, even in the presence of a noiseless communication channel, Bob's decoding cannot be noiseless since the Gaussian shape of the coherent state spreads over the whole of phase space. Such a spread inevitably leads to an *intrinsic error* in the decoding process, which occurs when the coherent state is projected by the measurement to wrong peripheral cells.

Let us evaluate the probability ε of an intrinsic error when Bob decodes Alice's bit U from the position quadrature $\hat{q}$ (the argument may be repeated for the other quadrature). Since Bob performs a heterodyne detection on the coherent state, the measured value q will be distributed around q_u according to a Gaussian distribution with noise variance equal to $\Delta = 1$, i.e., $G_1(q - q_u)$. Suppose, for simplicity, that $U = 0$ is encoded in $q_u = 0$. According to Fig. 2, an error occurs whenever the measured value q falls in one of the crossed cells, i.e., having odd index $u = \pm 1, \pm 3, \ldots$ (which would lead to the incorrect reconstruction of $U = 1$ by Bob). Hence, the probability of an intrinsic error (per quadrature) is equal to

$$\varepsilon(\Omega) = 2 \sum_{j=0}^{\infty} \int_{(4j+1)\Omega}^{(4j+3)\Omega} dq G_1(q). \tag{10}$$

Now, if we fix a tolerable value for the intrinsic error probability, we find the corresponding size Ω to be used for the lattice. In particular, tolerating $\varepsilon = 1\%$ implies adopting $\Omega \simeq 2.57$. On the one hand, the use of a low value for ε enables the honest users to approach noise-free communication. On the other hand, a large value for Ω makes the protocol particularly fragile to eavesdropping. In fact, Eve can optimize her attack on the structure of the lattice, e.g., by using a nonuniversal cloner that is optimized on the centers of the cells. More simply, Eve can detect the state, reconstruct its cell, and resend another state that is centered in that cell. By resorting to this intercept–center–resend strategy, Eve is able to remove the noise most of the time for a sufficiently large Ω. Luckily, we are able to preclude such strategies by resorting to the classical procedure shown in the next section.

C. Masking the Message and Testing the Channel

In order to hide the lattice from Eve, Alice can simply add a *mask* to her message. After the computation of the *message* amplitude $\alpha_{uu'}$, Alice classically adds a *mask* amplitude α_M, in such a way that the *total* amplitude $\bar{\alpha} := \alpha_M + \alpha_{uu'}$ is randomly distributed according to a complex Gaussian $\mathcal{G}_V(\bar{\alpha})$ with large variance $V \gg \Omega$ (see Fig. 1). Operationally, the whole encoding procedure can be described as follows.

1) *Lattice encoding*: Alice encodes the message bits (U, U') into a message amplitude $\alpha_{uu'}$.
2) *Masking*: Alice picks a signal amplitude $\bar{\alpha}$ from a wide Gaussian distribution and computes the mask $\alpha_M = \bar{\alpha} - \alpha_{uu'}$ connecting the signal and message.
3) *Quantum preparation*: Alice prepares a signal coherent state $|\bar{\alpha}\rangle$ to be sent to Bob.

Having prepared the triplet $\alpha_{uu'}$ (message), α_M (mask), and $|\bar{\alpha}\rangle$ (signal state), Alice can now perform her quantum and classical communications (see Fig. 3). First, Alice sends the signal state $|\bar{\alpha}\rangle$ to Bob, who heterodynes it with outcome $\beta \simeq \bar{\alpha}$. Then, after Bob's detection,[4] Alice classically publicizes the mask α_M. After these two steps, Bob gets the pair (β, α_M) from his detection and Alice's classical communication. Then, Bob is able to *unmask* the signal by computing $\beta - \alpha_M \simeq \bar{\alpha} - \alpha_M = \alpha_{uu'}$, and therefore estimates the message bits (U, U') via lattice decoding.

Clearly, the same decoding steps can be followed by Eve too. However, the key point is that Eve must choose the probing interaction before knowing the value of the mask. Since the signal $\bar{\alpha}$ is continuous (Gaussian) and highly modulated, Eve is prevented from using any kind of interaction, which privileges a particular portion of the phase space. The most natural choice is therefore a universal Gaussian interaction. A possible model is given by the universal Gaussian quantum cloning machine (UGQCM) [16]. 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), with each one equal to a Gaussian modulation of $|\bar{\alpha}\rangle\langle\bar{\alpha}|$, i.e.,

$$\rho_K = \int d^2\mu \mathcal{G}_{\sigma_K^2}(\mu) \hat{D}(\mu) |\bar{\alpha}\rangle\langle\bar{\alpha}| \hat{D}^\dagger(\mu), \qquad K = B, E \tag{11}$$

where the cloning-noise variances σ_B^2 and σ_E^2 symmetrically affect the quadratures and satisfy the optimality condition

$$\sigma_B^2 \sigma_E^2 = \frac{1}{4} \tag{12}$$

[3] Ideally, the two integers m and m' are both uniformly distributed on $\mathbb{Z}$. More realistically, we can choose two continuous values from a wide Gaussian distribution, and round them to the nearest integers.

[4] In order to be sure that Bob has received and detected the state, Alice must require a classical communication from him.

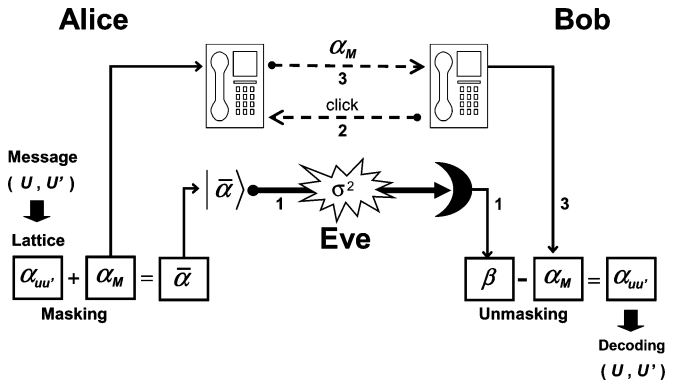

Fig. 3. MM: From the message bits (U, U'), Alice computes the message amplitude $\alpha_{uu'}$ (lattice encoding), and then adds the mask α_M achieving the signal amplitude $\bar{\alpha}$. Then, Alice prepares and sends to Bob the signal state $|\bar{\alpha}\rangle$, which is heterodyned by Bob with 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). Finally, Bob is able to unmask the signal $(\beta - \alpha_M)$, thus reconstructing $\alpha_{uu'}$, and therefore (U, U').

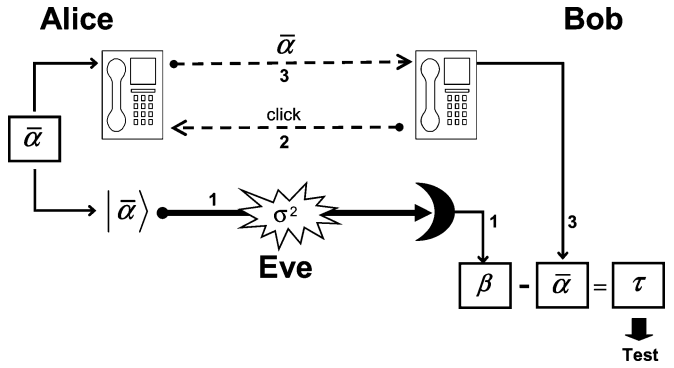

Fig. 4. CM: Alice picks up a Gaussian amplitude $\bar{\alpha}$ and prepares a coherent state $|\bar{\alpha}\rangle$. Such a state is sent to Bob and heterodyned with outcome β (step 1 in the picture). Then, Bob classically informs Alice (step 2), and Alice communicates the value of the signal $\bar{\alpha}$ (step 3). Finally, Bob computes the test variable $\tau := \beta - \bar{\alpha}$ to infer the amount of noise σ^2 in the channel.

directly imposed by (2).[5] As a consequence of (11), the arbitrary quadrature $\hat{x}$ of the clone $K = B, E$ has a marginal distribution equal to $G_{\Delta+\sigma_K^2}(x - \bar{x})$. The performance of the resulting attack will be explicitly studied in Section II-D.

The aforementioned procedure of directly communicating message bits is called the *message mode* (MM) of the protocol. However, Alice and Bob must also understand how much the channel is perturbed during the communication process in order to control the amount of information that is left to a potential eavesdropper. Assuming an attack with UGQCM, this corresponds to estimating the value of the noise $\sigma_B^2 := \sigma^2$ that is added by Eve to the channel. A real-time check of this noise is possible if Alice randomly switches from instances of MM to suitable instances of *control mode* (CM). In CM, Alice does not process any text message but only prepares and sends the signal state $|\bar{\alpha}\rangle$ (see Fig. 4). 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 nontolerable noise, i.e., $\sigma^2 > \tilde{\sigma}^2$ for some threshold noise $\tilde{\sigma}^2$, they stop the communication. Hereafter, we assume a zero-tolerance protocol where no added noise is tolerated in 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.[6]

Let us show how the real-time check of the quantum channel works in detail. Let us consider the Cartesian decomposition $\tau = (q + ip)/\sqrt{2}$ of Bob's test variable. If the channel is noiseless, then the arbitrary quadrature $x = q$ or p is only affected by heterodyne noise $\Delta = 1$, i.e., it is distributed according to a Gaussian distribution $G_1(x)$. By contrast, if Eve perturbs the quantum channel using a UGQCM with noise $\sigma^2 \neq 0$, then x follows a wider Gaussian distribution $G_{1+\sigma^2}(x)$. By reconstructing the experimental distribution of x from consecutive outcomes $\{x_1, x_2, \ldots\}$, Bob must therefore distinguish between the two theoretical distributions $G_1(x)$ and $G_{1+\sigma^2}(x)$. In other words, Bob must distinguish between the two hypotheses

$$\begin{cases} H_0 : (\text{Eve} = \text{no}) \Leftrightarrow \sigma^2 = 0 \\ H_1 : (\text{Eve} = \text{yes}) \Leftrightarrow \sigma^2 \neq 0. \end{cases} \tag{13}$$

Let us fix the confidence level r of this hypothesis test, i.e., the probability to reject H_0 though it is true. This level must be sufficiently low (e.g., $r = 5 \times 10^{-7}$), so that the direct communication can be effectively completed in absence of Eve. For each instance of CM, Bob makes two independent tests, one for each quadrature. Hence, after M CMs, he has collected $2M$ quadratures values $\{q_1, p_1, \ldots, q_M, p_M\} := \{x_1, x_2, \ldots, x_{2M-1}, x_{2M}\}$, and he can construct the estimator

$$v := \sum_{l=1}^{2M} x_l^2. \tag{14}$$

Then, the hypothesis H_0 is accepted if and only if

$$v < \mathcal{V}_{2M,1-r} \tag{15}$$

where $\mathcal{V}_{i,j}$ is the jth 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 (15) is satisfied in CM.

D. Gaussian Eavesdropping

Let us explicitly analyze what happens when the quantum communication channel is subject to Gaussian eavesdropping via a UGQCM.[7] In an individual UGQCM attack (see Fig. 5), Eve clones the signal input, and then heterodynes her output to derive her estimate γ of the signal amplitude $\bar{\alpha}$. After the release of the mask's value α_M, Eve infers the message amplitude

[5]Strictly speaking, the machine considered is a *symmetric* and *optimal* $1 \rightarrow 2$ UGQCM [16].

[6]A zero-tolerance protocol does not promptly stop in realistic situations (where $\sigma^2 \neq 0$) because the underlying hypothesis test is intrinsically imperfect (i.e., its probability to fail is always nonzero).

[7]Note that an individual UGQCM attack can be mapped into an individual entangling-cloner attack, corresponding to a lossy channel with thermal noise (see, e.g., [17]).

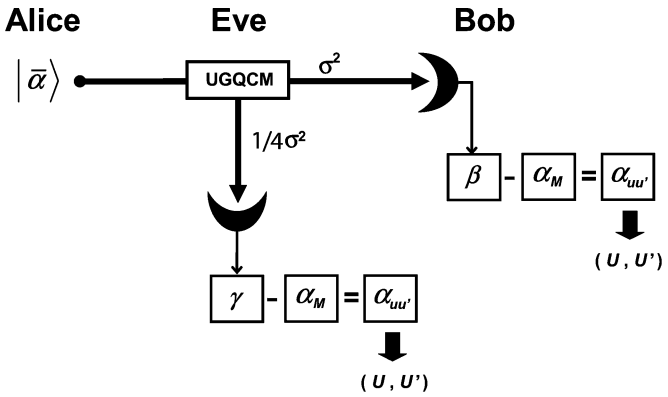

Fig. 5. Individual UGQCM attack. Eve uses a UGQCM to eavesdrop the quantum communication line. Eve heterodynes her clone to get her estimate γ of the signal amplitude $\bar{\alpha}$. After the public unmasking of the signal, Eve estimates $\alpha_{uu'}$, and therefore the message bits (U, U').

$\alpha_{uu'}$, and therefore the input bits (U, U'). In this process, Eve introduces an added noise σ^2 on the Alice–Bob channel (i.e., $\Delta_B = 1 + \sigma^2$), while her output is affected by a total noise equal to $\Delta_E = 1 + (4\sigma^2)^{-1}$. This is the sum of the cloning noise $\sigma_E^2 = (4\sigma^2)^{-1}$, given by the UGQCM, and the measurement noise $\Delta = 1$, given by the heterodyne detector.

First of all, we must evaluate the probability of accepting H_0 (hence continuing the communication) notwithstanding the presence of Eve. In other words, we must compute the probability $\Pi_M(\sigma^2)$ that Eve evades M CMs while introducing a noise $\sigma^2 \neq 0$. After M CMs, the estimator of (14) follows the distribution

$$P_M(v) = \frac{v^{M-1}}{2^M (M-1)!(1+\sigma^2)^M} \exp\left[-\frac{v}{2(1+\sigma^2)}\right]. \quad (16)$$

As a consequence, the probability to accept H_0 is equal to

$$\Pi_M(\sigma^2) = \int_0^{\mathcal{V}_{2M,1-r}} d\nu P_M(v) = \frac{\Gamma(M,0) - \Gamma\left(M, (\mathcal{V}_{2M,1-r}/2(1+\sigma^2))\right)}{(M-1)!} \quad (17)$$

where

$$\Gamma(z,a) := \int_a^{+\infty} dt\, t^{z-1} e^{-t} \quad (18)$$

is the incomplete gamma function.

Besides Eve's survival probability of (17), we must also evaluate the amount of information that Eve can get during her undetected life in the channel. Such a quantity is limited by the *total noise* experienced by Eve, which is equal to $\Delta_E = 1 + (4\sigma^2)^{-1}$. For a given Δ_E, we now calculate the average information Eve can steal in a single run of MM. Starting from the outcome of the measurement γ and the knowledge of the mask α_M, Eve estimates Alice's amplitude $\alpha_{uu'}$ via the variable $\gamma - \alpha_M$. The corresponding quadrature x will be distributed according to a Gaussian distribution $G_{\Delta_E}(x - x_u)$. Then, by repeating the same derivation leading to (10), we can compute Eve's error probability in decoding Alice's bit (U or U'), which is equal to

$$p(\Delta_E) = 2\sum_{j=0}^{\infty} \int_{(4j+1)\Omega}^{(4j+3)\Omega} dx G_{\Delta_E}(x). \quad (19)$$

Let us assume that every message bit is a bit of information, i.e., the input message is not compressible. As a consequence, the average amount of information, which is eavesdropped in a single MM, is given by

$$I_{AE}(\Delta_E) = 2\{1 - H[p(\Delta_E)]\} \quad (20)$$

where

$$H(p) := -p\log p - (1-p)\log(1-p). \quad (21)$$

By replacing $\Delta_E = 1 + (4\sigma^2)^{-1} := \Delta_E(\sigma^2)$ in (20), we derive $I_{AE} = I_{AE}(\sigma^2)$, i.e., the average amount of information that is stolen for a given noise σ^2 in the Alice–Bob channel. Such a quantity can be directly combined with $\Pi_M = \Pi_M(\sigma^2)$ of (17). This means that we can express Eve's survival probability as a function of the stolen information. In fact, let us fix the probability c of a CM, so that N runs of the protocol can be divided into cN CMs and $(1-c)N$ MMs, on average. As a consequence, Eve's survival probability is equal to

$$\Pi_{cN}(\sigma^2) := P \quad (22)$$

and the average number of stolen bits is equal to

$$(1-c)NI_{AE}(\sigma^2) := I. \quad (23)$$

Then, for every σ^2, we can consider the function $P = P(I)$. In particular, let us fix $c = 69/70$, so that the protocol has efficiency

$$\mathcal{E} := \frac{\text{number of bits}}{\text{number of transmitted systems}} = \frac{1}{35}. \quad (24)$$

For several values of σ^2, we can (numerically) evaluate the function $P = P(I)$, as shown in Fig. 6. From this figure, we can see that, 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. Note 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 aforementioned 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. 6, Eve's best strategy corresponds to using a UGQCM with $\sigma^2 \simeq 1/20$, so that she can steal a maximal amount of about 80 bits before being revealed (using a cutoff 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? The simplest solution consists in increasing the CM probability c, so that the possible presence of Eve is detected before sending too many bits. Clearly, this approach has a price

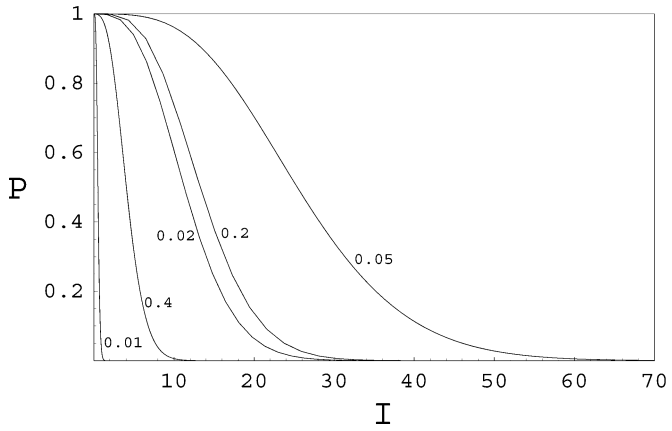

Fig. 6. Survival probability P versus the number of stolen bits I. QDC with parameters $\Omega = 2.57$ and $c = 69/70$ (so that $\varepsilon = 1\%$ and $\mathcal{E} = 1/35$). The curves refer to individual UGQCM attacks with different values of added noise σ^2.

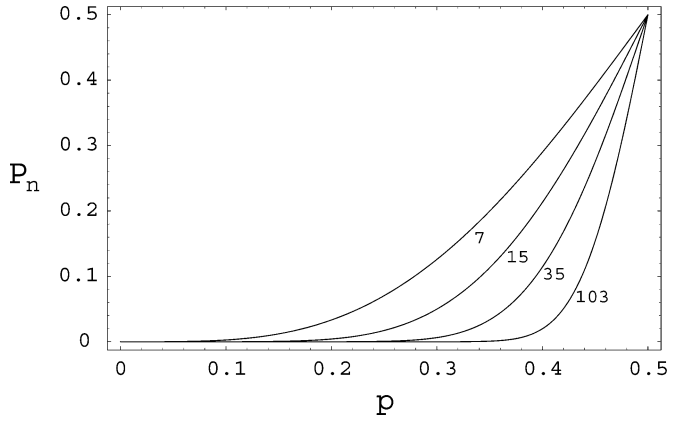

Fig. 7. Probability of an uncorrectable error P_n versus the single bit-flip probability p. Here, we consider repetition codes with $n = 7, 15, 35, 103$.

to pay, which is a decrease of the efficiency $\mathcal{E}$ of the protocol. An alternative 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, and its pros and cons are explored in the following section. In particular, this solution is good against Gaussian attacks but its advantages are not completely clear in the presence of non-Gaussian attacks.

III. QDC With Repetition Codes

A. Basic Idea in Using Classical Codes

In the basic scheme of QDC with continuous variables, a noiseless communication is possible up to an intrinsic error probability ε, which depends on the step Ω of the phase-space lattice. 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 for encoding/decoding. Such procedures are 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 nonlinear behavior, which makes their performance rapidly deteriorate. Such a nonlinear effect can be exploited to critically split the correction capabilities, and therefore the information gains, between the Alice–Bob channel and Alice–Eve channel.

Let us consider the simple case of an n-bit repetition code,[8] where 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

$$\bar{0} = \underbrace{00\cdots0}_{n} \qquad \bar{1} = \underbrace{11\cdots1}_{n}. \tag{25}$$

By choosing an odd $n = 2m + 1$ (with $m = 1, 2, \ldots$), we can apply a nonambiguous majority voting criterion. This means that every bit-flip error of weight $t < m + 1$ is correctable, while every bit-flip error of weight $t \geq m + 1$ 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 Gaussian attacks. Then, the probability of an uncorrectable error is simply given by

$$P_n(p) = \sum_{k=m+1}^{n} \binom{n}{k} p^k (1-p)^{n-k}. \tag{26}$$

As is evident from Fig. 7, the correction capability of the n-bit repetition code rapidly worsens as the single bit-flip probability approaches $1/2$. This is due to the nonlinear behavior of $P_n = P_n(p)$, which becomes more manifest when n increases. In particular, for a sufficiently large n, the curve displays a critical point $\tilde{p}$ after which the correction capability suddenly starts to deteriorate very quickly (e.g., $\tilde{p} \simeq 0.3$ for $n = 35$ and $\tilde{p} \simeq 0.4$ for $n = 103$). Exactly, these critical points can be exploited to improve the QDC by transforming the communication protocol into a threshold process, where the sensitivity to added noise is remarkably amplified.

For a repetition code of fixed length n, we have a corresponding critical value $\tilde{p}$. Then, we can choose a lattice whose step is critical. This is the value $\tilde{\Omega}$ such that the intrinsic error probability is critical, i.e., $\varepsilon(\tilde{\Omega}) = \tilde{p}$. 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 $P_B = P_n(\tilde{p})$. On the other hand, when the channel is noisy, Alice's information is split into two subchannels: 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

$$P_B = P_n(\tilde{p} + p_B) \qquad P_E = P_n(\tilde{p} + p_E) \tag{27}$$

where $p_B = p_B(\sigma_B^2)$ and $p_E = p_E(\sigma_E^2)$ are monotonic functions of the added noises (and 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 nonlinear region. As a consequence, Eve will tend to experience $P_E \simeq 1/2$ gaining her negligible information.

[8] Clearly, one can consider other and more efficient classical error-correcting codes like, e.g., the Hamming codes. For a review of classical error correction, see [18].

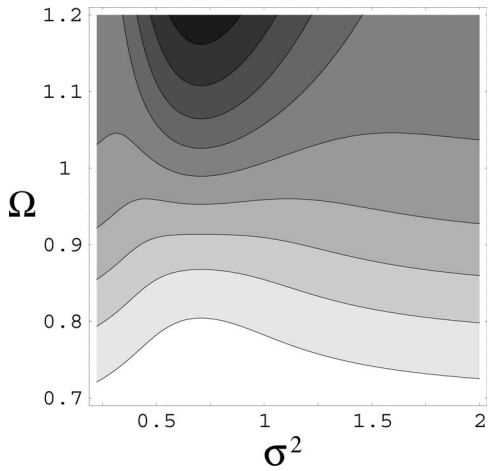

Fig. 8. Sum of the mutual information $I_{AB} + I_{AE}$ on the plane (Ω, σ^2). The values increase from 0 (white area) to 2 (black area). Note how the behavior of the borders changes around the critical value $\tilde{\Omega} \simeq 1$.

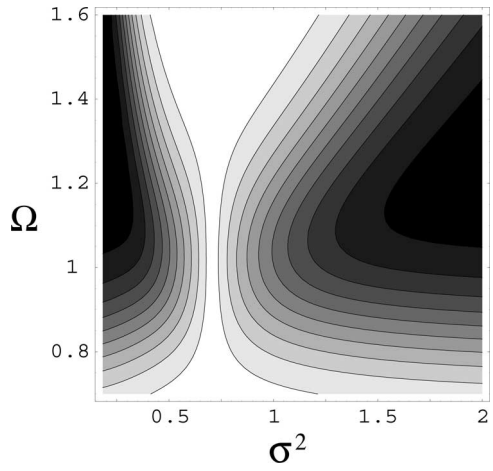

Fig. 9. Difference $D := |I_{AB} - I_{AE}|$ on the plane (Ω, σ^2). The values increase from $D = 0$ (white area) to $D = 1$ (black area). Note how the areas of separation (black areas) are broader at the critical value $\tilde{\Omega} \simeq 1$.

Let us explain the previous point in terms of mutual information. In particular, let us fix the repetition code to the value $n = 35$, so that we have $\tilde{p} \simeq 0.3$ and a corresponding critical value $\tilde{\Omega} \simeq 1$ for the lattice. Starting from an arbitrary Ω, one can see that $\tilde{\Omega}$ is indeed optimal for Alice and Bob. For every bit of information that is encoded by Alice, the amount of information decoded by Bob and Eve is, respectively, given by

$$I_{AB} = 1 - H(P_B) := I_{AB}(\Omega, \sigma^2) \tag{28}$$

$$I_{AE} = 1 - H(P_E) := I_{AE}(\Omega, \sigma^2) \tag{29}$$

where P_B and P_E are the logical error probabilities in (27) with $n = 35$. Since the added noises satisfy the uncertainty relation of (12), a similar relation holds for the mutual information, i.e.,

$$I_{AB}(\Omega, \sigma^2) + I_{AE}(\Omega, \sigma^2) = \mu(\Omega, \sigma^2) \tag{30}$$

where $\mu(\Omega, \sigma^2) \leq 2$ is numerically shown in Fig. 8. Let us also consider the difference of information

$$D(\Omega, \sigma^2) := \left| I_{AB}(\Omega, \sigma^2) - I_{AE}(\Omega, \sigma^2) \right|. \tag{31}$$

Such a quantity is a point-by-point measure of how much I_{AB} and I_{AE} are different. In particular, the maximum value $D = 1$ corresponds to the maximal separation $\{I_{AB}, I_{AE}\} = \{0, 1\}$ or $\{1, 0\}$. As we can see from Fig. 9, the points (Ω, σ^2) with $\Omega = 1$ (i.e., with $\Omega \simeq \tilde{\Omega}$) correspond to the broadest areas of separation. In other words, the critical condition $\Omega \simeq \tilde{\Omega}$ enhances the split between I_{AB} and I_{AE}.

B. Protocol With Repetition Codes

Let us explicitly show how to use an n-bit repetition code for encoding/decoding. This is possible by simply adding preencoding and postdecoding classical steps to the basic protocol of Section II. The message bits (U, U') are preencoded into a pair of logical bits

$$\bar{U} = U_1 U_2 \cdots U_n \qquad \bar{U}' = U_1' U_2' \cdots U_n' \tag{32}$$

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 MMs, Bob will have collected perturbed versions of the n pairs $(U_1, U_1'), \ldots, (U_n, U_n')$. By applying standard error recovery (majority voting), he will then perform the postdecoding 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. 4).

Let us choose a repetition code with $n = 35$ and a lattice with $\Omega = 1 \simeq \tilde{\Omega}$. The latter choice implies an intrinsic error probability ε in decoding the physical bits (U_k, U_k'), which is equal to the critical value of the code $\tilde{p} \simeq 32\%$. After error recovery, the intrinsic error probability $\bar{\varepsilon}$ affecting the logical bits $(\bar{U}, \bar{U}')$ is sufficiently low and corresponds to $P_{35}(\tilde{p}) \simeq 1\%$. Then, let us also choose $c = 1/2$ for the CM's probability, so that we have an efficiency $\mathcal{E} = 1/35$. Note that the values of $\bar{\varepsilon}$ and $\mathcal{E}$ correspond to the ones chosen for the basic protocol of Section II (where $\bar{\varepsilon} = \varepsilon$ of course). Such parameters equalize the performances of the two protocols in the case of a noiseless quantum channel. As a consequence, we are in a situation to make a fair comparison between the protocols when malicious noise is present in the channel.

C. Gaussian Eavesdropping

Let us analyze the effect of an individual UGQCM attack. On every cloned system, affected by a noise $\sigma_E^2 = (4\sigma^2)^{-1}$, Eve detects the complex amplitude γ via heterodyne detection. Then, she estimates the signal amplitude $\bar{\alpha}$ up to a total noise $\Delta_E = 1 + \sigma_E^2$. 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 $p(\Delta_E)$ as in (19). After n eavesdropped MMs, Eve will be able to decode Alice's logical bits $(\bar{U}, \bar{U}')$ by majority voting, up to an error probability $P_E = P_n[p(\Delta_E)]$ [see (26)]. For each logical bit, the acquired information is simply equal to

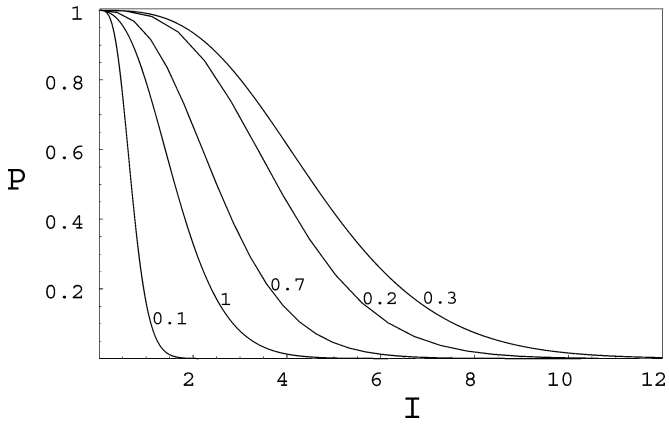

Fig. 10. Survival probability P versus the number of stolen bits I. QDC with repetition code $n = 35$, and parameters $\Omega = 1 \simeq \tilde{\Omega}$, $c = 1/2$ (so that $\bar{\varepsilon} \simeq 1\%$ and $\mathcal{E} = 1/35$). The curves refer to individual UGQCM attacks with different values of added noise σ^2.

$1 - H(P_E)$. As a consequence, for each MM, Eve acquires on average

$$I_{AE}(\sigma^2) = \frac{2[1 - H(P_E)]}{n} \tag{33}$$

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

Now, let us consider the probability that Eve evades M CMs. Since the CM is implemented exactly as before, we again have $\Pi_M(\sigma^2)$ as in (17). Such a quantity can be combined with the one of (33). After N runs of the protocol, we have an average of cN CMs and $(1-c)N$ MMs, so that Eve's survival probability is again $\Pi_{cN}(\sigma^2) := P$ and the stolen information equal to $(1-c)NI_{AE}(\sigma^2) := I$. Then, for every σ^2, we can again evaluate the curve $P = P(I)$, expressing Eve's survival probability as a function of the stolen bits. According to Fig. 10, the best choice for Eve is a UGQCM with $\sigma^2 \simeq 0.3$, which enables her to steal about ten bits of information before being detected. Such a result is a strong improvement with respect to the basic protocol, where 80 bits were left to Eve. Note 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.

It is important to note that the strong improvement brought by the classical codes is proven provided the eavesdropping strategy is fixed, i.e., Eve is restricted to an individual Gaussian attack where *all* the signal systems are attacked by a UGQCM. The idea of using repetition codes is, in fact, based on the condition that *all* the systems are perturbed exactly in the same way. However, this is not true in general, and we can design more appropriate strategies for Eve, which are specifically optimized against the use of classical codes. This is the argument of the following section.

D. Non-Gaussian Eavesdropping via Intermittent Attacks

In Section III-C, the QDC with repetition codes has been tested against the same kind of attack considered for the basic QDC. This attack is an individual UGQCM attack, which is indeed a Gaussian attack if it is applied to every quantum system that is sent through the channel. Note that the same Gaussian interaction provided by the UGQCM generates an overall non-Gaussian attack if it is applied to only a fraction of the signal systems. This because an *intermittent* use of Gaussian interactions corresponds to the generation of an average non-Gaussian interaction.

In this section, we introduce the notion of *intermittent attacks*, which are individual non-Gaussian attacks based on the intermittent use of a UGQCM. They are characterized by two parameters: the frequency parameter ω and the noise parameter σ^2. The frequency parameter ω defines the probability that Eve attacks a signal system via a UGQCM (and then detects the output clone via heterodyning). The noise parameter σ^2 defines the cloning noise variance, which is introduced by the UGQCM on the signals that are effectively attacked. Then, for N transmitted systems, a fraction $N\omega$ is subject to cloning interactions with noise σ^2, while another fraction $N(1-\omega)$ is not perturbed by Eve. On average, Bob's output quadrature $x = q, p$ will follow the non-Gaussian distribution

$$F_{\omega,\sigma^2}(x) = \omega G_{1+\sigma^2}(x) + (1-\omega)G_1(x) \tag{34}$$

where $G_\Delta(x - \bar{x})$ is defined in (6). Clearly, in the particular case of $\omega = 1$, this attack becomes Gaussian and coincides with an individual UGQCM attack.

An intermittent attack can allow Eve to probe a subset of the systems very heavily, instead of probing all the systems with a weaker interaction. This peculiarity plays a nontrivial role in the case of QDC with repetition codes, where the eavesdropping of a single bit of a codeword can be sufficient to reconstruct all the encoded logical information. Here, we explicitly show the superiority of the intermittent attacks against the use of repetition codes. For the sake of simplicity, we consider only those attacks whose frequencies can be written as $\omega = t/n$, where n is the length of the code and t is an odd integer between 1 and n.

After N runs of the protocol, an intermittent attack of frequency ω (and noise σ^2) will affect an average of $N\omega$ systems, where $cN\omega$ are in CM and $(1-c)N\omega$ are in MM. Let us consider the MM first. For each codeword of length n, there is an average of $t = n\omega$ bits attacked by Eve. Over these bits, Eve adopts the criterion of majority voting in order to reconstruct the codeword. As a consequence, the probability of a logical error is equal to the probability of having at least $(t+1)/2$ bit flips, i.e.,

$$P_E(t) = \sum_{k=\frac{t+1}{2}}^{t} \binom{t}{k} p^k (1-p)^{t-k} \tag{35}$$

where $p = p(\Delta_E)$ is the single bit-flip probability in the Alice–Eve channel, which is determined by $\Delta_E = 1 + (4\sigma^2)^{-1}$. Then, for each MM, Eve extracts on average

$$I_{AE}(\sigma^2, \omega) = \frac{2\{1 - H[P_E(t)]\}}{n} \tag{36}$$

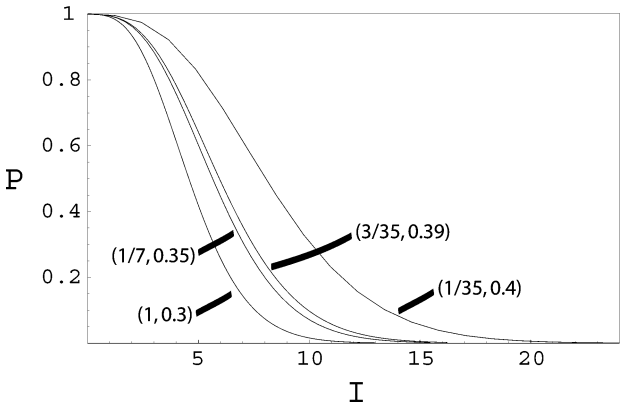

Fig. 11. Survival probability P versus the number of stolen bits I. QDC with repetition code $n = 35$, and parameters $\Omega = 1 \simeq \tilde{\Omega}$, $c = 1/2$ (so that $\bar{\varepsilon} \simeq 1\%$ and $\mathcal{E} = 1/35$). The curves refer to intermittent attacks with different parameters (ω, σ^2). In particular, we have chosen $\omega = 1, 1/7, 3/35, 1/35$ and the corresponding optimal noises $\sigma^2 = 0.3, 0.35, 0.39, 0.4$.

bits of information. After N runs of the protocol, we have an average of $(1-c)N$ instances of MM, and therefore, Eve has stolen $I = (1-c)NI_{AE}(\sigma^2, \omega)$ bits of information. Now, let us consider the CM. For each instance of CM, Bob performs two hypothesis tests, so that an average of $2cN$ tests are done after N runs of the protocol. Bob must distinguish between the two hypotheses of (13), which here means to distinguish between the two distributions $F_{\omega,0}(x) = G_1(x)$ (which is Gaussian) and $F_{\omega,\sigma^2}(x)$ with $\sigma^2 \neq 0$ (which is non-Gaussian). Suppose that Bob knows exactly which are the instances of CM that are attacked by Eve. This assumption clearly puts a lower bound on the eavesdropping capabilities of Eve, which is however sufficient to prove the result. In this case, Bob is able to isolate the $cN\omega$ attacked instances of CM from the $cN(1-\omega)$ instances that are not attacked. On the attacked subset, Bob can now perform $2cN\omega$ tests in order to distinguish between two Gaussian distributions, i.e., $G_{1+\sigma^2}(x)$ and $G_1(x)$. Then, we have to consider the estimator of (14), but now with $M = cN\omega$. As a consequence, the survival probability of Eve after N runs of the protocol is now given by $P = \Pi_{cN\omega}(\sigma^2)$.

For every intermittent attack specified by the pair $\{\omega, \sigma^2\}$, we can now relate the survival probability P to the number of stolen bits I, i.e., we can consider the function $P = P(I)$. By adopting the previous parameters for the QDC protocol, i.e., $n = 35$, $\Omega = 1$, and $c = 1/2$, we derive the curves of Fig. 11 for different values of the pair $\{\omega, \sigma^2\}$. In particular, we have chosen the frequencies ω in the set $\{1, 1/7, 3/35, 1/35\}$ and taken the corresponding optimal noises σ^2 that maximize Eve's stolen information. As expected, the value of the optimal noise increases for decreasing frequency. In particular, the best performance is achieved for $\omega = 1/35$ (lowest frequency) and $\sigma^2 = 0.4$ (highest noise), where Eve is able to eavesdrop 20 bits. Note that this value is actually a lower bound on Eve's capabilities, i.e., Eve is able to steal *at least* 20 bits. In fact, except for the case $\omega = 1$ (Gaussian attack), all the curves are actually lower bounds on the actual performances of Eve. Nevertheless, this is sufficient to prove the superiority of the intermittent attacks in the eavesdropping of QDC with repetition codes. Note that the actual performances of these non-Gaussian attacks could be much better. It is not excluded that they could completely annul the advantages brought by the use of the classical codes.

IV. Conclusion

In this paper, we have thoroughly reviewed the results of [14], and we have also provided a deeper analysis of possible eavesdropping strategies. In particular, the usage of classical correcting codes for QDC leads to the birth of new kind of attacks, the intermittent attacks, which are non-Gaussian and outperform the standard Gaussian attacks considered in [14]. Because of this new strategy, the real advantages of using classical codes for QDC are not completely clear. Despite this open problem, the adoption of a basic QDC, with a suitable CM probability, always enables the honest users to decrease the number of stolen bits to any desired value. Clearly, this is done at the expense of the efficiency of the protocol. This tradeoff between the degree of privacy and efficiency of the protocol is quite intuitive in our derivation. In future work, it would be interesting to investigate the existence of a precise relation between these two quantities. However, in order to derive this kind of relation, the cryptoanalysis of the QDC should be first extended to more general eavesdropping models, e.g., collective Gaussian attacks [19], [20]. At the present stage, our protocols represent a simple proof of principle of a confidential QDC in the framework of continuous variable systems, whose performances are not definitive at all and could be greatly improved in future investigations.

As already discussed in [14], our protocols for QDC allow an effective communication only when a small amount of noise affects the quantum channel, thus restricting their current application to relatively short distances. Despite this restriction, there are, however, nontrivial situations where they can be used in a profitable way. As explained in [14], one of the possible applications can be mutual entity authentication [21], where the two users identify each other by comparing the bits of a predistributed and secret *authentication key*. In this case, the usage of QDC is particularly profitable in the presence of quantum impersonation attacks [22], which are promptly revealed by small sessions of our protocols.

Appendix I
QDC Using Homodyne Detector

Simple variants of the previous protocols for QDC can be implemented via homodyne instead of heterodyne detection. It is sufficient that Alice encodes one single bit in the lattice by setting $U = U'$. Then, Bob randomly switches between $\hat{q}$ and $\hat{p}$ measurements, with the exact sequence being communicated to Alice at the end of the quantum communication. In such a case, Eve is forced to a delayed-choice strategy, where she has to keep all her ancillas before making the correct homodyne measurement on each of them. Similar results can be easily proven for these variants by considering that now the measurement noise is $\Delta = 1/2$.

APPENDIX II
UNIFYING CMS AND MMS

Whenever the QDC is based on heterodyne detection and implemented with a CM probability $c = 1/2$ (as in the case of the protocol of Section III-B), one can decide to distribute the CMs and MMs on all the quantum systems. This is possible by randomly choosing a quadrature for the encoding and the other for the check. Then, after Bob's heterodyne detection, Alice declares the quadrature to be used for public comparison.

APPENDIX III
POSTPONED QDC

In the basic protocol of Section II, after Bob's detection, Alice declares which mode she has used (MM or CM) and the corresponding classical information (mask amplitude α_M or signal amplitude $\bar{\alpha}$). An alternative protocol consists in delaying this declaration until the end of the quantum communication. At this point, Alice will only declare the instances in CM and the corresponding amplitudes. Such a procedure enables Alice and Bob to evaluate the noise of the channel before revealing any confidential information. From such an estimation, Alice computes the amount of information I_{AE} that Eve can steal if she unmasks the message. If I_{AE} is negligible (according to a preagreed tolerance level), then Alice unmasks all the MMs, communicating her message to Bob. Otherwise, she has to abort. Alternatively, when I_{AE} is not negligible but less than I_{AB}, Alice and Bob can possibly use the remaining systems for distributing a secret key. Note that such a postponed protocol takes no advantage from the use of codes. Furthermore, it can be simply implemented with $c = 1/2$, and therefore also modified according to Appendix II.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, Bengaluru, India, Dec.1984, pp. 175–179.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, 2002.

[3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, 1993.

[4] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, pp. 010303R-1–010303R-4, 1999.

[5] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and Ph. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," *Nature*, vol. 421, pp. 238–241, 2003.

[6] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous variable quantum cryptography: Beating the 3 dB loss limit," *Phys. Rev. Lett.*, vol. 89, pp. 167901-1–167901-4, 2005.

[7] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, "No-switching quantum key distribution using broadband modulated coherent light," *Phys. Rev. Lett.*, vol. 95, pp. 180503-1–180503-4, 2005.

[8] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, "Continuous variable quantum cryptography using two-way quantum communication," *Nature Phys.*, vol. 4, pp. 726–730, 2008.

[9] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, "Unconditional quantum teleportation," *Science*, vol. 282, pp. 706–709, 1998.

[10] S. L. Braunstein and H. J. Kimble, "Teleportation of continuous quantum variables," *Phys. Rev. Lett.*, vol. 80, pp. 869–872, 1998.

[11] S. Pirandola and S. Mancini, "Quantum teleportation with continuous variables: A survey," *Laser Phys.*, vol. 16, pp. 1418–1438, 2006.

[12] S. L. Braunstein and A. K. Pati, *Quantum Information Theory With Continuous Variables*. Dordrecht, The Netherlands: Kluwer, 2003.

[13] S. L. Braunstein and P. van Loock, "Quantum information with continuous variables," *Rev. Mod. Phys.*, vol. 77, pp. 513–577, 2005.

[14] S. Pirandola, S. L. Braunstein, S. Mancini, and S. Lloyd, "Quantum direct communication with continuous variables," *Europhys. Lett.*, vol. 84, pp. 20013-1–20013-6, 2008.

[15] D. F. Walls and G. J. Milburn, *Quantum Optics*. Berlin, Germany: Springer-Verlag, 1994.

[16] N. J. Cerf, A. Ipe, and X. Rottenberg, "Cloning of continuous quantum variables," *Phys. Rev. Lett.*, vol. 85, pp. 1754–1757, 2000.

[17] S. Pirandola, S. L. Braunstein, and S. Lloyd, "On the security and degradability of Gaussian channels," in *Proc. TQC2009, 4th Workshop Theory Quantum Comput., Commun., and Cryptography*, Waterloo, Canada, May 11–13, 2009.

[18] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.

[19] S. Pirandola, S. L. Braunstein, and S. Lloyd, "Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography," *Phys. Rev. Lett.*, vol. 101, pp. 200504-1–200504-4, 2008.

[20] S. Pirandola, R. Garcia-Patron, S. L. Braunstein, and S. Lloyd, "Direct and reverse secret-key capacities of a quantum channel," *Phys. Rev. Lett.*, vol. 102, pp. 050503-1–050503-4, 2009.

[21] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1997.

[22] M. Dušek, O. Haderka, M. Hendrych, and R. Myška, "Quantum identification system," *Phys. Rev. A*, vol. 60, pp. 149–156, 1999.

Stefano Pirandola received the Laurea degree (*summa cum Laude*) in physics from the University of Rome "La Sapienza," Rome, Italy, in 2001, and the Ph.D. degree in physics from the University of Camerino, Camerino, Italy, in 2005.

He is currently a Visiting Scientist in the Research Laboratory of Electronics (RLE) and the Center for Extreme Quantum Information Theory (xQIT), Massachusetts Institute of Technology (MIT), Cambridge. He is also a Marie Curie Fellow in the Department of Computer Science, University of York, York, U.K. From 2005 to 2007, he was a Postdoctoral Fellow in the Department of Physics, University of Camerino. His current research interests are quantum mechanics, quantum optics, and quantum information, including quantum information theory with continuous variable systems.

Samuel L. Braunstein (SM'09) received the B.Sc. (Hons.) and M.Sc. degrees in physics from the University of Melbourne, Melbourne, Vic., Australia, and the Ph.D. degree in physics from California Institute of Technology, Pasadena, in 1988.

In 2003, he joined the University of York, York, U.K., where he heads a group in the field of nonstandard computation. He was a German Humboldt Fellow at the University of Ulm. He is the editor of three books *Quantum Computing*, *Scalable Quantum Computing*, and *Quantum Information With Continuous Variables*. He is member of the Editorial Board of the journal *Fortschritte der Physik* for which he has prepared two special issues on quantum computation. He has initiated and is a Founding Managing Editor of *Quantum Information and Computation*—the first journal dedicated specifically to this field. He has authored or coauthored more than 100 papers published in refereed journals with an overall h-index of 39.

Prof. Braunstein was the recipient of the prestigious Royal Society-Wolfson Research Merit Award. He was awarded the honorary title of the 2001 Lord Kelvin Lecturer. He is a Fellow of the Institute of Physics and the Optical Society of America. His research on quantum teleportation, quantum computation, quantum lithography, and quantum information has received extensive coverage in prestigious scientific venues such as *Science*, *Nature*, *Physics Today*, *New Scientist*, and *Optics and Photonics News*, as well as on radio, television, and daily newspapers. His most cited work on quantum teleportation was among those chosen as the "top ten [scientific] breakthroughs" of that year by the journal *Science*.

Seth Lloyd received the A.B. degree from Harvard College, Cambridge, MA, in 1982, the Certificate of Advanced Study in Mathematics (Part III) and the M.Phil. degree in philosophy of science from Cambridge University, Cambridge, U.K., in 1983 and 1984, respectively, and the Ph.D. degree in physics from Rockefeller University, New York, in 1988.

He is a Principal Investigator in the Research Laboratory of Electronics (RLE), Massachusetts Institute of Technology (MIT), Cambridge, where he joined the Department of Mechanical Engineering in 1994. He was a Marshall Fellow at Cambridge University. From 1988 to 1991, he was a Postdoctoral Fellow in the High Energy Physics Department, California Institute of Technology, where he was engaged in research on applications of information to quantum mechanical systems. From 1991 to 1994, he was a Postdoctoral Fellow at Los Alamos National Laboratory, where he was engaged in research on quantum computation at the Center for Nonlinear Systems. Since 1988, he has also been an adjunct faculty member at the Sante Fe Institute. He was involved in the fields of quantum computation and quantum communications, including proposing the first technologically feasible design for a quantum computer, demonstrating the viability of quantum analog computation, proving quantum analogs of Shannon's noisy channel theorem, and designing novel methods for quantum error correction and noise reduction.

Stefano Mancini received the Ph.D. degree in physics from the University of Perugia, Perugia, Italy, in 1998.

He was a Postdoctoral Fellow at the University of Milan for three years. During 2000, he was a Lecturer of quantum information at the University of Milan. During 2001–2004, he was with the University of Camerino, Camerino, Italy, where he is a Researcher of theoretical physics since 2004. He was engaged in research in the field of quantum optics, and quantum control theory and quantum information theory. He has given a significant contribution to the development of mathematical formalism of quantum feedback and the quantum memory channels characterization. He has authored or coauthored more than 100 papers published in leading international journals. He has been the Editor of three journals for special issues devoted to quantum information topics. He is currently a member of the Editorial Board of the *International Journal of Quantum Information*.

Dr. Mancini was awarded two times by the Italian Ministry of Research under Young Researchers Program.