Quantum secure communication using continuous variable Einstein-Podolsky-Rosen correlations

Guangqiang He,* Jun Zhu,† and Guihua Zeng‡
State Key Lab of Advanced Optical Communication Systems and Networks, Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai 200030, China
(Received 9 October 2005; published 11 January 2006)

A quantum secure communication protocol using correlations of continuous variable Einstein-Podolsky-Rosen (EPR) pairs is proposed. The proposed protocol may implement both quantum key distribution and quantum message encryption by using a nondegenerate optical parametric amplifier (NOPA). The general Gaussian-cloner attack strategy is investigated in detail by employing Shannon information theory. Results show that the proposed scheme is secure, which is guaranteed physically by the correlations of the continuous variable EPR entanglement pairs generated by the NOPA.

DOI: 10.1103/PhysRevA.73.012314 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum cryptography [1] provides a secure communication way. The security is guaranteed by the law of quantum mechanics [2–4]. Many quantum key distribution (QKD) schemes based on a discrete variable (DV) [1] or continuous variable (CV) [5–11] are presented. In these schemes, the sender (Alice) can encode a binary bit into a quantum state and send it to the receiver (Bob), but Alice cannot determine the bit value that Bob finally decodes. This characteristic means that the previous QKD schemes are nondeterministic, which is very important for guaranteeing the security of these protocols. However, the nondeterministic property results in a loss of qubits; consequently, the efficiency is very low. In addition, these schemes can only distribute random keys but cannot transmit a deterministic message.

Recently several novel deterministic quantum communication schemes based on DV entanglement states [12,13] or nonorthogonal states [14] were proposed. These schemes improve obviously the efficiency of quantum communication protocols by employing the technique of ping-pong of photons. In addition, these schemes may be employed for both distributing meaningless random string of symbols and transmitting meaningful message. Since the DV is not easy in generation as well as detection, the CV becomes a favorable candidate in quantum cryptography [15]. Reid [16] proposed a QKD scheme with predetermined key using CV Einstein-Podolsky-Rosen (EPR) correlations, but the binary modulation on the CV carrier limits its efficiency.

In this paper, we propose a quantum secure communication scheme based on the correlations of the CV EPR pairs. The proposed scheme can be employed as a QKD scheme as well as a quantum encryption scheme for transmitting meaningful messages. The employed continuous Gaussian modulation on the CV carrier enhances markedly the efficiency of the quantum secret communication. Detailed proofs obtained by using Shannon information theory illustrate the security of the proposed scheme against the general Gaussian-cloner eavesdropping strategy.

This paper is organized as follows. In Sec. II, some prerequisite notations are presented so that the proposed scheme may be presented in a compact way in Sec. III. In Sec. IV, the general Gaussian-cloner eavesdropping strategy is analyzed in detail by calculating the information rate ΔI and the parameter F which is associated with the entanglement degree of the entanglement pair. The conclusion is drawn in Sec. V.

II. PREREQUISITE NOTATIONS

For convenience, we first recall some quantum optical notions [17] and define an important parameter F which will be described later. Define the canonical quantum quadratures of a single-mode electromagnetic field, $X=\frac{1}{2}(\hat{a}+\hat{a}^{\dagger})$ and $P=1/2i(\hat{a}-\hat{a}^{\dagger})$. Then X and P obey the Heisenberg uncertainty relation $\Delta X\Delta P \geqslant \frac{1}{4}$. Applying a displacement operator $\hat{D}(\alpha)=\exp(\alpha\hat{a}^{\dagger}-\alpha^{*}\hat{a})$ on an arbitrary input mode $\hat{a}_{in}$ yields

$$\hat{a}_{out}=\hat{D}(\alpha)^{\dagger}\hat{a}_{in}\hat{D}(\alpha)=\hat{a}_{in}+\alpha. \tag{1}$$

For the input and output modes, we have the relationships

$$X_{out}=X_{in}+\mathrm{Re}\{\alpha\},$$

$$P_{out}=P_{in}+\mathrm{Im}\{\alpha\}. \tag{2}$$

Similarly, applying a two-mode squeezing operator $\hat{S}(\xi)=\exp[\kappa t(\hat{a}_{in1}^{\dagger}\hat{a}_{in2}^{\dagger}-\hat{a}_{in1}\hat{a}_{in2})]$ on two arbitrary input modes $\hat{a}_{in1}$ and $\hat{a}_{in2}$ yields

$$\hat{a}_{out1}=\hat{a}_{in1}\cosh(r)+\hat{a}_{in2}^{\dagger}\sinh(r),$$

$$\hat{a}_{out2}=\hat{a}_{in2}\cosh(r)+\hat{a}_{in1}^{\dagger}\sinh(r), \tag{3}$$

where $r=\kappa t$ is the squeezed parameter. These modes have the relationships

$$X_{out1}=X_{in1}\cosh(r)+X_{in2}\sinh(r),$$

$$P_{out1}=P_{in1}\cosh(r)-P_{in2}\sinh(r),$$

*Electronic address: gqhe@sjtu.edu.cn
†Electronic address: bierhoff_24@126.com
‡Electronic address: ghzeng@sjtu.edu.cn

$$X_{out2} = X_{in2}\cosh(r) + X_{in1}\sinh(r),$$

$$P_{out2} = P_{in2}\cosh(r) - P_{in1}\sinh(r). \quad (4)$$

As the squeezed parameter r increases, the EPR correlation between $\hat{a}_{out1}$ and $\hat{a}_{out2}$ becomes increasingly perfect—i.e.,

$$\lim_{r\to+\infty} X_{out1} = X_{out2}, \quad \lim_{r\to+\infty} P_{out1} = -P_{out2}.$$

Apparently, the condition of $X_{out1}=X_{out2}$ and $P_{out1}=-P_{out2}$ implicates that the employed CV EPR pair is an ideal entanglement state—i.e., a maximal entanglement state. To describe generally the entanglement degree of the CV EPR pair, we define an important parameter

$$F = \langle[\Delta(X_{out1} - k_1 X_{out2})]^2\rangle_{min}\langle[\Delta(P_{out1} + k_2 P_{out2})]^2\rangle_{min}, \quad (5)$$

where k_1 and k_2 are coefficients employed for giving minimum variances of $\delta X = X_{out1} - k_1 X_{out2}$ and $\delta P = P_{out1} + k_2 P_{out2}$, respectively. Equation (5) gives the lower bound of the parameter F—i.e., $F_l=0$—at the conditions of the prepared CV EPR pair being a maximal entanglement state and $k_1=k_2=1$, where F_l denotes the lower bound. However, this lower bound $F_l=0$ is difficult to reach in practice since F_l is associated with the squeezed parameter $r=\kappa t$. Generally, a bigger r corresponds to a smaller lower bound F_l, but there is always $F_l>0$ in practice. For instance, when two input quantum states are vacuum states—i.e., $\langle(\Delta X_{ink})^2\rangle = \langle(\Delta P_{ink})^2\rangle = \frac{1}{4}$, $k=1,2$, the lower bound $F_l = 4.42\times10^{-3}$ with $r=1$ and $F_l = 2.325\times10^{-18}$ with $r=10$. Once the entanglement correlation was destroyed, F would quickly increase. While two modes are independent, F approaches infinity. Therefore, the parameter F may be employed to describe the entanglement degree of a two-mode entanglement system. Actually, $F < \frac{1}{16}$ for the EPR correlation has been obtained in Ref. [18].

III. PROTOCOL

The proposed scheme can be employed to distribute random secret key as well as transmit meaningful message via choosing different input parameters of a nondegenerate optical parametric amplifier (NOPA) (see Fig. 1). This protocol may be described generally by the following steps.

Step 1. Alice's modulation on two input modes $\hat{a}_1$ and $\hat{a}_2$ with displacement operators $\hat{D}(\alpha=x+ix)$ and $\hat{D}(\beta=y+iy)$, respectively, yields two new modes $\hat{a}_3=\hat{D}^\dagger(\alpha)\hat{a}_1\hat{D}(\alpha)$ and $\hat{a}_4=\hat{D}^\dagger(\beta)\hat{a}_2\hat{D}(\beta)$, which are the input modes of the NOPA. The corresponding output modes of the NOPA are $\hat{a}_5 = \hat{S}^\dagger(\xi)\hat{a}_3\hat{S}(\xi)$ and $\hat{a}_6=\hat{S}^\dagger(\xi)\hat{a}_4\hat{S}(\xi)$. When a squeezed parameter r is proper, the mode $\hat{a}_5$ correlates with mode $\hat{a}_6$, and this correlation increases with r to be larger. The random numbers x and y are drawn from the Gaussian probability distributions $X\sim N(0,\Sigma^2)$ and $Y\sim N(0,\sigma^2)$, respectively, where $\lambda\sim N(\mu,\sigma^2)$ denotes that the random variable λ follows a Gaussian probability distribution with average value μ and variance σ^2.

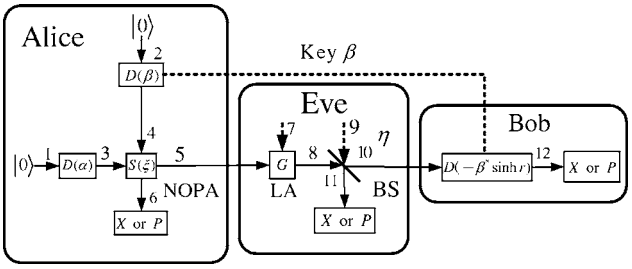

FIG. 1. Schematic representation of a quantum secure communication scheme based on continuous variable EPR correlations. NOPA: nondegenerate optical parametric amplifier. LA: linear amplifier. BS: beam splitter. $D(\alpha), D(\beta)$: displacement operators. $S(\xi)$: two-mode squeezing operator of NOPA. G: the gain of LA. η: the transmission coefficient of BS. The Arabic numerals denote the modes.

Step 2. Alice calculates the parameter F_a between $\hat{a}_5$ and $\hat{a}_6$ according to Eq. (5) and measures either X or P of $\hat{a}_6$ during some time slots. Alice writes down both the measurement results and the corresponding time slots for detecting Eve after finishing transmission, while the mode $\hat{a}_5$ is sent to Bob.

Step 3. Bob applies $D[-\beta^* \sinh(r)]$ to the received mode $\hat{a}_{10}$. The mode $\hat{a}_{10}$ is the same as $\hat{a}_5$ when the Eve is absent in the quantum channel. After finishing the operation, Bob measures either X or P of the output mode $\hat{a}_{12}$.

Step 4. Alice tells Bob both her measurement results and the corresponding time slots through a classical public channel. Bob estimates the parameter F_b according to Eq. (5) by comparing Alice's measurement results with his own measurement results with the corresponding time slots. If $F_b > F_a$, Eve exists; while if $F_b=F_a$, Eve does not exist.

Step 5. To distribute a meaningless random string of symbols—i.e., the quantum key distribution—the parameter y is chosen to be 0 in step 1; consequently, $\beta=0=\beta^*$. In terms of the measurement results, Alice and Bob may generate a quantum key. If Alice wants to transmit a meaningful message to Bob—i.e., as a quantum encryption algorithm—the parameter x is regarded as the message which needs to be transmitted to Bob while y acts as the private key shared between Alice and Bob. After finished step 3, Bob may decode Alice's message while the attacker is detected in step 4. In the quantum encryption process, the message will be divided into L blocks in order to prevent Eve from obtaining more useful information; the above four steps are executed for each block. Once Eve is found, the communication is stopped.

IV. SECURITY ANALYSIS

Security is an important issue in quantum cryptography. In this section, we investigate the security of the proposed scheme by employing Shannon information theory. The secret information rate ΔI and the entanglement parameter F are regarded as important parameters for showing the security and eavesdropping detection, respectively. In the quantum key distribution process, Alice and Bob are only concerned with the secret information rate $\Delta I = I(\alpha,\beta) - I(\alpha,\epsilon)$,

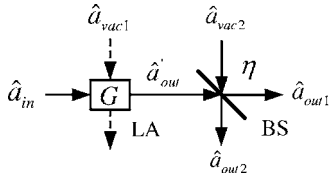

FIG. 2. The principle of a quantum Gaussian cloning machine for complete two quadrature copies. LA: linear amplifier. BS: beam splitter. G: the gain of LA. η: the transmission coefficient of BS.

where $I(\alpha,\beta)$ denotes the mutual information between Alice and Bob, and $I(\alpha,\epsilon)$ denotes the mutual information between Alice and Eve. In the quantum encryption process, Alice and Bob are concerned with the maximal mutual information between Alice and Eve $I_{max}(\alpha,\epsilon)$. In the proposed protocol, increasing the noise Y can make $I_{max}(\alpha,\epsilon)$ small as soon as possible and enhances the security level of the quantum encryption process.

A. Principle of general Gaussian-cloner attack strategy

Before the detailed analysis for security, we describe the general Gaussian-cloner attack strategy. The Gaussian cloner consists of a linear amplifier (LA) and beam splitter (BS); see Fig. 2. Let $\hat{a}_{in}$ and $\hat{a}_{vac1}$ be two input modes of the LA; one of the two output modes of LA is obtained by the equation

$$\hat{a}'_{out} = \sqrt{G}\hat{a}_{in} + \sqrt{G-1}\hat{a}^{\dagger}_{vac1}, \tag{6}$$

where $G \geqslant 1$ is the gain of the LA and $\hat{a}'_{out}$ and $\hat{a}_{vac2}$ are two input modes of the beam splitter. When $G=1$, the Gaussian cloner reduces to a beam splitter. Two output modes of the Gaussian cloner are given by

$$\begin{aligned}\hat{a}_{out1} &= \sqrt{\eta}\hat{a}'_{out} + \sqrt{1-\eta}\hat{a}_{vac2} \\ &= \sqrt{G\eta}\hat{a}_{in} + \sqrt{(G-1)\eta}\hat{a}^{\dagger}_{vac1} + \sqrt{1-\eta}\hat{a}_{vac2},\end{aligned}$$

$$\begin{aligned}\hat{a}_{out2} &= \sqrt{\eta}\hat{a}_{vac2} - \sqrt{1-\eta}\hat{a}'_{out} \\ &= \sqrt{\eta}\hat{a}_{vac2} - \sqrt{G(1-\eta)}\hat{a}_{in} - \sqrt{(G-1)(1-\eta)}\hat{a}^{\dagger}_{vac1},\end{aligned} \tag{7}$$

where η is the transmission coefficient of the BS. Based on above equations, we obtain the equations

$$X_{out1} = \sqrt{G\eta}X_{in} + \sqrt{(G-1)\eta}X_{vac1} + \sqrt{1-\eta}X_{vac2},$$

$$P_{out1} = \sqrt{G\eta}P_{in} - \sqrt{(G-1)\eta}P_{vac1} + \sqrt{1-\eta}P_{vac2},$$

$$X_{out2} = \sqrt{\eta}X_{vac2} - \sqrt{G(1-\eta)}X_{in} - \sqrt{(G-1)(1-\eta)}X_{vac1},$$

$$P_{out2} = \sqrt{\eta}P_{vac2} - \sqrt{G(1-\eta)}P_{in} + \sqrt{(G-1)(1-\eta)}P_{vac1}. \tag{8}$$

Making use of Eq. (8), one may investigate the properties of the output modes of the Gaussian cloner.

B. Secret information rate

If $\Delta I > 0$, Alice and Bob can obtain a secret key by employing the techniques of classical error correction and privacy amplification. In the following, we first determine the probability distribution of X and P in all modes as depicted in Fig. 1, then calculate $I(\alpha,\beta)$ and $I(\alpha,\epsilon)$ according to Shannon information theory. Using Eq. (2), the canonical quantum quadratures of the input modes of the NOPA are given by the equations

$$X_3 = X_1 + X, \quad P_3 = P_1 + X, \tag{9}$$

$$X_4 = X_2 + Y, \quad P_4 = P_2 + Y. \tag{10}$$

According to Eq. (4), two output modes of the NOPA are given by

$$\begin{aligned}X_5 &= X_3\cosh(r) + X_4\sinh(r), \\ P_5 &= P_3\cosh(r) - P_4\sinh(r), \\ X_6 &= X_4\cosh(r) + X_3\sinh(r), \\ P_6 &= P_4\cosh(r) - P_3\sinh(r).\end{aligned} \tag{11}$$

The modes $\hat{a}_5$ and $\hat{a}_6$ are entanglement beams; therefore,

$$\lim_{r\to+\infty} X_5 = X_6, \quad \lim_{r\to+\infty} P_5 = -P_6. \tag{12}$$

Suppose that Eve employs the Gaussian cloner to eavesdrop on the quantum channel. Employing Eq. (8) the output modes $\hat{a}_{10}$ and $\hat{a}_{11}$ of the cloner are given by the equations

$$\begin{aligned}X_{10} &= \sqrt{G\eta}X_5 + \sqrt{(G-1)\eta}X_7 + \sqrt{1-\eta}X_9, \\ P_{10} &= \sqrt{G\eta}P_5 - \sqrt{(G-1)\eta}P_7 + \sqrt{1-\eta}P_9, \\ X_{11} &= \sqrt{\eta}X_9 - \sqrt{G(1-\eta)}X_5 - \sqrt{(G-1)(1-\eta)}X_7, \\ P_{11} &= \sqrt{\eta}P_9 - \sqrt{G(1-\eta)}P_5 + \sqrt{(G-1)(1-\eta)}P_7.\end{aligned} \tag{13}$$

Combing Eqs. (9)–(11) and (13), one easily obtains

$$\begin{aligned}X_{11} = &-\sqrt{G(1-\eta)}\cosh(r)X - \sqrt{G(1-\eta)}\cosh(r)X_1 \\ &- \sqrt{G(1-\eta)}\sinh(r)X_2 - \sqrt{G(1-\eta)}\sinh(r)Y \\ &- \sqrt{(G-1)(1-\eta)}X_7 + \sqrt{\eta}X_9, \\ P_{11} = &-\sqrt{G(1-\eta)}\cosh(r)X - \sqrt{G(1-\eta)}\cosh(r)P_1 \\ &+ \sqrt{G(1-\eta)}\sinh(r)P_2 + \sqrt{G(1-\eta)}\sinh(r)Y \\ &+ \sqrt{(G-1)(1-\eta)}P_7 + \sqrt{\eta}P_9,\end{aligned} \tag{14}$$

where the random variables in the above equation follow the Gaussian distribution

$$X \sim N(0,\Sigma^2), \quad Y \sim N(0,\sigma^2), \quad X_i, P_i \sim N\left(0,\frac{1}{4}\right), \tag{15}$$

with $i=1,2,7,9$. Equation (15) means that all input states are vacuum states. Since X_{12} and P_{12} of $\hat{a}_{12}$ satisfy

$$X_{12} = X_{10} - \sinh(r)Y,$$

$$P_{12} = P_{10} + \sinh(r)Y, \tag{16}$$

the expressions of X_{12} and P_{12} are given by the equations

$$X_{12} = \sqrt{G\eta}\cosh(r)X + \sqrt{G\eta}\cosh(r)X_1 + \sqrt{G\eta}\sinh(r)X_2 + (\sqrt{G\eta} - 1)\sinh(r)Y + \sqrt{\eta(G-1)}X_7 + \sqrt{1-\eta}X_9,$$

$$P_{12} = \sqrt{G\eta}\cosh(r)X + \sqrt{G\eta}\cosh(r)P_1 - \sqrt{G\eta}\sinh(r)P_2 + (1 - \sqrt{G\eta})\sinh(r)Y - \sqrt{(G-1)\eta}P_7 + \sqrt{1-\eta}P_9. \tag{17}$$

According to Eqs. (14) and (15), one may easily calculate the variances of X_{11} and P_{11},

$$\langle(\Delta X_{11})^2\rangle = G(1-\eta)\cosh^2(r)\Sigma^2 + G(1-\eta) \times \left[\frac{1}{4}\cosh^2(r) + \frac{1}{4}\sinh^2(r) + \sinh^2(r)\sigma^2\right] + \frac{1}{4}(G-1)(1-\eta) + \frac{1}{4}\eta,$$

$$\langle(\Delta P_{11})^2\rangle = G(1-\eta)\cosh^2(r)\Sigma^2 + G(1-\eta) \times \left[\frac{1}{4}\cosh^2(r) + \frac{1}{4}\sinh^2(r) + \sinh^2(r)\sigma^2\right] + \frac{1}{4}(G-1)(1-\eta) + \frac{1}{4}\eta. \tag{18}$$

Obviously, in any case of measuring either X or P, the variance of the signal distribution is given by

$$M = G(1-\eta)\cosh^2(r)\Sigma^2 \tag{19}$$

and the variance of noise is given by

$$N = G(1-\eta) \times \left[\frac{1}{4}\cosh^2(r) + \frac{1}{4}\sinh^2(r) + \sinh^2(r)\sigma^2\right] + \frac{1}{4}(G-1)(1-\eta) + \frac{1}{4}\eta. \tag{20}$$

Thus, the signal-to-noise ratio in the communication between Alice and Eve can be easily obtained by using Eqs. (19) and (20)—i.e.,

$$\gamma_{\alpha\epsilon} = \frac{M}{N}. \tag{21}$$

According to Shannon information theory [19], the channel capacity of the additive white Gaussian noise (AWGN) channel is

$$I = \frac{1}{2}\log_2(1+\gamma), \tag{22}$$

where $\gamma = \Sigma^2/\sigma^2$ is the signal-to-noise ratio and Σ^2 and σ^2 are the variances of the signal and noise probability distributions, respectively. If the signal follows the Gaussian distribution and the channel is the AWGN channel, then the channel capacity is the mutual information of the communication parties. Consequently, the mutual information between Alice and Eve is

$$I(\alpha,\epsilon) = \frac{1}{2}\log_2(1+\gamma_{\alpha\epsilon}). \tag{23}$$

According to Eqs. (15) and (17), the variances of X_{12} and P_{12} are given by the equations

$$\langle(\Delta X_{12})^2\rangle = G\eta\cosh^2(r)\Sigma^2 + \frac{1}{4}G\eta[\cosh^2(r) + \sinh^2(r)] + (\sqrt{G\eta} - 1)^2\sinh^2 r\sigma^2 + \frac{1}{4}(G-1)\eta + \frac{1}{4}(1-\eta),$$

$$\langle(\Delta P_{12})^2\rangle = G\eta\cosh^2(r)\Sigma^2 + \frac{1}{4}G\eta[\cosh^2(r) + \sinh^2(r)] + (\sqrt{G\eta} - 1)^2\sinh^2 r\sigma^2 + \frac{1}{4}(G-1)\eta + \frac{1}{4}(1-\eta). \tag{24}$$

Equation (24) shows that the variance of the signal distribution is always given by

$$P = G\eta\cosh^2(r)\Sigma^2 \tag{25}$$

and the variance of noise is given by

$$Q = \frac{1}{4}G\eta[\cosh^2(r) + \sinh^2(r)] + (\sqrt{G\eta} - 1)^2\sinh^2 r\sigma^2 + \frac{1}{4}(G-1)\eta + \frac{1}{4}(1-\eta). \tag{26}$$

Then, we obtain the signal-to-noise ratio between Alice and Bob,

$$\gamma_{\alpha\beta} = \frac{P}{Q}. \tag{27}$$

According to Eq. (22), the mutual information between Alice and Bob is

$$I(\alpha,\beta) = \frac{1}{2}\log_2(1+\gamma_{\alpha\beta}). \tag{28}$$

Making use of Eqs. (23) and (28), one may obtain the mutual informations $I(\alpha,\beta)$ and $I(\alpha,\epsilon)$. The final key is secure if $I(\alpha,\beta) > I(\alpha,\epsilon)$ since in this situation Alice and Bob may distill a secure key by using the classical error correction and privacy amplification. Accordingly, the final key can be constructed according to the condition [9,20]

$$\Delta I = I(\alpha,\beta) - I(\alpha,\epsilon) > 0. \tag{29}$$

When Eve does not exist—i.e., $G=1$ and $\eta=1$—Eqs. (23) and (29) give

$$I(\alpha,\epsilon) = 0,$$

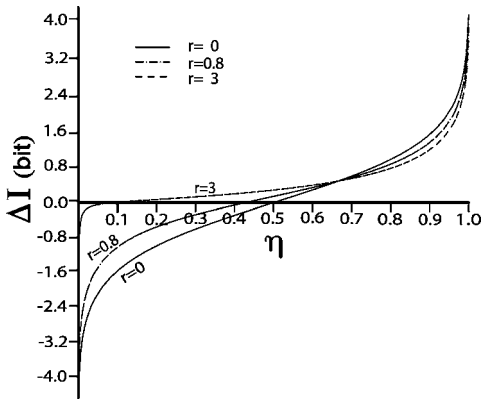

FIG. 3. The dependence of ΔI on η in the QKD process ($\Sigma=10$, $\sigma=0$, $G=1$).

$$\Delta I = I(\alpha,\beta) = \frac{1}{2}\log_2\left[1+\frac{4\Sigma^2}{1+\tanh^2(r)}\right]. \tag{30}$$

In this case the information rate ΔI is actually the channel capacity of the quantum communication between Alice and Bob. One may find that this capacity is larger than that in the DV quantum communication. In addition, Eq. (30) shows that the secret information ΔI increases with the variance of signal Σ^2 increasing, while it is almost a constant when $r \geqslant 3$.

For a QKD scheme, the condition for obtaining a secure key is $\Delta I>0$ [20]. For convenience, we specify $\Sigma=10$, $\sigma=0$ for the QKD process in the remaining text. Since the information rate ΔI depends on the parameter η, we plot Figs. 3 and 4 a demonstration of the relationship between ΔI and η. Figure 3 shows that η is smaller with larger r at $\Delta I=0$, which indicates that the CV EPR pair with a higher entanglement degree is more suitable for implementation of the secure key distribution. In Fig. 4 the relationship between η and G is demonstrated clearly. One may find that η is smaller with larger G at $\Delta I=0$. Especially, our scheme is reduced to Grosshans and Grangier's scheme [9] at the condition of $r=0$ and $G=1$, and the secure condition of Grosshans and Grangier's scheme—i.e., $\eta>0.5$—may be obtained by using our approach.

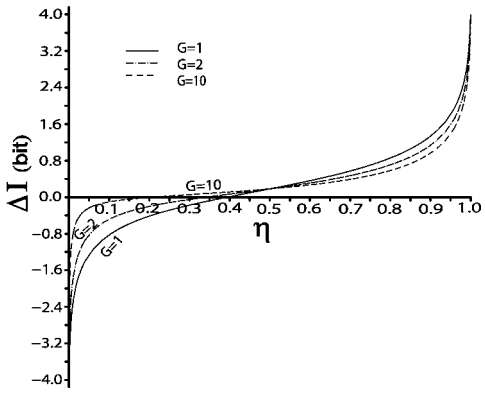

FIG. 4. The dependence of ΔI on η in the QKD process ($\Sigma=10$, $\sigma=0$, $r=1$).

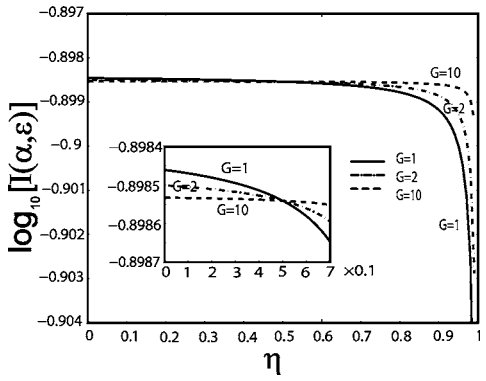

FIG. 5. The dependence of $I(\alpha,\epsilon)$ on η in the quantum encryption process. The parameters are $\Sigma=10$, $\sigma=30$, and $r=1$.

In a quantum encryption algorithm, what one is concerned with is how much information may Eve eavesdrop on the meaningful message. Therefore we focus on the mutual information $I(\alpha,\epsilon)$. To demonstrate the dependence of $I(\alpha,\epsilon)$ on η, we plot Fig. 5 with $r=1$, $\Sigma=10$, and $\sigma=30$. The smaller range of $0<\eta<0.7$ is zoomed in (see inset). The inset demonstrates when Eve taps off 30% of the signal beam—i.e., $\eta=0.7$—the information $I(\alpha,\epsilon)$ she obtains is 0.1262 bits. In addition, Eve may obtain 0.1263 bits when she taps off all signal beams—i.e., $\eta=0$. Figure 5 shows that the 0.1263 bits is the maximal information that Eve can obtain, which is much less than the mutual information $I(\alpha,\beta)=3.99$ bits without Eve. In addition, $I_{max}(\alpha,\epsilon)$ quickly decreases with σ^2 increasing: for example, $I_{max}(\alpha,\epsilon)=3.5\times10^{-6}$ bits with $\sigma=6000$. Therefore the proposed quantum encryption algorithm is regarded as a quasisecure scheme. In addition, the parameters r and σ may be properly selected to describe the security level demanded by the consumer.

From Fig. 5, we find that the mutual information $I(\alpha,\epsilon)$ seems invariable when $\eta<0.7$, which implies that Eve's information is almost a constant in this situation. Physically, it can be explained as follows. In the quantum encryption process the signal is disturbed by the key-controlling noise. The legitimate communicators, Alice and Bob, can remove the noise by using the shared key, but Eve cannot remove the noise correctly. A stronger key-controlling noise is more useful for preventing Eve from distinguishing the signal from the noise. When the noise becomes strong enough, Eve cannot obtain more information even if she taps off all the signal beam. In this situation the parameter η does not play a significant role. This is why $I(\alpha,\epsilon)$ seems invariable in the range of $0<\eta<0.7$.

C. Detecting Eve

Eve's attack inevitably disturbs the probability distribution of the travel beam $\hat{a}_5$, which will destroy the entanglement relation between $\hat{a}_5$ and $\hat{a}_6$. Using this characteristic, we propose an approach for detecting Eve by comparing F_a with F_b.

Define two random variables

$$\delta X_{Eve} = X_{10} - k_1 X_6,$$

$$\delta P_{Eve} = P_{10} + k_2 P_6. \tag{31}$$

If Eve does not exist—i.e., $\hat{a}_{10} = \hat{a}_5$—Eqs. (31) become

$$\delta X_{no\ Eve} = X_5 - k_1 X_6,$$

$$\delta P_{no\ Eve} = P_5 + k_2 P_6. \tag{32}$$

Combining Eqs. (9)–(11) and (32) gives

$$\langle [\Delta(\delta X_{no\ Eve})]^2 \rangle = [\cosh(r) - k_1 \sinh(r)]^2 \left(\Sigma^2 + \frac{1}{4}\right) + [\sinh(r) - k_1 \cosh(r)]^2 \left(\sigma^2 + \frac{1}{4}\right),$$

$$\langle [\Delta(\delta P_{no\ Eve})]^2 \rangle = [\cosh(r) - k_2 \sinh(r)]^2 \left(\Sigma^2 + \frac{1}{4}\right) + [\sinh(r) - k_2 \cosh(r)]^2 \left(\sigma^2 + \frac{1}{4}\right), \tag{33}$$

where the assumption of two input states of the NOPA being vacuum states is employed.

When

$$k_1 = k_2 = \frac{R}{S}, \tag{34}$$

where $R = 2\sinh(r)\cosh(r)(1 + 2\Sigma^2 + 2\sigma^2)$ and $S = \sinh^2(r) + \cosh^2(r) + 4\sinh^2(r)\Sigma^2 + 4\cosh^2(r)\sigma^2$, $\langle [\Delta(\delta X_{no\ Eve})]^2 \rangle$ and $\langle [\Delta(\delta P_{no\ Eve})]^2 \rangle$ reach the minimal values

$$\langle [\Delta(\delta X_{no\ Eve})]^2 \rangle_{min} = \langle [\Delta(\delta P_{no\ Eve})]^2 \rangle_{min} = \frac{W}{Z}, \tag{35}$$

where $W = 4\Sigma^2 + 16\Sigma^2\sigma^2 + 4\sigma^2 + 1$ and $Z = 8\cosh^2(r) + 16\cosh^2(r)(\Sigma^2 + \sigma^2) - 16\Sigma^2 - 4$. According to Eq. (5), Alice obtains

$$F = \langle [\Delta(\delta X_{no\ Eve})]^2 \rangle_{min} \langle [\Delta(\delta P_{no\ Eve})]^2 \rangle_{min}, \tag{36}$$

when Σ^2, σ^2, and r are specified.

According to Eqs. (9)–(11), (13), and (31), Bob obtains

$$\delta X_{Eve} = [\sqrt{G\eta}\cosh(r) - k_1 \sinh(r)](X_1 + X) + [\sqrt{G\eta}\sinh(r) - k_1 \cosh(r)] \times (X_2 + Y) + \sqrt{\eta(G-1)} X_7 + \sqrt{1-\eta} X_9,$$

$$\delta P_{Eve} = [\sqrt{G\eta}\cosh(r) - k_2 \sinh(r)](P_1 + X) + [k_2 \cosh(r) - \sqrt{G\eta}\sinh(r)](P_2 + Y) - \sqrt{\eta(G-1)} P_7 + \sqrt{1-\eta} P_9. \tag{37}$$

The variances of δX_{Eve} and δP_{Eve} can be obtained according to Eqs. (15) and (37):

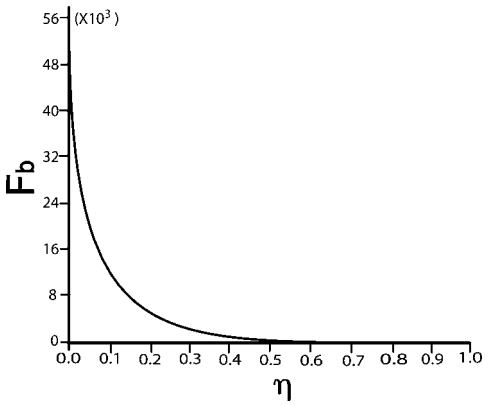

FIG. 6. The relation between F_b and η in the QKD process ($\Sigma = 10$, $\sigma = 0$, $r = 1$, $G = 1$).

$$\langle [\Delta(\delta X_{Eve})]^2 \rangle = [\sqrt{G\eta}\cosh(r) - k_1 \sinh(r)]^2 \left(\frac{1}{4} + \Sigma^2\right) + [\sqrt{G\eta}\sinh(r) - k_1 \cosh(r)]^2 \left(\frac{1}{4} + \sigma^2\right) + \frac{1}{4}\eta(G-1) + \frac{1}{4}(1-\eta),$$

$$\langle [\Delta(\delta P_{Eve})]^2 \rangle = [\sqrt{G\eta}\cosh(r) - k_2 \sinh(r)]^2 \left(\frac{1}{4} + \Sigma^2\right) + [\sqrt{G\eta}\sinh(r) - k_2 \cosh(r)]^2 \left(\frac{1}{4} + \sigma^2\right) + \frac{1}{4}\eta(G-1) + \frac{1}{4}(1-\eta). \tag{38}$$

Substituting Eq. (34) into Eqs. (38), Bob obtains

$$F_b = \langle [\Delta(\delta X_{Eve})]^2 \rangle \langle [\Delta(\delta P_{Eve})]^2 \rangle. \tag{39}$$

Figure 6 demonstrates the dependence of F_b on parameters η for the QKD process. The parameter F_b decreases rapidly with η increasing.

D. Relationship between ΔI and F_b

The relationship between ΔI and F_b is useful in practice. Since the analytical expression is very complex, we present a

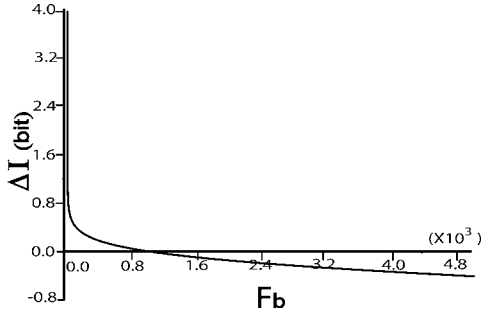

FIG. 7. The relation between ΔI and F_b in the QKD process ($\Sigma = 10$, $\sigma = 0$, $r = 1$, $G = 1$).

numerical solution, which is illustrated in Fig. 7. Obviously, ΔI decreases with F_b increasing. It illustrates that the less information Eve obtains, the smaller the probability that she is detected by Alice and Bob is. ΔI reaches its maximal value ΔI_{max} when F_b reaches the minimal value. For $\Sigma=10$, $\sigma=0$, $G=1$, $r=1$, $F_{bmin}=3.248\times10^{-2}<\frac{1}{16}$, and $\Delta I_{max}=3.995$ bits, which is higher than the information rate of DV communication [16]. Increasing the variance of the signal Σ^2 can enhance ΔI_{max}.

V. CONCLUSION

A quantum secure communication scheme based on the correlations of the CV EPR pairs is proposed. The proposed scheme can distribute the quantum key as well as transmit meaningful messages with a preshared key. By calculating the secret information rate ΔI and the Shannon mutual information $I(\alpha,\epsilon)$, the proposed scheme is proved to be secure against the Gaussian-cloner attack strategy. Physically, the security of the proposed scheme is guaranteed by the correlations of the CV EPR pair produced by the NOPA. In addition, by defining a useful parameter F which is associated with the entanglement degree, Eve can be detected by legitimate communicators.

ACKNOWLEDGMENT

This work is supported by the Natural Science Foundation of China, Grant No. 60472018.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002), and references therein.
[2] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[4] D. Mayers, J. ACM **48**, 351 (2001).
[5] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (1999).
[6] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
[7] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[8] N. J. Cerf, M. Lévy, and G. VanAssche, Phys. Rev. A **63**, 052311 (2001).
[9] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[10] Ch. Silberhorn, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **88**, 167902 (2002).
[11] F. Grosshans *et al.*, Nature (London) **421**, 238 (2003).
[12] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[13] A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003); Q.-Y. Cai, Phys. Rev. Lett. **91**, 109801 (2003).
[14] M. Lucamarini and S. Mancini, Phys. Rev. Lett. **94**, 140501 (2005).
[15] S. L. Braunstein and P. v. Loock, Rev. Mod. Phys. **77**, 513 (2005).
[16] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).
[17] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer-Verlag, New York, 1997).
[18] M. D. Reid, Phys. Rev. A **40**, 913 (1989); M. D. Reid and P. D. Drummond, Phys. Rev. Lett. **60**, 2731 (1988).
[19] C. E. Shannon, Bell Syst. Tech. J. **27**, 623 (1948).
[20] U. M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).