Generalization of continuous-variable quantum cloning with linear optics

Zehui Zhai,[1,2,*] Juan Guo,[1,2] and Jiangrui Gao[1,2,3,†]

[1]*State Key Laboratory of Quantum Optics and Quantum Optics Devices, Shanxi University, Taiyuan 030006, People's Republic of China*

[2]*College of Physics and Electronics Engineering, Shanxi University, Taiyuan 030006, People's Republic of China*

[3]*Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, People's Republic of China*

(Received 27 December 2005; published 3 May 2006)

We propose an asymmetric quantum cloning scheme. Based on the proposal and experiment by Andersen *et al.* [Phys. Rev. Lett. **94**, 240503 (2005)], we generalize it to two asymmetric cases: quantum cloning with asymmetry between output clones and between quadrature variables. These optical implementations also employ linear elements and homodyne detection only. Finally, we also compare the utility of symmetric and asymmetric cloning in an analysis of a squeezed-state quantum key distribution protocol and find that the asymmetric one is more advantageous.

DOI: 10.1103/PhysRevA.73.052302 PACS number(s): 03.67.Dd, 03.65.Ta, 42.50.Dv

I. INTRODUCTION

A quantum cloning machine was first considered by Buzek and Hillery for qubits [1], and later was extended to the continuous-variable (CV) regime by Cerf *et al.* [2]. CV quantum cloning has been examined extensively in the past ten years because of its relative ease in preparing and manipulating quantum states.

Quantum cloning plays a crucial role in quantum communication and quantum computation. It has been shown that quantum cloning might improve the performance of some computational tasks [3] and is believed to be the optimal eavesdropping attack for a certain class of quantum cryptography with coherent states and homodyne detection [4]. It also opens an avenue for further understanding of quantum mechanics and measurement theory. In particular, an asymmetric cloning machine, including asymmetries between the output clones and between the quadrature variables, can be used to assess the security of a CV quantum key distribution (QKD) protocol [5–7].

Possible experimental implementation of quantum cloning of coherent states was first proposed by D'Ariano *et al.* [8], Braunstein *et al.* [9], and Fiurasek [10]. In particular, the scheme proposed by Fiurasek can be extended to asymmetric quantum cloning, i.e., the output clones can have different fidelities. However, all of these schemes utilized a nondegenerate optical parametric amplifier. Recently a much simpler but efficient quantum cloning scheme was proposed and realized by Andersen *et al.* [11]. With linear optics, such as a beam splitter, modulator, and homodyne detection, they experimentally obtained high-fidelity 1-to-2 symmetric quantum cloning for the first time. This graceful experiment can be easily extended to various quantum cloning cases, such as optimal *N*-to-*M* cloning, asymmetric cloning, and so on.

In this paper, with a measure-and-prepare strategy used in CV quantum teleportation experiments [12] as well as Ref. [11], we generalize this scheme to two asymmetric cases and discuss its application in analysis of QKD.

*Electronic address: zhzehui@sxu.edu.cn

†Electronic address: jrgao@sxu.edu.cn

II. OPTIMALITY OF QUANTUM CLONING TRANSFORMATION

Let us first review the conditions of the optimal cloning transformation before introducing the extended cloning transformation. Here we suppose the quantum state to be cloned is a coherent state, which can be characterized by two canonical conjugate variables, e.g., amplitude $\hat{X}$ and phase $\hat{Y}$, with Gaussian statistics. It then can be described by its annihilation operator $\hat{a}_{in}=(\hat{X}_{in}+i\hat{Y}_{in})/2$, with variances of $V_{X_{in}}=\langle\Delta^2X_{in}\rangle$ and $V_{Y_{in}}=\langle\Delta^2Y_{in}\rangle$. The cloning process inevitably induces noise compared with the input state. Thus output clones are mixed states with quadrature components X^j_{clone} and Y^j_{clone} $(j=1,2)$, which can be characterized by a density operator $\hat{\rho}^i_{out}$. The quality of the cloned quantum state can be quantified by its fidelity $F_i=\langle\alpha_{in}|\hat{\rho}^i_{out}|\alpha_{in}\rangle$ [12], where $|\alpha_{in}\rangle$ is the input state. For unity gain (equal mean values between input and output), the fidelity can be written as

$$F_i=\frac{2}{\sqrt{(2+N_{X_i})(2+N_{Y_i})}}, \tag{1}$$

where N_{X_i} and N_{Y_i} represent the additional noise of the ith clone induced by the cloning process. For unity gain, it is defined as $N_{X_i(Y_i)}=V_{X_i(Y_i)}-V_{X_{in}(Y_{in})}$. For 1-to-2 quantum cloning, the cloning-induced noise satisfies the relations [13]

$$N_{X_1}N_{Y_2}\geqslant 1 \quad \text{and} \quad N_{X_2}N_{Y_1}\geqslant 1, \tag{2}$$

where the variance of the vacuum is normalized to 1. The lower bounds correspond to optimal cloning. This is just the noise required to forbid inferring the values of X_{in} and Y_{in} with a precision better than the Heisenberg limit by measuring X^1_{clone} and Y^2_{clone}. For the symmetric case, we have $N_{X_1(Y_1)}=N_{X_2(Y_2)}=1$, and the fidelity of each clone is 2/3.

In fact, the optimality of the quantum cloning transformation has been discussed in an intuitive way by Braunstein *et al.* [9]. They give three expected properties of the symmetric *N*-to-*M* $(N<M)$ optimal cloning transformation in the Heisenberg picture. Here we adopt these three require-

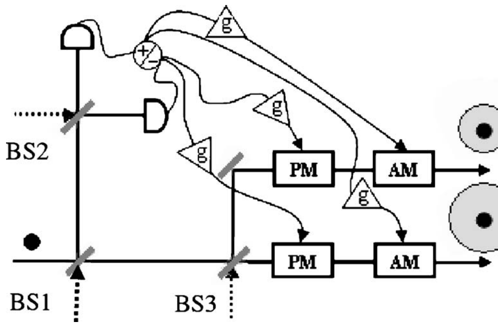

FIG. 1. Schematic setup of quantum cloning with asymmetry between output clones.

ments for our 1-to-2 asymmetric cases. The first is that the output state should have the same mean values as the input state, that is to say,

$$\langle X^i_{clone}\rangle = \langle X_{in}\rangle \quad \text{and} \quad \langle Y^i_{clone}\rangle = \langle Y_{in}\rangle, \tag{3}$$

where $i=1,2,\ldots$, which represent the output clones. The second requirement is covariance with respect to rotation in phase space. For a coherent state, its quadrature component $X^\theta_{in}=a_{in}e^{i\theta}+a^\dagger_{in}e^{-i\theta}$ has a variance independent of the phase angle θ, i.e., $V(X^\theta_{in})=1$ for any value of θ. Taking optimality into account, the variance of the quadrature component of the output clones should have a rotational covariance

$$V(X^\theta_{clone}) = 1 + \frac{2}{N} - \frac{2}{M}. \tag{4}$$

For symmetric 1-to-2 cloning, the variance of the optimal output clone is 2. That is to say, one additional noise is induced through the cloning process. It is coincident with the Heisenberg limit of inequalities (2). This requirement is only suitable for symmetric cases. For asymmetric cases, here we require the output clones to reach the Heisenberg limit [7,10], i.e., the cloning transformation should achieve the lower bounds 1 of inequalities (2). The third requirement is unitarity of the cloning transformation. In the Heisenberg picture, it is equivalent to demanding that commutation relations are preserved through evolution:

$$[X^j_{clone}, X^k_{clone}] = [Y^j_{clone}, Y^k_{clone}] = 0,$$

$$[X^j_{clone}, Y^k_{clone}] = 2i\delta_{jk}, \tag{5}$$

for $j,k=1,2,\ldots$. These three requirements will be used to determine the optimal cloning transformation below.

III. CLONING WITH ASYMMETRY BETWEEN OUTPUT CLONES

The schematic setup of 1-to-2 quantum cloning with asymmetry between output clones is shown in Fig. 1. The input coherent state $\hat{a}_{in}$ is split into two parts by a polarization beam splitter PBS1 with power transmission of T, $0<T<1$. The reflected part is detected with an optimal measurement strategy which includes a 50% beam splitter (BS2) and two detectors, and the transmitted part is further split into two parts by a beam splitter BS3 with transmission of these are then modulated by the foregoing measurement result. In contrast to the proposal of [11], we use two transmission variable beam splitters (BS1 and BS3) and transfer the modulations behind BS3 to introduce different gains. The gains of phase and amplitude modulation to clone 1 and clone 2 can be adjusted independently. In the Heisenberg picture, clone 1 can be written as

$$\hat{a}^1_{clone} = [\sqrt{(1-t)T} + g_1\sqrt{(1-T)/2}]\hat{a}_{in} + [g_1\sqrt{T/2} - \sqrt{(1-t)(1-T)}]\hat{\nu}_1^{(0)} + \frac{g_1}{\sqrt{2}}\hat{\nu}_2^{(0)} + \sqrt{t}\hat{\nu}_3^{(0)}, \tag{6}$$

where $\hat{\nu}_1^{(0)}$, $\hat{\nu}_2^{(0)}$, and $\hat{\nu}_3^{(0)}$ are the vacuums introduced by BS1, BS2, and BS3, respectively. g_1 is the scaling factor of modulation to clone 1. Taking the mean values of clone 1 and the input state to be equal by adjusting the coefficient of $\hat{a}_{in}$ in Eq. (6) to be 1, i.e., taking unity gain (the first requirement), the first clone becomes

$$\hat{a}^1_{clone} = \hat{a}_{in} + \left(\sqrt{\frac{T}{1-T}}(1-\sqrt{(1-t)T}) - \sqrt{(1-t)(1-T)}\right)\hat{\nu}_1^{(0)} + \frac{1-\sqrt{(1-t)T}}{\sqrt{1-T}}\hat{\nu}_2^{(0)+} + \sqrt{t}\hat{\nu}_3^{(0)}, \tag{7}$$

and similarly the second cloned quantum state becomes

$$\hat{a}^2_{clone} = \hat{a}_{in} + \left(\sqrt{\frac{T}{1-T}}(1-\sqrt{tT}) - \sqrt{t(1-T)}\right)\hat{\nu}_1^{(0)} + \frac{1-\sqrt{tT}}{\sqrt{1-T}}\hat{\nu}_2^{(0)+} - \sqrt{1-t}\hat{\nu}_3^{(0)}, \tag{8}$$

where the scaling factors of modulation are $g_1=[1-\sqrt{(1-t)T}]/\sqrt{(1-T)/2}$ and $g_2=[1-\sqrt{tT}]/\sqrt{(1-T)/2}$. It is easy and straightforward to check that transformations (7) and (8) satisfy the third aforementioned requirement, which assures the physical feasibility of the cloning transformation. The second requirement is satisfaction of the Heisenberg limit for the asymmetric cases. The equations $N_{X_1}N_{Y_2}=1$ and $N_{X_2}N_{Y_1}=1$ can be reached by choosing the transmission of BS1 and BS3 to satisfy $T=1/(\sqrt{t}+\sqrt{1-t})^2$. The corresponding scaling factors and additional noise are $g_1=\sqrt[4]{t/(1-t)}$, $g_2=\sqrt[4]{(1-t)/t}$ and $N_{X_1}=N_{Y_1}=\sqrt{t/(1-t)}$, $N_{X_2}=N_{Y_2}=\sqrt{(1-t)/t}$. Thus their fidelity reads $F_1=2/[2+\sqrt{t/(1-t)}]$ and $F_2=2[2+\sqrt{(1-t)/t}]$, respectively. Figure 2 gives the dependence of fidelity on the power transmission of the second beam splitter. It shows that the fidelity of clone 1 increases and that of clone 2 decreases when the transmission of BS3 varies from 0 to 1. The fidelity of both is 2/3 when $t=0.5$. This corresponds to the symmetric case [11]. According to the definition by Cerf *et al.* [6], the asymmetry of this cloning transformation can be characterized by the parameter $\chi=\sqrt{t/(1-t)}$. The further the parameter χ departs from 1, the more asymmetric the output clones are. This parameter together with the subsequent parameter λ will be used to assess the QKD protocol.

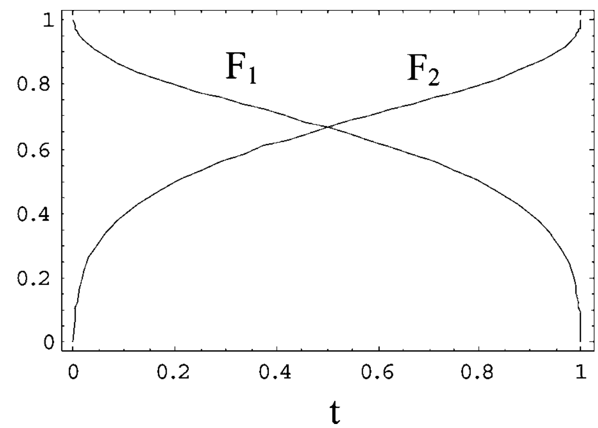

FIG. 2. Plot of fidelities of cloning with asymmetry between output clones.

IV. CLONING WITH ASYMMETRY BETWEEN QUADRATURE VARIABLES

In the proposal of Ref. [11], two vacuums are introduced inevitably to the output clones through BS2 and BS3, respectively. Here we seed a squeezed state to the vacuum input port, so that the output clones are squeezedlike. One quadrature is cloned better than the other, and the generalized Heisenberg inequalities (2) are still satisfied. A sketch of the setup is shown in Fig. 3. The transmission of both BS1 and BS3 is fixed to 50% in this case. Suppose both of the squeezed states are minimum uncertainty states, have equal squeezing strength, and have the same squeezing direction (e.g., both of them are amplitude-squeezed states). Their annihilation operators are

$$\hat{\nu}_2^S = (\hat{X}_{\nu 2}^{(0)} e^{-r} + i\hat{Y}_{\nu 2}^{(0)} e^{+r})/2,$$

$$\hat{\nu}_3^S = (\hat{X}_{\nu 3}^{(0)} e^{-r} + i\hat{Y}_{\nu 3}^{(0)} e^{+r})/2, \tag{9}$$

respectively, where r is the squeezing parameter. The cloning transformation is

$$a_{clone}^1 = a_{in} + \frac{1}{\sqrt{2}}(\hat{X}_{\nu 2}^{(0)} e^{-r} + \hat{X}_{\nu 3}^{(0)} e^{-r} + i\hat{Y}_{\nu 3}^{(0)} e^{+r} - i\hat{Y}_{\nu 2}^{(0)} e^{+r}),$$

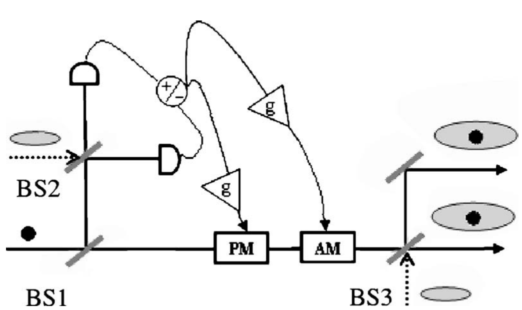

FIG. 3. Schematic setup of quantum cloning with asymmetry between quandrature variables.

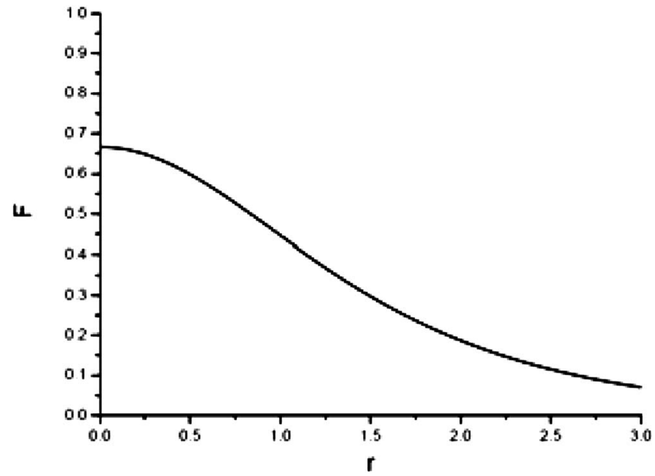

FIG. 4. Plot of fidelities of cloning with asymmetry between output clones.

$$a_{clone}^2 = a_{in} + \frac{1}{\sqrt{2}}(\hat{X}_{\nu 2}^{(0)} e^{-r} - \hat{X}_{\nu 3}^{(0)} e^{-r} - i\hat{Y}_{\nu 3}^{(0)} e^{+r} - i\hat{Y}_{\nu 2}^{(0)} e^{+r}). \tag{10}$$

It is obvious that the cloning-induced quadrature noise of the output state is

$$N_{X1} = e^{-2r}, \quad N_{X2} = e^{-2r},$$

$$N_{Y1} = e^{+2r}, \quad N_{Y2} = e^{+2r}. \tag{11}$$

This cloning transformation can also reach the Heisenberg limit $N_{X1}N_{Y2}=1$ and $N_{X2}N_{Y1}=1$; hence it is an optimal cloning scheme. The fidelity of both of the output clones is $2/\sqrt{(2+e^{-2r})(2+e^{+2r})}$. The dependence of fidelity on the squeezing parameter is shown in Fig. 4. Obviously the fidelity decreases as the squeezing strength increases. The fidelity equals 2/3 when $r=0$; this corresponds to the symmetric cloning case [11]. But from Eq. (11) it is shown that the cloning-induced noise of the quadrature amplitude and quadrature phase decreases and increases, respectively, as the squeezing parameter r increases. The asymmetry between the output clones can be characterized by the parameter $\lambda = e^{-2r}$, as defined in Ref. [7]. In the view of the quantum nondemolition (QND) measurement process, this also is a unity-gain QND scheme for quadrature amplitude of the input state. Interestingly, when the seeded squeezed states are substituted by continuous-variable entanglement states, partially disembodied transport of the quantum state can be realized [14].

It should be noted that the two above-mentioned schemes can be united to one, that is to say, a cloning process with asymmetry both between clones and between quadrature variables is possible. In the base of the first asymmetric case, by seeding squeezed state, we can obtain two squeezedlike clones, where one is noisier than the other in both quadrature variables. The schematic setup is shown in Fig. 5. By substituting $\hat{\nu}_1^{(0)}$, $\hat{\nu}_2^{(0)+}$, and $\hat{\nu}_3^{(0)}$ with the squeezed operators $\hat{\nu}_1^S$, $\hat{\nu}_2^{S+}$,

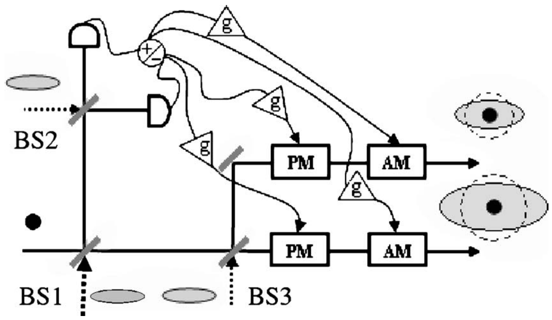

FIG. 5. Schematic setup of combination of two asymmetric quantum cloning machines.

and $\hat{\nu}_3^S$, where $\hat{\nu}_1^S=(X_{\nu 1}^{(0)}e^{-r}+i\hat{Y}_{\nu 1}^{(0)}e^{+r})/2$ and $\hat{\nu}_2^{S\dagger}, \hat{\nu}_3^S$ are given by Eq. (9), it is easy to obtain its input-output relations

$$\hat{a}^1_{clone} = \hat{a}_{in} + \left(\sqrt{\frac{T}{1-T}}[1-\sqrt{(1-t)T}] - \sqrt{(1-t)(1-T)}\right)\hat{\nu}_1^S + \frac{1-\sqrt{(1-t)T}}{\sqrt{1-T}}\hat{\nu}_2^{S+} + \sqrt{t}\hat{\nu}_3^S,$$

$$\hat{a}^2_{clone} = \hat{a}_{in} + \left(\sqrt{\frac{T}{1-T}}(1-\sqrt{tT}) - \sqrt{t(1-T)}\right)\hat{\nu}_1^S + \frac{1-\sqrt{tT}}{\sqrt{1-T}}\hat{\nu}_2^{S+} - \sqrt{1-t}\hat{\nu}_3^S. \quad (12)$$

The transformations (12) also satisfy the first and third aforementioned requirements as do Eqs. (7) and (8). The second requirement is to reach the Heisenberg limit for our asymmetric case. Assuming there is no correlation between input state and seeded squeezed states, it is easy to check that

$$N_{X_1} = e^{-2r}\sqrt{t/(1-t)} = \chi\lambda, \quad N_{Y_1} = e^{2r}\sqrt{t/(1-t)} = \chi\lambda^{-1},$$

$$N_{X_2} = e^{-2r}\sqrt{(1-t)/t} = \chi^{-1}\lambda, \quad N_{Y_2} = e^{2r}\sqrt{(1-t)/t} = \chi^{-1}\lambda^{-1} \quad (13)$$

when choosing the transmissions T and t of BS1 and BS3 to satisfy the equation $T=1/(\sqrt{t}+\sqrt{1-t})^2$, and thus have the equations $N_{X_1}N_{Y_2}=1$ and $N_{X_2}N_{Y_1}=1$. Their fidelities read

$$F_1 = \frac{2}{\sqrt{[2+e^{-2r}\sqrt{t/(1-t)}][2+e^{2r}\sqrt{t/(1-t)}]}},$$

$$F_2 = \frac{2}{\sqrt{[2+e^{-2r}\sqrt{(1-t)/t}][2+e^{2r}\sqrt{(1-t)/t}]}}, \quad (14)$$

respectively.

As the optimal individual eavesdropping strategy, this combined quantum cloning machine can be used to analyze the security of quantum key distribution. A detailed discussion of the application of asymmetric quantum cloning in the squeezed-state QKD protocol has been presented by Cerf *et al.* [7]. In this paper, we compare the utility of symmetric and asymmetric cloning in analysis of this protocol. In the original proposal [7], the Gaussian key is encoded into a displaced squeezed vacuum state. The squeezing and displacement is applied at random on quadrature X or Y. When imposing indistinguishability conditions, the total information in this channel is

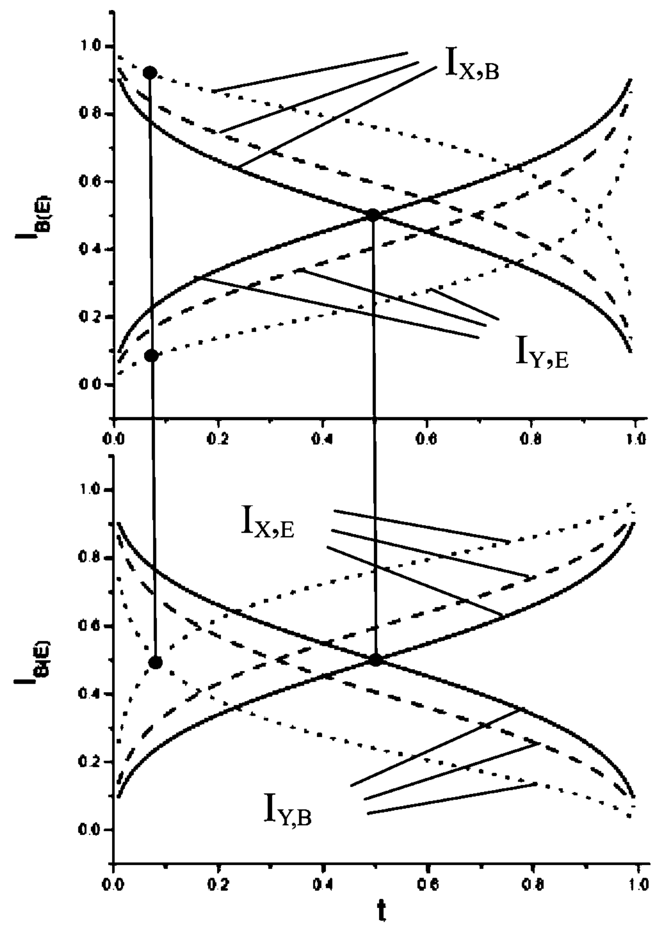

FIG. 6. Plot of information rate as transmission of BS3 is varied. $r=0$ (solid line), 0.2 (dashed line), and 0.6 (dotted line).

$$I = \frac{1}{2}\log_2\left(1+\Sigma^2_{X(Y)}/\sigma^2_{X(Y)}\right) = -\log_2\alpha, \quad (15)$$

where $\Sigma^2_{X(Y)}/\sigma^2_{X(Y)}$ is the signal-to-noise ratio, and α is related to the squeezing degree of Alice's sending system. When Eve intervenes, the information rate Bob receives unavoidably degrades. Interestingly, the information Eve gains on one quadrature is exactly the information that Bob lost on the other quadrature, when she eavesdrops by quantum cloning. The information rates of X Bob obtains and of Y Eve obtains are given by Eqs. (7) and (8) in Ref. [7], where the subscripts 1 and 2 should be X and Y here. At the same time, that of Bob's quadrature Y and that of Eve's quadrature X are

$$I_{Y,B} = \frac{1}{2}\log_2\left(\frac{1+\alpha\chi\lambda^{-1}}{\alpha^2+\alpha\chi\lambda^{-1}}\right), \quad (16)$$

$$I_{X,E} = \frac{1}{2}\log_2\left(\frac{1+\alpha\chi^{-1}\lambda}{\alpha^2+\alpha\chi^{-1}\lambda}\right). \tag{17}$$

Figure 6 gives the dependence of $I_{X,B}, I_{Y,E}$ (upper) and $I_{Y,B}, I_{X,E}$ (lower) on transmission of BS3 with different squeezing parameters r of Eve's squeezed state in the cloning machine. If Eve wants to tap quadrature X at some time, the proper compromise between the obtained information rate and the disturbance on Bob is an equal information rate between them [7,15] (crossing lower in the panel in Fig. 6). Here the disturbance on Bob is represented by the degradation of his information rate. The disturbance on Bob's quadrature Y induced by asymmetric attack is the same as in the symmetric case (crossing of dotted line and solid line in the lower panel of Fig. 6), but that of quadrature X is substantially less than in the symmetric case at the same time (upper panel in Fig. 6). This can be explained in that the disturbance on Bob's quadrature X is transferred to Eve's quadrature Y by means of asymmetry of cloning. Therefore asymmetric cloning is more advantageous than symmetric in some situations.

V. CONCLUSION

In conclusion, we generalize the symmetric 1-to-2 quantum cloning with linear optics to two kinds of asymmetric cases. They can be combined to one, and provide a more flexible quantum cloning machine. It is shown that asymmetric cloning is the optimal choice for Eve when attacking the squeezed-state QKD protocol. These proposals are useful for future quantum communication systems and are easy to implement with setups experimentally accessible at present.

ACKNOWLEDGMENTS

The authors would like to thank Prof. Jing Zhang and Prof. Junxiang Zhang for helpful discussion. This work was supported by the National Natural Science Foundation of China (Grant No. 60478008), the Teaching and Research Award Program for Outstanding Young Teachers in High Education Institute of MOE (TRAPOYT) of China, and Shanxi Provincial Science Foundation (Grants No. 20051001 and No. 2006021004).

[1] V. Buzek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[2] N. J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000).
[3] E. F. Galvao and L. Hardy, Phys. Rev. A **62**, 022301 (2000).
[4] F. Grosshans and N. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).
[5] S. L. Braunstein, V. Buzĕk, and M. Hillery, Phys. Rev. A **63**, 052313 (2001).
[6] N. J. Cerf, S. Iblisdir, and G. Van Assche, Eur. Phys. J. D **18**, 211 (2002).
[7] N. J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
[8] G. M. D'Ariano, F. De Martini, and M. F. Sacchi, Phys. Rev. Lett. **86**, 914 (2001).
[9] S. L. Braunstein, N. J. Cerf, S. Iblisdir, P. van Loock, and S. Massar, Phys. Rev. Lett. **86**, 4938 (2001).
[10] J. Fiurasek, Phys. Rev. Lett. **86**, 4942 (2001).
[11] U. L. Andersen, V. Josse, and G. Leuchs, Phys. Rev. Lett. **94**, 240503 (2005).
[12] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, Science **282**, 706 (1998).
[13] F. Grosshans and P. Grangier, Phys. Rev. A **64**, 010301(R) (2001).
[14] Jing Zhang, Changde Xie, and Kunchi Peng, Phys. Rev. Lett. **95**, 170501 (2005).
[15] C. E. Shannon, Bell Syst. Tech. J. **27**, 623 (1948).