Optimal real state cloning in d dimensions

Wen-Hai Zhang,[1,2] Tao Wu,[1,3] Liu Ye,[1] and Jie-Lin Dai[2]
[1] *School of Physics & Material Science, Anhui University, Hefei 230039, China*
[2] *Department of Physics & Electronic Engineering, Anhui Institute of Education, Hefei 230061, China*
[3] *Department of Physics, HuYang Normal College, HuYang 236041, China*

(Received 23 October 2006; revised manuscript received 1 March 2007; published 20 April 2007)

We present an explicit transformation of optimal asymmetric $1\to 2$ real state cloning in two dimensions. Interestingly, the distribution of the two fidelities of the cloning is the same as its counterpart in optimal asymmetric phase-covariant cloning. We also generalize the cloner to the d-dimensional case and derive the explicit transformation of the optimal symmetric $1\to 2$ real state cloning in the d-dimensional system. The maximal fidelity of two clones obtained coincides with the theoretical value [P. Vavez and N. J. Cerf, Phys. Rev. A **68**, 032313 (2003)].

DOI: 10.1103/PhysRevA.75.044303 PACS number(s): 03.67.−a, 02.50.Le

Quantum information emerges from the fruitful combination of quantum mechanics and information technology. In recent years, remarkably promising applications such as quantum cryptography, quantum cloning, quantum teleportation, quantum games, and quantum computers were implemented experimentally [1–5]. The no-cloning theorem [6] demonstrating the impossibility of perfectly cloning an arbitrary quantum state guarantees the security of the quantum key distribution (KQD) protocols [1], such as the Bennett-Brassard 1984 (BB84) protocol [7]. Since an exact copy cannot be reached, much more attention has been paid to approximate quantum cloning first introduced in a seminal paper of Bužek and Hillery [8]. For the copied quantum state in a d-dimensional Hilbert space defined as $|\psi\rangle=\Sigma_{i=0}^{d-1}\alpha_i e^{i\varphi_i}|i\rangle$ with α_i being real variables satisfying the normalization condition $\Sigma_{i=0}^{d-1}\alpha_i^2=1$ and $\varphi_i\in[0,2\pi)$, three types of quantum cloning machines nominated by different input states have been extensively investigated. If α_i and φ_i are completely unknown, it is so-called universal quantum cloning (UQC) [8,9]; if α_i are known (taking $\alpha_i=1/\sqrt{d}$) and φ_i are unknown, phase-covariant cloning (PCC) [10,11]; if α_i are unknown and φ_i are known (taking $\varphi_i=0$), real state cloning (RSC) [10,12].

In previous contributions, most works concentrated on optimal symmetric quantum cloning closely related to quantum cryptography [1]. The term "symmetric" means that the fidelity of each copy is equal and "optimal" naturally means that the fidelity is the highest (maximal). The emergence of the concept of optimal asymmetric quantum cloning [13,14] sheds light on the quantum cloning theory that quantum cloning machines can be regarded as well-defined distributors of quantum information from initial systems to final ones after quantum evolution. Transferability and reversibility of the quantum information of the quantum systems are discussed in Refs. [15–19]. For the simplest case of two clones in optimal asymmetric cloning, "asymmetric" means that the fidelities of copies are not necessary equal and "optimal" means that the fidelity of one copy must be highest for a given fidelity of the other [or the optimal match (trade-off) between the fidelities]. Certainly, optimal asymmetric cloning covers the optimal symmetric case. Recently, the explicit transformation of optimal asymmetric $1\to 1+1+1$ UQC (AUQC) in d dimensions [14] is derived. In experiment, optimal $1\to 2$ AUQC and telecloning [20] have been realized. So-called optimal economical phase-covariant quantum cloning machine (EPCC) working without ancilla was first proposed by Niu and Griffiths [21]. Later, this kind of cloner was further generalized by Fiurášek [22]. An experiment [23] using nuclear-magnetic-resonance (NMR) techniques has verified the transformation proposed in Ref. [22]. Recently, the EPCCM in d dimensions [24,25] has been further studied.

Optimal asymmetric cloning should be more efficient than its counterpart of optimal symmetric cloning in applications such as quantum cryptographic attacks or in some others to be discovered. More importantly, if three optimal asymmetric cloners of $N\to M$ in d dimensions [general APCC requires amplitudes $\alpha_i\in[0,1]$ known and φ_i unknown; the general ARSC requires $\varphi_i\in[0,2\pi)$ known and α_i unknown] are derived completely, maybe quantifying the information of a quantum state with the discrete variables by the amplitudes and the phase factors would be analyzed. Three optimal asymmetric cloners have an intimate relation to the foundations of quantum mechanics. Up to now, many investigations of optimal UQC and optimal PCC have been presented in recent years. To the best of our knowledge, there have been very few studies (only two [10,12]) touching upon RSC. In this paper we will consider this kind of cloner.

In this paper, we first present the explicit transformation of optimal $1\to 2$ ARSC in two dimensions as well as the expression of the two fidelities and then generalize this cloner to d dimensions to derive the explicit transformation of optimal $1\to 2$ SRSC. Interestingly, the distribution of the two fidelities of optimal ARSC coincides with that of optimal APCC in two dimensions [26]; in d dimensions, however, the fidelity of optimal $1\to 2$ SRSC is slightly higher than that of SPCC [11]. Moreover, the distribution of the two fidelities of ARSC is just as the same as that of optimal asymmetric Fourier-covariant cloning (AFCC) [27] in two dimensions, which sufficiently suggests that ARSC is another optimal eavesdropping as AFCC to the quantum cryptographic BB84 scheme [7]. We also discuss optimal eavesdropping to the quantum cryptographic BB84 protocol by use of ARSC.

This paper is organized as follows. We first review some previous contributions including AUQC, APCC, and SRSC. Then we present the derivation of optimal $1\to 2$ ARSC in two dimensions and generalize this cloner to d dimensions to derive optimal $1\to 2$ SRSC. Finally, we discuss the ARSC-based attack to the quantum cryptographic BB84 scheme. The paper ends with a summary.

First, we briefly review some previous contributions. If the input state takes the form of $|\psi\rangle_1^{(in)}=(|0\rangle+e^{i\varphi}|1\rangle)/\sqrt{2}$ with $\varphi\in[0,2\pi)$ unknown, the transformation of $1\to 2$ APCC in two dimensions can be expressed as [26]

$$|0\rangle_1|00\rangle_{2,A}\to(|000\rangle+p|011\rangle+q|101\rangle)_{1,2,A}/\sqrt{2},$$

$$|1\rangle_1|00\rangle_{2,A}\to(|111\rangle+p|100\rangle+q|010\rangle)_{1,2,A}/\sqrt{2},\qquad(1)$$

with $p,q\geq 0$ satisfying the constraint $p^2+q^2=1$. Here, we denote the subscripts 1 and 2, and A as the input state (the copied state $|\psi\rangle_1^{(in)}$), the blank copy, and the ancilla. The corresponding fidelities are ${}^2F_1^{(APCC)}=(1+p)/2$ and ${}^2F_2^{(APCC)}=(1+q)/2$. From the expressions of the two fidelities we can intuitively observe that the phase is covariant for PCC. In the case of $p=q=1/\sqrt{2}$, APCC becomes SPCC with ${}^2F_{1(2)}^{(SPCC)}=(1+1/\sqrt{2})/2\approx 0.854$ [10]. The concrete relation of the two fidelities of APCC can be expressed as ${}^2F_2^{(APCC)}=1/2+\sqrt{({}^2F_1^{(APCC)})[1-({}^2F_1^{(APCC)})]}$.

If one wants to clone the input state $|\psi\rangle_2^{(in)}=\alpha|0\rangle+\beta|1\rangle$ with α and β being real and unknown ($\alpha^2+\beta^2=1$), the transformation of optimal $1\to 2$ SRSC in two dimensions is presented as [10]

$$|000\rangle_{1,2,A}\to\left(\frac{1}{2}+\frac{1}{\sqrt{8}}\right)|000\rangle_{1,2,A}+\frac{1}{\sqrt{8}}(|01\rangle+|10\rangle)_{1,2}|1\rangle_A+\left(\frac{1}{2}-\frac{1}{\sqrt{8}}\right)|110\rangle_{1,2,A},$$

$$|100\rangle_{1,2,A}\to\left(\frac{1}{2}+\frac{1}{\sqrt{8}}\right)|111\rangle_{1,2,A}+\frac{1}{\sqrt{8}}(|10\rangle+|01\rangle)_{1,2}|0\rangle_A+\left(\frac{1}{2}-\frac{1}{\sqrt{8}}\right)|001\rangle_{1,2,A}.\qquad(2)$$

The two equal highest fidelities are ${}^2F_{1(2)}^{(SRSC)}=(1+1/\sqrt{2})/2\approx 0.854$ [10] which is equal to that of SPCC in two dimensions. This is the cloner we will investigate in this paper.

Next, we derive optimal $1\to 2$ ARSC in two dimensions. Parametrizing the cloning coefficients given by Eq. (2) first, we obtain

$$|000\rangle_{1,2,A}\to a|000\rangle_{1,2,A}+(b|01\rangle+c|10\rangle)_{1,2}|1\rangle_A+d|110\rangle_{1,2,A},$$

$$|100\rangle_{1,2,A}\to a|111\rangle_{1,2,A}+(b|10\rangle+c|01\rangle)_{1,2}|0\rangle_A+d|001\rangle_{1,2,A},\qquad(3)$$

with $a,b,c,d\geq 0$ satisfying the normalization condition $a^2+b^2+c^2+d^2=1$. The two fidelities can be calculated as

$${}^2F_1^{(ARSC)}=a^2+b^2+2\alpha^2\beta^2(d^2+c^2+2ab+2cd-a^2-b^2),$$

$${}^2F_2^{(ARSC)}=a^2+c^2+2\alpha^2\beta^2(b^2+d^2+2ac+2bd-a^2-c^2).\qquad(4)$$

Certainly, the two fidelities should be independent of the input state (α and β); the following equations thus must be satisfied:

$$d^2+c^2+2ab+2cd-a^2-b^2=0,$$

$$b^2+d^2+2ac+2bd-a^2-c^2=0.\qquad(5)$$

Solving the above equations, three solutions can be obtained as $\{a=-d,b=c\}$, $\{a=c,b=-d\}$, and $\{a=b+c+d\}$. The first solution implies the symmetric case because of $b=c$; that is, the transformation given by Eq. (3) does not change if we exchange the positions of particles 1 and 2. From the second solution $\{a=c,b=-d\}$, ${}^2F_1^{(ARSC)}=a^2+b^2=1/2$ and ${}^2F_2^{(ARSC)}=\max(2a^2)=1$ can be calculated as $a=c=1/\sqrt{2},b=-d=0$ under the reduced normalization condition $2a^2+2b^2=1$. Therefore, only the solution $\{a=b+c+d\}$ is reasonable. The two fidelities thus read

$${}^2F_1^{(ARSC)}=a^2+b^2,\quad {}^2F_2^{(ARSC)}=a^2+c^2.\qquad(6)$$

The two fidelities are constants determined by the cloning coefficients a, b, c, and d. But how can they reach the optimal match? Therefore, our tasks aim at finding the highest fidelity of one clone for a given fidelity of the other; that is, ${}^2F_2^{(ARSC)}$ (denoted as F_2 for convenience) should be maximal if set the value of ${}^2F_1^{(ARSC)}$ (denoted as F_1). After calculation we obtain

$$a=\frac{\sqrt{F_1-2\sqrt{F_1^3-F_1^4}}(F_1+2\sqrt{F_1^3-F_1^4})}{\sqrt{2}F_1(2F_1-1)},$$

$$b=\frac{1}{\sqrt{2}}\sqrt{F_1-2\sqrt{F_1^3-F_1^4}},$$

$$c=\frac{F_1(2F_1-1)(F_1-F_1^2+\sqrt{F_1^3-F_1^4})}{\sqrt{2}\sqrt{F_1-\sqrt{F_1^3-2F_1^4}}(F_1^2+\sqrt{F_1^3-F_1^4})},$$

$$d=\frac{\sqrt{F_1^3-F_1^4}\sqrt{F_1-2\sqrt{F_1^3-F_1^4}}}{\sqrt{2}F_1^2}.\qquad(7)$$

The fidelity ${}^2F_2^{(ARSC)}$ (denoted as F_2) of clone 2 reads

$$F_2=1/2+\sqrt{F_1(1-F_1)}.\qquad(8)$$

From Eq. (8), one can easily obtain ${}^2F_1^{(ARSC)},{}^2F_2^{(ARSC)}\in[1/2,1]$ due to ${}^2F_1^{(ARSC)}\leq 1,{}^2F_2^{(ARSC)}\geq 1/2$. Thus, we consider Eqs. (3) and (7) together with Eq. (8) as the standard form of ARSC in two dimensions. One can observe that ${}^2F_1^{(APCC)}=1/2$ cannot be satisfied by the cloning coefficient a given by Eq. (7). In this case, we have calculated the result—i.e., $(a=c=1/\sqrt{2},b=-d=0)\to({}^2F_1^{(ARSC)}=1/2,{}^2F_2^{(ARSC)}=1)$. For the sake of comparison between ARSC and APCC in two dimensions, we rewrite Eq. (1) as

$$|0\rangle_1|00\rangle_{2,A} \to (|000\rangle + \sqrt{2({}^2F_1^{(APCC)}) - 1}|011\rangle + \sqrt{2[1-({}^2F_1^{(APCC)})]}|101\rangle)_{1,2,A}/\sqrt{2},$$

$$|1\rangle_1|00\rangle_{2,A} \to (|111\rangle + \sqrt{2({}^2F_1^{(APCC)}) - 1}|100\rangle + \sqrt{2[1-({}^2F_1^{(APCC)})]}|010\rangle)_{1,2,A}/\sqrt{2}. \quad (9)$$

The fidelity of particle 2 is ${}^2F_2^{(APCC)}=1/2+\sqrt{({}^2F_1^{(APCC)})[1-({}^2F_1^{(APCC)})]}$ under the constraint ${}^2F_1^{(APCC)}, {}^2F_2^{(APCC)} \in [1/2,1]$. Strictly speaking, optimal asymmetric $1\to 2$ cloning should be represented by two conditions: (a) The coefficients p should be a function of F_1 (or F_2) and it is the same for q. (b) When fixing the fidelity of one clone, the other should reach maximal. One can observe the two conditions can be satisfied by APCC and ARSC.

Intuitively, the distributions of the fidelities of APCC and ARSC seem to imply the identity of the amplitudes and the phases in representing a quantum state, but this is not the case. We will show this in the following.

We now generalize SRSC to the d-dimensional case. If the input state in the form of $|\psi\rangle_3^{(in)}=\Sigma_{i=0}^{d-1}c_i|i\rangle$ with c_i being real and unknown and $\Sigma_{i=0}^{d-1}c_i^2=1$, the unitary transformation of ARSC can be written as

$$|i00\rangle_{1,2,A} \to \left(\alpha|ii\rangle + \beta\sum_{\substack{j=0\\j\neq i}}^{d-1}|jj\rangle\right)_{1,2}|i\rangle_A + \gamma\sum_{\substack{j=0\\j\neq i}}^{d-1}(|ji\rangle + |ij\rangle)_{1,2}|j\rangle_A, \quad (10)$$

with α, β, $\gamma \geq 0$ and the normalization condition $\alpha^2+(d-1)\beta^2+2(d-1)\gamma^2=1$. The corresponding fidelity of the two clones is calculated as

$$F=\sum_{i=0}^{d-1}c_i^4(A-C)+C+B, \quad (11)$$

where $A=\alpha^2-\beta^2+(d-2)\gamma^2$, $B=\beta^2+\gamma^2$, and $C=2\gamma(\alpha+\beta)+(d-2)\gamma^2$. Obviously, if the fidelity is independent of input states—e.g., c_i (implying $A-C=0$)—and it is the highest one [implying $F=\mathrm{Max}(C+B)$], the following equations then must be satisfied after combining the normalization conditions:

$$\alpha^2-\beta^2-2\gamma(\alpha+\beta)=0,$$

$$\alpha^2+(d-1)\beta^2+2(d-1)\gamma^2=1,$$

$$F=\mathrm{Max}[\beta^2+2\gamma(\alpha+\beta)+(d-1)\gamma^2]. \quad (12)$$

By use of the Lagrange multiplier we obtain the cloning coefficients as follows:

$$\alpha=(4+d+\sqrt{d^2+4d+20})[20+24d+5d^2+d^3+(6+3d+d^2)\sqrt{d^2+4d+20}]^{1/2},$$

$$\beta=2[20+24d+5d^2+d^3+(6+3d+d^2)\sqrt{d^2+4d+20}]^{1/2},$$

TABLE I. Comparison of the two fidelities of SRSC and SPCC in d dimensions and ${}^2F_{1(2)}^{(SRSC)}={}^2F_{1(2)}^{(SPCC)}$ only as $d=2$.

d	${}^2F_{1(2)}^{(SRSC)}$	${}^2F_{1(2)}^{(SPCC)}$
2	0.854	0.854
3	0.770	0.760
4	0.717	0.706
5	0.681	0.670
10	0.597	0.592

$$\gamma=\frac{1}{2}(2+d+\sqrt{d^2+4d+20})\times[20+24d+5d^2+d^3+(6+3d+d^2)\sqrt{d^2+4d+20}]^{1/2}. \quad (13)$$

The corresponding maximal fidelity reads

$${}^dF_{1(2)}^{(SRSC)}=1/2+(\sqrt{d^2+4d+20}-d+2)/4(d+2). \quad (14)$$

The fidelity we obtained coincides with the theoretic value of the maximal one presented in Ref. [12]. One can observe that Eq. (10) can be reduced to Eq. (2) as $d=2$.

Here, we complete the deviations of the explicit transformation of optimal $1\to 2$ SRSC in d-dimension systems. This is another main result of this paper.

As mentioned above, in the d-dimensional case the fidelity of optimal $1\to 2$ SRSC is slightly higher than that of optimal $1\to 2$ SPCC, which is given by [11]

$${}^dF_{1(2)}^{(SPCC)}=1/d+(d-2+\sqrt{d^2+4d-4})/4d. \quad (15)$$

In Table I, we show the fidelities of SRSC and SPCC for several values of d, which at least shows that the functions of the amplitudes and the phases in characterizing a quantum state are indeed different.

Finally, we analyze a relationship between ARSC and optimal eavesdropping in the BB84 scheme. Remember that the four BB84 states are given as [7] $|0\rangle$, $|\bar{0}\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$ and $|1\rangle$, $|\bar{1}\rangle=(|0\rangle-|1\rangle)/\sqrt{2}$. We first discuss a comparison between SRSC and ARSC in optimal eavesdropping against the BB84 scheme. If Eve, an eavesdropper, performs a individual symmetric attack by exploring SRSC, she will get as much as information as one legitimate receiver Bob due to ${}^2F_B^{(SRCC)}={}^2F_E^{(SRCC)}=(1+1/\sqrt{2})/2$ (here B and E are used instead of the two clones 1 and 2). Therefore, the most distinct advantage of the symmetric attack is that Eve can obtain the raw key as Bob can, so SRSC was regarded as an optimal attack on the BB84 scheme. In Ref. [28], the authors analyzed the optimal symmetric eavesdropping strategy in detail. If we choose SRCC as an attack, the disturbance defined as $D=1-F$, the mutual information I_{AB}, and the secret key rate R [27] will reach the lowest bound. Whether or not Eve can eavesdrop, the maximal information will depend on her luck; that is, either Eve obtains as much information as Bob does or risks the most danger of being detected. But for ARSC, Eve can decrease the obtained information (${}^2F_B^{(SRCC)}>{}^2F_E^{(SRCC)}$) to guarantee her security. For instance, Eve's selection of ARSC can make the values of D, I_{AB}, and R less than the lowest bound; thus, the communication between Alice and Bob will continue and Eve can do her job. It is a compromise for Eve to choose the values of ${}^2F_B^{(ARSC)} > {}^2F_E^{(ARSC)}$, which will depend on her need and requirement in practice. Note that Eve can also choose the symmetric attack by using ARSC if needed.

The input states of optimal AFCC [27] and ARSC differ in the d-dimensional system while in two dimensions the input states of AFCC and ARSC are identical—i.e., the BB84 states. In the case of $d=2$, the distribution of the two fidelities of AFCC has the same expression as that of APCC and ARSC—i.e., ${}^2F_2^{(AFCC)} = 1/2 + \sqrt{({}^2F_1^{(AFCC)})[1-({}^2F_1^{(AFCC)})]}$ [27]. The explicit AFCC transformation is not presented yet. However, the distributions of the two fidelities of ARSC and AFCC for cloning the BB84 states are the same, which sufficiently shows that the efficiencies of two cloners to attacking the BB84 states are equal. For detailed analyses, refer to Ref. [27].

In summary, we present two explicit transformations of real state cloning. One is optimal asymmetric $1 \to 2$ real state cloning in two-dimensional systems. The result covers the symmetric case. Another transformation is optimal symmetric $1 \to 2$ real state cloning in d-dimensional systems. The fidelity coincides with the theoretical value. Real state cloning is an indispensable ingredient of quantum cloning. It has a close relation to optimal eavesdropping in the BB84 scheme. Maybe this kind of cloning will find promising applications in quantum-information processing.

This work was funded by the National Science Foundation of China under Grants No. 10574001 and No. 10674001, and Educational Developing Project Facing the Twenty-first Century.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] H-K. Cummins *et al.*, Phys. Rev. Lett. **88**, 187901 (2002).
[3] N. Gisin, I. Marcikic, H. de Riedmatten, W. Tittel, and H. Zbinden, Nature (London) **421**, 509 (2003).
[4] J. Du *et al.*, Phys. Rev. Lett. **88**, 137902 (2002).
[5] S. Gulde, M. Riebe, G. P.-T. Lancaster, C. Becher, J. Eschner, H. Haffner, F. Schmidt-Kaler, I. L. Chuang, and R. Blatt, Nature (London) **421**, 48 (2003).
[6] W. K. Wooters and W. H. Zurek, Nature (London) **299**, 802 (1982); D. Dieks, Phys. Lett. **92A**, 271 (1982).
[7] C. H. Bennett, and G. Brassard, in *Proceedings of IEEE International Conference on Computers System and Signal Processing, Bangalore, India*, edited by (IEEE, New York, 1984), p. 175.
[8] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[9] R. F. Werner, Phys. Rev. A **58**, 1827 (1998).
[10] D. Bruss, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, Phys. Rev. A **62**, 12302 (2000).
[11] H. Fan, H. Imai, K. Matsumoto, and X. B. Wang, Phys. Rev. A **67**, 022317 (2003).
[12] P. Navez and N. J. Cerf, Phys. Rev. A **68**, 032313 (2003).
[13] N. J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).
[14] S. Iblisdir, A. Acin, N. J. Cerf, R. Filip, J. Fiurasek, and N. Gisin, Phys. Rev. A **72**, 042328 (2005).
[15] M. Murao, M. B. Plenio, and V. Vedral, Phys. Rev. A **61**, 032311 (2000).
[16] M. Horodecki, K. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. SenDe, and U. Sen, Phys. Rev. Lett. **90**, 100402 (2003).
[17] J. Oppenheim, M. Horodecki, and R. Horodecki, Phys. Rev. Lett. **90**, 010404 (2003).
[18] M. Horodecki, A. SenDe, and U. Sen, Phys. Rev. A **70**, 052326 (2004).
[19] M. Horodecki *et al.*, Phys. Rev. A **71**, 062307 (2005).
[20] Zhi Zhao, A. N. Zhang, X. Q. Zhou, Y. A. Chen, C. Y. Lu, A. Karlsson, and J. W. Pan, Phys. Rev. Lett. **95**, 030502 (2005).
[21] C. S. Niu and R. B. Griffiths, Phys. Rev. A **60**, 2764 (1999).
[22] Jaromír Fiurášek, Phys. Rev. A **67**, 052314 (2003).
[23] J. Du, T. Durt, P. Zou, H. Li, L. Kwek, C. Lai, C. Oh, and A. Ekert, Phys. Rev. Lett. **94**, 040505 (2005).
[24] F. Buscemi, G. M. D'Ariano, and Chiara Macchiavello, Phys. Rev. A **71**, 042327 (2005).
[25] Thomas Durt, Jaromír Fiurášek, and Nicolas J. Cerf, Phys. Rev. A **72**, 052322 (2005).
[26] N. J. Cerf, J. Mod. Opt. **47**, 187 (2000).
[27] N. J Cerf, M. Bourenanne, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[28] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).