Eur. Phys. J. D **18**, 211–218 (2002)
DOI: 10.1140/epjd/e20020025

THE EUROPEAN PHYSICAL JOURNAL D
EDP Sciences

Cloning and cryptography with quantum continuous variables

N.J. Cerf[1,2], S. Iblisdir[1], and G. Van Assche[1,a]

[1] École Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Brussels, Belgium
[2] Jet Propulsion Laboratory, California Institute of Technology, Pasadena CA 91109, USA

Received 6 July 2001

Abstract. The cloning of quantum variables with continuous spectra is investigated. We define a Gaussian 1-to-2 cloning machine that copies equally well two conjugate variables such as position and momentum or the two quadrature components of a light mode. The resulting cloning fidelity for coherent states, namely $F = 2/3$, is shown to be optimal. An asymmetric version of this Gaussian cloner is then used to assess the security of a continuous-variable quantum key distribution scheme that allows two remote parties to share a Gaussian key. The information *versus* disturbance tradeoff underlying this continuous quantum cryptographic scheme is then analyzed for the optimal individual attack. Methods to convert the resulting Gaussian keys into secret key bits are also studied. Finally, the extension of the Gaussian cloner to optimal N-to-M continuous cloners is discussed, and it is shown how to implement these cloners for light modes using a phase-insensitive optical amplifier and beam splitters. In addition, a phase-conjugate input cloner is defined, yielding M clones and M' anticlones from N replicas of a coherent state and N' replicas of its phase-conjugate (with $M' - M = N' - N$). This novel kind of cloners is shown to outperform the standard N-to-M cloners in some cases.

PACS. 03.67.Dd Quantum cryptography – 42.50.-p Quantum optics – 89.70.+c Information science

1 Introduction

Quantum information theory was originally developed for discrete quantum variables, in particular quantum bits (qubits). Recently, however, it has been realized that several concepts that were invented for qubits extend very naturally to the domain of continuous variables (*e.g.*, position and momentum of a particle, or the quadrature components of a mode of the electromagnetic field). The first results in this direction concerned quantum teleportation [8,28], and gave rise to a lot of interest in continuous-variable quantum information processing. In the present paper, we focus on the notions of quantum cloning and quantum key distribution, and investigate how they can be extended to continuous variables.

Cloning machines (which achieve the optimal approximate cloning transformation compatible with the so-called no-cloning theorem) have been a fundamental research topic in the last five years (see *e.g.*, [6] for an overview). In Section 2, we will define a Gaussian cloner, which achieves the optimal cloning of a continuous variable satisfying the requirement of covariance with respect to displacements and rotations in phase space. In other words, this cloner duplicates all coherent states with a same fidelity ($F = 2/3$). The optical implementation of this cloner and its extension to N-to-M cloners are also discussed. In Section 3, we then turn to quantum key distribution, and propose a continuous-variable cryptosystem that allows two remote parties to share a Gaussian key by exchanging continuous key elements carried by squeezed states. This scheme is the proper continuous counterpart of the protocol BB84 [2] for qubits. Our continuous cryptosystem is related to the Gaussian cloner in the sense that an asymmetric version of the latter achieves the optimal individual eavesdropping strategy. Thus, our results on continuous cloning can be used to analyze the information *versus* disturbance tradeoff in order to assess the security of this continuous cryptosystem. We find that the information gained by the eavesdropper is exactly upper bounded by the information lost by the authorized receiver. We also investigate a protocol to convert the raw Gaussian keys into a string of secret key bits, that is, we show how to apply reconciliation and privacy amplification on continuous key elements. Finally, in Section 4, we come back to the issue of cloning continuous variables and define a new class of "phase-conjugate input" cloners. These cloners produce several clones (and anticlones) from several replicas of an unknown coherent state *and* its phase conjugate. We show that adding these extra phase-conjugate input modes makes it possible to improve the cloning (and anticloning) fidelity with respect to the standard N-to-M cloners.

[a] e-mail: gvanassc@ulb.ac.be

2 Quantum cloning machines

Let us first seek for a transformation that duplicates with a same fidelity all coherent states $|\psi\rangle$, with $\psi = (x+\mathrm{i}p)/\sqrt{2}$. The fundamental requirement we put on this transformation is that it is covariant with respect to displacements in phase space. Thus, if two input states are identical up to a displacement $\hat{D}(x,p) = \mathrm{e}^{-\mathrm{i}x\hat{p}}\mathrm{e}^{\mathrm{i}p\hat{x}}$, then their respective copies should be identical up to the same displacement. (In this paper, we put $\hbar = 1$). Denoting by $\mathcal{H}$ the Hilbert space corresponding to a single system, cloning can be defined as a completely positive trace-preserving linear map $\mathcal{C}$: $\mathcal{H} \to \mathcal{H}^{\otimes 2}$: $|\psi\rangle\langle\psi| \to \mathcal{C}(|\psi\rangle\langle\psi|)$ such that

$$\mathcal{C}\left(\hat{D}(x,p)|\psi\rangle\langle\psi|\hat{D}^\dagger(x,p)\right) = \hat{D}^{\otimes 2}(x,p)\mathcal{C}(|\psi\rangle\langle\psi|)\hat{D}^{\dagger\otimes 2}(x,p), \quad (1)$$

for all displacements $\hat{D}(x,p)$ in phase space. A simple way to meet displacement covariance is to seek for a cloning transformation whose *individual* clone states are given each by a Gaussian mixture:

$$\rho(|\psi\rangle\langle\psi|) = \frac{1}{2\pi\sigma^2}\int \mathrm{d}x\ \mathrm{d}p\ \mathrm{e}^{-\frac{x^2+p^2}{2\sigma^2}} \times \hat{D}(x,p)|\psi\rangle\langle\psi|\hat{D}^\dagger(x,p), \quad (2)$$

where σ^2 is the cloning-induced error variance. In the following we will refer to such a transformation as a Gaussian cloner. Note that equation (2) is such that the cloning-induced noise on the quadratures $\hat{x}$ or $\hat{p}$ is invariant under rotations in phase space, which is certainly a desirable property since it is satisfied by coherent states. Consider the following unitary operator:

$$\hat{U}_{1,2,3} = \mathrm{e}^{-\mathrm{i}(\hat{x}_3-\hat{x}_2)\hat{p}_1}\mathrm{e}^{-\mathrm{i}\hat{x}_1(\hat{p}_2+\hat{p}_3)}\mathrm{e}^{-\mathrm{i}\hat{x}_2\hat{p}_3}, \quad (3)$$

where modes 1, 2 and 3 refer respectively to the original, the additional copy, and an auxiliary mode (also referred to as an ancilla). This operator can be used to build a Gaussian cloner if the additional copy and the ancilla are initially prepared in the vacuum state [13]. Indeed, it is readily checked that this transformation outputs two clones whose individual states are Gaussian-distributed, as in equation (2), with a variance $\sigma^2 = 1/2$ (*i.e.*, the vacuum noise variance as $\hbar = 1$). In particular, it copies all coherent states $|\psi\rangle$ with the same fidelity $f_{1,2} = \langle\psi|\rho(\psi)|\psi\rangle = 2/3$.

This machine is optimal in the sense that it is impossible to have $\sigma^2_{1,2} < 1/2$. To prove this, let us consider the following situation. A coherent state is processed through such a cloner, the observable $\hat{x}$ being measured on one output clone while the observable $\hat{p}$ is measured on the other one. Let us denote by Σ_x^2 and Σ_p^2 the respective error variances corresponding to this joint measurement. From the general theory on simultaneous measurement of conjugate observables [1], we know that

$$\Sigma_x^2\Sigma_p^2 \geq 1. \quad (4)$$

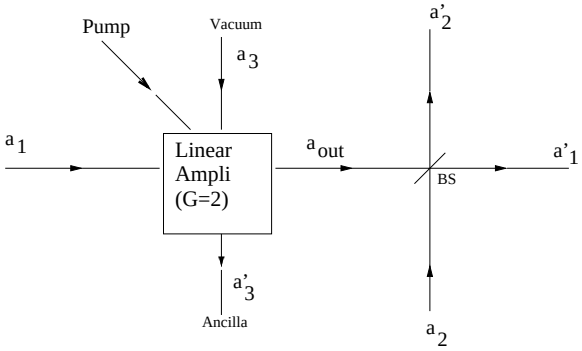

Fig. 1. Implementation of a $1 \to 2$ cloner using a phase-insensitive linear amplifier and a 50:50 beam-splitter (BS).

Using equation (2), we get

$$\left(\delta\hat{x}^2 + \sigma^2\right)\left(\delta\hat{p}^2 + \sigma^2\right) \geq 1, \quad (5)$$

where $\delta\hat{x}^2(\delta\hat{p}^2)$ is the intrinsic variance of $\hat{x}$ ($\hat{p}$) of the input state and σ^2 is the cloning-induced variance. Now, using the uncertainty principle $\delta\hat{x}^2\delta\hat{p}^2 \geq 1/4$ and the inequality $a^2 + b^2 \geq 2\sqrt{a^2b^2}$, we conclude that $\sigma^2 \geq 1/2$, implying that the unitary operator (3) is indeed optimal to achieve Gaussian cloning [10]. Physically, this means that duplicating an arbitrary coherent state cannot be performed without adding *at least* one unit of vacuum fluctuation.

A possible implementation of this machine (see Fig. 1) consists in processing the input mode $\hat{a}_1$ into a linear phase-insensitive amplifier [9] of gain $G = 2$:

$$\hat{a}_{\mathrm{out}} = \sqrt{2}\hat{a}_1 + \hat{a}_3^\dagger, \qquad \hat{a'}_3 = \hat{a}_1^\dagger + \sqrt{2}\hat{a}_3, \quad (6)$$

with $\hat{a}_j = (\hat{x}_j + \mathrm{i}\hat{p}_j)/\sqrt{2}$ denoting the annihilation operator for mode j. Then, one produces the two output clones by processing the output signal of the amplifier through a 50:50 phase-free beam-splitter:

$$\hat{a'}_1 = \frac{1}{\sqrt{2}}(\hat{a}_1 + \hat{a}_2), \qquad \hat{a'}_2 = \frac{1}{\sqrt{2}}(\hat{a}_1 - \hat{a}_2). \quad (7)$$

It is readily checked that this scheme leads to an equal x- and p-error variance of $1/2$ for both clones, that is, it achieves the optimal Gaussian cloning.

We will now present two generalizations of this $1 \to 2$ Gaussian quantum cloning machine. The first one consists in a transformation which from N (≥ 1) identical original input states produces M ($\geq N$) output copies whose individual states are again given by an expression similar to equation (2), but with a different error variance ${\sigma^2}_{N,M}$. Using an argument based on the concatenation of cloners, it is possible to derive a lower bound on ${\sigma^2}_{N,M}$, that is [10]

$${\sigma^2}_{N,M} \geq \frac{1}{N} - \frac{1}{M}, \quad (8)$$

so that the corresponding fidelity for coherent states satisfies

$$f_{N,M} \leq \frac{MN}{MN + M - N}\,. \quad (9)$$

Again, these bounds can be attained by a transformation whose implementation necessitates only a phase-insensitive linear amplifier and beam splitters [7,17]. Loosely speaking, the procedure consists in concentrating the N input modes into a single mode by use of a network of beam splitters, then in amplifying the resulting mode, and then in distributing the amplified mode into M output modes through a second network of beam-splitters. Note that the bounds in equations (8, 9) can also be derived using techniques similar to the ones used for describing quantum nondemolition measurements. This has been done in a paper establishing a link between cloning and teleportation for continuous variables [20]. Roughly speaking, the teleportation fidelity must exceed $f_{1,2} = 2/3$ in order to guarantee that the teleported state is of better quality than the state kept by the emitter.

The second generalization of the $1 \rightarrow 2$ Gaussian quantum cloning machine we will briefly consider here is the case where the $\hat{x}$ and $\hat{p}$ quadratures are not treated equally, and the case where the two output clones do not have the same fidelity. Equation (2) then has to be replaced by

$$\rho_i(|\psi\rangle\langle\psi|) = \frac{1}{2\pi\sqrt{\sigma_{i,x}^2\sigma_{i,p}^2}} \int \mathrm{d}x\ \mathrm{d}p\ \mathrm{e}^{-(\frac{x^2}{2\sigma_{i,x}^2}+\frac{p_{i,p}^2}{2\sigma^2{}_{i,p}})} \times \hat{D}(x,p)|\psi\rangle\langle\psi|\hat{D}^\dagger(x,p), \quad (10)$$

where $\sigma_{i,x}^2$ (resp. $\sigma_{i,p}^2$) stands for the cloning-induced error variance in the quadrature $\hat{x}$ (resp. $\hat{p}$) for the ith clone, in state ρ_i. In this case, it is possible to prove [13] that the following cloning uncertainty relations must hold:

$$\begin{aligned} \sigma_{1,x}^2\sigma_{2,p}^2 &\geq 1/4, \\ \sigma_{1,p}^2\sigma_{2,x}^2 &\geq 1/4, \end{aligned} \quad (11)$$

and are saturated by the Gaussian cloners. For these cloners, asymmetries between the output clones and between the x/p variables can be characterized by the following two parameters:

$$\chi = \frac{\sigma_{1,x}}{\sigma_{2,x}} = \frac{\sigma_{1,p}}{\sigma_{2,p}} \quad \text{and} \quad \lambda = \frac{\sigma_{1,x}}{\sigma_{1,p}} = \frac{\sigma_{2,x}}{\sigma_{2,p}}\,. \quad (12)$$

As suggested in [17], asymmetric Gaussian cloners (with $\chi \neq 1$) can be implemented by a scheme akin to Figure 1 in the sense that only two beam splitters and a single linear amplifier are needed. We will see in the following section how these asymmetric quantum cloning machines can be used to assess the security of a continuous-variable quantum key distribution protocol.

3 Quantum key distribution

In this section, we introduce a quantum protocol for the distribution of Gaussian key elements, which is a continuous-variable analogue of the protocol BB84 [2] – we assume here that the reader is familiar with BB84. Our protocol, introduced in [14], works like BB84 but with binary information being replaced by continuous information that behaves essentially as in a classical Gaussian channel. Other quantum cryptography protocols that involve continuous variables were proposed earlier [21,23, 25] but, in contrast to our scheme, they use a continuous quantum channel to carry *discrete* key elements.

Our protocol exploits a pair of canonically conjugate continuous variables x and p, for instance, the two quadratures of a mode of the electromagnetic field [26]. Alice randomly chooses a random key element r that follows a Gaussian distribution with mean zero and variance Σ^2, and randomly decides to encode it into either x (*i.e.*, $\langle x\rangle = r$) or p (*i.e.*, $\langle p\rangle = r$). An eavesdropper ignoring which of these two encoding rules is used cannot acquire information without disturbing the state.

Let us now describe the exact nature of the states used for encoding each key element. When encoding the value $r \sim N(0, \Sigma_x)$ in x, Alice creates a squeezed state such that $\langle x\rangle = r$, $\langle p\rangle = 0$, $\Delta x^2 = \sigma_x^2$ and thus $\Delta p^2 = 1/4\sigma_x^2$. Similarly, when the value $r \sim N(0, \Sigma_p)$ is encoded in p, the encoding state has $\langle p\rangle = r$, $\langle x\rangle = 0$, $\Delta p^2 = \sigma_p^2$ and thus $\Delta x^2 = 1/4\sigma_p^2$. On his side, Bob measures either x or p at random. Like in BB84, half of the measurements give results that are uncorrelated to Alice's values, so half of the samples must be discarded when Alice discloses the encoding variable. Unlike BB84, however, measuring the correct variable does not yield the exact value of r, even with a perfect apparatus, because of the intrinsic noise of the Gaussian state. The value r follows a Gaussian distribution $N(0, \Sigma_{x,p})$, to which some Gaussian noise is added $N(0, \sigma_{x,p})$, thus resulting in a Gaussian distribution with variance $\Sigma_{x,p}^2 + \sigma_{x,p}^2$. We can therefore model the transmission of r as a classical Gaussian channel with a signal-to-noise ratio (SNR) equal to Σ_x^2/σ_x^2 or Σ_p^2/σ_p^2.

An important requirement of the protocol is to make it impossible for Eve to be able to infer which encoding variable Alice used. For this, measuring the correct or incorrect variable (x or p) must yield statistically indistinguishable results. If, in contrast, Eve was able to detect (even not perfectly) whether she measured the wrong variable, then she could get and exploit this information to improve her attack. This indistinguishability requirement can be expressed as the equality of the density matrices resulting from the two encoding rules, or equivalently as [14]

$$1 + \frac{\Sigma_x^2}{\sigma_x^2} = 1 + \frac{\Sigma_p^2}{\sigma_p^2} = \frac{1}{4\sigma_x^2\sigma_p^2}\,. \quad (13)$$

A proof of this is given in Appendix A. This also means that the SNR is the same for both variables x and p, and that the information rate is given by Shannon's formula [16]

$$I = \frac{1}{2}\log_2(1 + \Sigma_x^2/\sigma_x^2) = -\log_2(2\sigma_x\sigma_p). \quad (14)$$

This information is non-zero provided that the x- or p-states (or both) are squeezed below the shot noise limit $\left(\sigma_{x,p}^2 < 1/2\right)$.

3.1 Eavesdropping by cloning

Let us now discuss an individual eavesdropping of this protocol with cloning machines such as those defined in Section 2. Eve makes two clones of the state sent by Alice, one of which is transmitted to Bob, and the other is measured in the correct variable when Alice reveals the encoding rule. This happens to be the optimal individual eavesdropping strategy as shown in [14,24].

We use a $1 \rightarrow 2$ cloning machine, and keep the freedom to make a better clone for Bob or Eve (parameter χ) and to get more accuracy in x or p (parameter λ). The subscripts 1 and 2 for the two copies are replaced respectively by B and E for the two recipients. According to equation (11), the added variances on the clones will be:

$$\sigma^2_{B,x} = \tfrac{1}{2}\chi\lambda, \qquad \sigma^2_{B,p} = \frac{1}{2}\chi\lambda^{-1}, \tag{15}$$

$$\sigma^2_{E,x} = \tfrac{1}{2}\chi^{-1}\lambda, \quad \sigma^2_{E,p} = \frac{1}{2}\chi^{-1}\lambda^{-1}. \tag{16}$$

Let us calculate the resulting information rates. When Bob measures x, the result is affected both by the intrinsic fluctuations of x and by the noise induced by the cloning operation, thus resulting in a total variance $\sigma^2_x + \chi\lambda/2$. This is the noise variance in the Gaussian channel representing the communication between Alice and Bob through Eve's cloning machine. Therefore, the information rate is now

$$I_{B,x} = \frac{1}{2}\log_2\left(1 + \frac{\Sigma^2_x}{\sigma^2_x + \frac{1}{2}\chi\lambda}\right). \tag{17}$$

Similarly, one can calculate the new variance of p measured by Eve on her clone, namely $\sigma^2_p + \chi^{-1}\lambda^{-1}/2$. This gives an information rate

$$I_{E,p} = \frac{1}{2}\log_2\left(1 + \frac{\Sigma^2_p}{\sigma^2_p + \frac{1}{2}\chi^{-1}\lambda^{-1}}\right). \tag{18}$$

Adding the last two information rates indicates the balance between Bob's and Eve's information. Remarkably, the information that Eve gains by using this attack on p is exactly equal to the information that Bob loses on x [14],

$$I_{B,x} + I_{E,p} = \frac{1}{2}\log_2\left(1 + \frac{\Sigma^2_x}{\sigma^2_x}\right) = I. \tag{19}$$

Of course, this balance also works when interchanging x and p, namely $I_{B,p} + I_{E,x} = I$.

This result is interesting because it allows Bob to bound from above the information gained by a possible eavesdropper. Assuming symmetry of the protocol in x and p, Bob can estimate $I - I_B$ and is then guaranteed that $I_E \leq I - I_B$ (in practice, a part of the information loss will be due to the channel noise). From reference [22], it is known that with reconciliation and privacy amplification carried out over a public authenticated channel, one is guaranteed to generate secret key bits whenever $I_B > I_E$. This last condition is in turn guaranteed provided that $I_B > I/2$, so that up to a 50% information loss on Bob's side is acceptable in order to generate key bits. In particular, an eavesdropping with $\chi \geq 1$ generates at least 50% of information loss so that it makes the scheme insecure.

3.2 From Gaussian key elements to secret bits

Let us now investigate the classical part of the key distribution protocol since we have to deal with reconciliation and privacy amplification based on *continuous* raw key elements here, in contrast to BB84. Shannon's formula gives us an upper limit on the number of bits one can send through a Gaussian channel with a given SNR. In our protocol, neither Alice nor Bob chooses the Gaussian random values. Yet, we want them to be able to extract a common string of bits out of their correlated Gaussian values, revealing as little information as possible on the public channel.

Our secret key distillation procedure [29] works in the following way. First, Alice and Bob are going to extract common bits out of their Gaussian-distributed values, using a binary correction algorithm such as Cascade or a variant [5,15,27,30]. They will use it several times, on several real-to-binary conversion functions. Then, the resulting bits will undergo the usual privacy amplification procedure [3,4,22], for instance using a universal class of hash functions.

Let X denote the random variable representing Alice's Gaussian values, and X' Bob's values. Alice uses a set of real-to-binary conversion functions $S_i(X) = 0, 1$, $(1 \leq i \leq m)$. These are called *slices*, in the sense that instead of performing reconciliation on the real-valued string $x_{1\ldots l}$, we operate on each string $S_i(x_{1\ldots l})$ sequentially, like slices of the main, real-valued string. On his side, Bob uses another set of functions $\tilde{S}_i$, called *slice estimators*, which reflects his best guess on the bit $S_i(X)$ given his current knowledge. The slice estimator $\tilde{S}_i$ is not only a function of X' but also of the previous slices, $\tilde{S}_i(X', S_1(X), \ldots, S_{i-1}(X))$. This results from the fact that the slices are corrected sequentially for $i = 1, \ldots, m$, so that upon correcting slice i Bob already knows $S_1(X), \ldots S_{i-1}(X)$. By carefully choosing the functions S_i and $\tilde{S}_i$, both parties can extract a common string of bits out of the correlated Gaussian values, while only disclosing a little more than $H(S_1(X), \ldots, S_m(X)|X')$ bits on the public channel. A more detailed analysis is given in [29].

Let us take an example. Assume the channel has $\Sigma^2/\sigma^2 = 15$, which means that Alice and Bob can share up to $I = \log_2(1+\Sigma^2/\sigma^2)/2 = 2$ bits per raw key element. We assume $m = 5$ slices as a trade-off between the efficiency of large m and the use of reasonable computing resources. The slice functions $S_i(X)$, $1 \leq i \leq 5$ are constructed in the following way. First, the Gaussian distribution of X is divided into $2^m = 32$ intervals. The interval labeling function $T(X)$, which associates an interval number (from 0 to 31) to each value of x, is chosen so as to maximize the mutual information $I(T(X); X')$. Thus, Bob starts with an optimal knowledge of $T(X)$. Then, we create the slice functions by assigning bit values to each of these intervals. Stated otherwise, we create a bijection between $S_{1\ldots5}(X)$ and $T(X)$ so that each vector of the 5 slice bits represents one (and only one) interval defined by $T(X)$. Much freedom is permitted at this step, but what we found to

work best is to assign the least significant bit of the interval number to $S_1(X)$, the second bit to $S_2(X)$, and so on up to the most significant bit to $S_5(X)$. Roughly speaking, this means that X and X' are first reconciliated on a fine-grained scale, then on a coarse-grained scale.

The slice estimator functions $\tilde{S}_{1\ldots5}(X', \ldots)$ are constructed from the slices $S_{1\ldots5}(X)$ and from the joint probability density $f_{X,X'}(x, x')$. Each estimator $\tilde{S}_i$ evaluates whether $S_i(X) = 0$ or $S_i(X) = 1$ is more likely conditionally on the arguments given to the estimator, namely X' and the previous slices $S_{j<i}(X)$.

In the present example, Alice's and Bob's bits are almost uncorrelated when correcting slices 1 and 2. The binary correction algorithm does not have to be used at this point – it is enough for Alice to entirely reveal $S_1(X)$ and $S_2(X)$ for the whole string. Then, slice 3 on Alice's side and the slice estimator 3 on Bob's side produce two bit strings that match 76% of the time – it is thus possible to proceed with error correction using a binary correction algorithm such as Cascade or a variant [5,27,30,15]. Note that the bit strings would be less correlated if the knowledge of $S_1(X)$ and $S_2(X)$ was not brought to Bob. Then for slice 4 (resp. slice 5), Alice's and Bob's string match 98% (resp. 99.999%) of the time, for which the binary correction will disclose only a small amount of information. Again, the knowledge of slices 1-3 helped Bob accurately estimate slice 4, which in turn helped him estimate slice 5.

As a result of this 5-step correction, Alice and Bob share a string of bits whose entropy is $H(S_{1\ldots5}) = 4.8$ bits per raw key element. Assuming a perfect binary correction algorithm, about 3 bits per raw key elements were disclosed. Roughly speaking, the net effect is thus $4.8 - 3 = 1.8$ bit of secret information per raw key element after privacy amplification (which is to be compared to the 2 bits per key element as given by Shannon's formula).

This is of course only an example. More elaborate constructions can be performed, such as gathering d Gaussian key elements at once. In fact, it was shown in [29] that the disclosed information reaches the Shannon bound as $d \to \infty$, just like for instance data compression works best for asymptotically large block sizes.

Now that we showed how quantum cryptography (followed by reconciliation and privacy amplification) can be set up with continuous variables, let us investigate another application of continuous variables to a special kind of quantum cloning machines.

4 Phase-conjugate input quantum cloning machines

It is known that an antiparallel pair of qubits is intrinsically more informative than a pair of parallel qubits if the goal is to encode a direction in space [19]. Similarly for quantum continuous variables, one can show that more information can be encoded in a pair of phase-conjugate coherent states $|\psi\rangle|\psi^*\rangle$ than in two identical replicas $|\psi\rangle|\psi\rangle$ [12]. Extending on these ideas, we present here a phase-conjugate input (PCI) quantum cloning machine, that is, a transformation which, taking as input

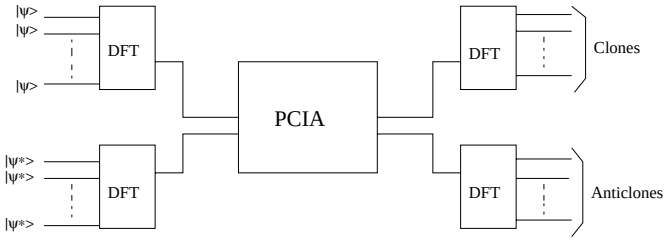

Fig. 2. PCI cloner that produces M clones and M' anti-clones from N replicas of $|\psi\rangle$ and N' replicas of $|\psi^*\rangle$. The modes are concentrated and distributed by a Discrete Fourier Transform (DFT) and amplified in a phase-conjugate input amplifier (PCIA).

N replicas of a coherent state $|\psi\rangle$ and N' replicas of its complex conjugate $|\psi^*\rangle$, produces M optimal clones of $|\psi\rangle$ [11]. Again, we will require that all the clones are treated equally, and that the cloner is covariant with respect to displacements and rotations in phase space. As a matter of fact, it turns out that such a transformation can be implemented optimally using a sequence of beam-splitters, a single non-linear crystal, followed by another sequence of beam-splitters, just as in the case of standard cloning. The procedure is the following (see Fig. 2).

(i) Concentrate the N replicas of $|\psi\rangle$ stored in the N modes $\{c_l\}$ $(l = 0 \ldots N-1)$ into a single mode a_1, resulting in a coherent state of amplitude $\sqrt{N}\,\psi$. This operation can be performed with a network of beam-splitters achieving a N-mode Discrete Fourier Transform (DFT) [7]. We get:

$$a_1 = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} c_l, \tag{20}$$

and $N-1$ vacuum modes. Similarly, with a N'-mode DFT, concentrate the N' replicas of $|\psi^*\rangle$ stored in the N' modes $\{d_l\}$ $(l = 0 \ldots N'-1)$ into a single mode a_2. This results in a coherent state of amplitude $\sqrt{N'}\,\psi^*$. We have:

$$a_2 = \frac{1}{\sqrt{N'}} \sum_{l=0}^{N'-1} d_l. \tag{21}$$

(ii) Apply the following transformation on the modes a_1 and a_2, resulting in modes b_1 and b_2 defined by

$$\begin{aligned} b_1 &= \sqrt{G}a_1 + \sqrt{G-1}a_2^\dagger, \\ b_2 &= \sqrt{G-1}a_1^\dagger + \sqrt{G}a_2, \end{aligned} \tag{22}$$

where

$$\sqrt{G} = \frac{\sqrt{N'M'} - \sqrt{NM}}{N' - N}, \tag{23}$$

with

$$M' - M = N' - N. \tag{24}$$

For obvious reasons, we call this transformation a "phase-conjugate input amplification" (PCIA).

(iii) Distribute the output mode b_1 into M clones $\{c'_l\}$ $(l = 0 \dots M-1)$ with a M-mode DFT:

$$c'_l = \frac{1}{\sqrt{M}}(b_1 + \sum_{k=1}^{M-1} \mathrm{e}^{\mathrm{i}2\pi kl/M} v_k), \tag{25}$$

where $\{v_k\}$ $(k = 1 \dots M-1)$ denote $M-1$ additional vacuum modes. It is readily verified that this procedure yields M clones of $|\psi\rangle$. Interestingly, the amplitude b_2 of the other output of the PCIA has a mean value $\sqrt{M'}\psi^*$. Therefore, it can be used to produce M' phase-conjugate clones (or anti-clones) of $|\psi\rangle$, $\{d'_l\}$ $(l = 0 \dots M'-1)$, using a M'-mode DFT:

$$d'_l = \frac{1}{\sqrt{M'}} \left(b_2 + \sum_{k=1}^{M'-1} \mathrm{e}^{\mathrm{i}2\pi kl/M'} w_k \right) \tag{26}$$

where $\{w_k\}$ $(k = 1 \dots M'-1)$ denote $M'-1$ additional vacuum modes.

Some algebra shows that this procedure is optimal to produce M clones, and that the additional M' anti-clones are also optimal [11]. Furthermore, since the step (ii) of our procedure is linear and phase-insensitive, the resulting PCI cloner is covariant with respect to translations and rotations of the state to be copied: all coherent states are copied equally well, and the cloning-induced noise is the same for all quadratures.

It is straightforward to calculate the noise variance of the clones and anti-clones:

$$\begin{aligned} (\Delta c'_l)^2 &= \frac{1}{2}\langle c'_l c'^{\dagger}_l + c'^{\dagger}_l c'_l\rangle - \langle c'_l\rangle\langle c'_l\rangle = \frac{1}{2} + \frac{G-1}{M}, \\ (\Delta d'_l)^2 &= \frac{1}{2} + \frac{G-1}{M'}\cdot \end{aligned} \tag{27}$$

As expected, the variance of the output clones exceeds $1/2$, reflecting that perfect cloning (anti-cloning) is indeed impossible. Instead, they suffer from an additional noise given by $\sigma^2_{N,N',M} = (G-1)/M$. The same conclusion holds for the anticlones.

4.1 Balanced phase-conjugate input cloner

Consider now the balanced case ($N = N'$, $M = M'$), for which simple expressions of the noise variance and the fidelity can be obtained. We then have $G = (M+N)^2/4MN$, giving

$$(\Delta c'_l)^2 = (\Delta d'_l)^2 = \frac{1}{2} + \frac{(M-N)^2}{4M^2N}\cdot \tag{28}$$

and

$$f^N_{N,M} = \frac{1}{1+\sigma^2_{N,N,M}} = \frac{4M^2N}{4M^2N + (M-N)^2}\cdot \tag{29}$$

Let us compare these quantities to the variance and fidelity of a $2N \to M$ usual cloning machine, as obtained by replacing N into $2N$ in equations (8, 9). Of course, in the trivial case where $M = 2N$, standard cloning can be achieved perfectly, while the balanced PCI cloner yields an additional variance equals to $1/(16N)$. However, if M is sufficiently large, the $(N,N) \to M$ PCI cloner outperforms the standard $2N \to M$ cloning machine. Also, comparatively more anti-clones with a higher fidelity are produced with the PCI cloner. Indeed, a standard $2N \to M$ cloning machine produces $M-2N$ anti-clones of fidelity $2N/(2N+1)$, which is actually the fidelity of an optimal measurement of $2N$ replicas of $|\psi\rangle$, whereas a PCI cloner produces M anti-clones with a higher fidelity, as given by equation (29). In particular, for $M \to \infty$, we see from equation (28) that the additional noise induced by a PCI cloner is $1/4N$, that is, *one half* of the noise induced by a standard $2N \to \infty$ cloner (*i.e.*, $1/2N$). In this case, the output of the PCIA can be considered as classical and the underlying process appears to be equivalent to a measurement. This reflects that more classical information can be encoded in N pairs of phase-conjugate replicas of a coherent state rather than in $2N$ identical replicas, a result which was first proven for $N = 1$ in [12]. More generally, in the unbalanced case ($N \neq N'$), it is readily checked, using equation (23), that the optimal measurement results in a noise that is equal to that obtained by measuring $(\sqrt{N} + \sqrt{N'})^2$ identical replicas of the input in the absence of phase-conjugate input modes.

4.2 Unbalanced phase-conjugate input cloner

As we have just shown, the balanced PCI cloner results in better cloning fidelities than a standard cloner. More generally, we may ask the following question: in order to produce M clones of a coherent state $|\psi\rangle$ from a fixed total number n of input modes, N of which being in the coherent state $|\psi\rangle$ and N' of which being in the phase-conjugate state $|\psi^*\rangle$, what is the phase-conjugate fraction $a = N'/n$ that minimizes the error variance of the clones?

From equation (23), we see that for fixed values of n and M, the gain G only depends on a and varies as

$$G(a) = \left(\frac{\sqrt{a}\sqrt{\frac{M}{n} + (2a-1)} - \sqrt{\frac{M}{n}}\sqrt{1-a}}{2a-1} \right)^2 . \tag{30}$$

In Figure 3, the value of $\sigma^2_{N,N',M}$ is plotted as a function of a for $n = 8$ and different values of $M \geq n$. In the trivial case where $M = n = 8$, the minimum additional variance is of course zero, and is obtained for $a = 0$. The cloning transformation is then just the identity. However, when $M \geq n+1$, using phase-conjugate input modes yields lower variances than standard cloning if a is correctly chosen (the lowest variance is then always attained for $a \neq 0$). Remarkably, the value of a achieving the minimum variance is not equal to $1/2$ for finite M, that is the optimal input partition contains more replicas than anti-replicas. In the limit of large M, however, the number of anti-replicas achieving the lowest variance tends to $n/2$, and the curve $G(a)$ tends to a symmetric curve around

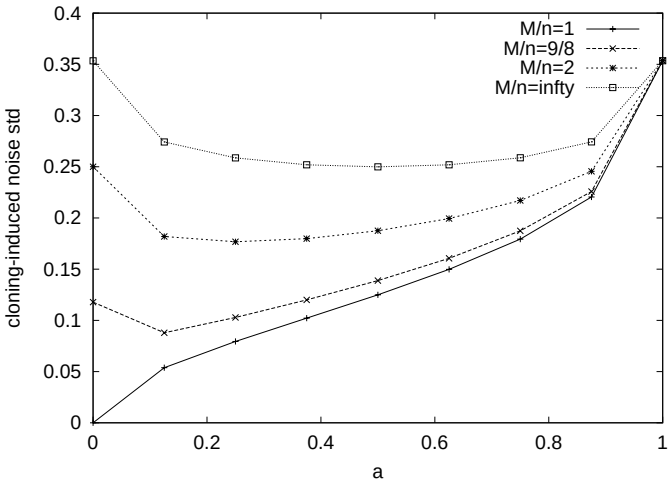

Fig. 3. Cloning-induced noise standard deviation $\sqrt{\sigma^2_{N,N',M}}$ as a function of the phase-conjugate input fraction $a = N'/n$, for $n = 8$ and several values of M/n. The lines are shown only to guide the eye.

$a = 1/2$. This behavior was expected since $M = \infty$ corresponds to a measurement and we expect that measuring the value of ψ from N replicas of $|\psi\rangle$ and N' replicas of $|\psi^*\rangle$ is equivalent to measuring ψ from N' replicas of $|\psi\rangle$ and N replicas of $|\psi^*\rangle$. So, we conclude that the optimal measurement is achieved with balanced inputs ($N = N'$), as previously mentioned. Finally, in the case where $a = 1$, the transformation consists in producing M clones of $|\psi\rangle$ from n replicas of $|\psi^*\rangle$. This is just phase-conjugation, for which we know that the best strategy is to perform a measurement [12]. The additional variance is therefore given by $1/n$, which does not depend on M. This explains why all curves converge to the same point at $a = 1$.

5 Conclusions

In summary, we have studied continuous-variable cloning machines, which produce several copies from one or more replicas of an arbitrary coherent state. We have derived the optimal fidelity of such cloners, as well as the cloning transformations that achieve this fidelity and the potential methods to implement them. We have then proposed a quantum key distribution protocol relying on continuous variables, and shown how to apply reconciliation and privacy amplification to the generated continuous key elements. We have investigated the balance between the information gained by the eavesdropper and that received by the authorized receiver, using cloning as an optimal individual eavesdropping strategy. It results from this analysis that our protocol can be made secure provided that the authorized receiver collects at least one half of the available information. Finally, we have analyzed a new class of continuous-variable cloning machines, which admit phase-conjugate input modes in addition to the normal inputs. By exploiting the antiunitarity of phase-conjugation, these new cloners can beat the standard cloners in some cases. In general, some non-zero optimal phase-conjugate input fraction must be used in order to maximize the cloning fidelity. Finally, it should be emphasized that these phase-conjugate input cloners do not extend on a qubit-based concept, in contrast with all previously developed information-theoretic processes for continuous quantum variables. Such a qubit cloner, admitting additional flipped qubits as inputs, has yet to be found.

We thank Frédéric Grosshans for comments on this manuscript, and Jean Cardinal and Serge Massar for useful discussions. N.J.C. is funded in part by the project EQUIP under the IST-FET-QJPC European programme. S.I. acknowledges support from the Belgian FRIA foundation. G.V.A. acknowledges support from the *Communauté Française de Belgique* under an *Action de Recherche Concertée*.

Appendix A: Density matrices of encoding rules

In this appendix, we give further details regarding the protocol defined in Section 3. In particular, we prove the equality of the density matrices ρ_x and ρ_p corresponding to Alice's two encoding rules provided that equation (13) is verified.

Define the Gaussian squeezed states $|\psi_x(r,\sigma_x)\rangle$ such that $\langle x\rangle = r$, $\langle p\rangle = 0$, $\Delta x^2 = \sigma_x^2$ and $\Delta p^2 = 1/4\sigma_x^2$. Similarly, let $|\psi_p(r,\sigma_p)\rangle$ be such that $\langle x\rangle = 0$, $\langle p\rangle = r$, $\Delta x^2 = 1/4\sigma_p^2$ and $\Delta p^2 = \sigma_p^2$. In the x basis, our states have the following amplitudes:

$$\langle x|\psi_x(r,\sigma_x)\rangle = \frac{1}{\sqrt{\sigma_x}\sqrt[4]{2\pi}}\mathrm{e}^{-(x-r)^2/4\sigma_x^2} \tag{31}$$

$$\langle x|\psi_p(r,\sigma_p)\rangle = \frac{\sqrt{2\sigma_p}}{\sqrt[4]{2\pi}}\mathrm{e}^{-\sigma_p^2x^2}\mathrm{e}^{\mathrm{i}rx}. \tag{32}$$

The density matrices ρ_x and ρ_p are defined as:

$$\rho_x = \int_{-\infty}^{+\infty}\mathrm{d}r\frac{\mathrm{e}^{-r^2/2\Sigma_x^2}}{\Sigma_x\sqrt{2\pi}}|\psi_x(r,\sigma_x)\rangle\langle\psi_x(r,\sigma_x)| \tag{33}$$

and

$$\rho_p = \int_{-\infty}^{+\infty}\mathrm{d}r\frac{\mathrm{e}^{-r^2/2\Sigma_p^2}}{\Sigma_p\sqrt{2\pi}}|\psi_p(r,\sigma_p)\rangle\langle\psi_p(r,\sigma_p)|. \tag{34}$$

Let us now calculate $\langle x|\rho_x|x'\rangle$ and $\langle x|\rho_p|x'\rangle$ in order to show that $\rho_x = \rho_p$

$$\langle x|\rho_x|x'\rangle = \int_{-\infty}^{+\infty}\mathrm{d}r\frac{\mathrm{e}^{-r^2/2\Sigma_x^2-(x-r)^2/4\sigma_x^2-(x'-r)^2/4\sigma_x^2}}{\sigma_x\Sigma_x 2\pi}. \tag{35}$$

The exponent of e in the above equation can be rewritten as

$$-\frac{\left(r-\frac{\Sigma_x^2(x+x')}{2(\sigma_x^2+\Sigma_x^2)}\right)^2}{2\Sigma_x^2\sigma_x^2/(\sigma_x^2+\Sigma_x^2)} - \frac{x^2+x'^2}{4(\sigma_x^2+\Sigma_x^2)} - \frac{\Sigma_x^2(x-x')^2}{8\sigma_x^2(\sigma_x^2+\Sigma_x^2)}. \tag{36}$$

After integration, this yields

$$\langle x|\rho_x|x'\rangle = \frac{\mathrm{e}^{-\frac{x^2+x'^2}{4(\sigma_x^2+\Sigma_x^2)}}\mathrm{e}^{-\frac{\Sigma_x^2(x-x')^2}{8\sigma_x^2(\sigma_x^2+\Sigma_x^2)}}}{\sqrt{2\pi}\sqrt{\sigma_x^2+\Sigma_x^2}}\cdot \tag{37}$$

For ρ_p, we have

$$\begin{aligned}\langle x|\rho_p|x'\rangle &= \int_{-\infty}^{+\infty}\mathrm{d}r\frac{2\sigma_p}{2\pi\Sigma_p}\mathrm{e}^{-r^2/2\Sigma_p^2} \\ &\quad\times \mathrm{e}^{\mathrm{i}r(x'-x)}\mathrm{e}^{-\sigma_p^2(x^2+x'^2)} \\ &= \frac{2\sigma_p}{\sqrt{2\pi}}\mathrm{e}^{-\sigma_p^2(x^2+x'^2)}\mathrm{e}^{-\frac{\Sigma_p^2}{2}(x-x')^2}. \end{aligned}\tag{38}$$

Taking (13) into account, we have $\langle x|\rho_x|x'\rangle = \langle x|\rho_p|x'\rangle$ for all x, x', hence $\rho_x = \rho_p$.

References

1. E. Arthurs, J.L. Kelly Jr, Bell Syst. Tech. J. **44**, 725 (1965).
2. C.H. Bennett, G. Brassard, Public-key distribution and coin tossing, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India (IEEE, New York, 1984), pp. 175–179.
3. C.H. Bennett, G. Brassard, C. Crépau, U.M. Maurer, IEEE Trans. Inform. Theor. **41**, 1915 (1995).
4. C.H. Bennett, G. Brassard, J.-M. Robert, SIAM J. Comp. **17**, 210 (1988).
5. G. Brassard, L. Salvail, *Secret-key reconciliation by public discussion*, Advances in Cryptology – Eurocrypt'93 (New York) edited by T. Helleseth, Lecture Notes in Computer Science (Springer-Verlag, 1993), pp. 411–423.
6. S.L. Braunstein, V. Buzek, M. Hillery, Phys. Rev. A **63**, 052313 (2001).
7. S.L. Braunstein, N.J. Cerf, S. Iblisdir, P. van Loock, S. Massar, Phys. Rev. Lett. **86**, 4438 (2001).
8. S.L. Braunstein, H.J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
9. C.M. Caves, Phys. Rev. D **26**, 1817 (1982).
10. N.J. Cerf, S. Iblisdir, Phys. Rev. A **62**, 040301 (2000).
11. N.J. Cerf, S. Iblisdir, Phys. Rev. Lett. **87**, 247903 (2001).
12. N.J. Cerf, S. Iblisdir, Phys. Rev. A **64**, 032307 (2001).
13. N.J. Cerf, A. Ipe, X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000).
14. N.J. Cerf, M. Lévy, G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
15. K. Chen, *Reconciliation by public discussion: Throughput and residue error rate*, unpublished, 2001.
16. T.M. Cover, J.A. Thomas, *Elements of information theory* (Wiley & Sons, New York, 1991).
17. J. Fiurasek, Phys. Rev. Lett. **86**, 4942 (2001).
18. N. Gisin, S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
19. N. Gisin, S. Popescu, Phys. Rev. Lett. **83**, 432 (1999).
20. F. Grosshans, P. Grangier, Phys. Rev. A **64**, 010301 (2001).
21. M. Hillery, Phys. Rev. A **61**, 022309 (2000).
22. U.M. Maurer, IEEE Trans. Inform. Theor. **39**, 733 (1993).
23. T.C. Ralph, Phys. Rev. A **61**, 010303 (2000).
24. T.C. Ralph, Phys. Rev. A **62**, 062306 (2000).
25. M.D. Reid, Phys. Rev. A **62**, 062308 (2000).
26. M.O. Scully, M.S. Zubairy, *Quantum optics* (Cambridge University Press, Cambridge, 1997).
27. T. Sugimoto, K. Yamazaki, IEICE Trans. Fund. **E83-A**, 1987 (2000).
28. L. Vaidman, Phys. Rev. A **49**, 1473 (1994).
29. G. Van Assche, J. Cardinal, N.J. Cerf, arXiv e-print: `cs.CR/0107030`, (2001).
30. K. Yamazaki, T. Sugimoto, On secret key reconciliation protocol, *Int. Symp. on Inf. Th. and Its App.*, 2000.