Vol 15 No 6, June 2006
1009-1963/2006/15(06)/1284-06

Chinese Physics

Deterministic quantum key distribution based on Gaussian-modulated EPR correlations*

He Guang-Qiang(何广强) and Zeng Gui-Hua(曾贵华)

The State Key Laboratory of Fibre-Optic Local Area Networks and Advanced Optical Communication Systems

Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai 200030, *China*

(Received 5 October 2005; revised manuscript received 25 February 2006)

This paper proposes a deterministic quantum key distribution scheme based on Gaussian-modulated continuous variable EPR correlations. This scheme can implement fast and efficient key distribution. The security is guaranteed by continuous variable EPR entanglement correlations produced by nondegenerate optical parametric amplifier. For general beam splitter eavesdropping strategy, the secret information rate $\Delta I = I(\alpha, \beta) - I(\alpha, \epsilon)$ is calculated in view of Shannon information theory. Finally the security analysis is presented.

Keywords: quantum key distribution, continuous variable EPR correlation, Gaussian modulation
PACC: 4250, 4230Q, 0365

1. Introduction

Quantum cryptography[1] provides secret communication, the security is guaranteed by the law of quantum mechanics.[2−4] Now many quantum cryptography schemes[5−12] are nondeterministic, their efficiency is low. Recently, based on discrete variable (DV) entanglement states[13,14] or the nonorthogonal states,[15] several novel deterministic communication schemes are proposed, they improve the efficiency of quantum communication protocols, but both the DV entanglement and single quanta are neither generated nor detected easily. The continuous variable (CV) can be more easily generated and manipulated than DV, the channel capacity of CV communication can be enhanced. Thus designing the CV deterministic quantum key distribution is a very interesting problem in this region, Reid provided a means to distribute a discrete predetermined key[16] based on CV entanglements produced by nondegenerate optical parametric amplifier (NOPA), but the binary modulation on CV limits its efficiency.

In this paper, we propose a deterministic quantum key distribution scheme based on Gaussian-modulated CV EPR correlations, which can distribute continuous predetermined secret keys. In Section 2, we introduce the prerequisite knowledge needed by this scheme. In Section 3, the scheme is presented in detail. In Section 4, the security of the scheme is analysed. The conclusion is drawn in Section 5.

2. The prerequisite knowledge

In this paper, we define the canonical quantum quadratures of a single mode electromagnetic field, $X = \frac{1}{2}(\hat{a} + \hat{a}^\dagger)$ and $P = \frac{1}{2\mathrm{i}}(\hat{a} - \hat{a}^\dagger)$. Then X and P obey the Heisenberg uncertainty relation

$$\Delta X \Delta P \geq \frac{1}{4}. \tag{1}$$

In quantum optics, [17] applying the displacement operator

$$\hat{D}(\alpha) = \exp(\alpha \hat{a}^\dagger - \alpha^* \hat{a}) \tag{2}$$

on an arbitrary input mode $\hat{a}_{\rm in}$ gives

$$\hat{a}_{\rm out} = \hat{D}(\alpha)^\dagger \hat{a}_{\rm in} \hat{D}(\alpha) = \hat{a}_{\rm in} + \alpha. \tag{3}$$

Then the following equations are satisfied

$$\begin{aligned} X_{\rm out} &= X_{\rm in} + {\rm Re}\{\alpha\}, \\ P_{\rm out} &= P_{\rm in} + {\rm Im}\{\alpha\}. \end{aligned} \tag{4}$$

Applying the two mode squeezing operator (NOPA)

$$\hat{S}(\xi) = \exp[\kappa t(\hat{a}_{\rm in1}^\dagger \hat{a}_{\rm in2}^\dagger - \hat{a}_{\rm in1} \hat{a}_{\rm in2})] \tag{5}$$

*Project supported by the National Natural Science Foundation of China (Grant No 60472018).

on two arbitrary input modes $\hat{a}_{\rm in1}$ and $\hat{a}_{\rm in2}$ gives

$$\begin{aligned}\hat{a}_{\rm out1} &= \hat{a}_{\rm in1}\cosh(r) + \hat{a}^{\dagger}_{\rm in2}\sinh(r),\\ \hat{a}_{\rm out2} &= \hat{a}_{\rm in2}\cosh(r) + \hat{a}^{\dagger}_{\rm in1}\sinh(r),\end{aligned} \tag{6}$$

where $r = \kappa t$ is the squeezed parameter. Then the following equations are satisfied:

$$\begin{aligned}X_{\rm out1} &= X_{\rm in1}\cosh(r) + X_{\rm in2}\sinh(r),\\ P_{\rm out1} &= P_{\rm in1}\cosh(r) - P_{\rm in2}\sinh(r),\\ X_{\rm out2} &= X_{\rm in2}\cosh(r) + X_{\rm in1}\sinh(r),\\ P_{\rm out2} &= P_{\rm in2}\cosh(r) - P_{\rm in1}\sinh(r).\end{aligned} \tag{7}$$

As the squeezed parameter r increases, EPR correlation between $\hat{a}_{\rm out1}$ and $\hat{a}_{\rm out2}$ becomes increasingly prefect, and

$$\begin{aligned}F =&\langle(\Delta(X_{\rm out1} - k_1 X_{\rm out2}))^2\rangle_{\rm min}\\ &\times\langle(\Delta(P_{\rm out1} + k_2 P_{\rm out2}))^2\rangle_{\rm min}\end{aligned} \tag{8}$$

is close to 0, where k_1 and k_2 are parameters which can be modified to give the minimum variances of $\delta X = X_{\rm out1} - k_1 X_{\rm out2}$ and $\delta P = P_{\rm out1} + k_2 P_{\rm out2}$ respectively. When $F < \dfrac{1}{16}$, the EPR correlation is obtained.[18]

In the Heisenberg picture, $\hat{a}_{\rm vac1}$ and $\hat{a}_{\rm vac2}$ are two input modes of beam splitter, then two output modes are

$$\begin{aligned}\hat{a}_{\rm out1} =&\sqrt{\eta}\hat{a}_{\rm vac1} + \sqrt{1-\eta}\hat{a}_{\rm vac2},\\ \hat{a}_{\rm out2} =&\sqrt{\eta}\hat{a}_{\rm vac2} - \sqrt{1-\eta}\hat{a}_{\rm vac1},\end{aligned} \tag{9}$$

where η is the transmittance coefficient of beam splitter (BS). Then the following equations are satisfied:

$$\begin{aligned}\hat{X}_{\rm out1} =&\sqrt{\eta}\hat{X}_{\rm vac1} + \sqrt{1-\eta}\hat{X}_{\rm vac2},\\ \hat{P}_{\rm out1} =&\sqrt{\eta}\hat{P}_{\rm vac1} + \sqrt{1-\eta}\hat{P}_{\rm vac2},\\ \hat{X}_{\rm out2} =&\sqrt{\eta}\hat{X}_{\rm vac2} - \sqrt{1-\eta}\hat{X}_{\rm vac1},\\ \hat{P}_{\rm out2} =&\sqrt{\eta}\hat{P}_{\rm vac2} - \sqrt{1-\eta}\hat{P}_{\rm vac1}.\end{aligned} \tag{10}$$

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

$$I = \frac{1}{2}\log_2(1+\gamma), \tag{11}$$

where $\gamma = \Sigma^2/\sigma^2$ is the signal-noise ratio, 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 AWGN channel, then the channel capacity is the mutual information of the communication parties.

In this paper, $X \sim N(\mu, \sigma^2)$ denotes that the random variable X follows Gaussian probability distribution with the average value μ and the variance σ^2.

3. The deterministic quantum key distribution protocol

The protocol is depicted as in Fig.1; Alice firstly modulates $\hat{a}_1$ by applying displacement operator $\hat{D}(\alpha = x + ix)$, where x is the random number drawn from Gaussian probability distribution. The modes $\hat{a}_3 = \hat{D}^{\dagger}(\alpha)\hat{a}_1\hat{D}(\alpha)$ and $\hat{a}_2$ are two input modes of NOPA, the output modes of NOPA are $\hat{a}_4 = \hat{S}^{\dagger}(\xi)\hat{a}_3\hat{S}(\xi)$ and $\hat{a}_5 = \hat{S}^{\dagger}(\xi)\hat{a}_2\hat{S}(\xi)$. As the squeezed parameter r increases, $\hat{a}_4$ becomes increasingly correlated with $\hat{a}_5$. Alice calculates F between $\hat{a}_4$ and $\hat{a}_5$, and measures either X or P of $\hat{a}_5$ during some time slots, Alice writes down both the measurement results and the corresponding time slots for detecting Eve after finishing transmission, $\hat{a}_4$ is sent to Bob. Bob then measures either X or P of $\hat{a}_7$, the mode $\hat{a}_7$ is the mode $\hat{a}_4$ without the presence of Eve. After finishing transmission, Alice tells Bob both her measurement results and the corresponding time slots through the classical public channel. Bob calculates $F_{\rm cal}$ by comparing Alice's measurement results with his own during the corresponding time slots, if $F_{\rm cal} > F$, Eve exists, if $F_{\rm cal} = F$, Eve doesn't exist. According to the Shannon information theory, the mutual $I(\alpha,\beta)$ and $I(\alpha,\epsilon)$ are calculated. Alice and Bob can obtain the secret key rate $\Delta I = I(\alpha,\beta) - I(\alpha,\epsilon)$ only by classical error correction and privacy amplification.[20] Let us give an explicit algorithm (see Fig.2) for the protocol. The useful plain text is divided into blocks with each block consisting of l useful messages, and m random authentication codes are randomly inserted into a block to form a transmittable block with the length being $l+m$.

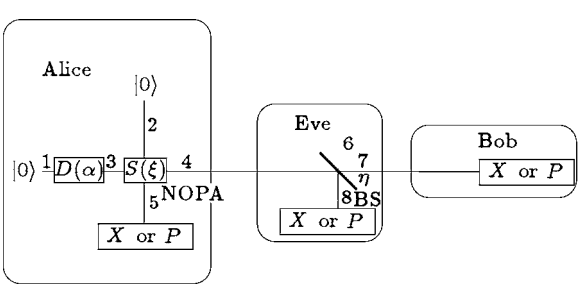

Fig.1. Schematic representation of deterministic quantum key distribution based on Gaussian-modulated CV EPR correlations. NOPA: nondegenerate optical parametric amplifier, BS: beam splitter, $D(\alpha)$: displacement operator, $S(\xi)$: two mode squeezing operator of NOPA, η: the transmittance coefficient of BS.

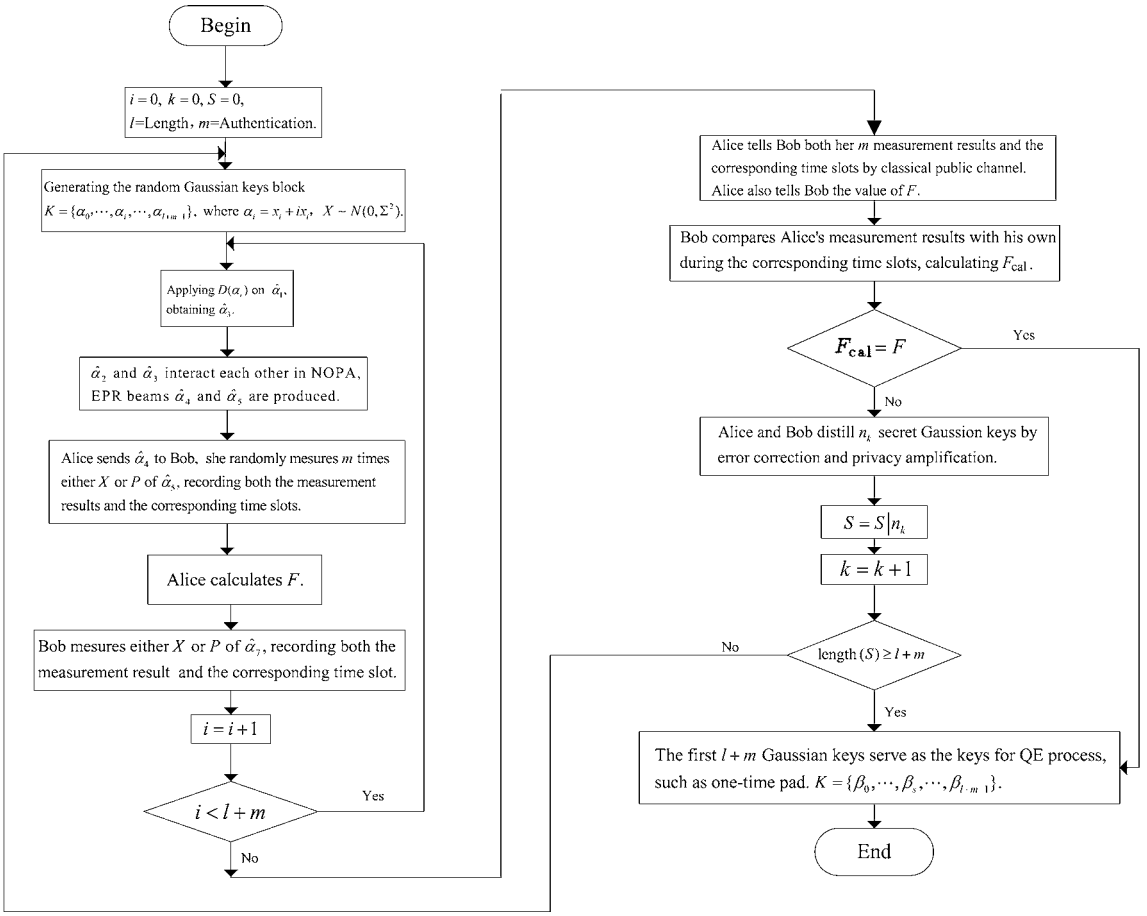

Fig.2. The flow chart of QKD process.

(p.0) Protocol is initialized, $i=0$, $k=0$, $S=0$, $l=$ the Length of useful messages in each transmittable block. $m=$ the length of the Authentication codes in each transmittable block.

(p.1) Alice generates the random Gaussian keys block $K=\{\alpha_0,...,\alpha_i,...,\alpha_{l+m-1}\}$, where $\alpha_i=x_i+ix_i$, $x_i(0\leq i\leq l+m-1)$ is drawn from Gaussian probability distribution, $X\sim N(0,\Sigma^2)$.

(p.2) Alice modulates $\hat{a}_1$ by applying $D(\alpha_i)$, obtains $\hat{a}_3$.

(p.3) $\hat{a}_2$ and $\hat{a}_3$ interact each other in NOPA, the EPR entanglement beams $\hat{a}_4$ and $\hat{a}_5$ are prepared by Alice.

(p.4) Alice calculates F.

(p.5) Alice sends $\hat{a}_4$ to Bob, she randomly measures m times either X or P of $\hat{a}_5$, thus she obtains m measurement results, then she records these m measurement results and the corresponding time slots.

(p.6) Bob measures either X or P of the mode $\hat{a}_7$, where $\hat{a}_7$ is $\hat{a}_4$ without the presence of Eve.

(p.7) $i=i+1$.

(p.8) If $i<l+m$, go to (p.2), otherwise go on.

(p.9) Alice tells Bob both her m measurement results and the corresponding time slots through the classical public channel. Alice tells Bob the value of F.

(p.10) Bob compares Alice's measurement results with his own during the corresponding time slots, then he estimates $F_{\rm cal}$.

(p.11) If $F=F_{\rm cal}$, go to (p.16), otherwise go on.

(p.12) Alice and Bob distill n_k secret Gaussian keys by classical error correction and privacy amplification.

(p.13) The secret Gaussian keys string n_k is orderly put into the register S, its head is connected with the tail of the former Gaussian keys string to form the longer secret Gaussian keys string.

(p.14) $k=k+1$.

(p.15) If the length of the secret keys string K is bigger than $l+m$, i.e., length$(S)\geq l+m$, go on, otherwise go to (p.1).

(p.16) Alice and Bob intercept the first $l+m$ Gaussian keys of S as the keys $K=\{\beta_0,...,\beta_s,...,\beta_{l+m-1}\}$ for other encryption processes, such

as one-time pad. Thus we can obtain secure Gaussian keys $K = \{\beta_0, ..., \beta_s, ..., \beta_{l+m-1}\}$ with its length $l + m$.

(p.17) end.

4. The security analysis

We firstly determines 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 Eq.(11). Then the secret information rate $\Delta I = I(\alpha, \beta) - I(\alpha, \epsilon)$ between Alice and Bob can be obtained. Finally, we present a method to detect Eve.

4.1. The secret information rate

After using Eqs.(4), X_3 and P_3 of $\hat{a}_3$ are given by the following equations,

$$\begin{aligned} X_3 &= X_1 + X, \\ P_3 &= P_1 + X. \end{aligned} \tag{12}$$

$\hat{a}_2$ and $\hat{a}_3$ are two input modes of NOPA, according to Eqs.(7), two output modes are given by the following equations,

$$\begin{aligned} X_4 &= X_3 \cosh(r) + X_2 \sinh(r), \\ P_4 &= P_3 \cosh(r) - P_2 \sinh(r). \\ X_5 &= X_2 \cosh(r) + X_3 \sinh(r), \\ P_5 &= P_2 \cosh(r) - P_3 \sinh(r). \end{aligned} \tag{13}$$

$\hat{a}_4$ and $\hat{a}_5$ are entanglement beams, i.e.,

$$\begin{aligned} \lim_{r\to\infty} X_4 &= X_5, \\ \lim_{r\to\infty} P_4 &= -P_5. \end{aligned} \tag{14}$$

After using Eqs.(10), $\hat{a}_7$ and $\hat{a}_8$ are given by the following equations:

$$\begin{aligned} X_7 &= \sqrt{\eta} X_4 + \sqrt{1-\eta} X_6, \\ P_7 &= \sqrt{\eta} P_4 + \sqrt{1-\eta} P_6, \\ X_8 &= \sqrt{\eta} X_6 - \sqrt{1-\eta} X_4, \\ P_8 &= \sqrt{\eta} P_6 - \sqrt{1-\eta} P_4. \end{aligned} \tag{15}$$

Using Eqs.(12)–(15), we can easily calculate the expressions of X_7 and P_7,

$$\begin{aligned} X_7 =& \sqrt{\eta}\cosh(r)(X + X_1) + \sqrt{\eta}\sinh(r) X_2 \\ &+ \sqrt{1-\eta} X_6, \\ P_7 =& \sqrt{\eta}\cosh(r)(X + P_1) - \sqrt{\eta}\sinh(r) P_2 \\ &+ \sqrt{1-\eta} P_6. \end{aligned} \tag{16}$$

The expressions of X_8 and P_8 are given by the following equations,

$$\begin{aligned} X_8 =& \sqrt{\eta} X_6 - \sqrt{1-\eta}\cosh(r)(X_1 + X) \\ &- \sqrt{1-\eta}\sinh(r) X_2, \\ P_8 =& \sqrt{\eta} P_6 - \sqrt{1-\eta}\cosh(r)(P_1 + X) \\ &+ \sqrt{1-\eta}\sinh(r) P_2, \end{aligned} \tag{17}$$

where all random variables follow a Gaussian distribution,

$$\begin{aligned} X &\sim N(0, \Sigma^2), \\ X_1, P_1 &\sim N(0, \frac{1}{4}), \\ X_2, P_2 &\sim N(0, \frac{1}{4}), \\ X_6, P_6 &\sim N(0, \frac{1}{4}). \end{aligned} \tag{18}$$

i.e., all input states are the vacuum states. According to Eqs.(16)and (18), we can easily calculate the variances of X_7 and P_7,

$$\begin{aligned} \langle(\Delta X_7)^2\rangle =& \eta\cosh^2(r)(\Sigma^2 + \frac{1}{4}) + \frac{1}{4}\eta\sinh^2(r) \\ &+ \frac{1}{4}(1-\eta), \\ \langle(\Delta P_7)^2\rangle =& \eta\cosh^2(r)(\Sigma^2 + \frac{1}{4}) + \frac{1}{4}\eta\sinh^2(r) \\ &+ \frac{1}{4}(1-\eta). \end{aligned} \tag{19}$$

Equations (19) show that whether Bob measures X_7 or P_7, the variance of signal distribution is always

$$M = \eta\cosh^2(r)\Sigma^2, \tag{20}$$

the variance of noise is

$$N = \frac{1}{4}\eta\cosh^2(r) + \frac{1}{4}\eta\sinh^2(r) + \frac{1}{4}(1-\eta). \tag{21}$$

The signal-noise ratio between Alice and Bob is

$$\gamma_{\alpha\beta} = \frac{M}{N}. \tag{22}$$

According to Eq.(11), the mutual information between Alice and Bob is

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

According to Eqs.(17) and (18), the variances of X_8 and P_8 are given by the following equations

$$\begin{aligned} \langle(\Delta X_8)^2\rangle =& \frac{1}{4}\eta + (1-\eta)\cosh^2(r)(\frac{1}{4} + \Sigma^2) \\ &+ \frac{1}{4}(1-\eta)\sinh^2 r, \\ \langle(\Delta P_8)^2\rangle =& \frac{1}{4}\eta + (1-\eta)\cosh^2(r)(\frac{1}{4} + \Sigma^2) \\ &+ \frac{1}{4}(1-\eta)\sinh^2 r. \end{aligned} \tag{24}$$

Equations (24) show that whether Eve measures X_8 or P_8, the variance of signal distribution is always

$$P = (1-\eta)\cosh^2(r)\Sigma^2, \tag{25}$$

the variance of noise is

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

The signal-noise ratio between Alice and Eve is

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

According to Eq.(11), the mutual information between Alice and Eve is

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

The secret information rate[20] obtained by classical error correction and privacy amplification is

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

When $\eta = 1$, i.e. Eve doesn't exist,

$$\begin{aligned} &I(\alpha,\epsilon) = 0,\\ &\Delta I = I(\alpha,\beta) = \frac{1}{2}\log_2\left[1+\frac{4\Sigma^2}{1+\tanh^2(r)}\right]. \end{aligned} \tag{30}$$

We can see that the secret information rate ΔI increases with the increase of the variance of signal Σ^2, in addition, when $r > 3$, ΔI is almost unchanged when r increases. When Eve exists, the relation between the secret key rate ΔI and η in QKD process is depicted in Fig.3. When $\eta > 0.09$, then $\Delta I > 0$. In this paper, for quantificationally evaluating our protocol, we assume that $\Sigma = 10, r = 3$.

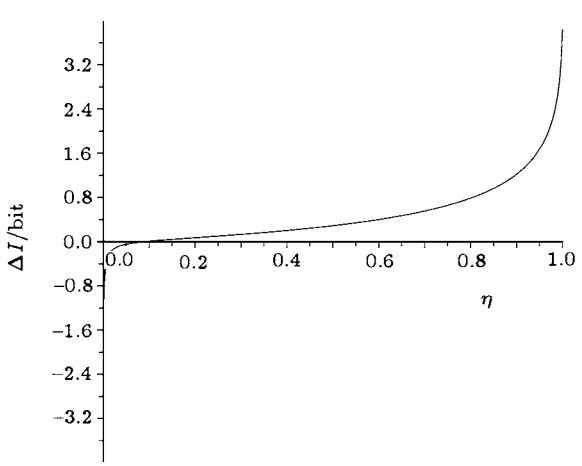

Fig.3. The relation between ΔI and η in QKD process, ($\Sigma = 10, r = 3$).

4.2. Detecting Eve

Eve inevitably disturbs the probability distribution of travel beam $\hat{a}_4$ if she wants to obtain Alice's information, thus she must destroy the entanglement relation between $\hat{a}_4$ and $\hat{a}_5$. After finishing communication, Alice and Bob can detect Eve by comparing the original F with the calculated $F_{\rm cal}$. Now, we give the explicit detecting process.

We firstly construct two random variables

$$\begin{aligned} \delta X_{\rm Eve} &= X_7 - k_1 X_5,\\ \delta P_{\rm Eve} &= P_7 + k_2 P_5. \end{aligned} \tag{31}$$

If Eve doesn't exist, i.e., $\hat{a}_7 = \hat{a}_4$, then Eqs.(31) becomes

$$\begin{aligned} \delta X_{\rm no-Eve} &= X_4 - k_1 X_5,\\ \delta P_{\rm no-Eve} &= P_4 + k_2 P_5. \end{aligned} \tag{32}$$

According to Eqs.(12)–(13) and (18), we can easily calculate the variances of $\delta X_{\rm no-Eve}$ and $\delta P_{\rm no-Eve}$.

$$\begin{aligned} &\langle(\Delta(\delta X_{\rm no-Eve}))^2\rangle\\ =&[\cosh(r) - k_1\sinh(r)]^2\left(\Sigma^2+\frac{1}{4}\right)\\ &+\frac{1}{4}[\sinh(r) - k_1\cosh(r)]^2,\\ &\langle(\Delta(\delta P_{\rm no-Eve}))^2\rangle\\ =&[\cosh(r) - k_2\sinh(r)]^2\left(\Sigma^2+\frac{1}{4}\right)\\ &+\frac{1}{4}[\sinh(r) - k_2\cosh(r)]^2. \end{aligned} \tag{33}$$

When

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

where

$$\begin{aligned} R &= 2\sinh(r)\cosh(r)(1+2\Sigma^2),\\ S &= \sinh^2(r) + \cosh^2(r) + 4\sinh^2(r)\Sigma^2, \end{aligned} \tag{35}$$

$\langle(\Delta(\delta X_{\rm no-Eve}))^2\rangle$ and $\langle(\Delta(\delta P_{\rm no-Eve}))^2\rangle$ reach the minimal values,

$$\begin{aligned} \langle(\Delta(\delta X_{\rm no-Eve}))^2\rangle_{\rm min} =&\langle(\Delta(\delta P_{\rm no-Eve}))^2\rangle_{\rm min}\\ =&\frac{W}{Z}. \end{aligned} \tag{36}$$

where

$$\begin{aligned} W &= 4\Sigma^2 + 1,\\ Z &= 8\cosh^2(r) + 16\cosh^2(r)\Sigma^2 - 16\Sigma^2 - 4. \end{aligned} \tag{37}$$

According to Eq.(8), Alice can calculate

$$F = \langle(\Delta(\delta X_{\rm no-Eve}))^2\rangle_{\rm min}\langle(\Delta(\delta P_{\rm no-Eve}))^2\rangle_{\rm min}, \tag{38}$$

when Σ^2 and r is specified.

When Eve does exist, Bob calculates $\delta X_{\rm Eve}$ and $\delta P_{\rm Eve}$ according to Eqs.(12), (13), (15) and (31),

$$\begin{aligned}\delta X_{\rm Eve} =&[\sqrt{\eta}\cosh(r) - k_1\sinh(r)](X_1 + X)\\ &+ [\sqrt{\eta}\sinh(r) - k_1\cosh(r)]X_2\\ &+ \sqrt{1-\eta}X_6,\\ \delta P_{\rm Eve} =&[\sqrt{\eta}\cosh(r) - k_2\sinh(r)](P_1 + X)+\\ &+ [k_2\cosh(r) - \sqrt{\eta}\sinh(r)]P_2\\ &+ \sqrt{1-\eta}P_6. \end{aligned} \quad (39)$$

The variances of $\delta X_{\rm Eve}$ and $\delta P_{\rm Eve}$ can be obtained according to Eqs.(18) and (39)

$$\begin{aligned}\langle(\Delta(\delta X_{\rm Eve}))^2\rangle =&[\sqrt{\eta}\cosh(r) - k_1\sinh(r)]^2\left(\frac{1}{4} + \Sigma^2\right)\\ &+ \frac{1}{4}[\sqrt{\eta}\sinh(r) - k_1\cosh(r)]^2\\ &+ \frac{1}{4}(1-\eta),\\ \langle(\Delta(\delta P_{\rm Eve}))^2\rangle =&[\sqrt{\eta}\cosh(r) - k_2\sinh(r)]^2\left(\frac{1}{4} + \Sigma^2\right)\\ &+ \frac{1}{4}[\sqrt{\eta}\sinh(r) - k_2\cosh(r)]^2\\ &+ \frac{1}{4}(1-\eta). \end{aligned} \quad (40)$$

Substituting Eq.(34) into Eqs.(40), Bob can obtain

$$F_{\rm cal} = \langle(\Delta(\delta X_{\rm Eve}))^2\rangle\langle(\Delta(\delta P_{\rm Eve}))^2\rangle. \quad (41)$$

Thus after finishing communication, Bob can calculate $F_{\rm cal}$ according to both the statistics he accumulates and what Alice tells him. The numerical relationship between $F_{\rm cal}$ and η is depicted as Fig.4. The parameter $F_{\rm cal}$ decreases rapidly with the increase of η. The fact shows that the less Eve disturbs the mode $\hat{a}_4$ (i.e., the less information Eve obtains), the smaller the probability detected by Eve is. Alice and Bob can determine whether Eve exists or not according to the value of $F_{\rm cal}$. If Eve doesn't exist, $F = 6.174\times10^{-6}$ ($r = 3, \Sigma = 10$). Thus after transmission, if the parameter $F_{\rm cal} > F = 6.174\times10^{-6}$, then Eve exists, if $F_{\rm cal} = F = 6.174\times10^{-6}$, then Eve doesn't exist. The secret information rate ΔI correlates with $F_{\rm cal}$.

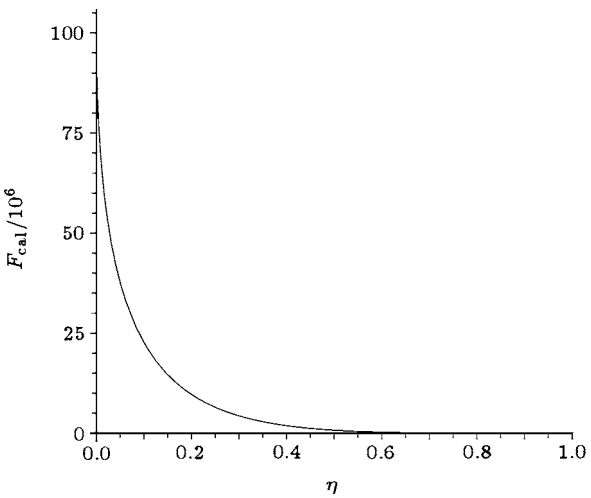

Fig.4. The relation between $F_{\rm cal}$ and η ($\Sigma = 10, r = 3$).

5. Conclusion

A deterministic quantum key distribution protocol based on Gaussian-modulated CV EPR entanglement correlations is presented in this paper. The security is guaranteed by CV EPR correlations produced by NOPA. For general beam splitter eavesdropping strategy, we can still obtain the secret information rate $\Delta I = I(\alpha,\beta) - I(\alpha,\epsilon)$. So the proposed deterministic quantum key distribution is secure.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Lo H K and Chau H F 1999 *Science* **283** 2050
[3] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[4] Mayers D 2001 *Journal of the ACM* **48** 351
[5] Liang C, Fu D H, Liang B, Liao J, Wu L An, Yao D C and Lu S W 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese)
[6] Ralph T C 1999 *Phys. Rev.* A **61** 010303(R)
[7] Hilery M 2000 *Phys. Rev.* A **61** 022309
[8] Gottesman D and Preskill J 2001 *Phys. Rev.* A **63** 022309
[9] Cerf N J, Lévy M and Assche G V 2001 *Phys. Rev.* A **63** 052311
[10] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[11] Silberhorn Ch, Korolkova N and Leuchs G 2002 *Phys. Rev. Lett.* **88** 167902
[12] Grosshans F, Assche G Van, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* (London) **421** 238
[13] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[14] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901
Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801
[15] Lucamarini M and Mancini S 2005 *Phys. Rev. Lett.* **94** 140501
[16] Reid M D 2000 *Phys. Rev.* A **62** 062308
[17] Walls D F and Milburn G J 1997 *Quantum Optics* (New York: Springer) p12–15
[18] Reid M D 1989 *Phys. Rev.* A **40** 913
Reid M D and Drummond P D 1988 *Phys. Rev. Lett.* **60** 2731
[19] Shannon C E 1948 *Bell. Syst. Tech. J.* **27** 623
[20] Maurer U M 1993 *IEEE Trans. Inf. Theory* **39** 733