Dense-coding quantum key distribution based on continuous-variable entanglement

Xiaolong Su, Jietai Jing, Qing Pan,* and Changde Xie
The State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan, 030006, People's Republic of China

(Received 29 April 2006; published 11 December 2006)

We proposed a scheme of continuous-variable quantum key distribution, in which the bright Einstein-Podolsky-Rosen entangled optical beams are utilized. The source of the entangled beams is placed inside the receiving station, where half of the entangled beams are transmitted with round trip and the other half are retained by the receiver. The amplitude and phase signals modulated on the signal beam by the sender are simultaneously extracted by the authorized receiver with the scheme of the dense-coding correlation measurement for continuous quantum variables, thus the channel capacity is significantly improved. Two kinds of possible eavesdropping are discussed. The mutual information and the secret key rates are calculated and compared with those of unidirectional transmission schemes.

DOI: 10.1103/PhysRevA.74.062305 PACS number(s): 03.67.Hk, 42.50.−p

I. INTRODUCTION

The quantum key distribution (QKD) based on the fundamental properties of quantum mechanics provides a way for two distant parties, usually named Alice (sender) and Bob (receiver), to share keys for encryption that can be absolutely secret in principle. Generally, we say, a communication channel is secure in the sense that any eavesdropper can be detected by the authorized communication partners. Initially, the discussions and experimentally demonstrations on QKD were concentrated within the setting of discrete variables (dv). There have been two basic schemes for qubit-based dv QKD, which are the sending of states from nonorthogonal bases, such as the original "BB84 protocol" proposed in 1984 by Bennett and Brassard [1], and those based on sharing entanglement between the sender and receiver, such as Ekert's scheme (E91) [2]. So far, a plenty of dv QKD schemes have been presented and its potential application in the long distance secure communication have been experimentally demonstrated [3–7]. However, the data transmission rates and the detection efficiency of single photons in dv QKD schemes are strongly restricted by the today availably technical resources. For pursuing high secret key rates, the continuous-variable (cv) QKD has attracted extensive interest in recent years [8–20]. In addition, another motivation to deal with cv QKD is that the mature technology in quantum optics utilizing continuous quadrature amplitudes of the quantized electromagnetic field, including the preparation, manipulation, and measurement of quantum states, can be used directly in cv quantum communication to provide efficient implementation. Due to the lack of fast and efficient single-photon detectors available at the moment, the nearly unit quantum efficiency of bright-light photodetectors at high speeds becomes the most attractive character for the explorers of cv QKD. On the other hand, the unconditionalness of cv entangled states emerged from the nonlinear optical interaction in an unconditional fashion is a valuable feature. Earlier, in 1993 Kimble's group in Pasadena accomplished the first experiment on quantum communication based on cv entanglement, in which the idea about the quantum secure communication was involved although the security of the protocol was not analyzed carefully [12]. Later, the cv entangled states has been successfully applied in various quantum communication protocols to demonstrate the unconditional quantum teleportation, entanglement swapping, quantum dense coding, and so on [21–23].

A variety of cv QKD schemes employing the entanglement of the amplitude and phase quadratures of optical fields were successively proposed. In the scheme proposed by Ralph [10] the entangled EPR fields, which are created by combining two independent amplitude-squeezed electromagnetic fields, are sent to Bob along with their local oscillators. A random phase shift is added to one of the fields to prevent an eavesdropper from retrieving the information by simple interference at a beam splitter. Reid proposed a similar scheme exploiting the quadrature entangled fields, in which the protection against eavesdropping is provided by observing a Bell inequality violation [11]. In Ref. [15], the quantum keys are generated by measuring randomly the amplitude or the phase quadrature of one of the entangled EPR optical beams. Any disturbance introduced by an eavesdropper will degrade the correlations and hence possibly be detected. Bencheikh *et al.* proposed a QKD protocol based on cv entanglement, in which the quantum key generation is achieved by distributing each mode of EPR entangled optical beams to sender and receiver who perform instantaneous measurements of quadratures [14]. The quantum correlation between the measurement outcomes are used to constitute the bits of the random secret key. In these protocols, 50% of the bits at least are rejected because the base incompatibility and both of EPR entangled beams can be intercepted. Obviously, for a given noisy channel the optimal individual attack is to take a fraction of the transmitted signal beam, which equals the line losses at the sender's site and then send the remainder to receiver through own lossless line. In this case, the eavesdropper is totally undetected, and gets maximum possible information according to the no-cloning theorem. Although in the abovementioned schemes the two-mode entangling optical fields are utilized, both of the entangling modes can be intercepted, so the security will not be more enhanced than

[*] Email address: panqing@sxu.edu.cn

that using a single mode coherent state of light when the optimal attack is used, which has been theoretically demonstrated in Ref. [16]. However, if only one of the entangling modes can be attacked and the other one can be exploited by the authorized receiver merely the entanglement will be helpful for increasing the mutual information between Alice and Bob and nothing to Eve. Based on this idea we propose a cv QKD scheme using the quadrature entanglement of two modes in which the security is enhanced and the transmission efficiency of the secret key is increased due to utilizing quantum dense-coding communication.

According to the condition of information theory for secure communication, i.e., for enabling extraction of a secure key using the error correction techniques and the privacy amplification [24,25], the mutual information between Alice and Bob I_{AB} must exceed the information that either of them shares with Eve (eavesdropper) I_{AE} and I_{BE}. It has been proven in Ref. [16] that the condition $I_{AB}>I_{AE}$ (I_{BE}) is always violated for the transmission losses beyond 3 dB (50%) no matter whether the carriers of the information are the coherent, squeezed, or entangled states of light. In the successively completed cv QKD experiments, the 3 dB loss limit was beaten by utilizing classical techniques, such as the method of the reverse reconciliation [18] or the post-selection procedure [19,20]. Is it possible to beat the apparent 3 dB loss limit only using the presently available quantum resources without demanding either the advanced or unrealized quantum techniques (quantum memories, entanglement purification, etc.) or the abovementioned classical methods? We note, in all communication schemes discussed by Ref. [16] the information is transmitted unidirectionally from Alice to Bob. In this case, the noise added in Alice's side cancels out because it disturbs equally Eve and Bob. Therefore, the security of these protocols does not rely on the noise feature of the used light beams. Especially, in the nonmodulated cv QKD scheme using Einstein-Podolsky-Rosen (EPR) entangled beams proposed by Silberhorn *et al.* [15], Alice keeps one of the EPR beams and sends the other to Bob. However, the photocurrent signals detected by Alice are opened on the classical channel, such that it is logically equivalent to a randomly modulated squeezed light beam thus brings no improvement of security [16].

In this paper, we propose a round-trip transmission cv QKD scheme based on EPR entanglement. A source producing EPR entangled light beams with the quadrature amplitude and phase correlations is placed inside the station of Bob. Only one of the EPR beams (signal beam) is sent to Alice. The other one (idler beam) is retained by Bob and never open even its classical photocurrents. For enhancing transmission capacity we embed the benefits of cv quantum dense coding [26] in the cv QKD scheme as was done by Degiovanni *et al.* in the dv protocol [27]. Two sets of independent random numbers are modulated on the amplitude and phase quadratures of Alice's EPR beam, respectively. Then she sends the modulated signal beam back to Bob. At Bob, the two sets of signals are simultaneously decoded with the aid of the retained EPR beam with homodyne detection [28]. Since each half of the EPR beam has huge noise individually and the correlation noises between a pair of EPR beams are below the shot noise limit (SNL), if there is not too much excess noise added in the beams the signal-to-noise ratios (SNRs) in Alice's signal beam must be lower than that decoded by Bob with the correlation measurements [12,23]. We found, in this scheme the condition of $I_{AB}>I_{AE}$ can be satisfied even when the transmission losses exceed 3 dB if higher EPR correlation is utilized. The security of the proposed system is based on the determinative cv entanglement of EPR light beams and the quantum no-cloning theorem. Two kinds of eavesdropper attack will be discussed. (1) The individual quantum-tap attack to the modulated signal beam on the way from Alice to Bob or to both unmodulated and modulated beams using an optical beam splitter according to the requiement of optimal cloning. (2) The intercept-resend or partial intercept-mixing attack to the nonmodulated beam on the way from Bob to Alice using the simulated EPR beams produced by Eve. The calculated results proved that the higher EPR entanglement is helpful to beat the 3 dB loss limit in the proposed scheme. The regions of the secure raw secret key $(I_{AB}-I_{AE})>0$ as functions of the line transmission and the EPR entanglement correlation factor are calculated. Additionally, as with the no-switching cv QKD scheme presented in Refs. [17,20], the usual random switching between measurement bases is not required and thus the channel capacity can be significantly improved due to the application of quantum dense-coding method. Further, in the dense-coding cv QKD scheme we utilize the bright EPR beams with the anticorrelated amplitude quadratures and the correlated phase quadratures as well as the Bell-state direct detection technique proposed and used in our previous papers [23,28], therefore the local oscillation optical beam is not needed in Bob's measurements for extracting the secret keys. Naturally, the protocol dispenses with the technical limitation on the communication bandwidth placed by the local oscillator switching and is relatively simple to implement. Here we should mention that although the proposed protocol can beat the loss limit of 3 dB in principle, however, due to practical difficulties to produce quadrature entangled light with a high entanglement degree and high susceptibility of cv entanglement to loss the reachable communication distance has to be strictly limited by the available entanglement quality. It has been theoretically demonstrated that the entanglement of a cv resource, though being degraded on a transmission line with loss never vanishes completely for any degree of the loss, thus once the technologies of cv entanglement distillation and purification are exploited the drawbacks will be possible to overcome [29,30].

The paper is organized as follows. In the second section the cv QKD system is described. The security against the quantum-tap attack and the intercept-resend attack are discussed in the third and the fourth section, respectively. A brief conclusion is given in the fifth section.

II. CV QKD SYSTEM USING EPR ENTANGLED OPTICAL BEAMS AND ROUND-TRIP TRANSMISSION

The schematic of the proposed cv QKD system is shown in Fig. 1. The bright EPR optical beams $\hat{a}$ and $\hat{b}$, with the anticorrelated amplitude quadratures and the correlated phase quadratures are produced from an entanglement source. For

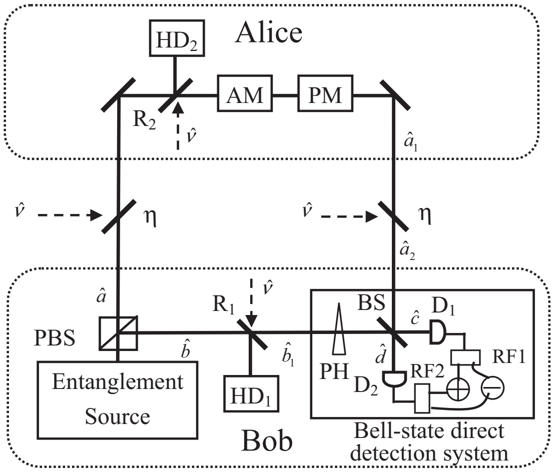

FIG. 1. The schematic of the quantum key distribution with bright EPR beams. AM: amplitude modulator, PM: phase modulator, R: reflection rates of the beam splitter R_1 and R_2, PBS: polarization beam splitter, HD: homodyne detection system, η: channel efficiency, PH: $\pi/2$ phase shifter, RF: radio-frequency splitter.

experiments, this kind of EPR beams can be obtained with a nondegenerate optical parametric amplifier (NOPA) below the pump threshold operating in the state of deamplification, which has been well described in Ref. [23]. The field annihilation operators $\hat{a}$ and $\hat{b}$ are expressed in terms of the amplitude ($\hat{X}_{a(b)}$) and phase ($\hat{Y}_{a(b)}$) quadrature operators

$$\hat{a} = \hat{X}_a + i\hat{Y}_a,$$

$$\hat{b} = \hat{X}_b + i\hat{Y}_b. \tag{1}$$

The quadrature operators can be written as the sum of a steady state and a fluctuating component

$$\hat{X} = \langle \hat{X} \rangle + \delta\hat{X},$$

$$\hat{Y} = \langle \hat{Y} \rangle + \delta\hat{Y}, \tag{2}$$

which have variances of $V(\hat{X}) = \langle (\delta\hat{X})^2 \rangle$ and $V(\hat{Y}) = \langle (\delta\hat{Y})^2 \rangle$. For the EPR entangled optical beams produced from a NOPA operating at deamplification, the variances for each individual beam ($\hat{a}$ or $\hat{b}$) and the correlation variances are determined by the correlation factor γ (or called squeezing factor), which depends on the strength and the time of parametric interaction [11,16]

$$V(\hat{X}_a) = V(\hat{Y}_a) = V(\hat{X}_b) = V(\hat{Y}_b) = (\gamma + 1/\gamma)/2, \tag{3}$$

$$V(\hat{X}_a + \hat{X}_b) = V(\hat{Y}_a - \hat{Y}_b) = 2\gamma, \tag{4}$$

where we have assumed that the two modes $\hat{a}$ and $\hat{b}$ are totally balanced during the process of measurements and this requirement is easily achieved in the experiments. The values of γ are taken from 0 to 1, $\gamma=0$, and $\gamma=1$ correspond to the ideally perfect correlation and no any correlation between $\hat{a}$ and $\hat{b}$, respectively. The modes $\hat{a}$ and $\hat{b}$ from NOPA have the orthogonal polarizations and can be separated with a polarizing beam splitter (PBS). The entanglement source is placed inside the station of Bob. The optical mode $\hat{a}$, say the signal mode, is sent to Alice as the quantum channel of the transmitted signals. The mode $\hat{b}$, say the idler mode, is retained by Bob and never is opened. The beam-splitter R_1 and R_2 with same reflectivity (such as $R=10\%$) are placed in Bob and Alice who extract a small part from $\hat{b}$ and $\hat{a}$ beam by means of R_1 and R_2, respectively. The extracted beam from $\hat{b}$ ($\hat{a}$) is detected by the balanced-homodyne-detector HD$_1$ (HD$_2$) for checking the possible eavesdropper on the way from Bob to Alice, which will be discussed in Sec. IV. As in the cv coherent state quantum cryptography protocol presented in Refs. [18,20], for the optimal information rate both amplitude and phase are modulated with Gaussian random numbers [29]. Alice draws two random real numbers X_s and Y_s from Gaussian distributions with zero mean and a variance of $V(X_s)$ and $V(Y_s)$. Then she modulates the amplitude and phase quadratures of the transmitted $\hat{a}$ from R_2 by X_s and Y_s with the amplitude (AM) and phase (PM) modulators, respectively. Alice transmits the modulated signal mode $\hat{a}$ back to Bob. We assume that the channel transmission efficiencies from Bob to Alice and from Alice to Bob without the presence of Eve are identical and equal to η. Bob demodulates simultaneously the modulated amplitude (X_s) and phase (Y_s) signals using the Bell-state direct detection under the help of the retained mode $\hat{b}$ [28]. The Bell-state direct detection system consists of a 50-50 beam splitter (BS), a pair of photoelectric detectors (D_1 and D_2), two radio-frequency splitter (RF1 and RF2), a $\pi/2$ phase shifter (PH), a positive and a negative power combiner (⊕ and ⊖). The beams $\hat{b}_1$ and $\hat{a}_2$ interfere on the beam splitter (BS) and then the output beams $\hat{c}$ and $\hat{d}$ are directly detected by D_1 and D_2, respectively. $\hat{v}$ stands for the vacuum noise added in the quantum channel due to losses. The vacuum noises in different terms are not correlated, thus they have to be considered independently. In the following we will calculate the physical conditions for satisfying $I_{AB} > I_{AE}$.

III. SECURITY CONDITIONS AGAINST OPTIMAL QUANTUM-TAP ATTACK

It has been theoretically demonstrated by Curty *et al.* [31] that the presence of detectable entanglement in a quantum state effectively distributed between Alice and Bob is a necessary precondition for successful key distillation. In the proposed scheme, the quantum entanglement of quadratures shared by Alice and Bob is always existent and detectable so far as the original EPR entanglement is not exhausted totally by the line losses. The existence of cv entanglement between Alice and Bob provides the base of security for the proposed protocol. The absolute theoretical security of cv QKD protocols against any type of attack has already been proven [13,32–34]. Here we do not address the issue of unconditional security and also do not involve the collective attack, which requires the quantum memory that is not easy to be prepared in today technical condition. We consider security against individual attacks only. Obviously, at the loss limit the optimal individual attack is that Eve replaces the lossy channel by a perfect one with an adapted beam splitter to mimic the losses and then generate a cloned signal with a fidelity depending on the beam splitter transmission. In this case Eve is totally not detected and gets the maximum possible information according to the no-cloning theorem which is the maximum information amount allowed by the laws of physics. Since there is no any signal on the quantum channel from Bob to Alice, we first consider a splitting attack on the channel from Alice to Bob. A splitting attack involving both channels will be considered later in this section.

We will use the Shannon formula of the optimum information rate to calculate the raw secret key rate. The optimum mutual information (I) of a noisy transmission channel is [35]

$$I = (1/2)\log_2(1 + S/N), \tag{5}$$

S/N is the signal-to-noise ratio (SNR). Alice and Bob can establish a secret key if and only if $I_{AB} > I_{AE}$, thus the secret key rate is expressed as [16]

$$\Delta I = I_{AB} - I_{AE}. \tag{6}$$

In the case of $\Delta I > 0$ the communication between Alice and Bob will be viewed as being secure. The simpler quantum-tap attack is to take a fraction $(1-\eta)$ of the beam with the modulated signals at Alice's site, and to send the fraction η to Bob through her own lossless line. The modulated optical mode at Alice is written as

$$\hat{a}_1 = \sqrt{1-R}(\sqrt{\eta}\hat{a} + \sqrt{1-\eta}\hat{\nu}) + \sqrt{R}\hat{\nu} + s, \tag{7}$$

and when the mode is transmitted back to Bob the mode $\hat{a}_1$ becomes $\hat{a}_2$ if without any interception:

$$\hat{a}_2 = \sqrt{\eta}\hat{a}_1 + \sqrt{1-\eta}\hat{\nu} = \sqrt{1-R}[\eta\hat{a} + \sqrt{\eta(1-\eta)}\hat{\nu}] + \sqrt{R\eta}\hat{\nu} + \sqrt{1-\eta}\hat{\nu} + \sqrt{\eta}s, \tag{8}$$

where R is the reflectivity of the beam splitter R_1 and R_2 and s stands for the state of the modulated signals. The signal state is prepared at Alice by displacing the amplitude and phase quadratures of a vacuum state by X_s and Y_s, respectively.

In order to measure the amplitude and phase signals by means of the Bell-state direct detection simultaneously, Bob has to attenuate the retained idler beam $\hat{b}$ to balance $\hat{a}_2$. The attenuated $\hat{b}$ is expressed by $\hat{b}_1$:

$$\hat{b}_1 = \sqrt{1-R}[\eta\hat{b} + \sqrt{\eta(1-\eta)}\hat{\nu}] + \sqrt{R\eta}\hat{\nu} + \sqrt{1-\eta}\hat{\nu}. \tag{9}$$

.

The two output fields from the 50-50 beam splitter (BS) of the Bell-state direct detection system are [28]

$$\hat{c} = \frac{1}{\sqrt{2}}(\hat{a}_2 + i\hat{b}_1), \tag{10}$$

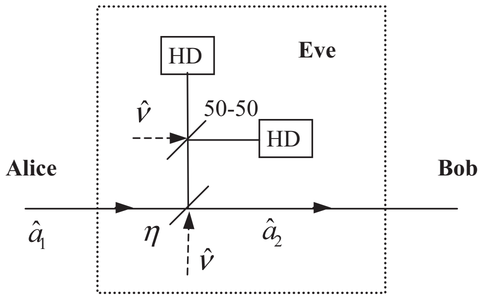

FIG. 2. Eve's detection system. HD: homodyne detection system, η: channel efficiency.

$$\hat{d} = \frac{1}{\sqrt{2}}(\hat{a}_2 - i\hat{b}_1). \tag{11}$$

The variances of the sum and the difference of $\hat{c}$ and $\hat{d}$ equal [28]

$$V_{BX} = \frac{1}{2}[(1-R)\eta^2 V(\hat{X}_a + \hat{X}_b) + 2(1-\eta^2 + R\eta^2) + \eta V(X_s)], \tag{12}$$

$$V_{BY} = \frac{1}{2}[(1-R)\eta^2 V(\hat{Y}_a - \hat{Y}_b) + 2(1-\eta^2 + R\eta^2) + \eta V(Y_s)], \tag{13}$$

where $V(\hat{X}_a + \hat{X}_b)$, $V(\hat{Y}_a - \hat{Y}_b)$ and $V(X_s)$, $V(Y_s)$ are the normalized correlation variances of the quadratures between $\hat{a}$ and $\hat{b}$ and the normalized variances of the signal quadratures, respectively. The SNR of Bob's measurement for the amplitude and the phase signals are, respectively,

$$(S/N)_{BX} = \frac{\eta V(X_s)}{(1-R)\eta^2 V(\hat{X}_a + \hat{X}_b) + 2(1-\eta^2 + R\eta^2)}, \tag{14}$$

$$(S/N)_{BY} = \frac{\eta V(Y_s)}{(1-R)\eta^2 V(\hat{Y}_a - \hat{Y}_b) + 2(1-\eta^2 + R\eta^2)}. \tag{15}$$

For the dense-coding QKD scheme, Eve takes a fraction $(1-\eta)$ of the beam $\hat{a}_1$ at Alice's site and then simultaneously measures the amplitude and phase quadratures of the intercepted beam by means of a 50-50 beam splitter and two sets of homodyne detectors (HDs) as shown in Fig. 2. The variances of the amplitude and phase quadratures measured by Eve are, respectively, expressed by

$$V_{EX} = \frac{1}{2}[\eta(1-\eta)(1-R)V(\hat{X}_a) + 2 - (1-R)\eta + (1-R)\eta^2 + (1-\eta)V(X_s)], \tag{16}$$

$$V_{EY} = \frac{1}{2}[\eta(1-\eta)(1-R)V(\hat{Y}_a) + 2 - (1-R)\eta + (1-R)\eta^2 + (1-\eta)V(Y_s)]. \tag{17}$$

The SNR of Eve's measurements equal

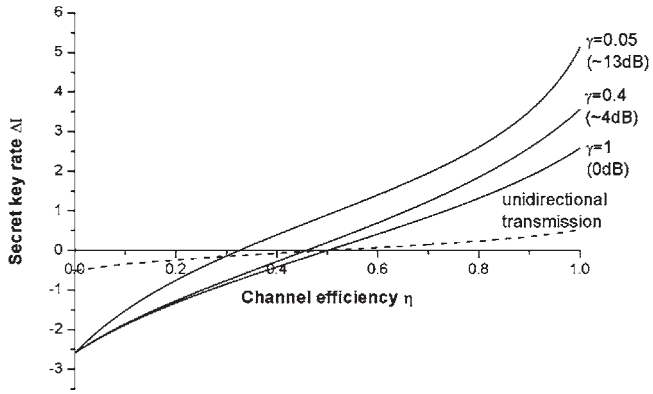

FIG. 3. The secret key rate versus channel efficiency at various correlation degrees for the case only tapping modulated beam. $V(X_s)=V(Y_s)=10$, $R=0.1$. Solid lines: the function curves of the presented scheme, dashed line-the function curves of the unidirectional transmission scheme.

$$(S/N)_{EX}=\frac{(1-\eta)V(X_s)}{(1-R)\eta(1-\eta)V(\hat{X}_a)+2-(1-R)\eta+(1-R)\eta^2}, \tag{18}$$

$$(S/N)_{EY}=\frac{(1-\eta)V(Y_s)}{(1-R)\eta(1-\eta)V(\hat{Y}_a)+2-(1-R)\eta+(1-R)\eta^2}. \tag{19}$$

Substituting Eqs. (14), (15), (18), and (19) into Eq. (5) we can calculate the mutual information I_{AB}^X, I_{AB}^Y and I_{AE}^X, I_{AE}^Y, as well as the total secret key rate ΔI, which is the sum of the secret key rates of the amplitude (ΔI^X) and phase (ΔI^Y) quadrature:

$$\Delta I=I_{AB}^X+I_{AB}^Y-I_{AE}^X-I_{AE}^Y=I_{AB}^X-I_{AE}^X+I_{AB}^Y-I_{AE}^Y=\Delta I^X+\Delta I^Y. \tag{20}$$

.

Figure 3 shows the secret key rate as a function of the channel efficiency η and the correlation factor γ for the given signal variances and the reflectivity R, where the normalized $V(X_s)=V(Y_s)=10$ and $R=0.1$. In the case of $\gamma=1$, i.e., without any EPR correlation between $\hat{a}$ and $\hat{b}$, the scheme is secure ($\Delta I>0$) only at $\eta>0.5$, which corresponds to the conclusion in Ref. [16] for the unidirect transmission. For comparison, the function of ΔI versus η in the unidirectional transmission [see Eq. (5) of Ref. [16]] is drawn in Fig. 3 with the dashed line. We can see, when $\eta>0.5$ our scheme is better than that of the unidirectional transmission even $\gamma=1$ because the dense-coding scheme is applied. However, for the lower η ($\eta<0.5$), the unidirectional transmission is advantaged since the transmission losses are doubled in the round-trip transmission protocol. For $\gamma=0.05$ and $\gamma=0.4$ (corresponding to the correlation degree of ~13 and ~4 dB, respectively), ΔI will be larger than zero once $\eta>0.33$ and $\eta>0.46$, respectively. This means that the limitation of 3 dB losses ($\eta>0.5$) can be beaten in our scheme using EPR entanglement if Eve only taps the modulated channel. It is obvious from the equations of SNR, for the channel with very high losses ($\eta\to 0$) the SNR will only depend on the variances of the modulated signal $V(X_s)$ or $V(Y_s)$, thus all figures cross to the same point on the ΔI axis [$\Delta I=-2.58$ in the case of $V(X_s)=V(Y_s)=10$].

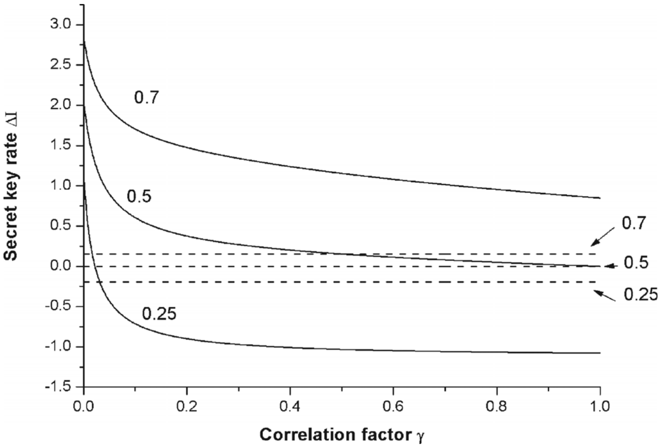

FIG. 4. The secret key rate versus correlation degree at various channel efficiencies for the case only tapping modulated beam. $V(X_s)=V(Y_s)=10$, $R=0.1$. Solid lines: the function curves of the presented scheme, dashed lines-the function curves of the unidirectional transmission scheme.

Figure 4 shows the dependences of the secret key rate on the correlation factor γ for $\eta=0.7$, 0.5, and 0.25, respectively. The three dashed lines correspond to the function curves of the unidirectional transmission with $\eta=0.7$, 0.5, and 0.25 also for comparison. When $\eta>0.5$, the secret key rates of the proposed scheme are always larger than that of the unidirectional transmission. For $\eta=0.25$, the unidirectional transmission is not secure always while our scheme can be secure if the EPR correlation is high enough ($\gamma<0.02$).

Another better clone attack scheme is where Eve taps both the unmodulated optical beam before Alice and the modulated signal beam after Alice, then substracts the two intercepted signal beams for performing the correlation measurement. In this case the two extracted beams are the thermal optical fields and very noisy due to the added vacuum noise on the beam splitter. According to the requirement of the above mentioned optimally individual attack, the extracted amount should match the line loss. Eve has to simultaneously measure the amplitude and phase quadratures of both the intercepted unmodulated optical beam and the modulated signal beam by means of four sets of homodyne detection systems. The measured amplitude and phase quadratures of the intercepted light beams on the ways before and after Alice are, respectively,

$$\hat{X}'_{E_1}=\frac{1}{\sqrt{2}}(\sqrt{1-\eta}\hat{X}_a-\sqrt{\eta}\hat{X}_\nu+\hat{X}_\nu), \tag{21}$$

$$\hat{Y}'_{E_1}=\frac{1}{\sqrt{2}}(\sqrt{1-\eta}\hat{Y}_a-\sqrt{\eta}\hat{Y}_\nu-\hat{Y}_\nu) \tag{22}$$

and

$$\hat{X}'_{E_2} = \frac{1}{\sqrt{2}}[\sqrt{\eta(1-\eta)(1-R)}\hat{X}_a + (1-\eta)\sqrt{1-R}\hat{X}_\nu + \sqrt{R(1-\eta)}\hat{X}_\nu - \sqrt{\eta}\hat{X}_\nu + \hat{X}_\nu + \sqrt{1-\eta}X_s], \tag{23}$$

$$\hat{Y}'_{E_2} = \frac{1}{\sqrt{2}}[\sqrt{\eta(1-\eta)(1-R)}\hat{Y}_a + (1-\eta)\sqrt{1-R}\hat{Y}_\nu + \sqrt{R(1-\eta)}\hat{Y}_\nu - \sqrt{\eta}\hat{Y}_\nu - \hat{Y}_\nu + \sqrt{1-\eta}Y_s]. \tag{24}$$

For eliminating the thermal-like component of the noises $[V(\hat{X}_a)$ and $V(\hat{Y}_a)]$, Eve multiplies the tapped unmodulated signal beam [Eqs. (21) and (22)] by $\sqrt{\eta(1-R)}$, that is to attenuate the optical beam by a factor of $\sqrt{\eta(1-R)}$, then subtracts the tapped modulated signal beam [Eqs. (23) and (24)] from it. The variances of $[\sqrt{\eta(1-R)}\hat{X}'_{E_1} - \hat{X}'_{E_2}]$ and $[\sqrt{\eta(1-R)}\hat{Y}'_{E_1} - \hat{Y}'_{E_2}]$ equal to

$$V'_{EX} = \frac{1}{2}\{[\eta\sqrt{1-R} - (1-\eta)\sqrt{1-R}]^2 + 1 + \eta(1-R) + \eta + R(1-\eta) + (1-\eta)V(X_s)\}, \tag{25}$$

$$V'_{EY} = \frac{1}{2}\{[\eta\sqrt{1-R} - (1-\eta)\sqrt{1-R}]^2 + 1 + \eta(1-R) + \eta + R(1-\eta) + (1-\eta)V(Y_s)\}. \tag{26}$$

The corresponding signal to noise ratios are

$$(S/N)'_{EX} = \frac{(1-\eta)V(X_s)}{[\eta\sqrt{1-R} - (1-\eta)\sqrt{1-R}]^2 + 1 + \eta(1-R) + \eta + R(1-\eta)}, \tag{27}$$

$$(S/N)'_{EY} = \frac{(1-\eta)V(Y_s)}{[\eta\sqrt{1-R} - (1-\eta)\sqrt{1-R}]^2 + 1 + \eta(1-R) + \eta + R(1-\eta)}. \tag{28}$$

Figure 5 shows the function curves of the secret key rate ΔI versus the channel efficiency η for the dual-tap attack, where the normalized $V(X_s)=V(Y_s)=10$ and $R=0.1$. For $\gamma=1$, the secret key rate is larger than zero only when $\eta > 0.5$, which is same to the case of only tapping the modulated signal. For $\gamma=0.05$ and $\gamma=0.4$, the secret key rate is positive when $\eta > 0.46$ and $\eta > 0.474$, respectively. We see, under this attack due to that the influence of the thermal-like component of noises involved in the two intercepted optical beams is canceled, the effect of increasing EPR correlation to the secret key rate will not be as strong as that only attacking modulated signal beam (Figs. 3 and 4). However, we still see the possibility to beat the apparent 3 dB loss limit of the raw secret key rate.

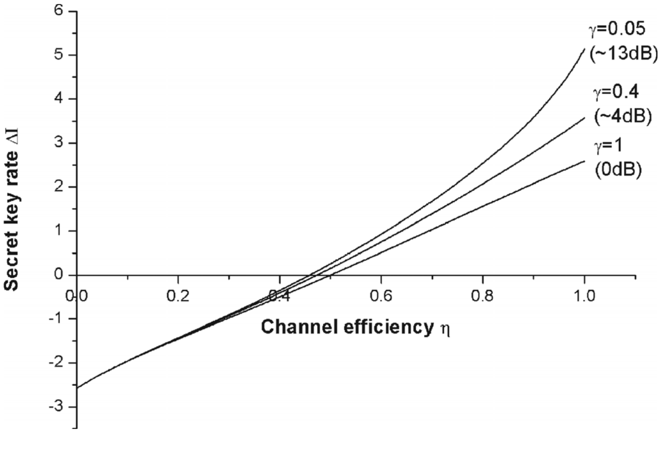

FIG. 5. The secret key rate versus channel efficiency at various correlation degrees for the case tapping both modulated and unmodulated beams. $V(X_s)=V(Y_s)=10$, $R=0.1$.

IV. SECURITY AGAINST INTERCEPT-RESEND ATTACK

Another possible attack on the way from Bob to Alice is where Eve totally intercepts the signal beam without the modulated signals and retains it in her station, then sends a simulated beam, which can be half of the simulated EPR entangled beam, to Alice. If Alice does not know that the beam is simulated, she will modulate the signals on it and send it out as usual. Eve intercepts the modulated signal beam again and demodulates the signals using the other half of the simulated EPR beams retained by herself as done by Bob. At last she modulates the same signals on the real signal beam and sends it back to Bob. Fortunately, in our scheme Bob retains a half of the real EPR beams and never opens it. Any simulated beam cannot be quantum-correlated with the real one. Bob and Alice take a part of the beam $\hat{b}$ and $\hat{a}$ from R_1 and R_2, respectively, then randomly measure the amplitude or phase quadrature of the taken partial beam with the homodyne detector (HD$_1$ and HD$_2$) during the communication. Alice sends her measurement results to Bob by a classical channel and Bob checks the quantum correlation between his quadratures and Alice's quadratures measured simultaneously. The correlation variances of the amplitude (V_{RX}) and the phase (V_{RY}) between the reflected beams from R_1 and R_2 are

$$V_{RX} = \frac{1}{2}R\eta V(\hat{X}_a + \hat{X}_b) + 1 - R\eta, \tag{29}$$

$$V_{RY} = \frac{1}{2} R\eta V(\hat{Y}_a - \hat{Y}_b) + 1 - R\eta. \tag{30}$$

Statistically, they simultaneously measure the same quadrature with 50% probability and the correlation variances of the two measured values will be below the shot noise limit (SNL) due to the existence of EPR correlations between $\hat{a}$ and $\hat{b}$ if there is no intercept-resend attack. When the simulated beam is used, the quantum correlation disappear thus the variances always are higher than the SNL. The quantum noncloning forbids Eve to copy the quantum fluctuation of the real signal beam and provides the physical mechanism of security for our scheme. In cv experiments the correlation variances of quadratures up to ~0.1 dB below the SNL can be precisely measured by means of homodyne detectors under today's technical condition. As a loose limitation we take 0.3 dB, which was detected in the early experiment of quantum optics in 1985 [36], to be a bound for detecting Eve with a high probability over 99%. For given original EPR entanglement and the line transmission, the requirement $V_{RX} = V_{RY} = 0.928$ (according to 0.32 dB below the SNL) is reached when

$$R = \frac{2(V_{RX} - 1)}{\eta[V(\hat{X}_a + \hat{X}_b) - 2]}. \tag{31}$$

For example, if $\gamma = 0.2$ [corresponding to $V(\hat{X}_a + \hat{X}_b) = V(\hat{Y}_a - \hat{Y}_b) = 0.4$, which is 7 dB below the SNL, which is experimentally reachable at present [37]], $\eta = 0.9$ and $V_{RX} = V_{RY} = 0.928$, we have R=0.1. In the calculations of Eqs. (7)–(20) the effect of R has been involved. The procedure checking the intercept-resend attack can be performed instantaneously during the communication proceeding and the communication will not be disturbed only the original quantum correlation is decreased, for example, if $R = 0.1$ the correlation is decreased from 7 to 5.5 dB.

If Eve partially mixes her own EPR beam with the transferred real one instead of totally replacing it, according to the optimally cloning scheme the replaced partial amplitude should equal $\sqrt{1-\eta}\hat{X}_e(\hat{Y}_e)$ [$\hat{X}_e(\hat{Y}_e)$ is the amplitude (phase) of a half of EPR beams prepared by Eve and $|\hat{X}_e| = |\hat{X}_a| = |\hat{Y}_e| = |\hat{Y}_a|$]. The amplitude and phase quadratures of the optical field received by Alice are

$$\hat{X}''_A = \sqrt{\eta}\hat{X}_a + \sqrt{1-\eta}\hat{X}_e, \tag{32}$$

$$\hat{Y}''_A = \sqrt{\eta}\hat{Y}_a + \sqrt{1-\eta}\hat{Y}_e, \tag{33}$$

and the remainders retained by Eve are

$$\hat{X}''_E = \sqrt{1-\eta}\hat{X}_a - \sqrt{\eta}\hat{X}_e, \tag{34}$$

$$\hat{Y}''_E = \sqrt{1-\eta}\hat{Y}_a - \sqrt{\eta}\hat{Y}_e. \tag{35}$$

Then Eve intercepts all modulated beam and performs the correlation measurement using the other half $(\hat{X}_f, \hat{Y}_f)$ of the entangled beams prepared by Eve. In this case, $V(\hat{X}_e + \hat{X}_f)[V(\hat{Y}_e - \hat{Y}_f)]$ should be smaller than SNL and depends on the correlation degree (γ_E) of Eve's EPR beams. The correlation variances measured by Eve equal to

$$V''_{EX} = \frac{1}{2}[(1-R)(1-\eta)V(\hat{X}_e + \hat{X}_f) + (1-R)\eta V(\hat{X}_a) + (1 - R)\eta + 2R + V(X_s)], \tag{36}$$

$$V''_{EY} = \frac{1}{2}[(1-R)(1-\eta)V(\hat{Y}_e - \hat{Y}_f) + (1-R)\eta V(\hat{Y}_a) + (1 - R)\eta + 2R + V(Y_s)]. \tag{37}$$

The corresponding SNRs are

$$(S/N)''_{EX} = \frac{V(X_s)}{(1-R)(1-\eta)V(\hat{X}_e + \hat{X}_f) + (1-R)\eta V(\hat{X}_a) + (1-R)\eta + 2R}, \tag{38}$$

$$(S/N)''_{EY} = \frac{V(Y_s)}{(1-R)(1-\eta)V(\hat{Y}_e - \hat{Y}_f) + (1-R)\eta V(\hat{Y}_a) + (1-R)\eta + 2R}. \tag{39}$$

The correlation degree between Bob's beam reflected from R_1 and Alice's beam from R_2 must be decreased since the partial noncorrelated light $[\hat{X}_e(\hat{Y}_e)]$ is mixed in the measured beams. The calculated variances are

$$V''_{RX} = \frac{1}{2}[R\eta V(\hat{X}_a + \hat{X}_b) + R(1-\eta)V(\hat{X}_e) + 2 - R - R\eta], \tag{40}$$

$$V''_{RY} = \frac{1}{2}[R\eta V(\hat{Y}_a - \hat{Y}_b) + R(1-\eta)V(\hat{Y}_e) + 2 - R - R\eta]. \tag{41}$$

The higher the EPR correlation between $\hat{X}_e(\hat{Y}_e)$ and $\hat{X}_f(\hat{Y}_f)$ is, the larger the $V(\hat{X}_e)[V(\hat{Y}_e)]$ is, thus $V''_{RX}(V''_{RY})$ increases. For example, taking $\gamma_E=0.05$ (corresponding to 13 dB below the SNL), when $\gamma=0.2$ (7 dB below the SNL), $V(X_s)=V(Y_s)=10$, $R=0.1$, and $\eta=0.9$, if the light intensity mixed by Eve is 10% of the total intensity, the correlation degree between Alice's and Bob's reflected beams will be reduced from 0.32 dB (without eavesdropper) to 0.11 dB, thus the presence of Eve will be revealed.

On the other hand, Eve has to add partial uncorrelation light into the beam retained by her to make Bob receiving equal intensity of light, otherwise she must be revealed immediately. The amplitude and phase quadratures of the light beam sent back to Bob are

$$\hat{X}''_a = \eta\sqrt{1-R}\hat{X}_a - \frac{\eta\sqrt{1-R}}{\sqrt{1-\eta}}\sqrt{\eta}\hat{X}_e + \sqrt{1-\frac{\eta^2(1-R)}{1-\eta}}\hat{X}_v + \sqrt{\eta}X_s, \tag{42}$$

$$\hat{Y}''_a = \eta\sqrt{1-R}\hat{Y}_a - \frac{\eta\sqrt{1-R}}{\sqrt{1-\eta}}\sqrt{\eta}\hat{Y}_e + \sqrt{1-\frac{\eta^2(1-R)}{1-\eta}}\hat{Y}_v + \sqrt{\eta}Y_s. \tag{43}$$

The correlation variances and the SNRs measured by Bob equal to

$$V''_{BX} = \frac{1}{2}\left[(1-R)\eta^2 V(\hat{X}_a+\hat{X}_b) + \frac{\eta^3(1-R)}{1-\eta}V(\hat{X}_e) + 2 - (1-R)\eta^2 - \frac{\eta^2(1-R)}{1-\eta} + \eta V(X_s)\right], \tag{44}$$

$$V''_{BY} = \frac{1}{2}\left[(1-R)\eta^2 V(\hat{Y}_a-\hat{Y}_b) + \frac{\eta^3(1-R)}{1-\eta}V(\hat{Y}_e) + 2 - (1-R)\eta^2 - \frac{\eta^2(1-R)}{1-\eta} + \eta V(Y_s)\right] \tag{45}$$

and

$$(S/N)''_{BX} = \frac{\eta V(X_s)}{(1-R)\eta^2 V(\hat{X}_a+\hat{X}_b) + \frac{\eta^3(1-R)}{1-\eta}V(\hat{X}_e) + 2 - (1-R)\eta^2 - \frac{\eta^2(1-R)}{1-\eta}}, \tag{46}$$

$$(S/N)''_{BY} = \frac{\eta V(Y_s)}{(1-R)\eta^2 V(\hat{Y}_a-\hat{Y}_b) + \frac{\eta^3(1-R)}{1-\eta}V(\hat{Y}_e) + 2 - (1-R)\eta^2 - \frac{\eta^2(1-R)}{1-\eta}}. \tag{47}$$

If Eve replaces 10% of total beam intensity the SNRs calculated with Eqs. (46) and (47) are $(S/N)''_{BX}=(S/N)''_{BY}=0.15$ [$\gamma_E=0.05$, $\gamma=0.2$, $V(X_s)=V(Y_s)=10$, $R=0.1$, and $\eta=0.9$] and the SNRs calculated with Eqs. (14) and (15), which only consider the optimal cloning attack of one channel, are $(S/N)_{BX}=(S/N)_{BY}=10.8$ with same parameters. The significant reduction of the SNRs will clearly reveal the presence of Eve also.

Although Eve might obtain more information by means of the correlation measurement using the EPR beams prepared by herself, her presence will also be revealed. Of course, if Eve has perfect entangled beams and perfect quantum memory the eavesdropping scheme might be better than totally intercepting. For more detailed discussion we have to compare the information amounts, respectively, obtained by Bob and Eve in this case and find the region for the secure transmission, which have been over the range of this paper.

V. CONCLUSION

We proposed a round-trip transmission cv QKD scheme based on the EPR entanglement of optical beams. We mixed the advantage of cv dense coding into QKD, thus the secret key rate is significantly improved. Due to Bob's simultaneously measuring both amplitude and phase quadratures the randomly switching between measurement bases is not required, such that the serious technical limitation on the communication bandwidth placed by the local oscillator switching and the technical difficulty of precisely controlling the phase of a local oscillator no longer exist.

At last, we should mention that, although the EPR optical beams with the anticorrelated amplitude and correlated phase quadratures are discussed in the paper, the scheme and all calculations are also appropriate to the EPR optical beams with the correlated amplitude and anticorrelated phase quadratures $[V(\hat{X}_a-\hat{X}_b)<\text{SNL}, V(\hat{Y}_a+\hat{Y}_b)<\text{SNL}]$, which can be produced from an optical parametric amplifier operating at amplification [12,21]. In this case, Bob only needs to substitute the Bell-state direct detection with two sets of the normal balanced homodyne detector's as described in the original cv dense-coding paper [26].

Several possible attack schemes have been discussed, however, the unconditional security for the proposed protocol has not been demonstrated. Although Eve's eavesdropping technologies are various, the discussed attack schemes are representative and usually used. Especially, the discussions about beam-splitter attack are based on the optimal individual attack allowed by the no-cloning theorem of quantum mechanics, thus have common significance. The theoretical demonstration of unconditional security for the proposed scheme is beyond the scope of the paper and remain an open question.

Due to the sensitivity of the optical quantum entanglement to losses the application of the proposed scheme in the long-distance communication is limited. However, the proposed scheme has shown the possiblility to beat the loss limit of 3 dB using the cv EPR entanglement. Along with the development of quantum optical technology higher and higher determinative cv entanglement can be reached, so the potential of the proposed scheme in future application is expected.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grants No. 60238010 and 60378014).

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference On Computers, Systems and Signal Processing*, Bangalore (IEEE Press, New York, 1984), p. 175.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[4] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, Jpn. J. Appl. Phys., Part 2 **43**, L1217 (2004).

[5] X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui, and G. C. Guo, Opt. Lett. **30**, 2632 (2005).

[6] G. Ribordy, J. Brendel, J. D. Gautier, N. Gisin, and H. Zbinden, Phys. Rev. A **63**, 012309 (2000).

[7] C. Z. Peng, T. Yang, X. H. Bao, J. Zhang, X. M. Jin, F. Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B. L. Tian, and J. W. Pan, Phys. Rev. Lett. **94**, 150501 (2005).

[8] M. Hillery, Phys. Rev. A **61**, 022309 (2000).

[9] N. J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2000).

[10] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (1999); **62**, 062306 (2000).

[11] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).

[12] S. F. Pereira, Z. Y. Ou, and H. J. Kimble, Phys. Rev. A **62**, 042311 (2000); H. J. Kimble, Z. Y. Ou, and S. F. Pereira, U.S. Patent No. 5,339,182, Issued 8/16/94.

[13] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).

[14] K. Bencheikh, TH. Symul, A. Tankovic, and J. A. Levenson, J. Mod. Opt. **48**, 1903 (2001).

[15] Ch. Silberhorn, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **88**, 167902 (2002).

[16] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[17] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).

[18] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[19] S. Lorenz, N. Korolkova, and G. Leuchs, Appl. Phys. A: Mater. Sci. Process. **79**, 273 (2004).

[20] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).

[21] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, Science **282**, 706 (1998).

[22] X. J. Jia, X. L. Su, Q. Pan, J. R. Gao, C. D. Xie, and K. C. Peng, Phys. Rev. Lett. **93**, 250503 (2004).

[23] X. Li, Q. Pan, J. Jing, J. Zhang, C. Xie, and K. Peng, Phys. Rev. Lett. **88**, 047904 (2002).

[24] G. Brassard and L. Salavail, in *Lecture Notes in Computer Science* (Springer, New York, 1994), Vol. 765.

[25] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[26] S. L. Braunstein and H. J. Kimble, Phys. Rev. A **61**, 042302 (2000).

[27] I. P. Degiovanni, I. Ruo Berchera, S. Castelletto, M. L. Rastello, F. A. Bovino, A. M. Colla, and G. Castagnoli, Phys. Rev. A **69**, 032310 (2004).

[28] J. Zhang and K. Peng, Phys. Rev. A **62**, 064302 (2000).

[29] S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and P. van Loock, Phys. Rev. A **64**, 022321 (2001).

[30] L. M. Duan, J. I.Cirac, P. Zoller, and E. S. Polzik, Phys. Rev. Lett. **85**, 5643 (2000).

[31] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[32] S. Iblisdir, G. Van Assche, and N. J. Cerf, Phys. Rev. Lett. **93**, 170502 (2004).

[33] F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005).

[34] M. Navascues and A. Acin, Phys. Rev. Lett. **94**, 020505 (2005).

[35] C. E. Shannon, Bell Syst. Tech. J. **27**, 623 (1948).

[36] R. E. Slusher, L. W. Hollberg, B. Yurke, J. C. Mertz, and J. F. Valley, Phys. Rev. Lett. **55**, 2409 (1985).

[37] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004); S. Suzuki, H. Yonezawa, F. Kannari, M. Sasaki, and A. Furusawa, Appl. Phys. Lett. **89**, 061116 (2006).