Multipartite asymmetric quantum cloning

S. Iblisdir,[1] A. Acín,[2] N. J. Cerf,[3] R. Filip,[4] J. Fiurášek,[3,4] and N. Gisin[1]
[1]*GAP-Optique, University of Geneva, 20 rue de l'Ecole-de-Médecine, CH-1211, Switzerland*
[2]*ICFO-Institut de Ciències Fotòniques, Jordi Girona 29, 08034 Barcelona, Spain*
[3]*QUIC, Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Brussels, Belgium*
[4]*Department of Optics, Palacký University, 17. listopadu 50, 77200 Olomouc, Czech Republic*
(Received 13 December 2004; published 26 October 2005)

We investigate the optimal distribution of quantum information over multipartite systems in asymmetric settings. We introduce cloning transformations that take N identical replicas of a pure state in any dimension as input and yield a collection of clones with nonidentical fidelities. As an example, if the clones are partitioned into a set of M_A clones with fidelity F^A and another set of M_B clones with fidelity F^B, the trade-off between these fidelities is analyzed, and particular cases of optimal $N \rightarrow M_A + M_B$ cloning machines are exhibited. We also present an optimal $1 \rightarrow 1+1+1$ cloning machine, which is an example of a tripartite fully asymmetric cloner. Finally, it is shown how these cloning machines can be optically realized.

DOI: 10.1103/PhysRevA.72.042328 PACS number(s): 03.67.−a, 03.65.−w, 42.50.Dv

A most intriguing feature of quantum mechanics is the impossibility to clone perfectly the state of a quantum system [1], generally referred to as the "no-cloning theorem." This impossibility, which is deeply related to the impossibility of superluminal communication [2], marks a fundamental difference between quantum and classical information, and has far-reaching implications. It puts strong limitations on the way we can protect quantum information [3] and is related to another "no-go" result of quantum mechanics, namely the impossibility to acquire full information about the state of a quantum system from a finite number of copies [4]. Although it may first sound negative, this no-cloning theorem can be turned as an advantage, as beautifully demonstrated by quantum cryptography. Two parties, willing to communicate privately, can exploit this impossibility to securely encode classical information in quantum systems. Any intervention of an eavesdropper causes a disturbance, making it visible (see, for example, [5] and references therein).

One then understands the importance of going beyond the no-cloning theorem and to formulate quantitatively the impossibility of cloning, that is, to address the problem: "*What is the best possible operation to produce approximate copies of a given quantum state*?" The simplest instance of this problem is the duplication of a qubit, as was considered in [6] and demonstrated experimentally in [7]. Many generalizations and variants have followed, such as the issue of producing M clones from N replicas of a qubit [8], the generalization to *qudits* (d level quantum systems) [9–11] and continuous-variable systems [12], the cloning of nonidentical states [13], or nonuniversal cloning [14]. Much attention has also been devoted to asymmetric $1 \rightarrow 1+1$ cloning machines, which produce two clones with different fidelities F^A and F^B [10,15]. This allows, for instance, one to investigate the trade-off between the information obtained by an eavesdropper and the disturbance of the receiver's state when cloning is used as an attack on quantum key distribution.

The present work introduces the concept of asymmetric cloning in a multipartite situation. A general asymmetric $N \rightarrow M_A + \cdots + M_P$ cloning machine can be defined as a transformation that produces $M = \Sigma_j M_j$ clones out of N identical replicas of an unknown pure state, such that the clones are partitioned into P parties, consisting of $\{M_A, \ldots, M_P\}$ clones having the fidelities $\{F^A, \ldots, F^P\}$. We want to characterize the trade-off between these fidelities. Such machines have at least two applications. First, some $N \rightarrow M_A + M_B$ cloning machines have been proven to be a useful tool when investigating the security of some quantum key distribution schemes [16]. Second, in the case where $M_A = N$ and $M_B \rightarrow \infty$, this allows us to study the trade-off between the gain of knowledge about the state of a quantum system and the disturbance undergone by this system. More generally, these machines can be used to elucidate how quantum information can be distributed unequally over many parties.

In this paper, we illustrate this general scenario of multipartite asymmetric cloning with two examples, namely (i) the optimal $1 \rightarrow 1+n$ qubit cloning machines, and (ii) the optimal $1 \rightarrow 1+1+1$ *qudit* cloning machines. In both cases, an optical scheme realizing the optimal cloning based on parametric down-conversion is exhibited in the case of qubits. A general analysis of multipartite asymmetric cloning going beyond these examples will be reported in [17,18].

(a) *Preliminaries.* The cloning operation is described by a trace-preserving completely positive (CP) map $\mathcal{S}$ [9]. We characterize the quality of the clones with single-clone fidelities. For the first set of clones, which we label A, the single-clone fidelity reads

$$F^A(\mathcal{S}) = \min_{\psi \in \mathcal{H}} \min_{1 \leq k \leq M_A} \langle \psi | \mathrm{Tr}'_k [\mathcal{S}(|\psi^{\otimes N}\rangle\langle\psi^{\otimes N}|)] | \psi \rangle .$$

In this expression, Tr'_k denotes the partial trace over all clones but the kth in the first set. A similar expression holds for the single-clone fidelity $F^B(\mathcal{S})$ of the second set of clones B, etc. In the case where there are only two sets of clones, A and B, the problem of finding the optimal $N \rightarrow M_A + M_B$ asymmetric cloner simply boils down to maximizing $F^B(\mathcal{S})$ for a given value of $F^A(\mathcal{S})$. This calculation, as well as the proof of optimality, will be presented in detail in [17,18]. Here, we only sketch the idea behind this optimization. Let $|\psi\rangle$ denote the state of each original we want to clone. As

demonstrated in [11], the effect of an optimal $N \to M$ symmetric cloning machine for *qudits* is to produce clones whose individual state reads $\rho = \eta|\psi\rangle\langle\psi| + (1-\eta)\mathbb{1}/d$, for some constant η called the "shrinking" factor. This isotropy property results from the fact that no state is preferred by an optimal universal cloning machine. Therefore the quality of the cloning process is completely characterized by η. This also applies to *asymmetric* universal cloning. If we require all the M_A clones to be of quality η^A, and all the M_B clones to be of quality η^B, then the problem of optimal asymmetric cloning reduces to finding some tight relation between η^A and η^B. This can be done by exploiting the same techniques as those used in [11] for symmetric cloners, that is, the Stinespring representation of CP maps, the U(d)-covariance, and permutation invariance. As an example of this technique, we treat below the $1 \to 1+n$ cloning of qubits. Alternatively, using the isomorphism between CP maps and positive semidefinite operators, the optimal asymmetric cloning machines can be found by analyzing the eigenstates and eigenvalues of certain operators. This second approach is illustrated below on the example of the $1 \to 1+1+1$ cloning of *qudits*.

(b) *Optimal* $1 \to 1+n$ *universal cloning of qubits.* According to the Clebsch-Gordan series $j_1 \otimes j_2 \approx |j_1 - j_2| \oplus \cdots \oplus (j_1 + j_2)$, the Hilbert space associated to $n+1$ qubits decomposes into irreducible subspaces as $\mathcal{H}^+_{n+1} \oplus \mathcal{H}^+_{n-1}$. Let S_{n+1} and S_{n-1} denote the corresponding projectors. We have found that optimal $1 \to 1+n$ machines are of the form

$$T{:}\rho \to (\alpha^* S_{n+1} + \beta^* S_{n-1})(\rho \otimes \mathbb{1}^{\otimes n})(\alpha S_{n+1} + \beta S_{n-1}).$$

This form naturally generalizes symmetric cloners found in [9]. The corresponding fidelities can be conveniently written as

$$F^A = 1 - \frac{2}{3}y^2, \quad F^B = \frac{1}{2} + \frac{1}{3n}[y^2 + \sqrt{n(n+2)}xy], \qquad (1)$$

where $x^2 + y^2 = 1$. [The relation between (α, β) and (x, y) is irrelevant for our discussion.] Note that these expressions are only valid for $n > 1$; for $n = 1$, the optimal cloning machines are those discussed in [10,15]. One readily checks that imposing $F^A = 1$ implies $F^B = 1/2$. This is consistent with the idea that in order to prepare a perfect clone, one has to take it from the input, which therefore cannot interact with any system [19]. Then, no quantum information is available to prepare the n extra clones, and the best one can do is to prepare n random states with fidelity 1/2. If, instead, one requires the n clones to have the fidelity of an optimal symmetric $1 \to n$ cloning machine, namely $F^B = (2n+1)/(3n)$, one finds $F^A = (2n+1)/[3(n+1)]$. Interestingly, this fidelity is larger than 1/2 for $n > 1$: not all quantum information needs to be used to produce the n optimal clones, and some quantum information remains to prepare a nontrivial $n+1$th clone.

This $1 \to 1+n$ cloner is also interesting in the limit of large n in the context of the connection between cloning and state estimation [4,8]. For universal symmetric cloning, it is known that there is a one-to-one correspondence between the $n \to \infty$ cloning machines and state estimation devices [20]. Such a relation still holds in the asymmetric case. Following the lines of [20], one finds that, in the limit $n \to \infty$, asymmetric $1 \to 1+n$ cloning machines interpolate between a (trivial) machine, leaving the quantum system unchanged, and a fully measuring device, estimating destructively the input state. Indeed, for $n \to \infty$, Eqs. (1) become

$$F^A = 1 - \frac{2}{3}y^2, \quad F^{\text{meas}} = \frac{1}{2} + \frac{1}{3}y\sqrt{1-y^2}, \qquad (2)$$

where only the range $0 \leqslant y \leqslant 1/\sqrt{2}$ is relevant. If $F^A = 1$, then one finds $F^{\text{meas}} = 1/2$, which means that no information can be gained if the input state is unperturbed. The maximum value of F^{meas} is 2/3, which is consistent with [21]. In that case, of course, $F^A = 2/3$. In between these two cases, Eqs. (2) express the optimal trade-off between the knowledge gained on a system and the disturbance effected by the measurement. This trade-off had previously been studied in the form of an inequality [22]. Our machine provides a concrete means to realize measurements saturating this inequality.

(c) *Optimal* $1 \to 1+1+1$ *universal cloning of qudits.* We now consider fully asymmetric tripartite universal cloning machines in dimension d, which produce clones A, B, and C with respective fidelities F^A, F^B, and F^C. The optimal cloners should be such that for a given pair of fidelities (say, F^A and F^B), the fidelity of the third clone (F^C) is maximal. This is equivalent to maximizing a convex mixture of the fidelities, $F = aF^A + bF^B + cF^C$, for fixed $a, b, c \geqslant 0$ with $a+b+c = 1$. The tripartite asymmetry is then controlled by the ratios a/b and a/c.

The optimal cloning transformation can be determined by exploring the isomorphism between trace-preserving CP maps $\mathcal{S}$ and positive semidefinite operators S on the tensor product of input and output Hilbert spaces. The mean fidelity F^A of the first clone averaged over all input states $|\psi\rangle$ can be expressed as $F^A = \text{Tr}[SL_A]$, where $L_A = \int_\psi \psi^T_{\text{in}} \otimes \psi_A \otimes \mathbb{1}_B \otimes \mathbb{1}_C d\psi$, T stands for transposition and $\psi = |\psi\rangle\langle\psi|$. The fidelities F^B and F^C can be expressed similarly, and one has to maximize $F = \text{Tr}[SL]$, where $L = aL_A + bL_B + cL_C$. The fidelity F is upper bounded by the maximum eigenvalue $\lambda_{\max}$ of L, $F \leqslant d\lambda_{\max}$ [23]. This bound happens to be tight here, and is saturated by the optimal cloner. The operator S describing this cloner is therefore proportional to the projector onto the subspace spanned by the eigenstates of L with eigenvalue $\lambda_{\max}$.

A unitary implementation of this tripartite asymmetric cloner requires two ancillas, E and F, so that any pure input state $|\psi\rangle$ transforms according to

$$\begin{aligned} |\psi\rangle \to \mathcal{C}[&\alpha|\psi\rangle_A(|\Phi^+\rangle_{BE}|\Phi^+\rangle_{CF} + |\Phi^+\rangle_{BF}|\Phi^+\rangle_{CE}) \\ &+ \beta|\psi\rangle_B(|\Phi^+\rangle_{AE}|\Phi^+\rangle_{CF} + |\Phi^+\rangle_{AF}|\Phi^+\rangle_{CE}) \\ &+ \gamma|\psi\rangle_C(|\Phi^+\rangle_{AE}|\Phi^+\rangle_{BF} + |\Phi^+\rangle_{AF}|\Phi^+\rangle_{BE})]. \end{aligned} \qquad (3)$$

Here, $\mathcal{C} = \sqrt{d/[2(d+1)]}$ is a normalization constant, $|\Phi^+\rangle = d^{-1/2}\sum_{j=1}^d |j\rangle|j\rangle$ is a maximally entangled state of two *qudits*, and α, β, $\gamma \geqslant 0$ obey

$$\alpha^2 + \beta^2 + \gamma^2 + \frac{2}{d}(\alpha\beta + \alpha\gamma + \beta\gamma) = 1. \qquad (4)$$

The transformation (3) is universal, that is, the single-clone fidelities do not depend on the input state and can be ex-

pressed in terms of the coefficients α, β, and γ as

$$F^A = 1 - \frac{d-1}{d}\left[\beta^2 + \gamma^2 + \frac{2\beta\gamma}{d+1}\right],$$

$$F^B = 1 - \frac{d-1}{d}\left[\alpha^2 + \gamma^2 + \frac{2\alpha\gamma}{d+1}\right],$$

$$F^C = 1 - \frac{d-1}{d}\left[\alpha^2 + \beta^2 + \frac{2\alpha\beta}{d+1}\right]. \quad (5)$$

In the special case where $\gamma=0$, the expressions of F^A and F^B exactly coincide with those for the $1\rightarrow 1+1$ asymmetric cloners found in [10,15]. This actually confirms the optimality of these cloners, which was only conjectured previously for $d>2$. Note that the third clone has a fidelity F^C exceeding $1/d$ here, which is again related to the information left in the anticlones.

(d) *Optical implementations.* We now focus on optical implementations in which the mechanism responsible for cloning is stimulated emission [24]. The optical scheme consists of a parametric down-conversion (PDC) process stimulated by N identical photons injected in the signal mode. Taking pulsed type-II frequency degenerated PDC whose Hamiltonian reads $H=\gamma(a^\dagger_{VS}a^\dagger_{HI}-a^\dagger_{HS}a^\dagger_{VI})+\mathrm{H.c.}$, and assuming that the photon to be cloned is in the state $(\alpha a^\dagger_{VS}+\beta a^\dagger_{HS})|\mathrm{vac}\rangle$ with $|\mathrm{vac}\rangle$ denoting the vacuum state, one obtains for the state after the crystal

$$|\psi_s\rangle = e^{-iHt}(\alpha a^\dagger_{VS} + \beta a^\dagger_{HS})^N|\mathrm{vac}\rangle. \quad (6)$$

Postselecting the events when M photons are detected in the signal mode, one recovers the optimal fidelities of the symmetric $N\rightarrow M$ cloning machine for qubits [24]. Note that when M photons are observed in the signal mode, N of them come from the initial state while $M-N$ were produced in the crystal, which means that there are $M-N$ photons in the idler mode too (these are the anticlones). This scheme can be modified in order to implement the asymmetric $1\rightarrow 1+1$ machine [25]. After a successful $1\rightarrow 2$ symmetric cloning (that is, when one photon pair is generated), the two clones are split at a first beam splitter, and one of them is combined with the anticlone at a second beam splitter of transmittance T in order to break the symmetry between the clones. Long but straightforward algebra shows that the fidelities at the modes A and B, depending on T, are those of the $1\rightarrow 1+1$ asymmetric cloning machine [10,15].

This modified scheme can be extended to implement the $1\rightarrow 1+2$ asymmetric cloning machine introduced above, as shown in Fig. 1(a). (The case $n>2$ will be discussed in subsequent papers.) The idea is again to postselect the events when there are five photons (three in the signal mode and two in the idler mode) and then to combine some of the signal photons with idler photons at a beam splitter of transmittance T. By postselecting the cases where $M_A=1$ and $M_B=2$, one gets the fidelities

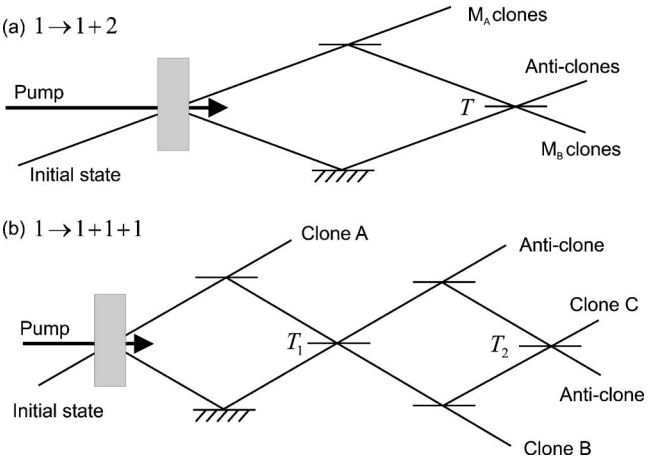

FIG. 1. Optical implementation of (a) the $1\rightarrow 1+2$ and (b) the $1\rightarrow 1+1+1$ optimal asymmetric cloning machines.

$$F^A = \frac{4T^2-4T+7}{12T^2-12T+9}; \quad F^B = \frac{8T^2-4T+3}{12T^2-12T+9} \quad (7)$$

as shown in Fig. 2 (solid line, for $1/2\leqslant T\leqslant 1$). The optimal symmetric machine is recovered for $T=1$. If T decreases, the quality of the first clone in mode A increases, while the quality of the two clones in mode B decreases. When $T=1/2$, all the information in mode B is lost, and a perfect copy of the initial state is obtained in mode A. The trade-off between the two fidelities exactly follows the optimal $1\rightarrow 1+2$ machine predicted by Eq. (1). However, it is not possible to recover the entire curve because Eq. (7) implies $F^A\geqslant F^B$. To get the remaining $1\rightarrow 1+2$ cloning machines for which $F^A\leqslant F^B$, one uses the same setup but postselects the events with $M_A=2$ and $M_B=1$. We then find the fidelities

$$F^A = \frac{7T^2-4T+4}{9T^2-12T+12}; \quad F^B = \frac{3T^2-4T+8}{9T^2-12T+12}. \quad (8)$$

The corresponding curve is also shown in Fig. 2 (dashed line). For example, when $T=2/3$ the two photons in mode A

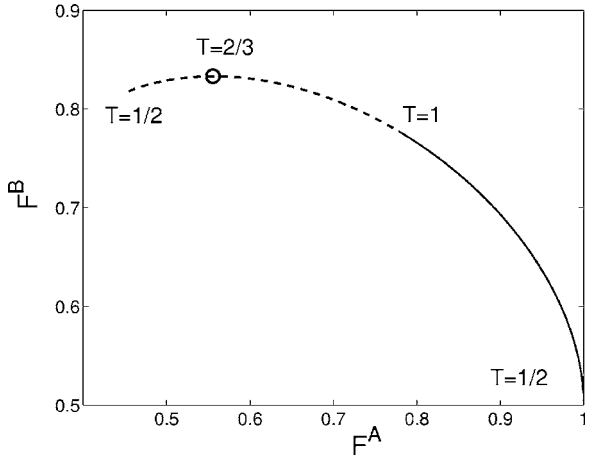

FIG. 2. Clone fidelities for the optical implementation of the $1\rightarrow 1+2$ optimal machine. The solid (dashed) line represents the case when $M_A=1$ and $M_B=2$ ($M_A=2$ and $M_B=1$) photons are postselected.

have a fidelity $5/9$, as in the case of the symmetric $1\rightarrow 2$ cloner, while the photon in mode B has fidelity $5/6$, slightly larger than $1/2$ as discussed above.

Let us notice that the output mode containing the two photons that have the same fidelity are not in a proper two-qubit state. Rather, we have two indistinguishable photons distributed amongst two polarization modes. This is a generic property of the cloning schemes based on parametric down conversion [26]; but as usual [13], upon using an array of beam-splitters, one can probabilistically separate the photons and get a proper two-qubit state. The output photons can then be detected, either destructively using photodetectors, or nondestructively with a photon nondemolition measurement device.

This optical scheme can also be adapted to realize the optimal $1\rightarrow 1+1+1$ cloning transformation, see Fig. 1(b). Here, the output of a symmetric $1\rightarrow 3$ machine is made asymmetric by combining some of the clones with anticlones at two beam splitters, with transmittance T_1 and T_2. After patient calculation, one can check that the obtained fidelities $F^A \geqslant F^B \geqslant F^C$, depending on T_1 and T_2, are optimal. The three fidelities are equal when $T_1=T_2=1$. Other interesting limiting cases are $(F^A,F^B,F^C)=(1,1/2,1/2)$ when $T_1=1/2$, while taking $T_2=1$ gives Eqs. (7) for the $1\rightarrow 1+2$ case. This construction can easily be generalized further.

In summary, we have introduced the concept of multipartite asymmetric quantum cloning machines, and have illustrated it with two examples. These devices have several remarkable properties. One of them is that if one wants to produce n clones from an input with a fidelity which is as high as possible, some quantum information still remains to produce a nontrivial $n+1$th clone. Multipartite cloning machines provide a new tool for analyzing the security of multipartite quantum cryptography, and the trade-off between disturbance and information gain. We have presented feasible optical realizations of our examples of optimal multipartite cloners. We have then seen that the noise that characterizes these cloning machines is related to the unavoidable spontaneous emission that necessarily accompanies stimulated emission. One is tempted to conjecture that all the $N\rightarrow M_1+\cdots+M_P$ cloning machines for qubits are only limited by spontaneous emission, and can therefore be implemented by splitting and then recombining the clones and anticlones produced by stimulated emission using a series of beam splitters, in a similar way as in Fig. 1. The corresponding fidelities would define the optimal distribution of a qubit among several parties.

Financial support by the EU projects SECOQC, RESQ, and CHIC is acknowledged. N.J.C. and J.F. also acknowledge support from the Communauté Française de Belgique under Grant No. ARC 00/05-251, and from the IUAP programme of the Belgian government under Grant No. V-18. J.F. and R.F. also acknowledge support from Grant No. MSM 6198959213 of the Czech Ministry of Education, and A.A. acknowledges support from the Spanish MCYT under "Ramón y Cajal" grant.

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[2] D. Dieks, Phys. Lett. **92**, 271 (1982); N. Gisin, Phys. Lett. A **242**, 1 (1998).
[3] J. Preskill, *Quantum Information and Computation, Lecture Notes in Physics* (1998).
[4] D. Bruss and C. Macchiavello, Phys. Lett. A **253**, 249 (1999).
[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[6] V. Buzek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[7] A. Lamas-Linares, C. Simon, J. C. Howell, and D. Bouwmeester, Science **296**, 712 (2002); S. Fasel, N. Gisin, G. Ribordy, V. Scarani, and H. Zbinden, Phys. Rev. Lett. **89**, 107901 (2002); F. DeMartini, D. Pelliccia, and F. Sciarrino, *ibid.* **92**, 067901 (2004); M. Ricci, F. Sciarrino, C. Sias, and F. DeMartini, *ibid.* **92**, 047901 (2004); W. T. M. Irvine, A. L. Linares, M. J. A. de Dood, and D. Bouwmeester, *ibid.* **92**, 047902 (2004).
[8] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997); D. Bruss, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, Phys. Rev. A **57**, 2368 (1998).
[9] R. F. Werner, Phys. Rev. A **58**, 1827 (1998); V. Buzek and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).
[10] N. J. Cerf, Acta Phys. Slov. **48**, 115 (1998).
[11] M. Keyl and R. F. Werner, J. Math. Phys. **40**, 3283 (1998).
[12] N. J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000); N. J. Cerf and S. Iblisdir, Phys. Rev. A **62**, 040301(R) (2000).
[13] J. Fiurasek, S. Iblisdir, S. Massar, and N. J. Cerf, Phys. Rev. A **65**, 040302(R) (2002).
[14] G. M. D'Ariano and P. Lo Presti, Phys. Rev. A **64**, 042308 (2001).
[15] N. J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000); N. J. Cerf, J. Mod. Opt. **47**, 187 (2000); C.-S. Niu and R. B. Griffiths, Phys. Rev. A **58**, 4377 (1998).
[16] A. Acín, N. Gisin, and V. Scarani, Phys. Rev. A **69**, 012309 (2004); M. Curty and N. Lütkenhaus, Phys. Rev. A **69**, 042321 (2004).
[17] S. Iblisdir, A. Acín, and N. Gisin, e-print quant-ph/0505152.
[18] J. Fiurasek, R. Filip, and N. J. Cerf, eprint quant-ph/0505212.
[19] R. Jozsa, e-print quant-ph/0204153.
[20] D. Bruss, A. Ekert, and C. Macchiavello, Phys. Rev. Lett. **81**, 2598 (1998).
[21] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
[22] K. Banaszek, Phys. Rev. Lett. **86**, 1366 (2001).
[23] J. Fiurášek, Phys. Rev. A **64**, 062310 (2001).
[24] C. Simon, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **84**, 2993 (2000).
[25] R. Filip, Phys. Rev. A **69**, 032309 (2004).
[26] D. E. Browne and M. B. Plenio, Phys. Rev. A **66**, 042307 (2002).