Quantum cloning

Valerio Scarani,* Sofyan Iblisdir,[†] and Nicolas Gisin[‡]

Group of Applied Physics, University of Geneva, 20, rue de l'Ecole-de-Médecine, CH-1211 Geneva 4, Switzerland

Antonio Acín[§]

ICFO-Institut de Ciències Fotòniques, 29 Jordi Girona, E-08034 Barcelona, Spain

The impossibility of perfectly copying (or cloning) an unknown quantum state is one of the basic rules governing the physics of quantum systems. The processes that perform the optimal approximate cloning have been found in many cases. These "quantum cloning machines" are important tools for studying a wide variety of tasks, e.g., state estimation and eavesdropping on quantum cryptography. This paper provides a comprehensive review of quantum cloning machines both for discrete-dimensional and for continuous-variable quantum systems. In addition, it presents the role of cloning in quantum cryptography, the link between optimal cloning and light amplification via stimulated emission, and the experimental demonstrations of optimal quantum cloning.

CONTENTS

*Electronic address: valerio.scarani@physics.unige.ch
[†]Electronic address: sofyan.iblisdir@physics.unige.ch
[‡]Electronic address: nicolas.gisin@physics.unige.ch
[§]Electronic address: antonio.acin@icfo.es

I. CLONING OF QUANTUM INFORMATION

A. Introduction

The concept of information is shaping our world: communication, economy, sociology, statistics, … all benefit from this wide-encompassing notion. During the last decade or so, information entered physics from all sides: from cosmology (e.g., entropy of black holes[1]) to quantum physics (the entire field of quantum information processing). Some physicists even try to reduce all natural sciences to mere information (Brukner and Zeilinger, 2002; Fuchs, 2002; Collins *et al.*, 2004). In this review, we concentrate on one of the essential features of information: the possibility of copying it. One might think that this possibility is an essential feature of any good encoding of information. This is, however, not the case: when information is encoded in quantum systems, in general it cannot be replicated without introducing errors. This limitation, however, does not make quantum information useless—quite the contrary, as we are going to show.

But we should first answer a natural question: why should one encode information in quantum systems? In the final analysis, the carriers of information can only be physical systems ("information is physical," as Rolf Landauer summarized it); and ultimately, physical systems obey the laws of quantum physics. So in some sense, the question that opened this paragraph can be answered with another question: do you know any carriers of information, other than quantum systems? The answer that most physicists give is, "No, because everything is quantum"—indeed, the boundary between the classical and the quantum world, if any such boundary exists, has not been identified yet. Other reasons to be interested in quantum information will soon become clear.

Still, even if the carrier of information is a quantum system, its encoding may be classical. The most striking example found in nature is DNA: information is encoded by molecules, which are definitely quantum systems, but it is encoded in the nature of the molecules

(adenine, thymine, cytosine, guanine) not in their state.[2] Such an encoding is classical, because one cannot find a superposition of "being adenine" and "being thymine." If information is encoded this way, it can be replicated perfectly: this process is called *cloning*. Nature performs it and biologists are struggling to master it as well.

Here, we concentrate on the *quantum encoding of information*, when information is encoded in the state ψ of quantum systems. The process of replicating the state, written $\psi \rightarrow \psi \otimes \psi$ and called cloning as well, can be done perfectly and with probability 1 if and only if a basis to which ψ belongs is known. Otherwise, perfect cloning is impossible: either the copies are not perfect or they are perfect but sometimes the copying process simply gives no outcome. These are the content and the consequences of the *no-cloning theorem* of quantum information. Similar to Heisenberg's uncertainty relations, the no-cloning theorem defines an intrinsic impossibility, not just a limitation of laboratory physics.

After some thinking though, one may object that the possibility of classical telecommunication contradicts the no-cloning theorem: after all, information traveling in optical fibers is encoded in the state of light, so it should be a quantum encoding; and this information is amplified several times from the source to the receiver, so it should degrade. Indeed, it does. However, a telecom signal consists of a large number of photons prepared in the very same quantum state, so amplification in telecom amounts to producing some new copies of ψ out of $\psi^{\otimes N}$. In short, the no-cloning theorem does apply to the amplification of telecom signals because spontaneous emission is always present in amplifiers; but the copy is almost perfect because stimulated emission is the dominating effect. The sensitivity of present-day devices is such that the quantum limit should be reached in the foreseeable future.[3]

We have left for the end of the Introduction the most surprising idea: an encoding of information that obeys the no-cloning theorem is helpful. The impossibility of perfectly copying quantum information does not invalidate the entire concept of quantum information. Quite the opposite, it provides an illustration of its power. There is no way for someone to perfectly copy the state of a quantum system for a clever encoding of information which uses a set of nonorthogonal states. Consequently, if such a system arrives unperturbed at a receiver, then, for sure, it has not been copied by any

---

[1]The widely discussed topic of black-hole evaporation is also a matter of information: is all the information that has entered a black hole lost forever—technically, does irreversible non-unitary dynamics exist in nature?

[2]This does not necessarily imply that the way Nature processes this information is entirely classical: this point is an open question.
[3]The security parameter for the acceptable error is presently set at $e = 10^{-9}$. Let us make a simple estimate of the ultimate quantum limit that corresponds to it: the signal is a coherent state $|\alpha\rangle$, and let us say that an error is possible for the vacuum component because for that component there is no stimulated emission. Then $e \approx |\langle \alpha | 0 \rangle|^2 = \exp(-|\alpha|^2)$, which is equal to 10^{-9} for an average number of photons $|\alpha|^2 \approx 20$. In actual networks, a telecom pulse that has traveled down a fiber reaches the amplifier with an intensity of some 100 photons on average.

adversary. Hence due to the no-cloning theorem, quantum information provides a means to perform some tasks that would be impossible using only ordinary information, such as detecting any eavesdropper on a communication channel. This is the idea of quantum cryptography.

The outline of the review will be given in Sec. I.D.3 after some concepts have been introduced. We start by stating and demonstrating the no-cloning theorem, and by sketching its history.

B. The no-cloning theorem

It is well known that one cannot measure the state $|\psi\rangle$ of a single quantum system: the result of any single measurement of an observable A is one of its eigenstates, bearing only very poor information about $|\psi\rangle$, namely, that it must not be orthogonal to the measured eigenstate. To reconstruct $|\psi\rangle$ (or more generally, any mixed state ρ) one has to measure the average values of several observables, and this implies making statistical averages over a large number of identically prepared systems (Wootters and Fields, 1989). One can imagine how to circumvent this impossibility in the following way: take the system in the unknown state $|\psi\rangle$ and let it interact with N other systems previously prepared in a blank reference state $|R\rangle$ in order to obtain $N+1$ copies of the initial state:

$$|\psi\rangle \otimes |R\rangle \otimes \cdots \otimes |R\rangle \overset{?}{\rightarrow} |\psi\rangle \otimes |\psi\rangle \otimes \cdots \otimes |\psi\rangle. \qquad (1)$$

Such a procedure would allow one to determine the quantum state of a single system without even measuring it because one could measure the N new copies and leave the original untouched. The no-cloning theorem of quantum information formalizes the suspicion that such a procedure is impossible:

No-cloning theorem: No quantum operation exists that can duplicate perfectly an arbitrary quantum state.

The theorem can be proved with a *reductio ad absurdum* by considering the $1 \rightarrow 2$ cloning. The most general evolution of a quantum system is a trace-preserving completely positive map. A well-known theorem (Kraus, 1983) says that any such map can be implemented by appending an auxiliary system (*ancilla*) to the system under study, let the whole undergo a unitary evolution, then trace out the ancilla. So let us suppose that perfect cloning can be realized as a unitary evolution, possibly involving an ancilla (the machine):

$$|\psi\rangle \otimes |R\rangle \otimes |\mathcal{M}\rangle \overset{U?}{\rightarrow} |\psi\rangle \otimes |\psi\rangle \otimes |\mathcal{M}(\psi)\rangle. \qquad (2)$$

In particular then, for two orthogonal states labeled $|0\rangle$ and $|1\rangle$, we have

$$|0\rangle \otimes |R\rangle \otimes |\mathcal{M}\rangle \rightarrow |0\rangle \otimes |0\rangle \otimes |\mathcal{M}(0)\rangle,$$

$$|1\rangle \otimes |R\rangle \otimes |\mathcal{M}\rangle \rightarrow |1\rangle \otimes |1\rangle \otimes |\mathcal{M}(1)\rangle.$$

But because of linearity (we omit tensor products) these conditions imply

FIG. 1. Setup devised by Herbert to achieve signaling. A source S produces pairs of qubits in a maximally entangled state; on the left, Alice measures either σ_x or σ_z. On the right, Bob applies a perfect quantum cloning machine (QCM) and then measures the two clones (the measurement M may be individual or collective).

$$(|0\rangle + |1\rangle)|R\rangle|\mathcal{M}\rangle \rightarrow |00\rangle|\mathcal{M}(0)\rangle + |11\rangle|\mathcal{M}(1)\rangle.$$

The right-hand side cannot be equal to $(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)|\mathcal{M}(0+1)\rangle = (|00\rangle + |10\rangle + |01\rangle + |11\rangle)|\mathcal{M}(0+1)\rangle$. So Eq. (2) may hold for states of an orthonormal basis, but cannot hold for all states. This concludes the proof using only the linearity of quantum transformations following the work of Wootters and Zurek (1982); a slightly different proof, using more explicitly the properties of unitary operations, can be found in Sec. 9-4 of Peres's textbook (Peres, 1995).

C. History of the no-cloning theorem

1. When "wild" ideas trigger deep results

Historically, the no-cloning theorem did not spring out of deep thoughts on the quantum theory of measurement. The triggering event was a rather unconventional proposal by Nick Herbert to use quantum correlations to communicate faster than light (Herbert, 1982). Herbert called his proposal FLASH, as an acronym for first light amplification superluminal hookup. The argument goes as follows (Fig. 1). Consider two parties, Alice and Bob, at an arbitrary distance, sharing two qubits[4] in the singlet state $|\Psi^-\rangle = (1/\sqrt{2})(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$. On her qubit, Alice measures either σ_x or σ_z. Because of the properties of the singlet, if Alice measures σ_z, she finds the eigenstate $|0\rangle$ or $|1\rangle$ (with probability $\frac{1}{2}$), and in this case she prepares Bob's qubit in the state $|1\rangle$ or $|0\rangle$, respectively. Without any knowledge of Alice, Bob sees the mixed state $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\mathbb{1}$, just as if Alice had done nothing. Similarly, if Alice measures σ_x, she finds the eigenstate $|+\rangle$ or $|-\rangle$ (with probability $\frac{1}{2}$), and in this case she prepares Bob's qubit in the state $|-\rangle$ or $|+\rangle$, respectively. Again, without any knowledge of Alice, Bob sees the mixed state $\frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| = \frac{1}{2}\mathbb{1}$.

However, suppose that Bob has a perfect $1 \rightarrow 2$ cloner, QCM in Fig. 1, and that he has his qubit pass through it. Now, if Alice measures σ_x, Bob's mixture is $\rho_x = \frac{1}{2}|++\rangle\langle ++| + \frac{1}{2}|--\rangle\langle --|$; if Alice measures σ_z, Bob's mixture is $\rho_z = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|$. It is easily verified that $\rho_x \neq \rho_z$ (for instance, $\langle 01|\rho_x|01\rangle = \frac{1}{4}$ while $\langle 01|\rho_z|01\rangle = 0$). Thus at

---

[4]A *qubit* is a two-dimensional quantum system. In this paper, the mathematics of qubits are used extensively: we use the standard notations of quantum information, summarized in the Appendix together with some useful formulas. We shall also use the term *qudit* to designate a *d*-level quantum system.

least with some probability, by measuring his two perfect clones, Bob could know the measurement that Alice has chosen without any communication with her.

This is an obvious violation of the no-signaling condition, but the argument was clever—that is why it was published (Peres, 2002)—and triggered the responses[5] of Dieks (1982), Milonni and Hardies (1982), Wootters and Zurek (1982) and slightly later Mandel (1983). In these papers, the no-cloning theorem was firmly established as a consequence of the linearity of quantum mechanics. It was also shown that the best-known amplification process, spontaneous and stimulated emission of a photon by an excited system, was perfectly consistent with this no-go theorem (Milonni and Hardies, 1982; Wootters and Zurek 1982; Mandel, 1983).

2. Missed opportunities

Once the simplicity of the no-cloning theorem is noticed, one cannot but wonder why its discovery was delayed until 1982. There is no obvious answer to this question. But we can review two missed opportunities:

In 1957 during a sabbatical in Japan, Charles Townes worked out with Shimoda and Takahasi the phenomenological equations which describe the amplification in the maser that he had demonstrated four years before (Shimoda *et al.*, 1957; Townes, 2002). In this paper (see the discussion in Sec. VI.A.3 for more details), some rate equations appear from which the fidelity of optimal quantum cloning processes[6] immediately follows. At that time, however, nobody used to look at physics in terms of information, so in particular, nobody thought of quantifying amplification processes in terms of the accuracy to which the input state is replicated.

The second missed opportunity involved Eugene Paul Wigner. In a *Festschrift*, he tackled the question of biological cloning (Wigner, 1961). Wigner tentatively identified the living state with a pure quantum-mechanical state, noted ν, and he then noticed that among all the possible unitary transformations, those that implement $\nu \otimes w \rightarrow \nu \otimes \nu \otimes r$ are a negligible set—but he did not notice that no transformation realizes that task for any ν, which would have been the no-cloning theorem. From his observation, Wigner concluded that biological reproduction "appears to be a miracle from the point of view of the physicist." We know nowadays that his tentative description of the living state is not correct, and that reproduction is possible because the encoding in DNA is classical (see the Introduction of this review).

3. From no cloning to optimal cloning

Immediately after its formulation, the no-cloning theorem became an important piece of physics, cited in connection with both no signaling (Ghirardi and Weber, 1983; Bussey, 1987), and amplification (Yuen, 1986). Interestingly, no cloning was invoked as an argument for the security of quantum cryptography from the very beginning (Bennett and Brassard, 1984). Section 9-4 of Peres's book (Peres, 1995) is a good review of the role of the theorem before 1996. In the first months of that same year, Barnum *et al.* (1996) considered the possibility of the perfect cloning of noncommuting mixed states, and reached the same no-go conclusion as for pure states. Everything fell into place.

The situation suddenly changed a few months later: in the September 1996 issue of *Physical Review A*, Vladimír Bužek and Mark Hillery published a paper, "Quantum copying: beyond the no-cloning theorem" (Bužek and Hillery, 1996). Of course, they did not claim that the no-go theorem was wrong. But the theorem applied only to perfect cloning, whereas Bužek and Hillery suggested the possibility of imperfect cloning. Specifically (see Sec. II.A for all details), they found a unitary operation

$$|\psi\rangle_A \otimes |R\rangle_B \otimes |\mathcal{M}\rangle_M \rightarrow |\Psi\rangle_{ABM}, \tag{3}$$

such that the partial traces on the original qubit A and on the cloned qubit B satisfied

$$\rho_A = \rho_B = F|\psi\rangle\langle\psi| + (1-F)|\psi^\perp\rangle\langle\psi^\perp|, \tag{4}$$

with a fidelity F that was "not too bad" $\left(\frac{5}{6}\right)$ and was the same for any input state $|\psi\rangle$. The Bužek-Hillery unitary transformation was the first *quantum cloning machine*; it triggered an explosion in the number of investigations on quantum cloning.

D. Quantum cloning machines (QCM): Generalities

1. Definition of cloning

Any interaction (i.e., any completely positive map) between two quantum systems A and B, possibly mediated by an ancilla M, has the effect of shuffling the quantum information between all the subsystems. When the input state takes the form $|\psi\rangle_A|R\rangle_B$, then at the output of any completely positive map, the quantum information contained in $|\psi\rangle$ will have been somehow distributed among A and B (and possibly the ancilla). This suggests the following definition of the process of *cloning of pure states*, that we generalize immediately to the case of $N \rightarrow M$ cloning:

$$(|\psi\rangle^{\otimes N}) \otimes (|R\rangle^{\otimes M-N}) \otimes |\mathcal{M}\rangle \overset{U}{\rightarrow} |\Psi\rangle, \tag{5}$$

where $|\psi\rangle$ is the state of $\mathcal{H}$ to be copied, $|R\rangle$ is a reference state arbitrarily chosen in the same Hilbert space $\mathcal{H}$, and $|\mathcal{M}\rangle$ is the state of the ancilla. In other words:

- The fact that the process is a form of cloning is determined by the form of the input state, left-hand side of Eq. (5): N particles (originals) carry the pure state $|\psi\rangle$ to be copied. In particular, the N originals are disentangled from the $M-N$ particles that are going to carry the copies (that start in a blank state) and from the ancillae. In fact, sometimes (e.g., in Secs. II.C and II.D) it will be convenient to consider that the copies and the ancillae start in an entangled state. This does not contradict Eq. (5): one simply omits to mention a "trivial" part of the QCM that prepares the copies and the ancillae in the suitable state. It is important to stress that we consider only pure states as inputs; to our knowledge, there are no results on QCM that would be optimal for mixed states.

- The cloning process (5) is defined by the quantum cloning machine (QCM), which is the trace-preserving completely positive map, or equivalently the pair

$$\text{QCM} = \{U, |\mathcal{M}\rangle\}. \tag{6}$$

A QCM can be seen as a quantum processor U that processes the input data according to some program $|\mathcal{M}\rangle$. Examples of QCMs that produce clones of very different quality are easily found: just take the identity $|\psi\rangle_A|R\rangle_B \rightarrow |\psi\rangle_A|R\rangle_B$ that transfers no information from A to B, or the swap $|\psi\rangle_A|R\rangle_B \rightarrow |R\rangle_A|\psi\rangle_B$ that transfers all the information from A to B—both unitary operations with no ancilla. The possibility of defining coherent combinations of such processes suggests that nontrivial QCMs can be found, and indeed, we shall see that this intuition is basically correct (see particularly Sec. II.C), although not fully, because ancillae play a crucial role.

2. Fidelity and the glossary of QCMs

Having defined the meaning of cloning, we introduce the basic glossary that is used in the study and classification of QCMs. The very first object to define is a *figure of merit* according to which the output of the QCM should be evaluated. The usual figure of merit is the *single-copy fidelity*, called simply *fidelity* unless some ambiguity is possible. This is defined for each of the outputs $j=1,\ldots,M$ of the cloning machine as the overlap between ρ_j and the initial state $|\psi\rangle$:

$$F_j = \langle\psi|\rho_j|\psi\rangle, \quad j = 1, \ldots, M, \tag{7}$$

where ρ_j is the partial state of clone j in the state $|\Psi\rangle$ defined in Eq. (5). Note that the worst possible fidelity for the cloning of a d-dimensional quantum system is $F_j = 1/d$, obtained if ρ_j is the maximally mixed state $\mathbb{1}/d$.

The following, standard classification of QCMs follows:

- A QCM is called *universal* if it copies equally well all the states, that is, if F_j is independent of $|\psi\rangle$. The notation UQCM is often used. Nonuniversal QCMs

are called *state dependent*.

- A QCM is called *symmetric* if at the output all the clones have the same fidelity, that is, if $F_j = F_{j'}$ for all $j, j' = 1, \ldots, M$. For asymmetric QCMs, further classifications are normally needed: for instance, in the study of $1 \rightarrow 3$ asymmetric QCMs, one may consider only the case $F_1 \neq F_2 = F_3$ (we write as $1 \rightarrow 1+2$) or consider the general case $1 \rightarrow 1+1+1$ where all three fidelities can be different.

- A QCM is called *optimal* if for a given fidelity of the original(s), the fidelities of the clones are the maximal ones allowed by quantum mechanics. More specifically, if $\mathcal{S}$ is the set of states to be cloned, optimality can be defined by maximizing either the average fidelity over the states $\bar{F} = \int_{\mathcal{S}} d\psi F(\psi)$ or the minimal fidelity over the states $F_{\min} = \min_{\psi \in \mathcal{S}} F(\psi)$. These definitions often coincide.

According to this classification, for instance, the Bužek-Hillery QCM is the optimal symmetric UQCM for the cloning $1 \rightarrow 2$ of qubits. The generalization to optimal symmetric UQCMs for the cloning $N \rightarrow M$ has been rapidly found, first for qubits (Gisin and Massar, 1997; Bruß, Di Vincenzo, *et al.*, 1998), then for arbitrary-dimensional systems (Werner, 1998; Keyl and Werner, 1999). The family of optimal asymmetric UQCMs for the cloning $1 \rightarrow 1+1$ of arbitrary dimension has also been fully characterized (Cerf, 2000b; Braunstein, Bužek, and Hillery, 2001; Iblisdir *et al.*, 2004; Fiuràšek, Filip, and Cerf, 2005; Iblisdir, Acín, and Gisin, 2005). The study of the optimal universal asymmetric QCM $N \rightarrow M_1 + M_2$ was undertaken later, motivated by the fact that the $2 \rightarrow 2+1$ QCM is needed for the security analysis of quantum cryptography protocols. As the reader may easily imagine, the full zoology of QCMs has not been explored: there are difficult problems that remain. For instance, very few examples of optimal state-dependent QCMs are known.

3. Outline of the paper

The outline of this review is as follows. In Sec. II, we review the cloning of discrete quantum systems, presenting the QCMs for qubits and stating the generalizations to larger-dimensional systems. We introduce at the end of this section the link between cloning and state estimation. In Sec. III, we review the cloning of continuous variables. Section IV is devoted to the application of quantum cloning to eavesdropping in quantum cryptography. The last two sections are devoted to the realization of quantum cloning. Section V shows how amplification based on the interplay of spontaneous and stimulated emission achieves optimal cloning of discrete systems encoded in different modes of the light field. We present a self-contained derivation of this claim. In Sec. VI, we review the experimental proposals and demonstrations of cloning for the polarization of photons and for other physical systems.

Some topics related to cloning are omitted in this review. One of them is *probabilistic exact cloning* (Duan

and Guo, 1998; Pati, 1999). While in the spirit of Bužek-Hillery one circumvents the no-cloning theorem by allowing imperfect cloning, in probabilistic cloning one wants to always obtain a perfect copy, but the price is that the procedure works only with some probability. This is related to unambiguous state discrimination procedures in state-estimation theory. In comparison to probabilistic cloning, the cloning procedures *à la* Bužek-Hillery that we describe in this review are called *deterministic cloning*, because the desired result, namely, imperfect copying, is always obtained. Hybrid strategies between probabilistic-exact and deterministic-imperfect cloning have also been studied and compared to results of state-estimation theory (Chefles and Barnett, 1999).

Another topic that will be omitted is *telecloning*, that is, cloning at a distance. In this protocol, a party Alice has a copy of an unknown quantum state and wants to send the best possibly copy to each of M partners. An obvious procedure consists in performing locally the optimal $1 \to M$ cloning, then teleporting the M particles to each partner; this strategy requires M singlets (that is, M bits of entanglement or *e*-bits) and the communication of $2M$ classical bits. It has been proved that other strategies exist that are much cheaper in terms of the required resources (Murao *et al.*, 1999). In particular, the partners can share a suitable entangled state of only $O(\log_2 M)$ *e*-bits, and in this case the classical communication is also reduced to public broadcasting of two bits.

E. No cloning and other limitations

As a last general discussion, we want to briefly sketch the link between cloning and other limitations that are found in quantum physics; specifically, the no-signaling condition and the uncertainty relations.

1. Relation to no signaling

As said in Sec. I.C, a perfect cloner would allow signaling through entanglement alone. Shortly after the idea of imperfect cloning was put forward, Gisin (1998) noticed that one can also study optimal imperfect cloning starting from the requirement that no signaling should hold. The proof was given for universal symmetric $1 \to 2$ cloning for qubits. The idea is to require that the input state $|\psi\rangle\langle\psi| = \frac{1}{2}(\mathbb{1} + \hat{m} \cdot \sigma)$ be copied into a two-qubit state such that the two one-qubit partial states are equal and read $\rho_1 = \rho_2 = \frac{1}{2}(\mathbb{1} + \eta \hat{m} \cdot \sigma)$: i.e., the Bloch vector points in the same direction as for the original but is shrunk by a factor η (*shrinking factor*), related to the fidelity defined in Eq. (7) through $F = (1 + \eta)/2$. On the one hand, we know from the no-cloning theorem that $\eta = 1$ is impossible and would lead to signaling; on the other hand, $\eta = 0$ is obviously possible by simply throwing the state away in a nonmonitored mode and preparing a new state at random. So there must be a largest shrinking factor η compatible with the no-signaling condition.

The form of the partial states $\rho_{1,2}$ implies that the state of systems 1 and 2 after cloning should read

$$\rho_{\text{out}}(\psi) = \frac{1}{4}\left(\mathbb{1}_4 + \eta(\hat{m} \cdot \sigma \otimes \mathbb{1} + \mathbb{1} \otimes \hat{m} \cdot \sigma) \right.$$
$$\left. + \sum_{i,j=x,y,z} t_{ij}\sigma_i \otimes \sigma_j \right). \quad (8)$$

The tensor t_{ij} has some structure because of the requirement of universality, which implies covariance:

$$\rho_{\text{out}}(U|\psi\rangle) = U \otimes U \rho_{\text{out}}(\psi)U^\dagger \otimes U^\dagger. \quad (9)$$

This means that the following two procedures are equivalent: either to apply a unitary U on the original and then the cloner, or to apply the cloner first and then U to both copies.

These are the requirements of universality, η accounting for imperfect cloning. With this definition of QCM, one can again run the gedanken experiment discussed in Sec. I.C (Fig. 1). Bob's mixtures after cloning read now $\rho_x = \frac{1}{2}\rho_{\text{out}}(+x) + \frac{1}{2}\rho_{\text{out}}(-x)$ and $\rho_z = \frac{1}{2}\rho_{\text{out}}(+z) + \frac{1}{2}\rho_{\text{out}}(-z)$. No signaling requires $\rho_x = \rho_z$. By using the fact that density matrices must be positive operators, one finds after some calculation the bound $\eta \leq \frac{2}{3}$ $(F \leq \frac{5}{6})$ for any universal symmetric $1 \to 2$ QCM for qubits. This analysis alone does not say whether this bound can be attained; but we know it can: the Bužek-Hillery QCM reaches up to it. Thus the no-signaling condition provides a bound for the fidelity of quantum cloning, and this bound is tight since there exists a QCM that saturates it; in turn, this provides a proof of the optimality of the Bužek-Hillery QCM. The argument was generalized by Simon for the $1 \to N$ symmetric cloning (Simon, 2001). Other QCMs on the edge of the no-signaling condition have been described more recently (Navez and Cerf, 2003).

In conclusion, the no-signaling condition has been found to provide tight bounds for cloning—in fact, this observation was extended to any linear trace-preserving completely positive map (Simon *et al.*, 2001). The converse statement also holds: no linear trace-preserving completely positive map (so in particular, no QCM) can lead to signaling (Bruß, D'Ariano, *et al.*, 2000). Finally, it has been proved recently that no cloning is a feature that holds for all nonlocal no-signaling theories (Masanes *et al.*, 2005).

2. Relation to uncertainty relations and knowledge

In addition to allowing signaling through entanglement alone, perfect cloning would also violate one of the main tenets of quantum mechanics, namely, that the state of a single quantum system cannot be known.[7] If

---

[7]Invoking the same argument as in Sec. 9-4 of Peres's book (Peres, 1995), perfect cloning would thus lead to a violation of the second law of thermodynamics. However, the cogency of this argument is disputed [see Mana *et al.* (2005) for a recent analysis]. In fact, to derive the violation of the second law, one makes the assumptions that (i) nonorthogonal states are deterministically distinguishable, and (ii) entropies are computed using the quantum formalism. Clearly, the two assumptions already look contradictory.

perfect cloning were possible, one could know everything of a single particle's state without even measuring it, just by producing clones and measureing these (see Sec. I.B). In turn, this would invalidate quantum cryptography (see Sec. IV) and lead to the violation of some information-theoretical principles, such as Landauer's erasure principle (Plenio and Vitelli, 2001). The link between optimal cloning and the amount of knowledge that one can obtain on the state of a limited number of quantum systems (in the limit, just one) can be made quantitative, see Sec. II.E in this review.

Of course, perfect cloning would not invalidate the existence of incompatible observables: having N copies of an eigenstate of σ_z does not mean that the result of a measurement of σ_x becomes deterministic. In particular, the relation between observables $\Delta A \Delta B \geq \frac{1}{2}|\langle[A,B]\rangle|$ would still hold in the presence of perfect cloning.

II. CLONING OF DISCRETE QUANTUM SYSTEMS

In this section we review the main results for cloning of discrete quantum systems, that is, systems described by the Hilbert space $\mathcal{H}=\mathbb{C}^d$. We start from the simplest case, $1 \rightarrow 2$ symmetric cloning for qubits, and describe the Bužek-Hillery QCM (Sec. II.A). Then we present the two natural extensions: $N \rightarrow M$ symmetric cloning (Sec. II.B) and $1 \rightarrow 1+1$ asymmetric cloning (Sec. II.C). The last paragraph of this section is devoted to state-dependent cloning (Sec. II.D). An important remark when comparing this review with the original articles: in this review, we use d systematically for the dimension, and capital letters such as N and M for the number of quantum systems. This notation is nowadays standard; however, until recently, N was often used to denote the dimension of the Hilbert space.

A. Symmetric $1 \rightarrow 2$ UQCM for qubits

1. Trivial cloning

In order to appreciate the performance of the optimal $1 \rightarrow 2$ cloning for qubits (Bužek-Hillery), it is convenient to begin by presenting two trivial cloning strategies. The first trivial cloning strategy is the measurement-based procedure: one measures the qubit in a randomly chosen basis and produces two copies of the state corresponding to the outcome. Suppose that the original state is $|+\vec{a}\rangle$, whose projector is $\frac{1}{2}(\mathbb{1}+\vec{a}\cdot\vec{\sigma})$, and that the measurement basis are the eigenstates of $\vec{b}\cdot\vec{\sigma}$. With probability $P_{\pm} = \frac{1}{2}(1\pm\vec{a}\cdot\vec{b})$, two copies of $|\pm\vec{b}\rangle$ are produced; in either case, the fidelity is $F_{\pm}=|\langle+\vec{a}|\pm\vec{b}\rangle|^2=P_{\pm}$. The average fidelity is

$$
\begin{aligned}
F_{\text{triv,1}} &= \int_{S_2} d\vec{b}(P_+F_+ + P_-F_-) \\
&= \frac{1}{2} + \frac{1}{2}\int_{S_2} d\vec{b}(\vec{a}\cdot\vec{b})^2 \\
&= \frac{2}{3},
\end{aligned} \tag{10}
$$

where S_2 is the two-sphere of unit radius (surface of the Bloch sphere). This cloning strategy is indeed universal: the fidelity is independent of the original state $|+\vec{a}\rangle$.

The second trivial cloning strategy can be called trivial amplification: let the original qubit fly unperturbed and produce a new qubit in a randomly chosen state. Suppose again that the original state is $|+\vec{a}\rangle$, and suppose that the new qubit is prepared in the state $|+\vec{b}\rangle$. We detect one particle: the original one with probability $\frac{1}{2}$ and in this case $F=1$; the new one with the same probability and in this case the fidelity is $F=|\langle+\vec{a}|+\vec{b}\rangle|^2=P_+$. Thus the average single-copy fidelity is

$$
F_{\text{triv,2}} = \frac{1}{2} + \frac{1}{2}\int_{S_2} d\vec{b}\left(\frac{1+\vec{a}\cdot\vec{b}}{2}\right) = \frac{3}{4}. \tag{11}
$$

This second trivial strategy is also universal. In conclusion, we shall keep in mind that a fidelity of 75% for universal $1 \rightarrow 2$ cloning of qubits can be reached by a rather uninteresting strategy.

2. Optimal symmetric UQCM (Bužek-Hillery)

It is now time to present explicitly the symmetric UQCM for $1 \rightarrow 2$ cloning of qubits found by Bužek and Hillery. This machine needs just one qubit as ancilla. Its action in the computational basis of the original qubit is[8]

$$
|0\rangle|R\rangle|\mathcal{M}\rangle \rightarrow \sqrt{\frac{2}{3}}|0\rangle|0\rangle|1\rangle - \sqrt{\frac{1}{3}}|\Psi^+\rangle|0\rangle,
$$

$$
(-|1\rangle)|R\rangle|\mathcal{M}\rangle \rightarrow \sqrt{\frac{2}{3}}|1\rangle|1\rangle|0\rangle - \sqrt{\frac{1}{6}}|\Psi^+\rangle|1\rangle, \tag{12}
$$

with $|\Psi^+\rangle=(1/\sqrt{2})[|1\rangle|0\rangle+|0\rangle|1\rangle]$. By linearity, these two relations induce the following action on the most general input state $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$:

$$
\begin{aligned}
|\psi\rangle|R\rangle|\mathcal{M}\rangle \rightarrow &\sqrt{\frac{2}{3}}|\psi\rangle|\psi\rangle|\psi^\perp\rangle \\
&- \sqrt{\frac{1}{6}}[|\psi\rangle|\psi^\perp\rangle + |\psi^\perp\rangle|\psi\rangle]|\psi\rangle, \tag{13}
\end{aligned}
$$

where $|\psi^\perp\rangle=\alpha^*|1\rangle-\beta^*|0\rangle$.

From Eq. (13), one sees immediately that A and B can be exchanged, and, in addition, that the transformation has the same form for all input states $|\psi\rangle$. Thus this QCM is symmetric and universal. The partial states for the original and the copy are

$$
\rho_A = \rho_B = \frac{5}{6}|\psi\rangle\langle\psi| + \frac{1}{6}|\psi^\perp\rangle\langle\psi^\perp| = \frac{1}{2}\left(\mathbb{1}+\frac{2}{3}\hat{m}\cdot\vec{\sigma}\right). \tag{14}
$$

From the standpoint of both A and B then the Bužek-Hillery QCM shrinks the original Bloch vector $\hat{m}$ by a shrinking factor $\eta=\frac{2}{3}$, without changing its direction. As

---

[8]We rewrite, with a change of notation for the ancilla states, Eq. (3.29) of Bužek and Hillery (1996).

mentioned previously, the fidelity is $F_A = F_B = \langle \psi | \rho_A | \psi \rangle = \frac{5}{6}$, outperforming the trivial strategies described above. This was proved to be the optimal value (Gisin and Massar, 1997; Bruß, DiVincenzo, *et al.*, 1998; Gisin, 1998) in their original paper, Bužek and Hillery proved the optimality of their transformation with respect to two different figures of merit.

3. The transformation of the ancilla: anticlone

Although everything was designed by paying attention to qubits A and B, the partial state of the ancilla turns out to have a quite interesting meaning too. We have

$$\rho_M = \frac{2}{3}|\psi^\perp\rangle\langle\psi^\perp| + \frac{1}{3}|\psi\rangle\langle\psi| = \frac{1}{2}\left(1 - \frac{1}{3}\hat{m}\cdot\vec{\sigma}\right). \tag{15}$$

This state is related to another operation which, like cloning, is impossible to achieve perfectly, namely, the NOT operation that transforms $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ into $|\psi^\perp\rangle = \alpha^*|1\rangle - \beta^*|0\rangle$. Because of the need for complex conjugation of the coefficients, the perfect NOT transformation is antiunitary and cannot be performed.[9] Just as for cloning, one can choose to achieve the NOT on some states while leaving other states unchanged; or one can find the operation that approximates at best the NOT on all states, called the universal NOT. This operation was anticipated in a remark by Bechmann-Pasquinucci and Gisin (1999), then fully described by Bužek, Hillery, and Werner (1999). The universal NOT gate gives precisely $\rho_{\rm NOT} = \rho_M$, and is thus implemented as a by-product of cloning.[10] It has become usual to say that, at the output of a QCM, the ancilla carries the optimal *anticlone* of the input state.

B. Symmetric UQCM $N \rightarrow M$

A symmetric, universal $N \rightarrow M$ QCM for qubits that generalizes the Bužek-Hillery QCM was found by Gisin and Massar (1997). Its fidelity is

$$F_{N \rightarrow M} = \frac{MN + M + N}{M(N+2)} \quad (d=2), \tag{16}$$

which reproduces $F_{1\rightarrow 2} = \frac{5}{6}$ for $N=1$ and $M=2$. They gave numerical evidence for its optimality. Later, an analytical proof of optimality was given by Bruß, Ekert, and Mac-

chivello (1998), who assumed that the output state belongs to the symmetric subspace of M qubits (this assumption is unjustified *a priori* but turns out to be correct, see below). The result was further generalized by Werner for systems of any dimension (Werner, 1998; Kevl and Werner, 1999).

1. Werner's construction

We consider d-dimensional quantum systems described by the Hilbert space $\mathcal{H} = \mathbb{C}^d$. We introduce the notation $\mathcal{H}_+^n$ for the symmetric subspace of the n-fold tensor product $\mathcal{H}^{\otimes n}$; the dimension of $\mathcal{H}_+^n$ is

$$d[n] = \binom{d+n-1}{n}.$$

The input state is $\rho_N = \sigma^{\otimes N} \in \mathcal{H}_+^N$, where $\sigma = |\psi\rangle\langle\psi|$ is a pure state. The QCM is described by a trace-preserving completely positive map $T: \mathcal{H}_+^N \rightarrow \mathcal{H}^{\otimes M}$. The remarkable fact is that one can restrict the maps to completely positive maps whose output is in the symmetric subspace $\mathcal{H}_+^M$. This is clearly true if one considers all-particle test criteria, such as minimizing the trace distance between ρ_M and $\sigma^{\otimes M}$ or maximizing the all-particle fidelity $F_{all} = {\rm Tr}[\sigma^{\otimes M}\rho_M]$ as figures of merit (Werner, 1998); but if one wants to optimize the single-copy fidelity, the restriction to the symmetric subspace is not apparent at all, and required further work before being demonstrated (Keyl and Werner, 1999).

In any case, the difficulty of the optimality proofs should not hide the simplicity of the result: a single T optimizes all the figures of merit that have been considered, and this T is in some sense the most intuitive one. One simply takes the nonsymmetric trivial extension $\rho_N \rightarrow \rho_N \otimes \mathbb{1}_{M-N}$, symmetrizes it, and normalizes the result. Explicitly the optimal symmetric UQCM for $N \rightarrow M$ cloning reads

$$T[\rho_N] = \frac{d[N]}{d[M]} S_M(\rho_N \otimes \mathbb{1}_{M-N}) S_M, \tag{17}$$

where S_M is the projector from $\mathcal{H}^{\otimes M}$ to $\mathcal{H}_+^M$. The constant

$$\frac{d[N]}{d[M]} = \{{\rm Tr}[S_M(\rho_N \otimes \mathbb{1}_{M-N}) S_M]\}^{-1} \tag{18}$$

ensures that the map T is trace preserving. The state of each clone is of the form

$$\rho_1 = \eta(N,M)|\psi\rangle\langle\psi| + [1 - \eta(N,M)]\frac{\mathbb{1}}{d}, \tag{19}$$

where $|\psi\rangle$ is the input state and where the shrinking factor is found to be

$$\eta(N,M) = \frac{N}{M}\frac{M+d}{N+d}. \tag{20}$$

The corresponding fidelity is

---

[9] Here is an intuitive version of this impossibility result: any unitary operation on a qubit acts as a rotation around an axis in the Bloch sphere, while the NOT is achieved as the point symmetry of the Bloch sphere through its center. Obviously, no rotation around an axis can implement a point symmetry. A rotation of π around the axis z achieves the NOT only for the states in the (x,y) plane, while leaving the eigenstates of σ_z invariant.

[10] Contrary to cloning, however (see the first trivial cloning strategy described above Sec. II.A.1), the optimal fidelity for the NOT can also be reached in a measurement-based scenario (Bužek, Hillery, and Werner, 1999).

$$F_{N \to M}(d) = \frac{N}{M} + \frac{(M-N)(N+1)}{M(N+d)}. \tag{21}$$

So this is the optimal fidelity for universal symmetric $N \to M$ cloning of d-dimensional systems. For qubits ($d=2$) it indeed recovers the Gisin-Massar result (16). For $N=1$ and $M=2$, $F=(d+3)/2(d+1)$. Note that for a fixed amplification ratio $r=M/N$, the fidelity goes as $F=1-(d-1)(1-1/r)(1/N)+O(N^{-2})$ for $N \to \infty$. Conversely, if out of a finite number N of originals one wants to obtain an increasingly large number M of clones, the fidelity of each clone decreases as $F \simeq (N+1)/(N+d)$ in the limit $M \to \infty$, in agreement with the results of state estimation (Massar and Popescu, 1995)—see Sec. II.E.

2. Calculation of the fidelity

We have just summarized, without any proof, the main results for the optimal universal symmetric $N \to M$ QCM with discrete quantum systems. It is a good exercise to compute the single-copy fidelity $F=\text{Tr}\{(\sigma \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1})T[\sigma^{\otimes N}]\}$ and recover Eq. (21). The first step is a symmetrization: denoting $\sigma^{(k)}$ the operator that acts as σ on the kth system and as the identity on the others, and replacing T by its explicit form (17), we have

$$F = \frac{d[N]}{d[M]} \frac{1}{M} \sum_{k=1}^{M} \text{Tr}[\sigma^{(k)} S_M(\sigma^{\otimes N} \otimes \mathbb{1}_{M-N}) S_M]$$

$$= \frac{d[N]}{d[M]} \frac{1}{M} \sum_{k=1}^{M} \text{Tr}[S_M \sigma^{(k)}(\sigma^{\otimes N} \otimes \mathbb{1}_{M-N}) S_M],$$

where the second equality is obtained using the linear and cyclic properties of the trace.[11] Now, since σ is a projector, $\sigma^{(k)}(\sigma^{\otimes N} \otimes \mathbb{1}_{M-N})$ is equal to $\sigma^{\otimes N} \otimes \mathbb{1}_{M-N}$ for $1 \leq k \leq N$, and is equal to $\sigma^{\otimes N+1} \otimes \mathbb{1}_{M-N-1}$ for $N+1 \leq k \leq M$, where the additional σ happens at different positions. However, this is not important since the expression is sandwiched between the S_M so it will be symmetrized anyway. Using Eq. (18) and some algebra, one obtains Eq. (21).

3. Trivial cloning revisited

We can now have a different look at trivial cloning. The trivial amplification strategy described in Sec. II.A.1 can be easily generalized to the general case: one forwards the original N particles, adds $M-N$ particles prepared in the maximally mixed state $\mathbb{1}/d$, and performs an *incoherent* symmetrization (i.e., instead of projecting into the symmetric subspace, one simply shuffles the particles). The fidelity is then

$$F_{\text{triv}}(N \to M, d) = \frac{N}{M} + \frac{M-N}{dM}. \tag{22}$$

As expected, Eq. (21) shows that the Werner construction performs better, but the difference vanishes in the limit $d \to \infty$. We have thus learned two new insights on optimal cloning: (i) it is the quantum symmetrization that makes optimal cloning nontrivial, and (ii) in the limit of large Hilbert-space dimension, trivial cloning performs almost optimally.

In summary, Werner's construction solves the problem of finding the optimal universal symmetric QCM for any finite-dimensional quantum system and for any number of input (N) and output ($M>N$) copies. We note that Werner did not provide the implementation of the QCM T as a unitary operation on the system plus an ancilla (6). This was provided by Fan *et al.* (2001), generalizing previous partial results (Bužek and Hillery, 1998; Albeverio and Fei, 2004). In the rest of this section, we move to the study of asymmetric and state-dependent (i.e., nonuniversal) QCMs.

C. Asymmetric UQCM $1 \to 1+1$

Asymmetric universal cloning refers to a situation where output clones possibly have different fidelities. Here we focus on $1 \to 1+1$ universal cloning. The study of more general cases has been undertaken recently (Iblisdir *et al.*, 2004; Fiuràšek, Filip, and Cerf, 2005; Iblisdir, Acín, and Gisin, 2005), motivated by the security analysis of practical quantum cryptography (Acín, Gisin, and Scarani, 2004; Curty and Lütkenhaus, 2004). We shall present some of these ideas together with their possible experimental realization (Sec. VI.A.2).

In their comprehensive study of the $1 \to 1+1$ cloning, Niu and Griffiths (1998) derived, in particular, the optimal asymmetric UQCM $1 \to 1+1$. The same result was found independently by Cerf (1998, 2000a) who used an algebraic approach, and by Bužek, Hillery, and Bendik (1998) who instead developed a quantum circuit approach, improving over a previous construction for symmetric cloning (Bužek *et al.*, 1997). Optimality is demonstrated by proving that the fidelities of two clones, F_A and F_B, saturate the no-cloning inequality[12]

$$\sqrt{(1-F_A)(1-F_B)} \geq \frac{1}{2} - (1-F_A) - (1-F_B). \tag{23}$$

The same authors extended their constructions beyond the qubit case to any d (Cerf, 2000b; Braunstein, Bužek, and Hillery, 2001), although optimality was only conjectured and was proved only recently (Iblisdir *et al.*, 2004; Fiuràšek, Filip, and Cerf, 2005; Iblisdir, Acín, and Gisin, 2005).

---

[11]Since the trace is linear, we can bring the sum into it, then use $(\Sigma_k \sigma^{(k)}) S_M = S_M(\Sigma_k \sigma^{(k)})$, and finally the cyclic properties of the trace.

[12]This inequality appears in all the meaningful papers with different notations. For example, in Bužek and Hillery (1998) it is Eq. (11) since $s_{0,1}=2F_{A,B}-1=1-2(1-F_{A,B})$; in Cerf (2000a) it is Eq. (6), since $F_A=1-2x^2$ and $F_B=1-2x'^2$.
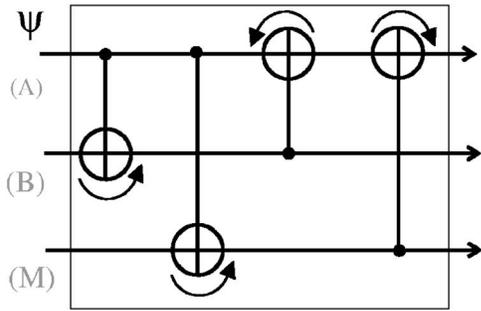
FIG. 2. The quantum circuit used for universal $1 \rightarrow 1+1$ cloning. For $d=2$, all the gates are the standard controlled NOT (CNOT). For $d>2$, the arrows play a role: the arrow towards the right, or left, defines the transformation $|k\rangle|m\rangle \rightarrow |k\rangle|m+k\rangle$, or $|k\rangle|m\rangle \rightarrow |k\rangle|m-k\rangle$, respectively—as usual, sums and differences in the kets are modulo d.

We review both Cerf's and the quantum circuit approaches, giving the explicit formalism for qubits and explaining how this generalizes to any dimension. We start with the quantum circuit formalism, which is somehow more intuitive.

1. Quantum circuit formalism

The quantum circuit that is used for universal $1 \rightarrow 1+1$ cloning in any dimension, which has been called a *quantum information distributor*,[13] is drawn in Fig. 2. It uses a single d-dimensional system as ancilla. Let us focus on qubits first. For states $|\sigma\rangle_A|\omega\rangle_B|\xi\rangle_M$ in the computational basis, i.e., $\sigma, \omega, \xi \in \{0,1\}$, the action of the circuit is

$$|\sigma\rangle_A|\omega\rangle_B|\xi\rangle_M \rightarrow |\sigma + \omega + \xi\rangle_A|\sigma + \omega\rangle_B|\sigma + \xi\rangle_M, \quad (24)$$

where all the sums are modulo 2. It is now an easy exercise to verify that

$$|\psi\rangle_A|\Phi^+\rangle_{BM} \rightarrow |\psi\rangle_A|\Phi^+\rangle_{BM}, \quad (25)$$

$$|\psi\rangle_A|0\rangle_B|+\rangle_M \rightarrow |\psi\rangle_B|\Phi^+\rangle_{AM}, \quad (26)$$

where $|\Phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$ and $|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$. Figuratively, one can say that the state of BM acts as the program for the processor defined by the circuit; in particular, $|\Phi^+\rangle_{BM}$ makes the processor act as the identity on A; $|0\rangle_B|+\rangle_M$ makes the processor swap the state $|\psi\rangle$ into mode B. Now the optimal asymmetric QCM follows quite intuitively: just take as an input state a coherent superposition of all the information in A and all the information in B:

---

[13]This quantum circuit is interesting beyond the interests of quantum cloning. Specifically, Hillery *et al.* (2004) have identified in it a *universal programmable quantum processor*. In short, the idea is to have a circuit of logic gates coupling an input state with an ancilla such that any operation on the input state is obtained by a convenient choice of the ancilla state (the program). No such circuit exists if one requires it to work deterministically; the present circuit does the job probabilistically (one knows when the operation has succeeded).

$$|\psi\rangle_A|\Psi_{\text{in}}\rangle_{BM} = |\psi\rangle_A(a|\Phi^+\rangle_{BM} + b|0\rangle_B|+\rangle_M)$$
$$\rightarrow a|\psi\rangle_A|\Phi^+\rangle_{BM} + b|\psi\rangle_B|\Phi^+\rangle_{AM}. \quad (27)$$

The parameters a and b are real; for the input state of BM to be normalized, they must satisfy $a^2+b^2+ab=1$. The partial states for the two clones after the transformation read $\rho_{A,B} = F_{A,B}|\psi\rangle\langle\psi| + (1-F_{A,B})|\psi^\perp\rangle\langle\psi^\perp|$, where the fidelities are

$$F_A = 1 - b^2/2, \quad F_B = 1 - a^2/2. \quad (28)$$

It is easy to verify that these fidelities saturate the no-cloning inequality (23). As expected, for $b=0$ or $a=0$, we find all the information in A or B, respectively. The symmetric case corresponds to $a=b=1/\sqrt{3}$, in which case we recover the Bužek-Hillery result $F_A = F_B = \frac{5}{6}$.

The generalization to $d>2$ goes exactly along the same lines. The state $|\Phi^+\rangle_{BM}$ is now the maximally entangled state of two qudits $(1/\sqrt{d})\Sigma_{k=0}^{d-1}|k\rangle_B|k\rangle_M$, the state $|+\rangle_M$ is the superposition[14] $(1/\sqrt{d})\Sigma_{k=0}^{d-1}|k\rangle_M$. After the transformation, the partial states of the two clones read $\rho_A = (1-b^2)|\psi\rangle\langle\psi| + b^2\mathbb{1}/d$ and $\rho_B = (1-a^2)|\psi\rangle\langle\psi| + a^2\mathbb{1}/d$, from which the fidelities

$$F_A = 1 - \frac{d-1}{d}b^2, \quad F_B = 1 - \frac{d-1}{d}a^2. \quad (29)$$

The normalization condition now reads $a^2+b^2+2ab/d = 1$; in particular, for the symmetric case we recover Werner's result $F_A = F_B = (d+3)/2(d+1)$; see Eq. (21).

2. Cerf's formalism

Cerf's formalism also uses a third d-dimensional system as ancilla. For qubits, the transformation reads

$$|\psi\rangle_A|\Phi^+\rangle_{BM} \rightarrow |\Psi\rangle_{ABM} = V|\psi\rangle_A|\Phi^+\rangle_{BM}, \quad (30)$$

where

$$V = \left[v\mathbb{1} + x\sum_{k=x,y,z}(\sigma_k \otimes \sigma_k \otimes \mathbb{1})\right], \quad (31)$$

where the real coefficients v and x must satisfy $v^2+3x^2 = 1$ to conserve the norm. Note that V, as written here, is not unitary, however, Eq. (30) defines a unitary transformation. In other words, V is the restriction of a unitary operation when acting on input states of the form $|\psi\rangle_A|\Phi^+\rangle_{BM}$. Here lies the appeal of Cerf's formalism: the unitary that defines the QCM reduces to the very compact and easily written transformation (31) when acting on suitable input states. By inspection, one can verify that the state $|\Psi\rangle$ in the right-hand side of Eq. (30) is equal to Eq. (27) with the identification $a=v-x$, $b=2x$. In particular, the identity is $v=1$, $x=0$, the swap is $v=x = \frac{1}{2}$, and the symmetric QCM is $v=3x$, that is, $x=1/2\sqrt{3}$.

---

[14]Written $|p_0\rangle$ in Braunstein, Bužek, and Hillery (2001); see Eq. (2.1) in that reference.

The generalization to $d > 2$ goes along the same lines (Cerf, 2000b; Cerf, Bourennane, *et al.*, 2002). The transformation, acting on the $|\psi\rangle_A |\Phi^+\rangle_{BM}$ as defined above for qudits, reads

$$V = \left(v\mathbb{1} + x \sum_{(m,n) \in K} (U_{m,n} \otimes U_{m,n} \otimes \mathbb{1}) \right), \qquad (32)$$

where $K = \{(m,n) | 0 \le m, n \le d-1\} \backslash \{(0,0)\}$, from which the normalization condition $v^2 + (d^2 - 1)x^2 = 1$, and in which the unitary operations $U_{m,n}$ that generalize the Pauli matrices are defined as[15]

$$U_{m,n} = \sum_{k=0}^{d-1} e^{2\pi i(kn/d)} |k+m\rangle\langle k|. \qquad (33)$$

The link with the parameters a and b of the quantum circuit formalism is provided here by[16] $a = v - x$, $b = dx$.

D. State-dependent cloning

1. Cloning of two states of qubits

The first study of state-dependent cloning was based on a different idea, simply, to clone at best two arbitrary pure states of a qubit (Bruß, DiVincenzo, *et al.*, 1998). This is a hard problem because of the lack of symmetry and was not pursued further. One wants to perform the optical symmetric cloning of two states of qubits $|\psi_0\rangle$ and $|\psi_1\rangle$, related by $|\langle\psi_0|\psi_1\rangle| = s$. The resulting fidelity for this task is given by a quite complicated formula:

$$F = \frac{1}{2} + \frac{\sqrt{2}}{32s}(1+s)(3 - 3s + \sqrt{1 - 2s + 9s^2})$$
$$\times \sqrt{-1 + 2s + 3s^2 + (1-s)\sqrt{1 - 2s + 9s^2}}. \qquad (34)$$

For $s=0$ and $s=1$, one finds $F=1$ as it should, because the two states belong to the same orthogonal basis. The minimum is $F \approx 0.987$, much better than the value obtained with the symmetric phase-covariant cloner (see below). Oddly enough, this minimum is achieved for $s = \frac{1}{2}$, while one would have expected it to occur for states belonging to mutually unbiased bases ($s = 1/\sqrt{2}$).

2. Phase covariant 1→2 for qubits: generalities

The best-known example of state-dependent QCM are the so-called *phase-covariant QCMs*. For qubits, these are defined as the QCMs that copy at best states of the form

$$|\psi(\varphi)\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle). \qquad (35)$$

These are the states whose Bloch vector lies in the equator $(x-y)$ of the Bloch sphere; the name "phase covariant," used for the first time by Bruß, Cinchetti, *et al.* (2000), comes from the fact that the fidelity of cloning will be independent of φ. Here we restrict our attention to 1→2 asymmetric phase-covariant cloning for qubits.

The phase-covariant QCM has a remarkable application in quantum cryptography since it is used in the optimal incoherent strategy for eavesdropping on the Bennett and Brassard, 1984 (BB84) protocol, see Sec. IV.B.2. Note that the eavesdropper on BB84 wants to gather information only on four states, defined by $\varphi = 0, \pi/2, \pi, 3\pi/2$: the eigenstates of σ_x and σ_y, that is, two maximally conjugated bases. But the two problems (cloning all the equator, or cloning just two maximally conjugated bases on it) yield the same solution. In fact, consider a machine, a completely positive map T, that clones optimally the four states of BB84 in the sense that when acting on $|\pm x\rangle$ and $|\pm y\rangle$ it gives two approximate clones of the form[17]

$$T[|\pm x\rangle\langle\pm x|] = \eta|\pm x\rangle\langle\pm x| + (1 - \eta)\frac{\mathbb{1}}{2},$$

$$T[|\pm y\rangle\langle\pm y|] = \eta|\pm y\rangle\langle\pm y| + (1 - \eta)\frac{\mathbb{1}}{2}. \qquad (36)$$

Any state in the equator of the Bloch sphere can be written as

$$|\psi(\varphi)\rangle\langle\psi(\varphi)| = \frac{1}{2}(\mathbb{1} + \cos\varphi\,\sigma_x + \sin\varphi\,\sigma_y). \qquad (37)$$

Now, using the linearity of T one can see that $T[\sigma_x] = \eta\sigma_x$ and the same holds for σ_y. Since $T(\mathbb{1}) = \mathbb{1}$, one has

$$T[|\psi(\varphi)\rangle\langle\psi(\varphi)|] = \eta|\psi(\varphi)\rangle\langle\psi(\varphi)| + (1 - \eta)\frac{\mathbb{1}}{2} \qquad (38)$$

for all φ. This shows that the optimal cloning of the four states employed in the BB84 protocol is equivalent to optimally cloning the whole equator of the Bloch sphere. A similar argument applies if the z basis is also included: to clone all mutually unbiased bases in the Bloch sphere, i.e., the states $|\pm x\rangle$, $|\pm y\rangle$, and $|\pm z\rangle$, is equivalent to universal cloning.

3. Phase covariant 1→2 for qubits: explicit transformation

The task of copying at best the equator of the Bloch sphere, even in the asymmetric case, can be accomplished without ancilla (Niu and Griffiths, 1999); this is

---

[15]In $|k+m\rangle$, the sum is modulo d. Note also that, in the notation of Cerf, Bourennane, *et al.* (2002), the transformation (32) is written using $U_{m,n} \otimes \mathbb{1} \otimes U_{m,-n}$ instead of $U_{m,n} \otimes U_{m,n} \otimes \mathbb{1}$. This is indeed the same, since $U_{m,-n} = U_{m,n}^*$ and it is well known that $U \otimes \mathbb{1}|\Phi^+\rangle = \mathbb{1} \otimes U^*|\Phi^+\rangle$ holds for the maximally entangled state $|\Phi^+\rangle$.

[16]To derive this, replace $F = F_A$ given in Eq. (28) into Eq. (16) of Cerf, Bourennane, *et al.* (2002).

[17]Notice that it is assumed here that the cloning process only shrinks the Bloch vector of the initial input state.

definitely impossible for universal cloning (Durt and Du, 2004). The QCM is then just part of a two-qubit unitary transformation that reads

$$|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle,$$

$$|1\rangle|0\rangle \rightarrow \cos\eta|1\rangle|0\rangle + \sin\eta|0\rangle|1\rangle, \qquad (39)$$

with $\eta \in [0, \pi/2]$ and we have chosen $|R\rangle = |0\rangle$. Then

$$|\psi(\varphi)\rangle|0\rangle \rightarrow (1/\sqrt{2})(|0\rangle|0\rangle + \cos\eta e^{i\varphi}|1\rangle|0\rangle$$
$$+ \sin\eta e^{i\varphi}|0\rangle|1\rangle);$$

the partial states ρ_A and ρ_B are readily computed, and one finds the fidelities

$$F_A^{x-y} = \frac{1}{2}(1 + \cos\eta), \quad F_B^{x-y} = \frac{1}{2}(1 + \sin\eta). \qquad (40)$$

As desired, these fidelities are independent of φ. It is easily verified numerically that this QCM is better than the universal one for the equatorial states: one simply fixes $F_A = F_A^{x-y}$ and verifies that $F_B^{x-y} \geq F_B$, where F_B is given in Eq. (28). In particular, for the symmetric case $\eta = \pi/4$, one has $F_{A,B}^{x-y} = \frac{1}{2}(1 + 1/\sqrt{2}) \simeq 0.8535 > \frac{5}{6}$.

Niu and Griffiths introduced the two-qubit QCM in the context of eavesdropping in cryptography. It was later realized that a version with ancilla of the phase-covariant QCM (Griffiths and Niu, 1997; Bruß, Cinchetti, *et al.*, 2000), while equivalent in terms of fidelity of the clones on the equator, is generally more suited for the task of eavesdropping (Acín, Gisin, Masanes, *et al.*, 2004; Acín, Gisin, and Scarani, 2004; Durt and Du, 2004). This machine can be constructed by symmetrizing Eq. (39) with the help of an ancilla qubit as follows:

$$|0\rangle|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle|0\rangle,$$

$$|1\rangle|0\rangle|0\rangle \rightarrow (\cos\eta|1\rangle|0\rangle + \sin\eta|0\rangle|1\rangle)|0\rangle,$$

$$|0\rangle|1\rangle|1\rangle \rightarrow (\cos\eta|0\rangle|1\rangle + \sin\eta|1\rangle|0\rangle)|1\rangle,$$

$$|1\rangle|1\rangle|1\rangle \rightarrow |1\rangle|1\rangle|1\rangle \qquad (41)$$

and letting this unitary act on the input state $|\psi\rangle_A|\Phi^+\rangle_{BM}$. This reminds us of Cerf's formalism, and indeed the unitary Eq. (41) acts on $|\psi\rangle_A|\Phi^+\rangle_{BM}$ as the operator (Cerf, 2000b),

$$V = F\mathbb{1}_{ABM} + (1 - F)\sigma_z \otimes \sigma_z \otimes \mathbb{1} + \sqrt{F(1-F)}(\sigma_x \otimes \sigma_x$$
$$+ \sigma_y \otimes \sigma_y) \otimes \mathbb{1}, \qquad (42)$$

where $F = F_A^{x-y}$. Notice again how Cerf's formalism appeals to intuition: it is manifest in Eq. (42) that the x-y plane is treated differently from the z direction. For a practical illustration of the use of the phase-covariant QCM for eavesdropping in cryptography, we refer the reader to Sec. IV.B.2.

4. Other state-dependent QCMs

Most of the state-dependent QCMs that have been studied are generalizations of the phase-covariant one,

often called phase covariant as well. The idea is to clone at best some maximally conjugated bases. Specifically, the following state-dependent cloners have been studied:

- Asymmetric $1 \rightarrow 2$ phase-covariant QCM that clones at best two maximally conjugated bases in any dimension (Cerf, Bourennane, *et al.*, 2002; Fan *et al.*, 2003). For $d = 3$ (Cerf, Durt, and Gisin, 2002) and $d = 4$ (Durt and Nagler, 2003), asymmetric $1 \rightarrow 2$ QCMs have been provided that clone three or four maximally conjugated bases. For any d, the symmetric QCMs that are optimal for cloning real quantum states—that is, a basis and all the states obtained from it using $SO(d)$—have been found; optimality has been demonstrated using the no-signaling condition (Navez and Cerf, 2003).

- Symmetric $N \rightarrow M$ phase-covariant QCM for arbitrary dimension (Buscemi *et al.*, 2005), generalizing previous results (D'Ariano and Macchiavello, 2003). In particular, machines have been found that work without ancilla (economical QCM) thus generalizing the Niu-Griffiths construction given above Eq. (39)—which, however, provides also the asymmetric case.

- QCMs not related to phase-covariant cloning: Fiuràšek *et al.* (2002) have studied the cloning of two orthogonal qubits. It is known that for the task of estimating a direction $\hat{n}$, the two-qubit state $|\hat{n}, -\hat{n}\rangle$ gives a better estimate than the state $|\hat{n}, \hat{n}\rangle$ (Gisin and Popescu, 1999). For cloning, the task is to produce M clones of $|\hat{n}\rangle$ starting from either of those two-qubit states. For $M \leq 6$, better copies are obtained when starting from $|\hat{n}, -\hat{n}\rangle$.

Finally, another issue that has been discussed is the optimal cloning of entangled states (Lamoureux *et al.*, 2004).

E. Quantum cloning and state estimation

One could anticipate that there might exist a strong relation between cloning the state of a quantum system and acquiring knowledge about this state. After all, there is a strong analogy between the two processes. In both cases, the (quantum) information contained in the input is transferred into some larger system: the output clones in the case of cloning, and the measuring device in the case of state estimation. In this section, we shall see that there is more than a mere analogy. In fact, as first appreciated by Gisin and Massar (1997) and further elaborated by Bruß, Ekert, and Macchiavello (1998): (i) There is an equivalence between optimal universal $N \rightarrow \infty$ quantum cloning machines of pure states and optimal state-estimation devices taking as input N replicas of an unknown pure state. (ii) Bounds on optimal cloning can be derived from this equivalence. We are going to present these results. To simplify the presentation, we shall only consider universal cloning of qubits, but the

subsequent analysis can be generalized, without difficulty, to qudits (Keyl, 2002).

The equivalence between optimal universal symmetric cloning and state estimation can be established using the notion of a shrinking factor, already introduced for cloners. Indeed, we stressed in Sec. II.B that the quality of the optimal $N \rightarrow M$ UQCM is fully characterized by its shrinking factor $\eta(N, M)$: if the input state to clone reads $\rho_{in} = |\psi\rangle\langle\psi|$, then the individual state of each output clone reads $\eta(N, M)|\psi\rangle\langle\psi| + [1 - \eta(N, M)]\mathbb{1}/2$. A similar structure arises in the case of state estimation. Given N copies of an unknown qubit state $|\psi\rangle$, there exists an optimal positive-operator-valued measure,

$$P_\mu \geq 0, \quad \sum_\mu P_\mu = S_N, \tag{43}$$

which[18] yields the best possible estimate of ψ taking the fidelity as the figure of merit (Massar and Popescu, 1995). To each measurement outcome μ, a guess $|\psi_\mu\rangle$ of the input state is associated. During one instance of the state-estimation experiment, the outcome μ can appear with probability tr $P_\mu|\psi\rangle\langle\psi| = p_\mu(\psi)$. Thus on average, the positive-operator-valued measure (43) yields the estimate $\rho_{est}(\psi) = \sum_\mu p_\mu(\psi)|\psi_\mu\rangle\langle\psi_\mu|$. It turns out that this average estimate can be written as (Massar and Popescu, 1995)

$$\eta_*(N)|\psi\rangle\langle\psi| + [1 - \eta_*(N)]\frac{\mathbb{1}}{2}, \tag{44}$$

and the average fidelity of the state estimation is thus given by $[1 + \eta_*(N)]/2$. In turn, the performance of the positive-operator-valued measure that describes the best state estimation can also be characterized by a shrinking factor $\eta_*(N)$.

We can now state precisely what we mean when stating that there exists an equivalence between an optimal $N \rightarrow \infty$ quantum cloning machine and an optimal state-estimation device. We have

$$\eta_*(N) = \eta(N, \infty). \tag{45}$$

This relation tells us that using N qubits identically prepared in the state $|\psi\rangle$ to estimate ψ or to prepare an infinite number of clones of $|\psi\rangle$ (and then infer an estimate of ψ) are essentially equivalent procedures: the amount of information one can extract about the input preparation is the same in both cases.

To prove Eq. (45), we shall show that both $\eta_*(N) \leq \eta(N, \infty)$ and $\eta_*(N) \geq \eta(N, \infty)$ hold. The first of these inequalities is almost obvious. Consider a $N \rightarrow M$ cloning procedure in which we first perform state estimation on the N input originals, and then prepare M output clones according to the (classical) outcome we get. If the input

state is $|\psi\rangle^{\otimes N}$, then on average the state of each clone will be of the form (44), and thus characterized by a shrinking factor $\eta_*(N)$. By definition, such a cloning procedure cannot be better than using an optimal $N \rightarrow M$ quantum cloning machine. Thus $\eta_*(N) \leq \eta(N, M)$ for all M, and in particular $\eta_*(N) \leq \eta(N, \infty)$.

To prove the second inequality, $\eta_*(N) \geq \eta(N, \infty)$, we shall conversely consider a situation in which we want to achieve state estimation from N input originals with an intermediate cloning step. Let us remark that the output of an optimal $N \rightarrow M$ UQCM belongs to the symmetric subspace $\mathcal{H}_+^N$. Therefore for any input state $|\psi\rangle^{\otimes N}$, the output state can be written as a pseudomixture (Bruß, Ekert, and Macchiavello, 1998),

$$\sum_i \alpha_i(\psi)|\psi_i\rangle\langle\psi_i|^{\otimes M}, \tag{46}$$

that is, $\sum_i \alpha_i(\psi) = 1$ but the coefficients $\alpha_i(\psi)$ may be negative. Also, from $|\psi_i\rangle\langle\psi_i|^{\otimes M}$, our optimal state-estimation device yields (on average) the estimate $\eta_*(M)|\psi_i\rangle\langle\psi_i| + [1 - \eta_*(M)]\mathbb{1}/2$. Thus by linearity, our estimation procedure yields the estimate

$$\rho_{est} = \sum_i \alpha_i(\psi)\left(\eta_*(M)|\psi_i\rangle\langle\psi_i| + [1 - \eta_*(M)]\frac{\mathbb{1}}{2}\right).$$

Clearly $\sum_i \alpha_i(\psi)|\psi_i\rangle\langle\psi_i| = \eta(N, M)|\psi\rangle\langle\psi| + [1 - \eta(N, M)]\mathbb{1}/2$. By definition, this state-estimation scheme cannot outperform an optimal state estimation on the N input originals. Thus $\eta(N, M)\eta_*(M) \leq \eta_*(N)$. From the fact that in the limit of large M states estimation can be accomplished perfectly, $\lim_{M \rightarrow \infty} \eta_*(M) = 1$ (Massar and Popescu, 1995), we deduce that $\eta(N, \infty) \leq \eta_*(N)$. This concludes the proof of Eq. (45).

We are now in a position to further connect quantum cloning and state estimation. Starting from Eq. (45), we can show that a limit on the quality of $N \rightarrow M$ cloning can be derived from state estimation, modulo-1 assumption: the output state of an $N \rightarrow M$ cloning machine should be supported by the symmetric subspace $\mathcal{H}_M^+$. To establish such a limit, our first task is to prove that the shrinking factors of two cascaded cloners multiply. Let us construct an $N \rightarrow L$ cloning machine by concatenating an $N \rightarrow M$ machine with an $M \rightarrow L$ machine, and let such a cloning machine act on some input state $\psi^{\otimes N}$. Since the output state of the first cloner is assumed to be supported by $\mathcal{H}_M^+$, it admits the decomposition (46). Processing this output state into the second cloning machine yields

$$\sum_j \beta_j(\psi_i)|\psi_j\rangle\langle\psi_j|^{\otimes L}, \tag{47}$$

where $\sum_j \beta_j(\psi_i)|\psi_j\rangle\langle\psi_j| = \eta(M, L)|\psi_i\rangle\langle\psi_i| + [1 - \eta(M, L)]\mathbb{1}/2$. Thus the individual state of each clone at the output of the second cloner reads $\eta(N, M)\eta(M, L)|\psi\rangle\langle\psi| + [1 - \eta(N, M)\eta(M, L)]\mathbb{1}/2$. Of course, this cloning in stages cannot be better than directly using an optimal $N \rightarrow M$ cloner. Thus

---

[18]Note that the elements of the positive-operator-valued measure sum up to the projector S_N onto the symmetric subspace $\mathcal{H}_+^N$, and not to the identity. In fact, one can complete the measure with the operator $\mathbb{1} - S_N$, but the corresponding outcome will never be observed because the input state belongs to $\mathcal{H}_+^N$.

$$\eta(N,M)\,\eta(M,L) \leq \eta(N,L).$$

In particular, $\eta(N,M)\,\eta(M,\infty) \leq \eta(N,\infty)$. Using Eq. (45), we deduce the important relation

$$\eta(N,M) \leq \frac{\eta_*(N)}{\eta_*(M)}. \tag{48}$$

From $\eta_*(N) = N/(N+2)$ (Massar and Popescu, 1995), we find

$$\eta(N,M) \leq \frac{N}{M}\frac{M+2}{N+2}. \tag{49}$$

Comparing with Eq. (20), we see that, perhaps not so surprisingly, this last inequality is saturated by optimal UQCM.

The foregoing analysis establishes a precise connection between optimal cloning and optimal state estimation, valid when one considers all possible pure states of qubits—in fact, it extends to all pure states of qudits for any d—and looks like a miracle. One could argue that the main reason why this connection appears is that the output state of an optimal $N \rightarrow M$ cloning machine turns out to be supported by the symmetric subspace $\mathcal{H}_M^+$, the crucial ingredient in deriving Eqs. (45) and (48). But this latter fact, although established on a firm mathematical ground (Keyl and Werner, 1999), is still lacking a physical interpretation. A recent result has strengthened this connection: it has been proved (Iblisdir *et al.*, 2004; Fiuràšek, Filip, and Cerf, 2005; Iblisdir, Acín, Gisin, 2005) that the optimal asymmetric $1 \rightarrow 1+N$ UQCM, in the limit $N \rightarrow \infty$, achieves the optimal "disturbance versus gain" tradeoff for the measurement of one qubit (Banaszek, 2001).

One might wonder if the connection between state estimation and cloning holds in general. To our knowledge, the question is still open. It certainly deserves further investigation, for answering it would allow us to understand whether the neat relation between cloning and state estimation is a fundamental feature of quantum theory or a mere peculiarity of the set of all pure states of qudits.

III. CLONING OF CONTINUOUS VARIABLES

This section reviews the issue of approximate cloning for continuous-variable systems (or quantum oscillators). Our analysis will be focused on $N \rightarrow M$ Gaussian machines, cloning equally well all coherent states (Cerf and Iblisdir, 2000; Cerf, Ipe, and Rottenberg, 2000; Lindblad, 2000; Braunstein, Cerf, *et al.*, 2001; Fiuràšek, 2001). The optimality of such machines will be investigated. Upper bounds on the minimal amount of noise the clones should feature will be derived for qubits (Sec. III.A) via a connection with quantum estimation theory, using techniques similar to those we have presented in Sec. II.E. Then we shall present transformations achieving these bounds (Sec. III.B). Finally, we shall briefly discuss possible variants of our analysis (Sec. III.C).

A. Optimal cloning of Gaussian states

1. Definitions and results

The Hilbert space associated with a quantum oscillator is $\mathcal{H} \equiv L^2(\mathbf{R})$ and is infinite dimensional. Let us first consider what we can get from asking for universality in such a Hilbert space. Considering the limit for $d \rightarrow \infty$ of Eq. (21), we see that

$$\lim_{d \rightarrow \infty} F_{N \rightarrow M}(d) = \frac{N}{M}, \tag{50}$$

where N is the number of input replicas, and $M > N$ the number of clones. Moreover, this limit can also be reached by trivial cloning; see Sec. II.B.3. Can we do better than Eq. (50) by dropping the requirement of universality or taking a different perspective? After all, in some circumstances such as quantum cryptography, it is natural to consider cloners which are optimal only for a subset of states $\mathcal{S} \subset \mathcal{H}$. Also, the fidelity is not always the most interesting figure of merit to consider.

Here, we shall concentrate on the situation in which we only want to clone the set of coherent states, denoted by $\mathcal{S}$. Let $\hat{x}$ and $\hat{p}$ denote two mutually conjugated quadratures of a harmonic oscillator, $[\hat{x},\hat{p}] = i(\hbar = 1)$. The set of coherent states is the set of states that satisfy

$$\Delta\hat{x}^2 = \langle\hat{x}^2\rangle - \langle\hat{x}\rangle^2 = \Delta\hat{p}^2 = \langle\hat{p}^2\rangle - \langle\hat{p}\rangle^2 = 1/2, \tag{51}$$

and can be parametrized as

$$\mathcal{S} = \left\{ |\alpha\rangle : \alpha = \frac{1}{\sqrt{2}}(x+ip), x, p \in \mathbf{R} \right\}, \tag{52}$$

where $\langle\alpha|\hat{x}|\alpha\rangle = x$ and $\langle\alpha|\hat{p}|\alpha\rangle = p$. We shall consider $N \rightarrow M$ symmetric Gaussian cloners. These cloners are linear, trace-preserving, completely positive maps $\mathcal{C}$ outputting M clones from $N \leq M$ identical replicas of an unknown coherent state $|\alpha\rangle$. To simplify the analysis, we require that the joint state of the M clones $\mathcal{C}(|\alpha\rangle\langle\alpha|^{\otimes N})$ be supported on the symmetric subspace of $\mathcal{H}^{\otimes M}$ and be such that the partial trace over all output clones but (any) one is the bivariate Gaussian mixture:

$$\rho_1(\alpha) = \mathrm{Tr}_{M-1}\mathcal{C}(|\alpha\rangle\langle\alpha|^{\otimes N})$$

$$= \frac{1}{\pi\sigma_{N,M}^2}\int d^2\beta e^{-|\beta|^2\sigma_{N,M}^2}D(\beta)|\alpha\rangle\langle\alpha|D^\dagger(\beta), \tag{53}$$

where the integral is performed over all values of $\beta = (x+ip)/\sqrt{2}$ in the complex plane ($\hbar = 1$), and the operator $D(\beta) = \exp(\beta a^\dagger - \beta^* a)$ achieves a displacement of x in position and p in momentum, with $\hat{a} = (1/\sqrt{2})(\hat{x}+i\hat{p})$ and $\hat{a}^\dagger = (1/\sqrt{2})(\hat{x}-i\hat{p})$ denoting the annihilation and creation operators, respectively. Thus the copies yielded by a symmetric Gaussian cloner are affected by an equal Gaussian noise $\sigma_x^2 = \sigma_p^2 = \sigma_{N,M}^2$ on the conjugate variables x and p. The fidelity of the optimal $N \rightarrow M$ symmetric Gaussian cloner when a coherent state $|\alpha\rangle$ is copied can be computed using Eq. (53) and the identity $|\langle\alpha|\alpha'\rangle|^2 = \exp(-|\alpha-\alpha'|^2)$. One finds

$$f_{N,M} = \langle \alpha | \rho_1 | \alpha \rangle = \frac{1}{1 + \bar{\sigma}_{N,M}^2}. \tag{54}$$

We shall prove in the following paragraphs that a lower bound on the noise variance $\sigma_{N,M}^2$ is given by

$$\bar{\sigma}_{N,M}^2 = \frac{1}{N} - \frac{1}{M}, \tag{55}$$

implying in turn that the optimal cloning fidelity for Gaussian cloning of coherent states is bounded by

$$f_{N,M} = \frac{MN}{MN + M - N}. \tag{56}$$

Thus all coherent states are copied with the same fidelity—recall that this property does not extend to all states of $\mathcal{H}$. One can also check that Eqs. (55) and (56) fulfill the natural requirement that the cloning fidelity increases with the number of input replicas. At the limit $N \to \infty$, we have $f_{N,M} \to 1$ for all M, that is, classical copying is allowed. Finally, for $M \to \infty$, that is, for an optimal measurement, we get $f_{N,M} \to N/(N+1)$.

It is worth noting that the optimal cloning of squeezed states requires a variant of these symmetric Gaussian cloners. For instance, the best symmetric cloner for the family of quadrature squeezed states with squeezing parameter r must have the form of Eq. (53), but using the definition $\beta = (x/\kappa + i\kappa p)/\sqrt{2}$ with $\kappa = \exp(r)$. These cloners naturally generalize the symmetric Gaussian cloners and give the same cloning fidelity, Eq. (56), for those squeezed states.

2. Proof of the bounds for $1 \to 2$ cloning

Let us first prove Eq. (55) in the simplest case, $(N,M) = (1,2)$. This case is interesting to single out because it demonstrates the link between quantum cloning and the problem of simultaneously measuring a pair of conjugate observables on a single quantum system. Our starting point is thus the relation derived by Arthurs and Kelly (1965), which constrains any attempt to measure $\hat{x}$ and $\hat{p}$ simultaneously on a quantum system:

$$\sigma_x^2(1)\sigma_p^2(1) \geq 1, \tag{57}$$

where $\sigma_x^2(1)$ and $\sigma_p^2(1)$ denote the variance of the measured values of $\hat{x}$ and $\hat{p}$, respectively, when simultaneously measuring $\hat{x}$ and $\hat{p}$ on some quantum state ρ.

It is crucial to clearly distinguish between the Arthurs and Kelly relation (57), and the Heisenberg uncertainty relation:[19]

_____

[19]In this paper, we adopt the usual notation ΔA for the intrinsic variance of the observable A, and use δA for other variances in Eq. (59). Obviously, $\delta A \geq \Delta A$; this is what motivates the use of the opposite convention in the papers on cloning that we are reviewing here.

$$\Delta \hat{x}^2 \Delta \hat{p}^2 \geq 1/4, \tag{58}$$

where $\Delta \hat{x}^2$ or $\Delta \hat{p}^2$ are the intrinsic variance of the observable $\hat{x}$ or $\hat{p}$, respectively, for any quantum state ρ. The Heisenberg relation is valid independent of any measurement performed on the state ρ; in particular, it holds even if we have a perfect knowledge of the state ρ. In contrast, the tradeoff between the information about $\hat{x}$ and the information about $\hat{p}$ that one can acquire during a single measurement on the state ρ is quantified by the Arthurs-Kelly relation (57). In particular, the best possible simultaneous measurement of $\hat{x}$ and $\hat{p}$ with a same precision satisfies $\sigma_x^2(1) = \sigma_p^2(1) = 1$. Compared with the intrinsic noise of a coherent state $\Delta \hat{x}^2 = \Delta \hat{p}^2 = 1/2$, we see that the joint measurement of x and p effects an additional noise of minimum variance $1/2$.

Now, let a coherent state $|\alpha\rangle$ be processed by a $1 \to 2$ symmetric Gaussian cloner, and let $\hat{x}$ be measured at one output of the cloner while $\hat{p}$ is measured at the other output. This is a way of simultaneously measuring x and p, and as such it must obey the Arthurs-Kelly relation (57). Consequently, the intrinsic variances of the observables $\hat{x}$ and $\hat{p}$ in the state $\rho_1(\alpha)$, denoted, respectively, as $\delta\hat{x}$ and $\delta\hat{p}$, must fulfill

$$\delta\hat{x}^2 \delta\hat{p}^2 \geq 1. \tag{59}$$

Using Eq. (53), we get

$$(\Delta \hat{x}^2 + \sigma_{1,2}^2)(\Delta \hat{p}^2 + \sigma_{1,2}^2) \geq 1. \tag{60}$$

Now using Eq. (58), we conclude that the noise variance is constrained by

$$\sigma_{1,2}^2 \geq \bar{\sigma}_{1,2}^2 = 1/2, \tag{61}$$

thus verifying Eq. (55) in the case $(N,M) = (1,2)$.

A similar argument can be used to characterize the output copies of an asymmetric quantum cloning machine, in which the qualities of the clones are not identical and in which one might desire that the added noise due to cloning is different for both quadratures. Using Eq. (57), one easily shows that the following relations hold:

$$\sigma_{x,1}^2 \sigma_{p,2}^2 \geq 1/4, \tag{62}$$

$$\sigma_{p,1}^2 \sigma_{x,2}^2 \geq 1/4, \tag{63}$$

where $\sigma_{x,1}^2$ or $\sigma_{p,1}^2$ refers to the added x-quadrature or p-quadrature added noise for the first clone, and where $\sigma_{x,2}^2$ and $\sigma_{p,2}^2$ are defined likewise. These cloning uncertainty relations are useful when assessing the security of some continuous-variables quantum cryptographic schemes (Cerf, Lévy, and Van Assche, 2001).

3. Proof of the bounds for $N \to M$ cloning

Let us now prove Eq. (55) in the general case. Our proof is connected to quantum state-estimation theory similar to what was done for quantum bits in Sec. II.E. The key idea is that cloning should not be a way of circumventing the noise limitation encountered in any

measuring process. More specifically, our bound relies, as in the discrete case, on the fact that cascading an $N \rightarrow M$ cloner with an $M \rightarrow L$ cloner results in a $N \rightarrow L$ cloner which cannot be better that the optimal $N \rightarrow L$ cloner. We make use of the property that cascading two symmetric Gaussian cloners results in a single symmetric Gaussian cloner whose variance is simply the sum of the variances of the two component cloners (Cerf and Iblisdir, 2000). Hence the variance $\bar{\sigma}_{N,L}^2$ of the optimal $N \rightarrow L$ symmetric Gaussian cloner must satisfy

$$\bar{\sigma}_{N,L}^2 \leq \sigma_{N,M}^2 + \sigma_{M,L}^2. \tag{64}$$

In particular, if the $M \rightarrow L$ cloner is itself optimal and $L \rightarrow \infty$,

$$\bar{\sigma}_{N,\infty}^2 \leq \sigma_{N,M}^2 + \bar{\sigma}_{M,\infty}^2. \tag{65}$$

As for the discrete case, in the limit $M \rightarrow \infty$, estimators and quantum cloning machines tend to become essentially identical devices. Thus Eq. (65) means that cloning the N replicas of a system before measuring the M resulting clones does not provide a means to enhance the accuracy of a direct measurement of the N replicas.

Let us now estimate $\bar{\sigma}_{N,\infty}^2$, that is, the variance of an optimal joint measurement of $\hat{x}$ and $\hat{p}$ on N replicas of a system. From quantum estimation theory (Holevo, 1982), we know that the variance of the measured values of $\hat{x}$ and $\hat{p}$ on a single system, respectively, $\sigma_x^2(1)$ and $\sigma_p^2(1)$, are constrained by

$$g_x \sigma_x^2(1) + g_p \sigma_p^2(1) \geq g_x \Delta \hat{x}^2 + g_p \Delta \hat{p}^2 + \sqrt{g_x g_p} \tag{66}$$

for all values of the constants $g_x, g_p > 0$. Note that for each value of g_x and g_p, a specific positive-operator-valued measure based on a resolution of identity in terms of squeezed states, whose squeezing Δ is a function of g_x and g_p, achieves this bound (Holevo, 1982). Squeezed states satisfy $\Delta \hat{x}^2 = \kappa^2/2$ and $\Delta \hat{p}^2 = 1/2\kappa^2$. Moreover, when a measurement is performed on N independent and identical systems, the right-hand side of Eq. (66) is reduced by a factor N^{-1}, as in classical statistics (Helstrom, 1976). So, applying N times the optimal single-system positive-operator-valued measure is the best joint measurement when N replicas are available since it yields $\sigma_x^2(N) = N^{-1}\sigma_x^2(1)$ and $\sigma_p^2(N) = N^{-1}\sigma_p^2(1)$. Hence using Eq. (66) for a coherent state ($\Delta \hat{x}^2 = \Delta \hat{p}^2 = 1/2$) and requiring $\sigma_x^2(N) = \sigma_p^2(N)$, the tightest bound is obtained for $g_x = g_p$. It yields

$$\bar{\sigma}_{N,\infty}^2 = 1/N,$$

which, combined with Eq. (65), gives the minimum noise variance induced by cloning, Eq. (55).

B. Implementation of Gaussian QCMs

Now that we have derived upper bounds on optimal cloning, we shall show that these bounds are achievable and exhibit explicit optimal cloning transformations. Remarkably, these transformations have a fairly simple implementation when the quantum oscillator corre-

sponds to a light mode: it requires only a phase-insensitive linear amplifier and a network of beam splitters.[20] We shall also discuss the link between the issue of optimal quantum cloning and that of optimal amplification of quantum states.

1. Definitions and requirements

Let us first state what we expect from a quantum cloning machine. Let $|\Psi\rangle = |\alpha\rangle^{\otimes N} \otimes |0\rangle^{\otimes M-N} \otimes |0\rangle_z$ denote the initial joint state of the N input modes to be cloned (all prepared in the coherent state $|\alpha\rangle$), the additional $M - N$ blank modes, and an ancillary mode z. The blank modes and the ancilla are assumed to be initially in the vacuum state $|0\rangle$. Let $\{\hat{x}_k, \hat{p}_k\}$ denote the pair of quadrature operators associated with each mode k involved by the cloning transformation,[21] $k = 0, \ldots, N-1$ refers to the N original input modes, and $k = N, \ldots, M-1$ refers to the additional blank modes. Cloning can be thought of as some unitary transformation,

$$U: \mathcal{H}^{\otimes M+1} \rightarrow \mathcal{H}^{\otimes M+1}: |\Psi\rangle \rightarrow U|\Psi\rangle = |\Psi''\rangle.$$

Alternatively, in the Heisenberg picture, this transformation can be described by a canonical transformation of the operators $\{x_k, p_k\}$:

$$x_k'' = U^\dagger x_k U, \quad p_k'' = U^\dagger p_k U. \tag{67}$$

We work in the Heisenberg picture because cloning turns out to be much simpler to study from that point of view. We now impose several requirements on the transformation Eq. (67) that translate the expected properties for an optimal cloning transformation.

First, we require the M output modes quadratures have the same mean values as the the input mode:

$$\langle x_k'' \rangle = \langle \psi | x_0 | \psi \rangle, \quad k = 0, \ldots, M-1, \tag{68}$$

$$\langle p_k'' \rangle = \langle \psi | p_0 | \psi \rangle, \quad k = 0, \ldots, M-1. \tag{69}$$

This means that the state of the clones is centered on the original coherent state. Our second requirement is covariance with respect to rotation in phase space. Coherent states have the property that quadrature variances are left invariant by complex rotations in phase space. That is, for any mode k involved in the cloning process and for any operator $v_k = cx_k + dp_k$ (where c, d are complex numbers satisfying $|c|^2 + |d|^2 = 1$), we have

$$\Delta v_k^2 = \langle v_k^2 \rangle - \langle v_k \rangle^2 = \text{vacuum fluct.} = 1/2. \tag{70}$$

We impose that this property be conserved through the cloning process. Taking optimality into account, Eq. (55), rotation covariance yields

---

[20]Note that another implementation, with the same performances, involving a circuit of controlled-NOT gates has also been proposed (Cerf, Ipe, and Rottenberg, 2000).

[21]In what follows, we sometimes omit the hats on operators when the context is clear.

$$\sigma_{v''_k}^2 = \left(\frac{1}{2} + \frac{1}{N} - \frac{1}{M}\right), \tag{71}$$

where $v''_k = cx''_k + dp''_k$.

The third requirement is, of course, the unitarity of the transformation. In the Heisenberg picture, unitarity translates into demanding that the commutation rules be conserved through the evolution (Caves, 1982)

$$[x''_j, x''_k] = [p''_j, p''_k] = 0, \quad [x''_j, p''_k] = i\delta_{jk}. \tag{72}$$

2. Optimal Gaussian 1→2 QCM

Let us first focus on duplication ($N=1$, $M=2$). A simple transformation meeting the three conditions mentioned above is given by

$$x''_0 = x_0 + \frac{x_1}{\sqrt{2}} + \frac{x_z}{\sqrt{2}}, \quad p''_0 = p_0 + \frac{p_1}{\sqrt{2}} - \frac{p_z}{\sqrt{2}},$$

$$x''_1 = x_0 - \frac{x_1}{\sqrt{2}} + \frac{x_z}{\sqrt{2}}, \quad p''_1 = p_0 - \frac{p_1}{\sqrt{2}} - \frac{p_z}{\sqrt{2}},$$

$$x'_z = x_0 + \sqrt{2}x_z, \quad p'_z = -p_0 + \sqrt{2}p_z. \tag{73}$$

This transformation clearly conserves the commutation rules and yields the expected mean values ($\langle x_0\rangle, \langle p_0\rangle$) for the two clones (modes $0''$ and $1''$). One can also check that the quadrature variances of both clones are equal to 1, in accordance with Eq. (71). This transformation actually coincides with the cloning machine introduced by Cerf, Ipe, and Rottenberg (2000). Interestingly, we note here that the state in which the ancilla z is left after cloning is centered on ($x_0, -p_0$), that is, the *phase-conjugated* state $|\bar{a}\rangle$. This means that in analogy with the universal qubit cloning machine (Bužek and Hillery, 1996), the continuous-variable cloner generates an anticlone (or time-reversed state) together with the two clones.

Now, let us show how this duplicator can be implemented in practice. Equation (73) can be interpreted as a two-step transformation:

$$a'_0 = \sqrt{2}a_0 + a^\dagger_z, \quad a'_z = a^\dagger_0 + \sqrt{2}a_z,$$

$$a''_0 = \frac{1}{\sqrt{2}}(a'_0 + a_1), \quad a''_1 = \frac{1}{\sqrt{2}}(a'_0 - a_1). \tag{74}$$

As shown in Fig. 3, the interpretation of this transformation is straightforward: the first step (which transforms a_0 and a_z into a'_0 and a'_z) is a phase-insensitive amplifier whose (power) gain G is equal to 2, while the second step (which transforms a'_0 and a_1 into a''_0 and a''_1) is a phase-free 50:50 beam splitter. Clearly, rotational covariance is guaranteed here by the use of a phase-insensitive amplifier. As discussed by Caves (1982), the ancilla z involved in linear amplification can always be chosen such that $\langle a_z\rangle = 0$, so that we have $\langle a''_0\rangle = \langle a''_1\rangle = \langle a_0\rangle$ as required. Finally, the optimality of our cloner can be confirmed from known results on linear amplifi-
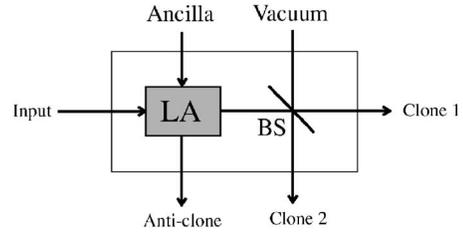

FIG. 3. Implementation of the optimal Gaussian 1→2 QCM for light modes. LA stands for linear amplifier and BS represents a balanced beam splitter.

ers. For an amplifier of gain G, the quadrature variances of a_z are bounded by (Caves, 1982)

$$\sigma_{a_z}^2 \geq (G-1)/2. \tag{75}$$

Hence the optimal amplifier of gain $G=2$ yields $\sigma_{a_z}^2 = 1/2$, so that our cloning transformation is optimal according to Eq. (55).

3. Optimal Gaussian N→M QCM

Let us now derive an $N \to M$ cloning transformation. To achieve cloning, energy has to be brought to each of the $M-N$ blank modes in order to drive them from the vacuum state to a state which has the desired mean value. We shall again perform this operation with the help of a linear amplifier. From Eq. (75), we see that the cloning-induced noise essentially originates from the amplification process and grows with the gain of the amplifier. So, we shall preferably amplify as little as possible. Loosely speaking, the cloning procedure should then be as follows: (i) concentrate the N input modes into one single mode, which is then amplified; (ii) symmetrically distribute the output of this amplifier amongst the M output modes. A convenient way to achieve these concentration and distribution processes is provided by the discrete Fourier transform. Cloning is then achieved by the following three-step procedure (see Fig. 4). First step: a discrete Fourier transform (acting on N modes),

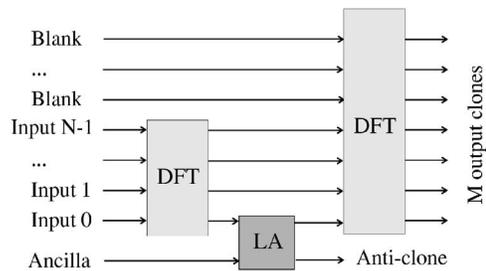$$a'_k = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \exp(ikl2\pi/N)a_l, \tag{76}$$

FIG. 4. Implementation of the optimal Gaussian $N \to M$ QCM for light modes. LA stands for linear amplifier and DFT for discrete Fourier transform.

with $k=0,\ldots,N-1$. This operation concentrates the energy of the N input modes into one single mode (renamed a_0) and leaves the remaining $N-1$ modes $(a_1',\ldots,a_{N-1}')$ in the vacuum state. Second step: the mode a_0 is amplified with a linear amplifier of gain $G=M/N$. This results in

$$a_0' = \sqrt{\frac{M}{N}}a_0 + \sqrt{\frac{M}{N}-1}a_z^\dagger,$$

$$a_z' = \sqrt{\frac{M}{N}-1}a_0^\dagger + \sqrt{\frac{M}{N}}a_z. \tag{77}$$

Third step: amplitude distribution by performing a discrete Fourier transform (acting on M modes) between the mode a_0' and $M-1$ modes in the vacuum state:

$$a_k'' = \frac{1}{\sqrt{M}}\sum_{l=0}^{M-1} \exp(ikl2\pi/M)a_l', \tag{78}$$

with $k=0,\ldots,M-1$, and $a_i'=a_i$ for $i=N,\ldots,M-1$. The discrete Fourier transform now distributes the energy contained in the output of the amplifier amongst the M output clones.

It is readily checked that this procedure meets our three requirements and is optimal provided that the amplifier is optimal, that is, $\sigma_{a_z}^2=(M/N-1)/2$. The quadrature variances of the M output modes coincide with Eq. (55). As in the case of duplication, the quality of cloning decreases as $\sigma_{a_z}^2$ increases, that is, amplifying coherent states, or cloning them with the same error for each clone, are two equivalent problems. For $1\to2$ cloning, we have seen that the final amplitude distribution among the output clones is achieved with a single beam splitter. In fact, any unitary matrix such as the discrete Fourier transform used here can be realized with a sequence of beam splitters and phase shifters (Reck *et al.*, 1994). This means that the $N\to M$ cloning transformation can be implemented using only passive elements except for a single linear amplifier. An explicit sequence of beam splitters achieving a discrete Fourier transform on M modes is given by Braunstein, Cerf, *et al.* (2001).

Finally, we note that if squeezed states are put in rather than coherent states, the transformations and circuits presented here maintain optimum cloning fidelities, provided all auxiliary vacuum modes (the blank modes and the ancillary mode z) are correspondingly squeezed. This means, in particular, that the amplifier mode z needs to be controlled, which requires a device different from a simple phase-insensitive amplifier, namely, a two-mode parametric amplifier. One can say that the cloning machine capable of optimum cloning of all squeezed states with fixed and known squeezing then operates in a nonuniversal fashion with respect to all possible squeezed states at the input (Cerf and Iblisdir, 2000).

C. Other continuous-variable QCMs

We conclude this section by summarizing some interesting developments in continuous-variable cloning.

Other figures of merit. The universal Gaussian machines presented in Secs. III.A and III.B have been derived requiring that the noise of the output clones be minimum, but one could have used other figures of merit to judge the quality of the output clones. Then, would we have obtained different solutions? Another related issue is: do we get better cloners if the Gaussian assumption is relaxed? Cerf, Krüger, *et al.* (2004) have proved that if one chooses the global fidelity[22] as figure of merit, then the universal Gaussian cloner turns out to be optimal too. But surprisingly, the Gaussian assumption is too restrictive if the goal is to optimize the single-clone fidelity. For instance, for $1\to2$ cloning there exists a non-Gaussian operation whose output clones have a fidelity of 0.6826 with the original for all coherent states, improving on the universal Gaussian machine, which achieves a fidelity of $2/3\approx0.6666$; see Eq. (56).

Optimal cloning for finite distributions of coherent states. In devising optimal cloning machines, we require that all coherent states be cloned with an equal quality. In other words, we devised cloning machines which are optimal for a distribution of coherent states in phase space which is flat. But for practical reasons, it is interesting to consider situations where the coherent states to be cloned are produced according to a *finite* distribution over phase space—in other words, to drop the requirement of universality over all coherent states. In particular, the case has been studied (Grosshans, 2002; Cochrane *et al.*, 2004) in which the coherent states to be cloned are produced according to a Gaussian distribution

$$P(\alpha) = \frac{1}{2\pi\Sigma^2}e^{-|\alpha|^2/2\Sigma^2}. \tag{79}$$

It is easily seen that in this setting the cloning procedures we have considered so far do not produce clones with optimal fidelities. For instance, if $P(\alpha)$ is a sufficiently peaked distribution, then a very trivial cloning machine, from which the first output clone is the unaffected original and the second clone is a mode prepared in the vacuum state, already achieves better fidelities than the universal Gaussian cloner. Actually, one can prove that for all values of Σ, there is a cloning machine achieving a single-clone fidelity of

---

[22]Global fidelity was introduced in Sec. II.B.1 for the case of discrete variables. Recall that in that case, the optimization of the global and of the single-copy fidelity leads to the same optimal UQCM.

$$F = \begin{cases} \dfrac{4\Sigma^2 + 2}{6\Sigma^2 + 1}, & \Sigma^2 \geqslant \dfrac{1}{2} + \dfrac{1}{\sqrt{2}}, \\[4mm] \dfrac{1}{(3 - 2\sqrt{2})\Sigma^2 + 1}, & \Sigma^2 \leqslant \dfrac{1}{2} + \dfrac{1}{\sqrt{2}}. \end{cases} \quad (80)$$

Interestingly, such a cloning machine can be achieved using the setup shown in Fig. 3, but where the gain is adapted to the distribution of coherent states:

$$G = \frac{8\Sigma^4}{(2\Sigma^2 + 1)^2}.$$

IV. APPLICATION OF QUANTUM CLONING TO ATTACKS IN QUANTUM CRYPTOGRAPHY

A. Generalities

As stated in the Introduction, the relationship between the no-cloning theorem and the security of quantum cryptography was already pointed out in the first protocol (Bennett and Brassard, 1984). Let us briefly sketch here the common structure behind any protocol; we refer the reader to the review by Gisin *et al.* (2002) for a more thorough view on quantum cryptography. A sender, Alice, encodes some classical information on a quantum state chosen among a set of nonorthogonal alternatives $\{|\psi_i\rangle_A\}$. The so-prepared particle goes to a receiver, Bob, who randomly chooses a measurement from a preestablished set of measurements. When more than two states are used for the encoding, the exchange of the particles is usually followed by a sifting phase, in which Alice reveals something of the encoding (e.g., the basis to which each state belongs) allowing Bob to know if he has done a good measurement. After this process, Alice and Bob share a list of classically correlated symbols. Using well-established techniques from classical information theory, this list can be transformed into a secret key,[23] which is later consumed for sending private information by means of the one-time pad. So quantum cryptography is actually quantum key distribution.

Although everything that takes place in Alice and Bob's sites is secure,[24] this is no longer the case for the channel connecting them. This means that an eavesdropper, usually called Eve, can freely interact with the states while they propagate and try to extract information. Eve is allowed to perform the most general action consistent

---

[23]Actually, when discrete-level quantum states are used, one normally tailors the protocol in such a way that in the absence of an eavesdropper and of errors the correlation between Alice and Bob is perfect without any classical processing, i.e., it already constitutes a perfect secret key. However, this can no longer be done for protocols using continuous variables.

[24]This is a very reasonable assumption for any cryptographic scenario. Indeed, it seems difficult to design a secure protocol if one cannot exclude the possibility that Eve has access to Alice's preparation of quantum states or Bob's measurement results.

with quantum mechanics. In particular, then, she is limited by the no-cloning theorem: contrary to what happens for classical information that can be amplified at will, when Eve obtains information on the state sent by Alice, the state used for the encoding is perturbed and she introduces errors. The larger the information obtained by Eve is, the more the state is perturbed, and consequently the larger is the error rate in the correlations between Alice and Bob.

In fact, quantum key distribution is secure because one of the following cases happens: either the error rate observed by Alice and Bob is lower than a critical value D_c, in which case a secret key can be extracted using techniques of classical information theory; or the error rate is larger than D_c, in which case Alice and Bob throw their data away and never use them to encode any message. In other words, the eavesdropper can either lose the game or prevent any communication, but will never gain any information.

All this reasoning is nice, provided that Alice and Bob are able to find the value of the threshold D_c for the protocol that they want to use. That is why it is important to establish quantitative tradeoffs between the information acquired by Eve and the error rate. For this calculation, one should assume that Eve has applied the most powerful strategy consistent with quantum mechanics. Therefore the problem of estimating Eve's information for a given disturbance is equivalent to finding her optimal eavesdropping attack on the protocol that is used. This is a very difficult problem and, to date, the complete solution is not known for any of the existing protocols. Nevertheless, the problem can be solved if Eve is restricted to the so-called incoherent attacks. In what follows, we mainly focus on these attacks that involve QCMs. The last paragraph of this subsection, however, will be devoted to the possibility of more general quantitative links between quantum key distribution and cloning.

B. Incoherent attacks and QCMs

1. Generalities

An *incoherent attack* is defined by two conditions: (i) Eve interacts individually and in the same way with the states traveling from Alice to Bob; (ii) she measures the quantum systems she has kept after the possible sifting phase[25] but before any reconciliation process has started. In other words, the hypothesis is that after the sifting phase, Alice, Bob, and Eve share a list of classical random variables, identically distributed according to a probability law $P(A, B, E)$. Under this hypothesis, the fraction of secret bits R that can be extracted by Alice and Bob using reconciliation protocols with one-way communication satisfies the bound of Csiszár and Körner (1978),

---

[25]Therefore individual attacks require a quantum memory.

$$R \geqslant I(A:B) - \min\{I(A:E), I(B:E)\}, \tag{81}$$

where $I(X:Y) = H(X) + H(Y) - H(XY)$ is the mutual information between two parties.[26] This result formalizes the intuition according to which, if Eve has as much information as Alice and Bob, it is impossible to extract a secret key. Therefore Eve's optimal individual attack is the one that, for a given error rate D—that is, for a given value of $I(A:B) = 1 - H(D)$—maximizes $I(A:E)$ and $I(B:E)$. This defines the figure of merit for eavesdropping with incoherent attacks.

If we go back to the physical implementation of such attacks, we see that Eve is going to transfer some information about the original state onto the state of a particle that she keeps and measures later. Under this perspective, it seems rather natural to guess that the interaction defining the best individual attack is the $1 \rightarrow 2$ asymmetric QCM that clones in an optimal way all possible preparations by Alice, i.e., the set of states $\{|\psi_i\rangle_A\}$; although there is no *a priori* link between the optimality of cloning based on the single-copy fidelity (7) and the optimality of eavesdropping defined just above. This intuition was proved to hold in the following cases:

- BB84 protocol (Bennett and Brassard, 1984): Alice chooses her preparation among the four states $|\pm x\rangle$ and $|\pm y\rangle$ of a qubit, which belong to the equator of the Bloch sphere. One can see that Eve's optimal individual attack uses the asymmetric phase-covariant cloning machine (see Sec. II.D; Fuchs *et al.*, 1997). The security condition assumes an easy form: a secret key can no longer be extracted as soon as $F_{\text{Bob}} = F_{\text{Eve}}$, that is, the critical value for the error rate is $D_c^{\text{incoh}} = 1 - F_{\text{Eve}}$. Using Eq. (40), $D_c^{\text{incoh}} \simeq 14.6\%$. We shall come back to this example in full detail in the next subsection.

- Six-state protocol (Bruß, 1998; Bechmann-Pasquinucci and Gisin, 1999): Alice's preparation is the same as in BB84 plus the states at the poles of the sphere, $|\pm z\rangle$. Again, the interaction defining the optimal attack is the universal asymmetric QCM (see Sec. II.C). Indeed, it turns out that to optimally clone these six states is equivalent to cloning all the states in the Bloch sphere. One can see that the critical disturbance such that R from Eq. (81) goes to zero is

---

[26]The function H is the usual Shannon entropy. While we were finishing this review, the idea of preprocessing was introduced in quantum cryptography (Kraus *et al.*, 2004; Renner *et al.*, 2005). Quite astonishingly, these authors found that security bounds can be improved by letting Alice randomly flip some of her bits. The reason is that this procedure decreases Alice's correlations with Eve much more than her correlations with Bob. This result implies that, apart from the six-state protocol in which the attacks depend on a single parameter, which is the quantum bit error rate, the truly optimal incoherent attacks may not be those which have been presented in the previous literature. Since this is an open research problem, we have not taken these new considerations into account in the main text.

$D_c^{\text{incoh}} \simeq 15.7\%$. Note that in the six-state protocol Eve's attack is more limited than in BB84 because she has to (imperfectly) clone all the states in the sphere. This intuitively explains why Alice and Bob can tolerate a larger disturbance.

- Continuous-variable protocols, using both squeezed and coherent states (Cerf, Lévy, and Van Assche, 2001; Grosshans and Grangier, 2002): there also exists a link between security and the no-cloning theorem. Indeed, the well-known security limit of 3 dB, common to all these protocols for the case of direct reconciliation, can be understood as the point where Eve's clone becomes equal to Bob's.

The connection between cloning machines and eavesdropping attacks has also been exploited for other protocols and scenarios. For instance, asymmetric $2 \rightarrow 2+1$ cloning machines have been discussed for eavesdropping on practical implementations of quantum key distribution with no claim of optimality (Acín, Gisin, Masanes, *et al.*, 2004; Curty and Lütkenhaus, 2004; Niederberger *et al.*, 2005). Going to higher-dimensional systems, the relation between cloning machines and incoherent eavesdropping strategies has been analyzed (Bruß and Macchiavello, 2002; Cerf, Bourennane, *et al.*, 2002). Here, optimality is conjectured but not proved [see in this context Kaszlikowski *et al.* (2004)]. In the case of the protocol invented by Scarani *et al.* (2004) (called SARG04), the optimal incoherent eavesdropping is not known, but the best attack which has been found by Branciard *et al.* (2005) does not make use of the corresponding optimal cloner (which would be the phase-covariant one, as for BB84).

2. Optimal incoherent attack on the BB84 protocol

As a completely worked-out example, we describe the optimal incoherent attack on the BB84 protocol. Suppose that the BB84 protocol is run with the bases of the eigenstates of σ_x and σ_y. It is then no surprise that the optimal incoherent attack is obtained when Eve makes a copy of each qubit using the phase-covariant cloner described in Sec. II.D (Fuchs *et al.*, 1997). However, for eavesdropping in cryptography there is a difference between the two implementations that we presented, the one (39) without ancilla and the one (41) with an ancillary qubit (Acín, Gisin, Masanes, *et al.*, 2004; Acín, Gisin, and Scarani, 2004; Durt and Du, 2004). Intuitively, the reason is that some kind of information is stored in the ancilla as well, and Eve has access to it. Here we show in detail what happens.

Let us study the cloner without ancilla first. For simplicity, we focus on an item where Alice has sent $|+x\rangle$, and suppose that Bob has measured σ_x so that the item will be kept after the bases reconciliation. Using Eq. (39), the flying qubit becomes entangled to Eve's qubit according to

$$|\Gamma\rangle_{BE} = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + \cos\eta|1\rangle|0\rangle + \sin\eta|0\rangle|1\rangle). \qquad (82)$$

Bob's qubit is thus in the state $\rho_B = \frac{1}{2}(1 + \sin^2\eta\sigma_z + \cos\eta\sigma_x)$, so that the measurement of σ_x gave him the correct outcome with the probability $F_{AB} = \langle+x|\rho_B|+x\rangle = \frac{1}{2}(1 + \cos\eta)$, which is indeed the fidelity of his clone as expected. The Alice-Bob mutual information is therefore $I(A:B) = 1 - H(F_{AB})$. Similarly, Eve's qubit is in the state $\rho_E = \frac{1}{2}(1 + \cos^2\eta\sigma_z + \sin\eta\sigma_x)$, from which she will guess the state sent by Alice correctly with probability $F_{AE} = \frac{1}{2}(1 + \sin\eta)$. The Alice-Eve mutual information is therefore $I(A:E) = 1 - H(F_{AE})$. Obviously, $I(A:B) = I(A:E)$ for $\eta = \pi/4$, that is, for an error rate $D_{AB} = 1 - F_{AB} \simeq 0.1464$. However, the security criterion for one-way communication (81) says that $I(A:B)$ must be larger than the minimum between $I(A:E)$ and $I(B:E)$, so we need to compute the Bob-Eve mutual information as well. From the state (82), we can compute the probability that Eve's symbol is equal to Bob's, knowing that both measure σ_x: $P_{BE} = |\langle+x,+x|\Psi_{BE}\rangle|^2 + |\langle-x,-x|\Psi_{BE}\rangle|^2 = \frac{1}{2}(1 + \frac{1}{2}\sin 2\eta)$, from which the mutual information $I(B:E) = 1 - H(P_{BE})$. It can be verified that $I(B:E) < I(A:B)$ whenever $D_{AB} < \frac{1}{2}$; from Eq. (81), Alice and Bob could always extract a key, as long as their correlation is not zero.[27] This is too good to be true; and, indeed, the use of the machine with an ancillary qubit yields a more reasonable scenario.

To study the machine with an ancilla, we suppose that Alice and Bob use the same basis, but we consider both eigenstates of σ_x. Using Eq. (41), the flying qubit $|\pm x\rangle_A$ becomes entangled to Eve's two qubits according to

$$|\Gamma^\pm\rangle_{BE_1E_2} = \frac{1}{2}(|000\rangle + c|011\rangle$$
$$+ s|101\rangle \pm c|100\rangle \pm s|010\rangle \pm |111\rangle), \qquad (83)$$

where $c = \cos\eta$ and $s = \sin\eta$. Bob's qubit is in the state $\rho_B = \frac{1}{2}(1 \pm \cos\eta\sigma_x)$, which gives the same fidelity as above as expected. The easiest way to see what Eve can do with her two qubits consists of writing $|\Gamma^\pm\rangle_{BE_1E_2}$ using the basis $|\pm x\rangle$ for B and the Bell basis $|\Phi^\pm\rangle = (1/\sqrt{2})(|00\rangle \pm |11\rangle)$, $|\Psi^\pm\rangle = (1/\sqrt{2})(|01\rangle \pm |10\rangle)$ for Eve's qubits, then in applying on Eve's qubits the unitary transformation $|\Phi^+\rangle \to |00\rangle$, $|\Psi^+\rangle \to |10\rangle$, $|\Phi^-\rangle \to |11\rangle$, $|\Psi^-\rangle \to |01\rangle$. After this transformation, the states read

$$|\tilde{\Gamma}^\pm\rangle = \sqrt{F}|\pm x\rangle|\chi_\pm\rangle|0\rangle \mp \sqrt{D}|\mp x\rangle|\chi_\mp\rangle|1\rangle, \qquad (84)$$

where $F = (1+c)/2$ is Bob's qubit fidelity, $D = 1 - F$ the disturbance, and $|\chi_\pm\rangle = \sqrt{F}|0\rangle \pm \sqrt{D}|1\rangle$. Now Eve's strategy is clear. First, she measures σ_z on qubit E_2: if she finds $|0\rangle$ or $|1\rangle$, she knows that Bob's bit is identical or oppo-

---

[27]We note here that this analysis was done first in the Introduction of the article by Scarani and Gisin (2001), but an unfortunate mistake in the computation of P_{BE}, Eq. (5), prevented them from reaching the correct conclusion.

site, respectively, to Alice's bit. This information is deterministic and implies that Eve has as much information on Bob's bit as she has on Alice's bit: $I(A:E) = I(B:E)$. This solves the main problem of the machine without ancilla. For completeness, let us conclude the calculation by computing $I(A:E)$. To guess Alice's bit, Eve must distinguish between the two nonorthogonal states $|\chi_\pm\rangle$ of qubit E_1, with *a priori* probabilities $p_+ = p_- = \frac{1}{2}$ since Alice sends $|+x\rangle$ and $|-x\rangle$ with the same probability. It is known (Helstrom, 1976) that the maximal information she can obtain is $I(A:E) = 1 - H(P)$, where $P = \frac{1}{2}(1 + \sqrt{1 - |\langle\psi_1|\psi_2\rangle|^2})$. Since $|\langle\chi_+|\chi_-\rangle| = \cos\eta$, we recover the expected result $P = \frac{1}{2}(1 + \sin\eta)$.

In summary, without ancilla, Eve can make the best possible guess on the bit sent by Alice (because the machine realizes the optimal phase-covariant cloning) but has very poor information about the result obtained by Bob. Adding the ancilla does not modify the estimation of Alice's bit but allows Eve to deterministically symmetrize her information on Alice and Bob's symbols. However, the two machines are equally good from the point of view of cloning.

C. Beyond incoherent attacks

All the links that we have discussed between quantum key distribution and quantum cloning hold in the case of incoherent attacks. However, one can also expect a relation between cloning and eavesdropping in a more general security analysis. Consider the BB84 protocol and assume that Eve interacts individually with the states sent by Alice but that she can delay her measurement until the end of the reconciliation process and then possibly perform collective measurements. These types of attacks are often called *collective*. The results of Renner and König (2004) and of Devetak and Winter (2005) imply that there exists a protocol achieving a key rate

$$R = I(A:B) - \min\{\chi(A:E_Q), \chi(B:E_Q)\}, \qquad (85)$$

which can be understood as the generalization of Eq. (81) to the case where Eve's variables are quantum (the index Q). The quantity χ is the so-called Holevo bound (Holevo, 1973), which bounds the maximal information on Alice or Bob's symbol accessible to Eve through her quantum states. Indeed, the presence of Eve's attack defines an effective channel between Alice (or Bob) and Eve. For this channel, when Alice encodes the symbol $X = 0,1$ on the quantum state $|\psi_X\rangle$, Eve receives the state ρ_E^X obtained by tracing out the qubit that goes to Bob. Holevo's bound then reads

$$\chi(X:E) = S(\rho_E) - \frac{1}{2}S(\rho_E^0) - \frac{1}{2}S(\rho_E^1), \qquad (86)$$

where S denotes the von Neumann entropy and $\rho_E = (\rho_E^0 + \rho_E^1)/2$.

If Eve uses the phase-covariant cloning machine, we know $\rho_E^{0,1} = \mathrm{Tr}_B(|\Gamma^\pm\rangle\langle\Gamma^\pm|)$ from Eq. (84) and can compute R. After some simple algebra, one can see that the criti-

cal error D_c at which R (85) is zero is defined by $1-2H(D_c)=0$. Remarkably, this equation is the same as in the Shor and Preskill (2000) proof of security of the BB84 protocol and leads to a critical disturbance of $D_c \approx 11\%$. Shor-Preskill proof of security does not make any assumption on Eve's attack: it is thus remarkable that the same bound can be reached by a collective attack in which the individual quantum interaction is defined by the phase-covariant QCM. Actually, the attack based on the phase-covariant cloning machine is optimal, in the sense that it minimizes Eq. (85) for a fixed disturbance.

D. Conclusive balance

The relationship between the no-cloning theorem and the security of quantum cryptography is certainly deep. However, it is not clear at all how to associate quantitative results for cryptography to some explicit form of imperfect cloning because cloning is not strictly equivalent to eavesdropping, in particular the relevant figure of merit that defines Eve's optimal attack is *a priori* unrelated to the single-copy fidelity (7) that is optimized when constructing QCMs—see also the discussion in Bruß, DiVincenzo, *et al.* (1998). Still, the connection has proved to be strong and fruitful in the case of individual attacks, and possibly even beyond.

V. STIMULATED EMISSION AS OPTIMAL CLONING OF DISCRETE VARIABLES IN OPTICS

In this section, we discuss how the well-known amplification phenomenon of stimulated and spontaneous emission of light is closely related to optimal universal cloning. The results are stated and commented on in Sec. V.A; in Section V.B, we rederive the main results using a phenomenological model.

A. Cloning as amplification

1. Encoding of discrete states in different modes

Section III was devoted to the cloning of coherent states of a quantum oscillator; all the discussion, especially about the implementations, was carried out having in mind a single mode of the light field as an example of a quantum oscillator. In this section, we consider the light field too, but in a different perspective: the quantum system is now the discrete-level system encoded in some modes of the field. The typical example here is polarization: for a given energy ω, the light field has two independent modes $a_H(\omega)$ and $a_V(\omega)$, corresponding to two orthogonal polarizations, horizontal and vertical. We can then define a qubit as

$$a_H^\dagger(\omega)|\text{vac}\rangle = |\mathbf{0}\rangle, \tag{87}$$

$$a_V^\dagger(\omega)|\text{vac}\rangle = |\mathbf{1}\rangle, \tag{88}$$

where $|\text{vac}\rangle$ is the vacuum state of the field. According to this correspondence, for any pair of complex numbers c_H, c_V such that $|c_H|^2 + |c_V|^2 = 1$, we can define a creation operator $a_\psi^\dagger = [c_H a_H^\dagger(\omega) + c_V a_V^\dagger(\omega)]$ such that

$$a_\psi^\dagger|\text{vac}\rangle = |\psi\rangle = c_H|\mathbf{0}\rangle + c_V|\mathbf{1}\rangle. \tag{89}$$

In this sense, polarization in a given frequency mode defines a qubit. Obviously, the N-photon Fock state in which all the photons are prepared in the state $|\psi\rangle$ reads

$$|\psi\rangle^{\otimes N} = \frac{(a_\psi^\dagger)^N}{\sqrt{N!}}|\text{vac}\rangle. \tag{90}$$

The construction clearly generalizes: we can encode a qudit with any d orthogonal modes $a_1, \ldots, a_d$.

In Sec. III the unknown parameters were the parameters defining a coherent state in a given mode (i.e., a quantum continuous variable); here, a Fock state of N photons is prepared in a mode a_ψ which is a linear combination of d modes a_j: the unknown parameters are the coefficients of the linear combination (that is, a qudit). Therefore we are going to refer back to the cloning of discrete-level systems (Sec. II). In all that follows, for simplicity, we discuss explicitly the example of polarization in a single energy mode. As might be expected, the results extend to any discrete-level system encoded in field modes (Fan *et al.*, 2002); we sketch it in Sec. VI.A.3 for the case of time-bin encoding.

2. Main result

Consider a light amplification process based on stimulated emission. We consider two orthogonal polarization modes of a monochromatic component of the field, and suppose that (i) N photons of a given unknown polarization are already present in the medium, and (ii) the component of the field associated to exactly $M > N$ photons is post-selected after amplification. Because spontaneous emission is always present, it is impossible that all M photons are deterministically emitted in the same polarization mode as the input ones: even for large N, there will always be a small probability that a photon is emitted in the orthogonal mode. The claim is that if the probabilities of emission are independent of the polarization, this amplification process attains the optimal fidelity for universal $N \to M$ cloning of qubits. This was noticed in the very early days of quantum cloning (Milonni and Hardies, 1982; Wootters and Zurek, 1982; Mandel, 1983) for the $1 \to 2$ process, and was generalized more recently to any cloning process (Kempe *et al.*, 2000; Simon *et al.*, 2000). In the rest of this section, we derive the same results using the more phenomenological approach sketched in Fasel *et al.* (2002).

B. Phenomenological model

1. Definition and fidelity $1 \to 2$

Consider an inverted medium that can emit photons of any polarization with the same probability (thus we introduce by hand the assumption of universality). We focus on a monochromatic component of the field. Suppose that N photons are initially present in a given po-

larization mode, say $|V\rangle$, and suppose that at the output of the amplifier $M=N+k$ photons are found, the initial ones plus k new ones that have been emitted by the medium.[28] For this amplification process, the single-copy fidelity is the probability of an output photon picked at random to be polarized as the input ones. The no-cloning theorem tells us that the k additional photons cannot be deterministically in the same polarization mode $|V\rangle$ as the N input ones; and indeed, we know that stimulated emission is always associated with spontaneous emission.

The derivation of the fidelity for an amplification $1 \rightarrow 2$ can be easily described. If a photon is present in mode $|V\rangle$, a second photon in this mode can be emitted either by spontaneous or by stimulated emission, the two processes being equiprobable; while a photon in mode $|H\rangle$ can be emitted only by spontaneous emission. Thus the probabilities $P[2,0|1,0]$ and $P[1,1|1,0]$ that the new photon is emitted in the same mode as the input or in the orthogonal mode are related to one another as $P[2,0|1,0]=2P[1,1|1,0]$. The probability for the new photon to be polarized along $|V\rangle$ is $\frac{2}{3}$. If we now pick a photon out of the two, with probability $\frac{1}{2}$ it is the original one whose polarization is certainly $|V\rangle$; with probability $\frac{1}{2}$, it is the new one. So, the probability for finding one of the output photons in mode $|V\rangle$ (the fidelity) is $\frac{1}{2}\times 1+\frac{1}{2}\times\frac{2}{3}=\frac{5}{6}$, exactly the same as for optimal symmetric universal $1\rightarrow 2$ cloning.

In the rest of this section, we generalize the same considerations to derive the fidelity for the $N\rightarrow M$ cloning.

2. Statistics of stimulated emission

As a preliminary for what follows, we need to give the statistics of the process of stimulated and spontaneous emission. This amplification process will be completely described by the probabilities $P[N+l,k-l|N,0]$, $0\leq l \leq k$, that l photons are emitted in mode $|V\rangle$ and $k-l$ in mode $|H\rangle$. We normalize these probabilities so that they sum up to the total probability of the process:

$$\sum_{l=0}^{k} P[N+l,k-l|N,0] = P(N\rightarrow M). \tag{91}$$

We stated above the simplest example, $P[2,0|1,0] =2P[1,1|1,0]$; now we want to show that the general expression is

---

[28]Photons are bosons: the output state will be a symmetrized state of the M photons in which N photons are certainly in state $|V\rangle$ and the other ones are in a suitable state. So it does not really make sense to speak of the initial photons as if they had conserved any distinctive property whatsoever after amplification. Still, one can use this loose language provided that the relation between spontaneous and stimulated emission, Eq. (92), is assumed. This relation is a consequence of the bosonic nature of the field.

$$P[N+l,k-l|N,0] = \frac{(N+l)!}{N!l!}P[N,k|N,0]. \tag{92}$$

For definiteness, we consider a medium formed of $\mathcal{N}$ lambda atoms, in which a unique excited state $|e\rangle$ can decay into two orthogonal ground states $|g_H\rangle$ and $|g_V\rangle$ through the emission of the correspondingly polarized photon. Omitting coupling constants, the Hamiltonian describing the interaction between the medium and the field is

$$H = \sum_{j=1}^{\mathcal{N}} (a_H^\dagger \sigma_{H,j}^- + a_V^\dagger \sigma_{V,j}^-) + \text{adj}, \tag{93}$$

where $\sigma_{H,j}^-=|g_H\rangle\langle e|$ and $\sigma_{V,j}^-=|g_V\rangle\langle e|$ acting on atom j. The system is prepared so that all the atoms are in the excited state, N photons are in mode $|V\rangle$, and none in mode $|H\rangle$: $|\text{in}\rangle=|N,0;e,e,\ldots,e\rangle$. The interaction leads to $|\psi(\tau)\rangle=e^{-iH\tau/\hbar}|\text{in}\rangle$, where τ is the interaction time.

At the output, we post-select on the states such that exactly k photons have been emitted; more specifically, we want l additional photons in mode $|V\rangle$ and $k-l$ in mode $|H\rangle$. By reading the state of the atoms after the interaction, one could in principle know which atom has emitted which photon, so all the possible output states are distinguishable. Consider all the possible processes in which the first k atoms have emitted a photon—all the other processes contribute with equal weight: $|\text{out}(\xi)\rangle =|N+l,k-l;g_{\xi(1)},\ldots,g_{\xi(k)},e,\ldots,e\rangle$, where ξ is a k-item sequence containing l times the symbol V and $k-l$ times the symbol H. Then the probability $P[N+l,k-l|N,0]$ is proportional to

$$\sum_{\xi} |\langle \text{out}(\xi)|H^k|\text{in}\rangle|^2 = \binom{k}{l}|\langle N+l,k-l|a_V^{\dagger l}a_H^{\dagger k-l}|n,0\rangle|^2$$

$$= k!\frac{(N+l)!}{N!l!}.$$

This proves Eq. (92). As a consequence, Eq. (91) becomes

$$P(N\rightarrow M) = P[N,k|N,0]\frac{(N+k+1)!}{(N+1)!k!} \tag{94}$$

since $\sum_{l=0}^{k}(N+l)!/N!l!=(N+k+1)!/(N+1)!k!$. We can now go back to cloning and prove the main result of this section.

3. Fidelity $N\rightarrow M$

The fidelity of the amplification process is defined as usual as the probability of finding a photon in the same mode as those of the input:

$$F_{N\rightarrow M} = \frac{N+\langle l\rangle_{NM}}{M}, \tag{95}$$

where

$$\langle l \rangle_{NM} = \sum_{l=0}^{k} l \frac{P[N+l, k-l|N, 0]}{P(N \to M)} \qquad (96)$$

is the average number of additional photons produced in the same mode as the input. Inserting Eqs. (92) and (94) into Eq. (96) and using $\Sigma_{l=0}^{k} l(N+l)!/N!l! = \Sigma_{m=0}^{k-1}(N+1+m)!/N!m!$, we obtain $\langle l \rangle_{NM} = k(N+1)/(N+2)$. Replacing $k = M - N$ we obtain $F_{N \to M} = (1/M)\{N + (N-M)[(N+1)/(N+2)]\}$, which is exactly the Gisin-Massar result (16).

Our phenomenological model shows that the link between amplification by an inverted medium and quantum cloning is semiclassical in the following sense: the relation (92) is derived rigorously from quantum mechanics (the bosonic nature of the field), but once this relation is admitted, the rest becomes just classical event counting. Note, in particular, how due to Eq. (92), $\langle l \rangle_{NM}$ and consequently $F_{N \to M}$ become independent of both $P[N, k|N, 0]$ and $P(N \to M)$. These last probabilities, i.e., how frequent the process $N \to M$ is, are in general difficult to compute and depend on the detailed physics of the inverted medium [Kempe *et al.* (2000) and Simon *et al.* (2000) provide some examples]. However, we know that whenever such an amplification process takes place, it realizes the optimal symmetric $N \to M$ UQCM.

VI. EXPERIMENTAL DEMONSTRATIONS AND PROPOSALS

This section reviews the experiments that have been proposed and often performed to demonstrate quantum cloning. They all refer to universal cloning, symmetric or asymmetric. Phase-covariant cloning has also been the object of recent proposals (Fiuràšek, 2003; De Chiara *et al.*, 2004).

A. Polarization of photons

The connection between stimulated emission and quantum cloning (Sec. V) is the essential ingredient in most of the optical implementations of qubit $1 \to 2$ cloning machines. The usual scheme consists of sending a single photon into an amplifying medium. In the absence of this photon, the medium will spontaneously emit photons of any polarization (or mode). But if the photon is present, it stimulates the emission of another photon in the same mode, i.e., this mode is enhanced. However, the process of spontaneous emission can never be suppressed, which means that the quality of the amplification process is never perfect. This is indeed a manifestation of the no-cloning theorem; remarkably, as discussed in detail in the previous section, it achieves optimal cloning.

Before discussing this kind of cloning, we mention that one of the first optical experiments that implemented the Bužek-Hillery cloning (Sec. II.A) was an experiment using only linear optics (Huang *et al.*, 2001). The idea there was to realize the three needed qubits with a single photon: one qubit is the polarization, the
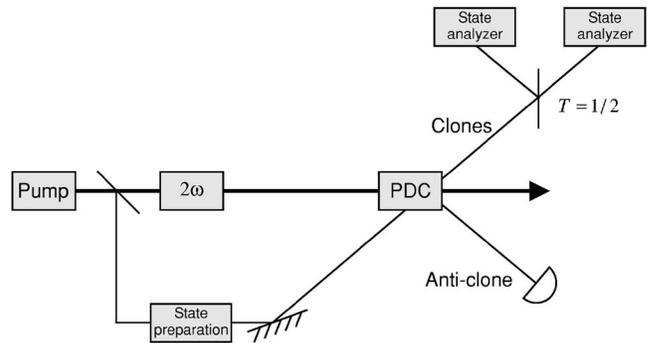

FIG. 5. Experimental implementation of the $1 \to 2$ universal cloning machine for qubits. The laser works in pulsed mode. A very small fraction of the pulse, below single-photon level, serves as probabilistic preparation of the photon to clone. The rest of the pump pulse is frequency doubled and sent to a nonlinear crystal. If the prepared photon is indistinguishable from one of the two down-converted photons, optimal cloning is achieved. The other down-converted photon is often called anticlone.

other two are defined by the location of the photon into four possible paths. As is well known, the optical device called the polarizing beam splitter realizes the controlled NOT gate between polarization and the path mode. The experimental setup to achieve cloning is a suitable arrangement of polarizing beam splitter and optical rotators. This being mentioned, we focus on cloning through amplification processes.

1. Experiments with parametric down-conversion

Most optical implementations of the $1 \to 2$ cloning machine (De Martini *et al.*, 2000, 2002; Lamas-Linares *et al.*, 2002) use *parametric down-conversion* as the amplification phenomenon (see Fig. 5). A strong laser pulse pumps a nonlinear crystal. With small probability the pulse is split into two photons, called signal S and idler I. For pulsed type-II frequency-degenerate parametric down-conversion the Hamiltonian reads

$$H = \gamma(a_{VS}^\dagger a_{HI}^\dagger - a_{HS}^\dagger a_{VI}^\dagger) + \text{H.c.} \qquad (97)$$

Notice that this Hamiltonian is invariant under the same unitary operation in both polarization modes (VS, HS) and (VI, HI). The photon to be cloned and the the pump pulse propagate through the crystal at the same time. Because of the Hamiltonian symmetry, one can take as the state to clone, $|1, 0\rangle_S = a_{VS}^\dagger |\text{vac}\rangle$, without losing generality. Indeed the rotational symmetry of the Hamiltonian guarantees the covariance of the transformation. The state after the crystal is

$$|\psi_{\text{out}}\rangle = e^{-iHt} a_{VS}^\dagger |\text{vac}\rangle. \qquad (98)$$

We can expand the previous expression into a Taylor series. Since the down-conversion process only happens with small probability, we restrict our considerations to the first terms in the expansion. The zero-order term simply corresponds to the case where no pair of photons is produced, so at the output one finds the initial state

unchanged. The first-order term is more interesting since the resulting normalized state gives

$$|\psi_{1\to 2}\rangle = \sqrt{\frac{2}{3}}|2,0\rangle_S|0,1\rangle_I - \sqrt{\frac{1}{3}}|1,1\rangle_S|1,0\rangle_I, \qquad (99)$$

i.e., the searched cloning transformation (13). It is straightforward to see that if the two photons in the signal mode are separated, for instance, by means of a beam splitter, the obtained fidelity is equal to 5/6. Indeed the first term corresponds to ideal cloning, while only one of the two photons in the second term is equal to the initial state, so

$$F = 1 \times \frac{2}{3} + \frac{1}{2} \times \frac{1}{3} = \frac{5}{6}. \qquad (100)$$

The factor $\sqrt{2}$ is a manifestation of the stimulated emission process. It only appears when the initial photon is completely indistinguishable from the down-converted photon in the signal mode. That is, the two photons should perfectly overlap in space, time, and frequency. Any effect increasing the distinguishability of these two photons, such as a difference in the coherence lengths of the pump pulse and down-converted photons, must be compensated in order to achieve a near to optimal cloning. Moreover, it has to be stressed that this implementation of the cloning machine is conditioned on the fact that the three detectors (the one for the idler mode and the two in the state analyzers) click. Then it is assumed that one photon was present in each mode. Note that there are cases in which more than one pair is produced by the crystal, or the initial state to be cloned actually contains more than one photon. These spurious processes slightly decrease the optimality of the cloning transformation. In any case, the reported fidelities are equal to 0.81 ± 0.01 (Lamas-Linares *et al.*, 2002) and 0.810 ± 0.008 (De Martini *et al.*, 2002, 2004; Pelliccia *et al.*, 2003), very close to the theoretical value $5/6 \approx 0.83$. Interestingly, the photon in the idler mode, or anticlone, gives the optimal realization of the quantum universal NOT gate. The optimal fidelity for this transformation is $2/3$, while the reported experimental fidelity is 0.630 ± 0.008 (De Martini *et al.*, 2002, 2004; Pelliccia *et al.*, 2003).

More recently, an alternative realization of the $1 \to 2$ quantum cloner for qubits has been proposed and carried out by Irvine *et al.* (2004) and by Ricci *et al.* (2004). This is based on the fact that two identical photons bunch at a beam splitter. The experiment is much simpler but cannot be generalized to $N \to M$ cloning. The experimental setup[29] is schematically shown in Fig. 6. The initial state is combined with one of the down-converted photons into a balanced beam splitter. It is a well-known result that if the photons separate after the
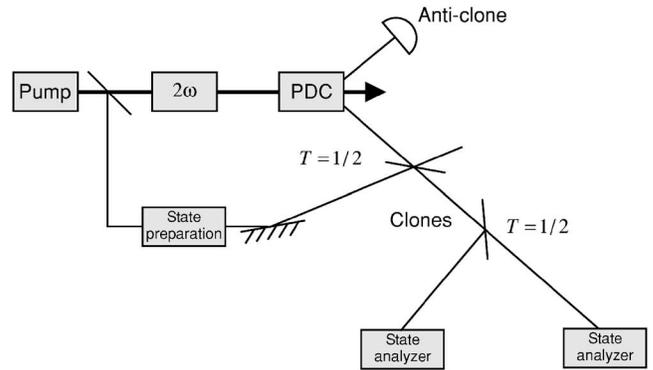
---

[29]Note that this is the same setup as for the teleportation of a qubit (Bennett *et al.*, 1993).

FIG. 6. Alternative implementation of the $1 \to 2$ universal cloning machine for qubits. The photon to be cloned is now combined into a balanced beam splitter with one of the down-converted photons. When the two photons stick together, two optimal clones of the initial state are obtained. As in the first scheme, the second down-converted photon provides the anti-clone.

beam splitter, a projection onto the singlet state $|\Psi^-\rangle$ has been achieved. In the other cases, the photons have been projected with

$$S_2 = 1 - |\Psi^-\rangle\langle\Psi^-| \qquad (101)$$

onto the two-qubit symmetric subspace. Tracing out the second down-converted photon, the transformation on the photons impinging the beam splitter is indeed equal to Eq. (17), conditioned on the fact that they stick together. On the other hand, it is straightforward to see that the transformation on the second down-converted photon is the optimal universal NOT gate, i.e., the photon in the idler mode is equal to the anticlone (compare with Sec. II.A.3). In a similar way as for the previous implementation, the quality of the cloning process crucially depends on the fact that the two photons arriving at the beam splitter define the same mode. This means that, as above, they have to be completely indistinguishable. Moreover, multiphoton pulses also deteriorate the quality of the cloning process. The observed fidelities for cloning were approximately 0.81.

2. Proposals for asymmetric cloning

In this section we show how the previous realizations can be modified in order to cover asymmetric cloning machines. Indeed, it has been shown very recently that some of these transformations can be obtained by combining into beam splitters the photons produced by a symmetric cloning machine (Filip, 2004; Iblisdir *et al.*, 2004; Fiuràšek, Filip, and Cerf, 2005; Iblisdir, Acín, and Gisin, 2005). At the moment of writing, these experiments have not yet been performed.

A proposal for the experimental realization of the asymmetric $1 \to 1+1$ cloning machine for qubits was given by Filip (2004). It is represented in Fig. 7. It is convenient for the analysis of this scheme to rewrite the output of the symmetric machine (99) using Cerf's formalism,
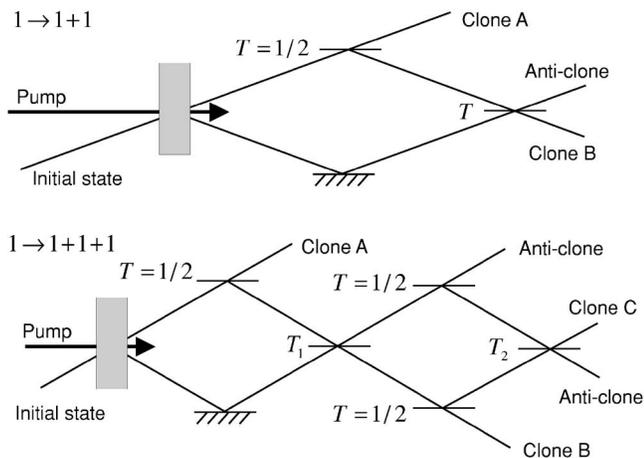
FIG. 7. The optical implementation of the $1 \to 1+1$ and $1 \to 1+1+1$ optimal cloning machines. For the $1 \to 1+1$ case, the symmetry between the clones of the $1 \to 2$ cloning machines is broken by combining one of the clones with the anticlone into a beam splitter. The degree of asymmetry depends on the transmittivity T. The idea can be naturally generalized to the $1 \to 1+1+1$ case.

$$|\psi_{1 \to 2}\rangle = \left(\frac{\sqrt{3}}{2} \mathbb{1} + \frac{1}{2\sqrt{3}} \sum_{k=x,y,z} (\sigma_k \otimes \sigma_k \otimes \mathbb{1}) \right) |\psi\rangle |\Psi^-\rangle,$$

$$(102)$$

where $|\Psi^-\rangle$ is the singlet state. It is simple to see that this state is equivalent to Cerf's construction when $v = \sqrt{3}/2$ (31), but with a simple relabeling of the Bell states for the second clone and the anticlone. The asymmetry between the clones can now be introduced by changing the ratio of the amplitudes for the first term and the rest. A possible way of achieving this is by successfully applying the projector $P_{\text{asym}} = a\mathbb{1} + b|\Psi^-\rangle\langle\Psi^-|$ to the second clone and the anticlone, where a and b are such that $\mathbb{1} - P_{\text{asym}} \geq 0$. Indeed, the states $P_{\text{asym}}|\psi_{1 \to 2}\rangle$ define, up to normalization, the family of states (31). Changing the ratio between a and b, one can optimally adjust the asymmetry between the quality of the two clones, i.e., the ratio between v and x, according to Cerf's notation. A beam splitter of transmittivity T conditioned on the fact that the photons at the output are separated gives a simple optical implementation of this projector. Indeed, some simple algebra shows that the corresponding operation is equal to

$$P_{\text{asym}}(T) = (2T - 1)\mathbb{1} + 2(1 - T)|\Psi^-\rangle\langle\Psi^-|. \quad (103)$$

When $T = 1$ no operation is performed, $P_{\text{asym}}(T=1) = \mathbb{1}$, and the two clones are symmetric, $F_A = F_B = 5/6$. When T decreases, some asymmetry is introduced between the two clones since F_A increases while F_B worsens. In the limiting case $T = 1/2$, a projection onto the singlet is achieved, as expected, and the state in mode A is projected onto the initial state, $F_A = 1$ and $F_B = 1/2$, that is, the cloning transformation has been undone. In fact, since a projection onto the singlet is realized, the detected photons after the beam splitter were the ones

produced in the crystal. This implies that the photon in mode A must be equal to the initial state. All the interesting values lie between these two limiting cases, $1/2 \leq T \leq 1$. Indeed, one can see that the tradeoff between the obtained fidelities F_A and F_B saturates the cloning inequality (23).

Note that for all these experimental proposals the successful implementation of the searched cloning transformation depends on the detection of three photons (all the detectors click). Interestingly, one can see that changing the number of post-selected photons gives other asymmetric cloning machines (Iblisdir *et al.*, 2004; Fiuràšek, Filip, and Cerf, 2005; Iblisdir, Acín, and Gisin, 2005) in a way similar to what happens for the symmetric case (Simon *et al.*, 2000). Indeed, denoting by N, M_A, and M_B the number of photons in the initial mode and modes A and B (see Fig. 7), it has been shown in that the optimal $1 \to 1+2$ cloning machine is recovered when $N = 1$ and $M_A = 1$, $M_B = 2$, and $M_A = 2$, $M_B = 1$, and also the $2 \to 2+1$ case when $N = 2$ and same post-selection for modes A and B. Unfortunately, the transformation when $N = M_A = M_B = 2$ does not correspond to the optimal $2 \to 2+2$ machine. At present, it seems that the previous construction only works for the $1 \to 1+N$ and $N \to N+1$ cases, and a feasible optical implementation of the $N \to M_1 + M_2$ machine with $M_1, M_2 > 1$ remains as an open question.

Remarkably, Filip's construction can be further generalized. Indeed, exploiting the antisymmetrization by means of a beam splitter allows us to extend this scheme to the $1 \to 1+1+1$ case, where three copies of the initial state are produced in such a way that the tradeoff between the fidelities is optimal. As shown in Fig. 7, it is possible to consider a more complex situation when the production of two pairs by the pump pulse, instead of one, is stimulated by the presence of the photon to be cloned. The corresponding state is equal to the output of a $1 \to 3$ symmetric machine, as discussed by Simon *et al.* (2000). Actually, there are three clones and two anticlones, namely, the two photons in the idler mode. Now, one can apply twice the antisymmetrization explained above, as shown in Fig. 7. After much algebra, one can see that the fidelities for the clones in modes A, B, and C are equal to those defining the optimal $1 \to 1+1+1$ cloning machine of Iblisdir *et al.* (2004, 2005) and Fiuràšek, Filip, and Cerf (2005). Although unproven, it seems quite likely that this construction works for any number of clones, and that all $1 \to 1 + \cdots + 1$ cloning machines can be optimally realized by combining into beam splitters, and conditioned on the number of photons, the output of the $1 \to N$ symmetric machine.

3. Cloning in an erbium-doped fiber

Parametric down-conversion is an amplification medium that has been studied intensively because it allows us to create entangled photons. In the field of telecommunication optics, however, the common devices used for amplification of light are optical fibers doped with erbium ions. These rare-earth ions can be pumped onto
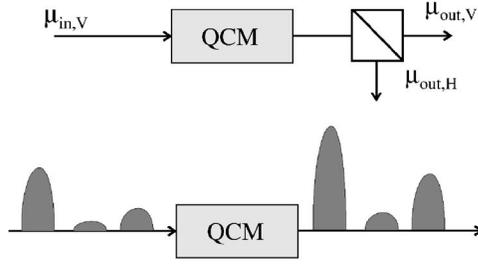
FIG. 8. Scheme of the experimental setup of Fasel *et al.* (2002), see Sec. VI.A.3. Everything takes place in optical fibers, the QCM itself being a pumped Er-doped fiber. Upper: effectively realized experiment for cloning of polarization states (qubit). Lower: possible variation using time-bin encoding, which would lead to optimal cloning of qudits (here, $d=3$).

an excited state and then constitute an inverted medium that can lase at telecom wavelengths. Fasel *et al.* (2002) studied quantum cloning due to such an amplifier. The experiment consisted of sending classical, very weak pulses of (say) vertically (V) polarized light into an erbium-doped fiber. At the output, light is amplified but is no longer perfectly polarized because of spontaneous emission: some light has developed in the polarization mode orthogonal to the input one (horizontal, H). The fidelity of the classical amplification is defined as the ratio of the intensities $F_{cl}=I_{out,V}/I_{out,tot}$.

A theoretical analysis based on a seminal paper on maser amplification (Shimoda *et al.*, 1957) provides a remarkable prediction: let $\mu_{in,out}$ be, respectively, the mean number of photons in the input and the output field (i.e., the intensity of these fields, in suitable units). Then it holds that

$$F_{cl} = \frac{Q\mu_{out}\mu_{in} + \mu_{out} + \mu_{in}}{Q\mu_{out}\mu_{in} + 2\mu_{out}}. \qquad (104)$$

Here the parameter Q is related to the phenomenology of the emission process: $Q=1$ means that all erbium ions are excited, so that there is no absorption; $Q=0$ means that emission and absorption compensate exactly; and $Q<0$ means that the absorption in the medium overcomes the emission. We see that in the ideal case $Q=1$, the formula (104) for F_{cl} looks exactly like the one for the optimal symmetric $N \rightarrow M$ cloning of qubits (16), but for the fact that μ_{in} and μ_{out} are not restricted to taking integer values. This is a signature of the underlying quantum cloning in an experiment with classical states of light. In the actual experiment, the fit yielded $Q=0.8$; for the cloning $\mu_{in}=1 \rightarrow \mu_{out}=1.94 \simeq 2$, a fidelity $F_{cl} \approx 0.82$ was observed, close to the optimal value $\frac{5}{6} \simeq 0.833$.

Although the experiment was performed with polarization, the same setup would allow the cloning of quantum states encoded in time bins. With time-bin encoding, it is very easy to go beyond the qubit case (De Riedmatten *et al.*, 2004; Thew *et al.*, 2004). In particular, the present setup (Fig. 8) would allow us to demonstrate optimal cloning for higher-dimensional quan-

tum systems. As an example to support this claim, we compute the fidelity in the computational basis for $1 \rightarrow 2$ cloning—that is, one photon was prepared in a given time bin, and two photons are found in the outcome. The probability of finding the new photon in the good time bin (associated to $F=1$) is just twice the probability of finding it in any of the other $d-1$ time bins (in which case $F=1/2$, because half of the times we pick the original photon). The average fidelity is then

$$F_{1 \rightarrow 2}(d) = \frac{2 \times 1 + (d-1) \times \frac{1}{2}}{2 + (d-1)} = \frac{d+3}{2(d+1)}, \qquad (105)$$

which is the optimal result; see Sec. II.B.1. Of course, one should show that the same fidelity holds for any superposition state, which is, however, quite evident when one is familiar with the physics of light amplification. As we mentioned above, this result is not limited to time bins but holds for any encoding of a qudit in different modes of the field (Fan *et al.*, 2002); the time-bin encoding is possibly the most easily analyzed and implemented.

B. Other quantum systems

1. Nuclear spins in nuclear magnetic resonance

A way to achieve quantum cloning of nuclear spins using nuclear magnetic resonance (NMR) has been presented by Cummins *et al.* (2002), together with its experimental realization. As usual in quantum information processing with NMR, many molecules are present in the sample and the process takes place among nuclear spins within each molecule.

In the present experiment, the molecule is *E*-(2-chloroethenyl)phosphonic acid. After the peculiar pulse sequences needed to prepare the sample in a pseudopure state, a spin direction is encoded into the first qubit, which is the spin of the ^{31}P nucleus. The main part of the scheme is a pulse sequence that implements a version of the optimal symmetric $1 \rightarrow 2$ QCM (Bužek *et al.*, 1997) that maps the quantum information onto the two other qubits—here, nuclear spins of two ^{1}H atoms. Because of several unwanted mechanisms and imperfections, however, the measured fidelity for both clones was only $F \approx 0.58$, even lower than the value achievable with trivial cloning strategies (see Sec. II.A.1).

2. Atomic states in cavity QED

Implementations of the $1 \rightarrow 2$ UQCM for qubits using the techniques of cavity QED have been proposed. The scheme by Milman *et al.* (2003) uses four Rydberg atoms interacting with two cavities. Atom 2 carries the input state. After the suitable pulse sequence, atoms 3 and 4 are the two clones: as in the NMR experiment described just above, the transformation is similar to the one of Bužek *et al.* (1997). Here however, the circuit is a new

one, and the ancilla is not a single qubit, but two atoms (1 and 2) and the state of the light field in the two cavities.

Zou, Pahlke, and Mathis (2003) proposed a scheme that uses three atoms and three cavities; interaction between atoms within each cavity is required for this scheme.

VII. PERSPECTIVES

A. Some open questions

At the end of this review, we address a few of the questions that are still open at the moment of writing. As far as possible, we list them in the same order as the corresponding themes appear in this review.

- To our knowledge, the study of optimal cloning has always supposed pure input states. The optimal cloning of mixed states is thus a completely open domain. Also, as mentioned several times, there is no general result concerning state-dependent cloning and the zoology of cases is *a priori* infinite.

- We have seen several times in this review (especially Secs. III and IV) that the single-copy fidelity is not always the most meaningful figure of merit. However, most of the QCMs are optimal according to it. What about other figures of merit? If the resulting QCMs are found to be different, is there a deep connection among all the results?

- The role of entanglement in cloning may be further elucidated. The trivial strategies discussed in Secs. II.A.1 and II.B.3 show that the fidelity F_{triv} given in Eq. (22) can be achieved without using any coherent interaction between the clone and the copy. It seems quite plausible that this is the optimal value one can attain using strategies without quantum interaction. Therefore it would be interesting to understand more precisely what role entanglement plays in optimal cloning, e.g., by studying the entangling power of the optimal cloning machine or the entanglement properties of the corresponding output states (Bruß and Macchiavello, 2003). Note that in the limit of large dimension, no entanglement is required for an optimal cloning. One could also look for links between these results and the entanglement cloning machine of Lamoureux *et al.* (2004).

- The link between cloning and Bell's inequalities is not clear. Consider the setup of Fig. 1. The QCM is an existing one (not Herbert's hypothetical perfect cloner), and let us suppose it universal and symmetric for simplicity. Alice and Bob started with the singlet, which obviously violates Bell's inequalities. Alice keeps the quantum system A, Bob now has two quantum systems B_1 and B_2. Does $\rho_{AB_1} = \rho_{AB_2}$ violate a Bell inequality? Certainly it cannot violate any inequality with two settings on Bob's side because Bob could measure one setting on ρ_{AB_1} and the other set-

ting on ρ_{AB_2} (Terhal *et al.*, 2003). But the general answer is unknown.

- The connection between optimal cloning and state estimation looks natural and, indeed, in Sec. II.E we presented several results in that direction. However, it is still not known whether this connection holds in general. Is it true for any arbitrary set of states, possibly with unequal *a priori* probabilities, that the fidelities are equal for the optimal state estimation and for the optimal cloning in the limit of a large number of copies?

- The relation to optimal eavesdropping is also not yet fully understood. For individual attacks on some quantum cryptography protocol, such as BB84 or the six-state protocol, it has been proven that the best strategy uses the cloning machines that are optimal to clone the set of states used for encoding. As we stressed in Sec. IV, this correspondence is not obvious since cloning is optimized for fidelities, whereas in eavesdropping one optimizes mutual Shannon information; and indeed, it seems that the correspondence breaks down for the SARG04 protocol. More generally, it has been proven that security bounds can be obtained by restricting attacks to the so-called collective attacks (Kraus *et al.*, 2004; Renner *et al.*, 2005), and it is meaningful to ask whether the quantum interaction is described by the corresponding optimal cloner.

- The concepts and tools of cloning have proved useful for the foundations of quantum mechanics, for state estimation, and for cryptography. Are there other domains, tasks, situations, etc. in which cloning can be useful? Or, can one find a more general principle which unifies optimal cloning, state estimation, and eavesdropping in cryptography, possibly with spontaneous and stimulated emission?

- Qubits obey fermionic commutation relations, e.g., $\{\sigma_x, \sigma_y\} = 0$. Optimal cloning of qubits can be implemented using spontaneous and stimulated emission that comes from bosonic commutation relations, i.e., $[a, a^\dagger] = 1$. What is the exact relation? A link between the particle statistics and state estimation has been discussed (Bose *et al.*, 2003), but to our knowledge there is no such study for cloning.

- Many questions are also still open in the field of implementations of quantum cloning. Obviously, any form of cloning can (in principle) be implemented with linear optics using the Knill, Laflamme, and Milburn (2001) scheme for quantum computation. Can one implement any cloning transformation using amplification through stimulated emission? If yes, can it be done by linear optics elements, or are other nonlinear devices needed? Are there other natural phenomena that directly implement quantum cloning?

This list will possibly shrink in the coming years as some of these questions are answered. A regularly up-

dated list of open problems in quantum information is available on the website of Reinhard Werner's group: www.imaph.tu-bs.de/qi/problems/problems.html. At the moment of this writing, no problems related to cloning are listed there, apart from, possibly, "complexity of product preparations" proposed by Knill.

B. Conclusion: the role of cloning in quantum physics

Quantum cloning is likely to remain an active topic for basic research, while simultaneously an ideal subject for teaching elementary quantum physics. The proof of the no-cloning theorem is so simple that it can be presented to students as soon as the linearity of the quantum dynamics has been introduced, and much of quantum mechanics can be presented as a consequence of this deep no-go theorem. Such a presentation would not follow the history of the discovery of quantum physics, but is much closer to the modern view of it in the light of quantum information theory. Optimal cloning clearly shows that incompatible quantities can be measured simultaneously (first clone the system, next perform different measurements on each clone), while illustrating that such measurements cannot be ideal, i.e., cannot be immediately reproducible.

Apart from the issue of measurement, quantum cloning is closely related to many other aspects of quantum physics: to the no-signaling condition, both historically (Sec. I.C) and as a limit for optimal cloning (Sec. I.E.1); to the phenomenon of spontaneous and stimulated emissions, well known in quantum optics; see Sec. V. The no-cloning theorem also introduces in a natural way the idea of quantum cryptography, and optimal cloning suggests the way eavesdropping can be analyzed. Finally, it elucidates what is so special about quantum teleportation (Bennett *et al.*, 1993): the original has to be destroyed in the process and the Bell-state measurement should not provide any information of the state to be teleported, otherwise there would be a contradiction with the no-cloning theorem (more precisely, with the optimal asymmetric cloning result presented in Sec. II.C).

APPENDIX: NOTATIONS AND BASIC FORMULAS FOR QUBITS

A *qubit* is the simplest possible quantum system, described by the two-dimensional Hilbert space $\mathbb{C}^2$. The algebra of operators acting on this space is generated by the Pauli matrices:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

In particular, $\mathrm{Tr}(\sigma_k) = 0$ and $\sigma_k^2 = \mathbb{1}$ for $k = x, y, z$; also, $\sigma_x \sigma_y = -\sigma_y \sigma_x = i\sigma_z$ and all the cyclic permutations hold. In the set of states, the computational basis $\{|0\rangle, |1\rangle\}$ is universally assumed to be the eigenbasis of σ_z, so that

$$\sigma_z |0\rangle = |0\rangle, \quad \sigma_z |1\rangle = -|1\rangle. \tag{A1}$$

Normally, everything is always written in the computational basis; only the eigenstates of σ_x have a standard notation for convenience: $|+x\rangle \equiv |+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ and $|-x\rangle \equiv |-\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$. The eigenstates of σ_y are $|\pm y\rangle = (1/\sqrt{2})(|0\rangle \pm i|1\rangle)$.

The generic pure state of a qubit will be written

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle. \tag{A2}$$

The associated projector reads

$$|\psi\rangle\langle\psi| = \frac{1}{2}(\mathbb{1} + \hat{n} \cdot \vec{\sigma}), \tag{A3}$$

where the vector $\hat{n} = (\langle\sigma_x\rangle_\psi, \langle\sigma_y\rangle_\psi, \langle\sigma_z\rangle_\psi) = (2\,\mathrm{Re}(\alpha\beta^*), 2\,\mathrm{Im}(\alpha\beta^*), |\alpha|^2 - |\beta|^2)$ is called the Bloch vector. For pure states (the case we are considering here) its norm is 1: actually, all these vectors cover the unit sphere (called the *Bloch sphere*, or the Poincaré sphere if the two-level system is the polarization of light). Thus there is a one-to-one correspondence between unit vectors and pure states of a two-level system given by the following parametrization in spherical coordinates:

$$|\psi\rangle \equiv |+\hat{n}\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{A4}$$

is the eigenstate for the eigenvalue +1 of $\hat{n} \cdot \vec{\sigma}$, with $\hat{n} \equiv \hat{n}(\theta, \varphi) = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$, with as usual $\theta \in [0, \pi]$ and $\varphi \in [0, 2\pi]$. Given that any projector takes the form (A3), the general form of any mixed state can then be written

$$\rho = \sum_k p_k |\psi_k\rangle\langle\psi_k| = \frac{1}{2}(\mathbb{1} + \vec{m} \cdot \vec{\sigma}), \tag{A5}$$

with $\vec{m} = \Sigma_k p_k \vec{m}_k$; the norm of the Bloch vector is $|\vec{m}| \leq 1$, with equality if and only if the state is pure.

For the present review, it is also useful to mention some formulas and notations for the description of two qubits. As is well known, a composed system is described by the tensor product of the Hilbert spaces of its components. So the Hilbert space that describes a two-qubit system is $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$. The natural (induced) computational basis on this space is the basis of the four eigenstates of $\sigma_z \otimes \sigma_z$, namely (we omit the symbol of tensor product for states when not necessary), $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$, and $|1\rangle|1\rangle$. The most general pure state is any linear combination of these. Although probably redundant in a paper on quantum information, we recall here

that the most important feature of composed systems is the existence of entangled states, that is, states that cannot be written as products $|\psi_1\rangle \otimes |\psi_2\rangle$.

The basis formed with four orthogonal maximally entangled states (*Bell basis*) plays an important role; the notations are standardized by now:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle), \tag{A6}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle), \tag{A7}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle), \tag{A8}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle). \tag{A9}$$

We recall that $|\Psi^-\rangle$ is invariant under identical unitaries on both qubits, i.e., it keeps the same form in all the bases. If the eigenstates of $\sigma_x \otimes \sigma_x$ or of $\sigma_y \otimes \sigma_y$ were taken as computational bases states, the Bell basis remains the same, simply relabeled $|\Phi^+\rangle_x = |\Psi^+\rangle_y = |\Phi^+\rangle_z$, $|\Phi^-\rangle_x = -i|\Phi^-\rangle_y = |\Psi^+\rangle_z$, and $|\Psi^+\rangle_x = |\Phi^+\rangle_y = |\Phi^-\rangle_z$.

The general form of a density matrix of two qubits is

$$\rho_{AB} = \frac{1}{4}\Big(\mathbb{1}_4 + \hat{n}_A \cdot \vec{\sigma} \otimes \mathbb{1} + \mathbb{1} \otimes \hat{n}_B \cdot \vec{\sigma}$$
$$+ \sum_{i,j=x,y,z} t_{ij}\sigma_i \otimes \sigma_j\Big), \tag{A10}$$

where $t_{ij} = \mathrm{Tr}(\rho\sigma_i \otimes \sigma_j)$. From this form, the partial traces are computed leading to

$$\rho_{A,B} = \frac{1}{2}(\mathbb{1} + \hat{n}_{A,B} \cdot \vec{\sigma}). \tag{A11}$$

If $|\hat{n}_A| = 1$, then $\rho_A = P_A$, a projector on a pure state; since a projector is an extremal point of a convex set, this necessarily implies $\rho_{AB} = P_A \otimes \rho_B$ and, in particular, $t_{ij} = (n_A)_i(n_B)_j$.

REFERENCES

Acín, A., N. Gisin, L. Masanes, and V. Scarani, 2004, Int. J. Quantum Inf. **2**, 23.

Acín, A., N. Gisin, and V. Scarani, 2004, Phys. Rev. A **69**, 012309.

Albeverio, S., and S. M. Fei, 2000, Eur. Phys. J. B **14**, 669.

Arthurs, E., and J. L. Kelly, 1965, Bell Syst. Tech. J. **44**, 725.

Banaszek, K., 2001, Phys. Rev. Lett. **86**, 1366.

Barnum, H., C. Caves, C. Fuchs, R. Jozsa, and B. Schumacher, 1996, Phys. Rev. Lett. **76**, 2818.

Bechmann-Pasquinucci, H., and N. Gisin, 1999, Phys. Rev. A **59**, 4238.

Bennett, C. H., and G. Brassard, 1984, *Proceedings IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York), p. 175.

Bennett, C. H., G. Brassard, C. Crépeau, R. Jozsa, A. Peres,

and W. K. Wootters, 1993, Phys. Rev. Lett. **70**, 1895.

Bose, S., A. Ekert, Y. Omar, S. Paunković, and V. Vedral, 2003, Phys. Rev. A **68**, 052309.

Branciard, C., N. Gisin, B. Kraus, and V. Scarani, 2005, Phys. Rev. A **72**, 032301.

Braunstein, S. L., V. Bužek, and M. Hillery, 2001, Phys. Rev. A **63**, 052313.

Braunstein, S. L., N. J. Cerf, S. Iblisdir, P. van Loock, and S. Massar, 2001, Phys. Rev. Lett. **86**, 4938.

Bruß, D., 1998, Phys. Rev. Lett. **81**, 3018.

Bruß, D., M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, 2000, Phys. Rev. A **62**, 012302.

Bruß, D., G. M. D'Ariano, C. Macchiavello, and M. F. Sacchi, 2000, Phys. Rev. A **62**, 062302.

Bruß, D., D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, 1998, Phys. Rev. A **57**, 2368.

Bruß, D., A. Ekert, and C. Macchiavello, 1998, Phys. Rev. Lett. **81**, 2598.

Bruß, D., and C. Macchiavello, 2002, Phys. Rev. Lett. **88**, 127901.

Bruß, D., and C. Macchiavello, 2003, Found. Phys. **33**, 1617.

Brukner, Č., and A. Zeilinger, 2002, e-print quant-ph/0212084.

Buscemi, F., G. M. D'Ariano, and C. Macchiavello, 2005, Phys. Rev. A **71**, 042327.

Bussey, P. J., 1987, Phys. Lett. A **123**, 1.

Bužek, V., S. L. Braunstein, M. Hillery, and D. Bruß, 1997, Phys. Rev. A **56**, 3446.

Bužek, V., and M. Hillery, 1996, Phys. Rev. A **54**, 1844.

Bužek, V., and M. Hillery, 1998, Phys. Rev. Lett. **81**, 5003.

Bužek, V., M. Hillery, and M. Bendik, 1998, Acta Phys. Slov. **48**, 177.

Bužek, V., M. Hillery, and R. F. Werner, 1999, Phys. Rev. A **60**, R2626.

Caves, C. M., 1982, Phys. Rev. D **26**, 1817.

Cerf, N. J., 1998, Acta Phys. Slov. **48**, 115.

Cerf, N. J., 2000a, Phys. Rev. Lett. **84**, 4497.

Cerf, N. J., 2000b, J. Mod. Opt. **47**, 187.

Cerf, N. J., M. Bourennane, A. Karlsson, and N. Gisin, 2002, Phys. Rev. Lett. **88**, 127902.

Cerf, N. J., T. Durt, and N. Gisin, 2002, J. Mod. Opt. **49**, 1355.

Cerf, N. J., and S. Iblisdir, 2000, Phys. Rev. A **62**, 040301.

Cerf, N. J., A. Ipe, and X. Rottenberg, 2000, Phys. Rev. Lett. **85**, 1754.

Cerf, N. J., O. Krüger, P. Navez, R. F. Werner, and M. M. Wolf, 2005, Phys. Rev. Lett. **95**, 070501.

Cerf, N. J., M. Lévy, and G. Van Assche, 2001, Phys. Rev. A **63**, 052311.

Chefles, A., and S. M. Barnett, 1999, Phys. Rev. A **60**, 136.

Cochrane, P. T., T. C. Ralph, and A. Dolinska, 2004, Phys. Rev. A **69**, 042313.

Collins, D., L. Diósi, N. Gisin, S. Massar, and S. Popescu, 2004, e-print quant-ph/0409221.

Csiszár, I., and J. Körner, 1978, IEEE Trans. Inf. Theory **24**, 339.

Cummins, H. K., C. Jones, A. Furze, N. F. Soffe, M. Mosca, J. M. Peach, and J. A. Jones, 2002, Phys. Rev. Lett. **88**, 187901.

Curty, M., and N. Lütkenhaus, 2004, Phys. Rev. A **69**, 042321.

D'Ariano, G. M., and C. Macchiavello, 2003, Phys. Rev. A **67**, 042306.

De Chiara, G., R. Fazio, C. Macchiavello, S. Montangero, and G. M. Palma, 2004, Phys. Rev. A **70**, 062308.

De Martini, F., V. Bužek, F. Sciarrino, and C. Sias, 2002, Nature (London) **419**, 815.

De Martini, F., V. Mussi, and F. Bovino, 2000, Opt. Commun. **179**, 581.

De Martini, F., D. Pelliccia, and F. Sciarrino, 2004, Phys. Rev. Lett. **92**, 067901.

De Riedmatten, H., I. Marcikic, V. Scarani, W. Tittel, H. Zbinden, and N. Gisin, 2004, Phys. Rev. A **69**, 050304(R).

Devetak, I., and A. Winter, 2005, Proc. R. Soc. London, Ser. A **461**, 207.

Dieks, D., 1982, Phys. Lett. **92A**, 271. (As a curiosity, the title reads *Communication by Electron-Paramagnetic-Res Devices*: the shortcut "EPR" in the title was spelled by the editors of the review as "Electron Paramagnetic Resonance" instead of, obviously, Einstein-Podolski-Rosen.).

Duan, L.-M., and G.-C. Guo, 1998, Phys. Rev. Lett. **80**, 4999.

Durt, T., and J. Du, 2004, Phys. Rev. A **69**, 062316.

Durt, T., and B. Nagler, 2003, Phys. Rev. A **68**, 042323.

Fan, H., H. Imai, K. Matsumoto, and X. B. Wang, 2003, Phys. Rev. A **67**, 022317.

Fan, H., K. Matsumoto, and M. Wadati, 2001, Phys. Rev. A **64**, 064301.

Fan, H., G. Weihs, K. Matsumoto, and H. Imai, 2002, Phys. Rev. A **66**, 024307.

Fasel, S., N. Gisin, G. Ribordy, V. Scarani, and H. Zbinden, 2002, Phys. Rev. Lett. **89**, 107901.

Filip, R., 2004, Phys. Rev. A **69**, 032309.

Fiuràšek, J., 2001, Phys. Rev. Lett. **86**, 4942.

Fiuràšek, J., 2003, Phys. Rev. A **67**, 052314.

Fiuràšek, J., R. Filip, and N. J. Cerf, 2005, e-print quant-ph/0505212.

Fiuràšek, J., S. Iblisdir, S. Massar, and N. J. Cerf, 2002, Phys. Rev. A **65**, 040302.

Fuchs, C. A., 2002, e-print quant-ph/0205039.

Fuchs, C. A., N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, 1997, Phys. Rev. A **56**, 1163.

Ghirardi, G. C., and T. Weber, 1983, Nuovo Cimento Soc. Ital. Fis., B **78**, 9.

Gisin, N., 1998, Phys. Lett. A **242**, 1.

Gisin, N., and S. Massar, 1997, Phys. Rev. Lett. **79**, 2153.

Gisin, N., and S. Popescu, 1999, Phys. Rev. Lett. **83**, 432.

Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden, 2002, Rev. Mod. Phys. **74**, 145.

Griffiths, R. B., and C.-S. Niu, 1997, Phys. Rev. A **56**, 1173.

Grosshans, F., 2002, Ph.D. thesis (Université Paris 11, Numéro 7080).

Grosshans, F., and P. Grangier, 2002, Phys. Rev. Lett. **88**, 057902.

Helstrom, C. W., 1976, *Quantum Detection and Estimation Theory* (Academic, New York).

Herbert, N., 1982, Found. Phys. **12**, 1171.

Hillery, M., M. Ziman, and V. Bužek, 2004, Phys. Rev. A **69**, 042311.

Holevo, A. S., 1973, Probl. Inf. Transm. **9**, 177.

Holevo, A. S., 1982, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam).

Huang, Y.-F., W.-L. Li, C.-F. Li, Y.-S. Zhang, Y.-K. Yiang, and G.-C. Guo, 2001, Phys. Rev. A **64**, 012315.

Iblisdir, S., A. Acín, and N. Gisin, 2005, e-print quant-ph/0505152.

Iblisdir, S., A. Acín, N. Gisin, J. Fiuràšek, R. Filip, and N. J. Cerf, 2004, e-print quant-ph/0411179.

Irvine, W. T. M., A. Lamas Linares, M. J. A. de Dood, and D. Bouwmeester, 2004, Phys. Rev. Lett. **92**, 047902.

Kaszlikowski, D., A. Gopinathan, Y. C. Liang, L. C. Kwek, and B.-G. Englert, 2004, Phys. Rev. A **70**, 032306.

Kempe, J., C. Simon, and G. Weihs, 2000, Phys. Rev. A **62**, 032302.

Keyl, M., 2002, Phys. Rep. **369**, 431.

Keyl, M., and R. F. Werner, 1999, J. Math. Phys. **40**, 3283.

Knill, E., R. Laflamme, and G. J. Milburn, 2001, Nature (London) **409**, 46.

Kraus, K., 1983, *States, Effects, and Operations* (Springer Verlag, Berlin).

Kraus, B., N. Gisin, and R. Renner, 2005, Phys. Rev. Lett. **95**, 080501.

Lamas-Linares, A., C. Simon, J. C. Howell, and D. Bouwmeester, 2002, Science **296**, 712.

Lamoureux, L.-P., P. Navez, J. Fiuràšek, and N. J. Cerf, 2004, Phys. Rev. A **69**, 040301(R).

Lindblad, G., 2000, J. Phys. A **33**, 5059.

Mana, P. G. L., A. Maansson, and G. Björk, 2005, e-print quant-ph/0505229.

Mandel, L., 1983, Nature (London) **304**, 188.

Masanes, L., A. Acín, and N. Gisin, 2005, e-print quant-ph/0508016.

Massar, S., and S. Popescu, 1995, Phys. Rev. Lett. **74**, 1259.

Milman, P., H. Ollivier, and J. M. Raimond, 2003, Phys. Rev. A **67**, 012314.

Milonni, P. W., and M. L. Hardies, 1982, Phys. Lett. **92A**, 321.

Murao, M., D. Jonathan, M. B. Plenio, and V. Vedral, 1999, Phys. Rev. A **59**, 156.

Navez, P., and N. J. Cerf, 2003, Phys. Rev. A **68**, 032313.

Niederberger, A., V. Scarani, and N. Gisin, 2005, Phys. Rev. A **71**, 042316.

Niu, C.-S., and R. B. Griffiths, 1998, Phys. Rev. A **58**, 4377.

Niu, C.-S., and R. B. Griffiths, 1999, Phys. Rev. A **60**, 2764.

Pati, A. K., 1999, Phys. Rev. Lett. **83**, 2849.

Pelliccia, D., V. Schettini, F. Sciarrino, C. Sias, and F. De Martini, 2003, Phys. Rev. A **68**, 042306.

Peres, A., 1995, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht).

Peres, A., 2002, e-print quant-ph/0205076.

Plenio, M., and V. Vitelli, 2001, Contemp. Phys. **42**, 25.

Reck, M., A. Zeilinger, H. J. Bernstein, and P. Bertani, 1994, Phys. Rev. Lett. **73**, 58.

Renner, R., N. Gisin, and B. Kraus, 2005, Phys. Rev. A **72**, 012332.

Renner, R., and R. König, 2004, e-print quant-ph/0403133.

Ricci, M., F. Sciarrino, C. Sias, and F. De Martini, 2004, Phys. Rev. Lett. **92**, 047901.

Scarani, V., A. Acín, G. Ribordy, and N. Gisin, 2004, Phys. Rev. Lett. **92**, 057901.

Scarani, V., and N. Gisin, 2001, Phys. Rev. A **65**, 012311.

Shimoda, K., H. Takahasi, and C. H. Townes, 1957, J. Phys. Soc. Jpn. **12**, 686.

Shor, P. W., and J. Preskill, 2000, Phys. Rev. Lett. **85**, 441.

Simon, C., 2001, private communication.

Simon, C., V. Bužek, and N. Gisin, 2001, Phys. Rev. Lett. **87**, 170405.

Simon, C., G. Weihs, A. Zeilinger, 2000, Phys. Rev. Lett. **84**, 2993.

Terhal, B. M., A. C. Doherty, and D. Schwab, 2003, Phys. Rev. Lett. **90**, 157903.

Thew, R., A. Acín, H. Zbinden, and N. Gisin, 2004, Quantum Inf. Comput. **4**, 93.

Townes, C. H., 2002, *How the Laser Happened* (Oxford University Press, Oxford).

Werner, R. F., 1998, Phys. Rev. A **58**, 1827.

Wigner, E. P., 1961, "The probability of the existence of a self-reproducing unit," in *The Logic of Personal Knowledge: Essays Presented to Michael Polanyi on his Seventieth Birthday* (Routledge & Kegan Paul, London). Reprinted in E. P. Wigner, 1967, *Symmetries and Reflections* (Indiana University Press, Bloomington), and in 1997, *The Collected Works of Eugene Paul Wigner*, Part A, Vol. III (Springer-Verlag, Berlin).

Wootters, W. K., and B. D. Fields, 1989, Ann. Phys. (N.Y.) **191**, 363.

Wootters, W. K., and W. H. Zurek, 1982, Nature (London) **299**, 802.

Yuen, H. P., 1986, Phys. Lett. **113A**, 405.

Zou, X. B., K. Pahlke, and W. Mathis, 2003, Phys. Rev. A **67**, 024304.