Vol 17 No 4, April 2008
1674-1056/2008/17(04)/1263-06

Chinese Physics B



# Security of quantum key distribution using two-mode squeezed states against optimal beam splitter attack*

He Guang-Qiang(何广强)†, Zhu Si-Wei(朱思维),
Guo Hong-Bin(郭红斌), and Zeng Gui-Hua(曾贵华)

*The State Key Laboratory on Fiber-Optic Local Area Networks and Advanced Optical Communication Systems, Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai 200030, China*

(Received 1 June 2007; revised manuscript received 19 November 2007)

For the beam splitter attack strategy against quantum key distribution using two-mode squeezed states, the analytical expression of the optimal beam splitter parameter is provided in this paper by applying the Shannon information theory. The theoretical secret information rate after error correction and privacy amplification is given in terms of the squeezed parameter and channel parameters. The results show that the two-mode squeezed state quantum key distribution is secure against an optimal beam splitter attack.

**Keywords:** quantum key distribution, two-mode squeezed states, optimal beam splitter attack
**PACC:** 4250, 4230Q, 0365

## 1. Introduction

Quantum key distribution (QKD) provides a way to securely distribute keys between the sender and the receiver, traditionally as Alice and Bob.[1−4] The security of QKD is guaranteed by the foundational law of quantum mechanics.[5−7] At present, although some weak laser pulse QKD protocols[8−12] offer the same level of security as those based on single photon sources, the detection of single photon necessary in the discrete variable (DV) QKD is still very difficult, while the Gaussian operation and heterodyne or homodyne detection in the continuous variable (CV) QKD[13−24] are easily experimentally implemented. In addition, the CV QKD can provide a high channel capacity, thus the CV QKD attracts the interest of scientists around the world. Gaussian states, e.g. coherent state and two-mode squeezed state (CV entangled states), are the suitable quantum carriers for processing the CV quantum information.[25] In addition, entanglement is the unique characteristic of quantum physics,[26] and it is an important resource in quantum information and quantum computation.[27] And the entanglement plays a very important role in the CV QKD. It is virtual entanglement that guarantees the security of the CV QKD.[28] To take advantage of both the experimentally mature homodyne detection and the CV entangled states, the two-mode squeezed state QKD using CV entangled states, which theoretically has a higher channel capacity than the coherent state QKD,[18] is proposed and analysed against a beam splitter attack,[29] but the transmission coefficient of beam splitter in Eve's measurement device is assumed to be 0.5 and its analytical expression is not given.

In this paper, the security of two-mode squeezed state QKD against an optimal beam splitter attack is analysed by applying the Shannon information theory. The optimal beam splitter parameter and the theoretical secret key rate are obtained. The paper is organized as fellows. In Section 2, the two-mode squeezed state QKD protocol is outlined. In Section 3, the optimal beam splitter parameter and the theoretical secret key are given. In Section 4, the conclusions are drawn.

*Project supported by the Shanghai Jiaotong University (SJTU) Young Teacher Foundation, China (Grant No A2831B), the SJTU Participating in Research Projects (PRPs), China (Grant No T03011030), and the National Natural Science Foundation of China (Grant No 60472018).
†E-mail: gqhe@sjtu.edu.cn

## 2. Two-mode squeezed state QKD protocol

The two-mode squeezed state QKD can efficiently distribute keys between Alice and Bob (see Fig.1). This protocol may be described generally by the following steps.

**Step 1** Alice prepares entangled optical modes $\hat{a}_3$ and $\hat{a}_4$ by applying two-mode squeezed operator $\hat{S}(\pm r)$ to modes $\hat{a}_1$ and $\hat{a}_2$ according to the bit string $n_1$. If the $i$th bit of $n_1$ is 0, apply $\hat{S}(r)$, otherwise apply $\hat{S}(-r)$, i.e. $n_1^{\mathrm{i}} = 0, \hat{U} = \hat{S}(r); n_1^{\mathrm{i}} = 1, \hat{U} = \hat{S}(-r)$.

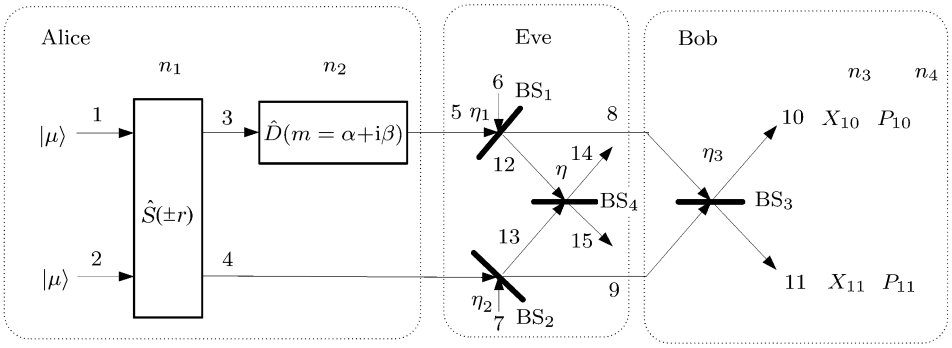


**Fig.1.** Schematic representation of quantum key distribution using two-mode squeezed states. $\hat{S}(\pm r)$: two-mode squeezing operator, $\hat{D}(m)$: displacement operator, BS: beam splitter, $\eta$: the transmission coefficient of BS. Arabic numerals denote the optical modes.

**Step 2** Alice applies the displacement operator $D(M = A + \mathrm{i}B)$ to mode $\hat{a}_3$, produces mode $\hat{a}_5$, encodes the messages $m = \alpha + \mathrm{i}\beta$ onto quantum carrier $\hat{a}_3$, where $\alpha$ and $\beta$ are drawn from Gaussian probability density distributions (PDF) $A \sim N(0, \Sigma^2)$ and $B \sim N(0, \sigma^2)$ respectively, where $\Gamma \sim N(\mu, \Sigma^2)$ denotes that random variable $\Gamma$ obeys Gaussian PDF with the mean value $\mu$ and the variance $\Sigma^2$. Repeating the above procedures will produce the key string $n_2$.

**Step 3** Alice sends modes $\hat{a}_4$ and $\hat{a}_5$ to Bob through a quantum channel.

**Step 4** Bob combines modes $\hat{a}_8$ and $\hat{a}_9$ (those are $\hat{a}_5$ and $\hat{a}_4$ respectively in the absence of attacker Eve) using beam splitter, producing modes $\hat{a}_{10}$ and $\hat{a}_{11}$.

**Step 5** Bob selects measurement bases ($X_{11}$, $P_{10}$) or $(X_{10}, P_{11})$ according to the random bit string $n_3$, obtaining message bit string $n_4$. If the $i$th bit of $n_3$ is 0, i.e. $n_3^{\mathrm{i}} = 0$, Bob selects $(X_{11}, P_{10})$; if $n_3^{\mathrm{i}} = 1$ Bob selects $(X_{10}, P_{11})$. Here $X = \dfrac{1}{2}(\hat{a} + \hat{a}^{\dagger})$ and $P = \dfrac{1}{2\mathrm{i}}(\hat{a} - \hat{a}^{\dagger})$ denote the quadrature of mode $\hat{a}$.

**Step 6** Alice and Bob communicate with each other and compare the encode basis and measurement basis by a classical channel, if $n_1^{\mathrm{i}} = n_3^{\mathrm{i}}$, then store the corresponding $n_2^{\mathrm{i}}$ and $n_4^{\mathrm{i}}$; if $n_1^{\mathrm{i}} \neq n_3^{\mathrm{i}}$, discard $n_2^{\mathrm{i}}$ and $n_4^{\mathrm{i}}$. Then the remaining bit strings $n_2$ and $n_4$ are distilled into a secret key by classical key reconciliation and privacy amplification. From the calculation of the mutual information $I(\alpha, \beta)$,[29] we can understand the rationality of the basis selection.

## 3. Optimal beam splitter attack strategy

The security analysis is an important issue in designing quantum cryptography schemes. To analyse the theoretical security of QKD, we must assume that Eve can make any attack machine that is only restricted by the physical laws, build its mathematical mode and investigate its security by exploiting the information theory. It is an important and very difficult task. Here we investigate only the security of QKD against the special attack strategies.

### 3.1. Optimal beam splitter attack parameter

In this paper, the simple beam splitter attack strategy is investigated (See Fig.1). Assuming that Eve processes the quantum memory technology to store quantum states tapped by beam splitter, then she can measure them by applying the same measurement base as that applied by Bob after Alice and Bob have finished the key reconciliation. This fact will simplify the calculation of the secret key rate.

Firstly, the optimal measurement parameter is determined by the exact analytical expression. Since quadratures $X$ and $P$ are symmetrical, to simplify analysis, here we discuss only the quadrature $X$, the quadrature $P$ can be analysed in a similar way. According to the results by He *et al*,[29] the quadrature $X_{15}$ of mode $\hat{a}_{15}$ is easily calculated as follow:

$$\begin{aligned} X_{15} =& \sqrt{\eta}X_{12} - \sqrt{1-\eta}X_{13} \\ =& \sqrt{\eta\eta_1}X_6 - \sqrt{\eta(1-\eta_1)}A \\ & - \sqrt{(1-\eta)\eta_2}X_7 - [\sqrt{\eta(1-\eta_1)}\cosh r \\ & - \sqrt{(1-\eta)(1-\eta_2)}\sinh r]X_1 \\ & - [\sqrt{\eta(1-\eta_1)}\sinh r \\ & - \sqrt{(1-\eta)(1-\eta_2)}\cosh r]X_2. \end{aligned} \tag{1}$$

Here $X_i \sim N(0, \frac{1}{4}), i = 1, 2, 6, 7$, i.e. the input quantum states are vacuum states, $A \sim N(0, \Sigma^2)$. Obviously the signal-to-noise ratio between Alice and Eve is

$$\mathrm{SNR}(\mathrm{Alice}, \mathrm{Eve}) = \frac{P}{Q}, \tag{2}$$

where $P = \Sigma^2\eta(1-\eta_1)$ and $Q = \frac{1}{4}\{[(\eta_1-\eta_2)+(\eta_2-\eta_1)\cosh 2r]\eta - 2\sqrt{\eta(1-\eta)(1-\eta_1)(1-\eta_2)}\sinh 2r + (1-\eta_2)\cosh 2r + \eta_2\}$ are signal variance and noise variance respectively. To eavesdrop the maximal information about Alice, Eve selects optimal beam splitter coefficient value $\eta_\mathrm{m}$ with SNR(Alice, Eve) reaching its maximal value.

According to expression (2), the derivative is as follows:

$$\frac{\mathrm{dSNR}(\mathrm{Alice}, \mathrm{Eve})}{\mathrm{d}\eta} = \frac{4\Sigma^2(1-\eta_1)\left(Q - \frac{\mathrm{d}Q}{\mathrm{d}\eta}\eta\right)}{Q^2}. \tag{3}$$

Let $\frac{\mathrm{dSNR}(\mathrm{Alice}, \mathrm{Eve})}{\mathrm{d}\eta} = 0$, then the optimal beam splitter parameter will be obtained as follows:

$$\eta_\mathrm{E} = \eta_\mathrm{m} = \frac{M}{N}, \tag{4}$$

where $M = [(1-\eta_2)\cosh 2r + \eta_2]^2$, and $N = (1-\eta_1)(1-\eta_2)\sinh^2 2r + [(1-\eta_2)\cosh 2r + \eta_2]^2$.

To substitute $\eta = \eta_\mathrm{m}$ into expression (2), we can obtain Eve's maximal signal-to-noise ratio,

$$\mathrm{SNR}_{\max}(\mathrm{Alice}, \mathrm{Eve}) = \mathrm{SNR}(\mathrm{Alice}, \mathrm{Eve})(\eta_\mathrm{m}). \tag{5}$$

In the following, we will discuss Bob's optimal value of $\mathrm{BS}_3$. Since Bob does not know Eve's attack strategy, he selects only its optimal value provided that Eve does not exist. When $\eta_1 = \eta_2 = 0$, then Eve's measurement procedure simulates that of Bob without Eve. According to expression (4), we can easily obtain the optimal coefficient of Bob without Eve:

$$\eta_\mathrm{B} = \eta_\mathrm{m}|_{\eta_1=\eta_2=0} = \frac{\cosh^2 2r}{\sinh^2 2r + \cosh^2 2r}. \tag{6}$$

According to expression (6), we can discuss the two situations of the proposed scheme.

(1) When the squeezed parameter $r = 0$, i.e. the coherent states are applied, then $\eta_\mathrm{B} = 1$;

(2) When the squeezed parameter $r \to \infty$, i.e. the perfect entanglement is used, then $\eta_\mathrm{B} = 1/2$.

The first situation indicates that Bob will directly measure $X_{11}$ of mode $\hat{a}_{11}$ in order to obtain the maximal Alice's information $A$, and this fact is compatible with the Grosshans's QKD scheme using direct reconciliation.[18] The second situation shows that Bob will set $\eta_\mathrm{B} = \frac{1}{2}$ when the perfect entanglement is used. This fact proves the rationality of the hypothesis in Ref.[29].

The expression of $X_{11}$ is as follows:

$$\begin{aligned} X_{11} =& (\sqrt{\eta_1\eta_4}\cosh r - \sqrt{(1-\eta_4)\eta_2}\sinh r)X_1 \\ & (\sqrt{\eta_1\eta_4}\sinh r - \sqrt{(1-\eta_4)\eta_2}\cosh r)X_2 \\ & \sqrt{\eta_4(1-\eta_1)}X_6 - \sqrt{(1-\eta_2)(1-\eta_4)}X_7 \\ & + \sqrt{\eta_1\eta_4}A. \end{aligned} \tag{7}$$

If Bob applies the optimal beam splitter parameter, i.e. $\eta_4 = \eta_\mathrm{B}$, to measuring the $X_{11}$ of mode $\hat{a}_{11}$, then the signal-to-noise ratio is as follows:

$$\mathrm{SNR}(\mathrm{Alice}, \mathrm{Bob}) = \frac{R}{S}, \tag{8}$$

where $R = 4\Sigma^2\eta_\mathrm{B}\eta_1$, and $S = (1-\eta_1)\eta_\mathrm{B} + (1-\eta_2)(1-\eta_\mathrm{B}) + [\eta_\mathrm{B}\eta_1 + (1-\eta_\mathrm{B})\eta_2]\cosh 2r - 2\sqrt{\eta_\mathrm{B}(1-\eta_\mathrm{B})\eta_1\eta_2}\sinh 2r$.

## 3.2. The secret information rate

According to the Shannon information theory,[30] the channel capacity of the additive white Gaussian noise (AWGN) channel is

$$I = \frac{1}{2}\log_2(1+\gamma), \tag{9}$$

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

Consequently, the mutual information between Alice and Bob is

$$I(\text{Alice},\text{Bob}) = \frac{1}{2}\log_2[1+\text{SNR}(\text{Alice},\text{Bob})]. \quad (10)$$

According to expressions (5) and (9), the maximal mutual information between Alice and Eve is

$$\begin{aligned} &I_{\max}(\text{Alice},\text{Eve}) \\ =&\frac{1}{2}\log_2[1+\text{SNR}_{\max}(\text{Alice},\text{Eve})]. \end{aligned} \quad (11)$$

According to the Maurer theory,[31] the final key is secure if $I(\text{Alice},\text{Bob}) > I_{\max}(\text{Alice},\text{Eve})$, for in this situation Alice and Bob may distill a secure key by using the classical error correction and privacy amplification.

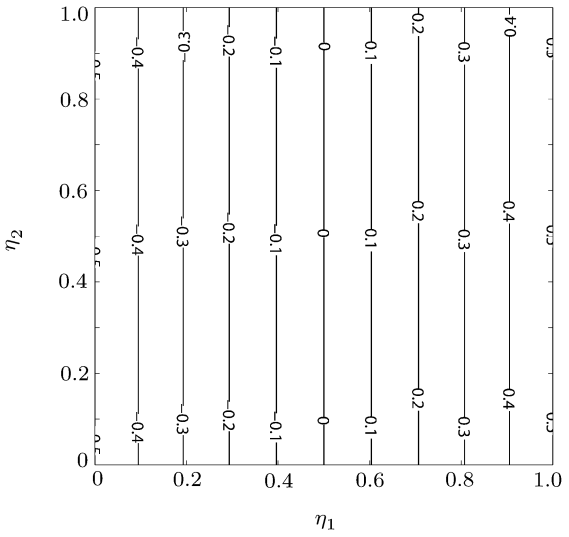


**Fig.2.** The contour line of secret key rate. $r = 0, \Sigma = \frac{1}{4}$.

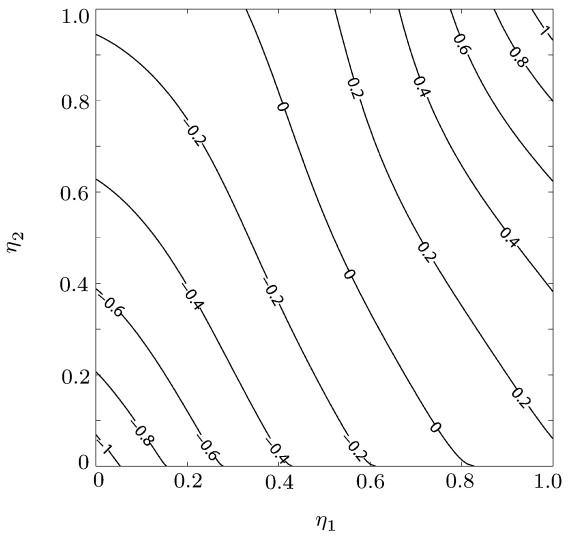


**Fig.3.** The contour line of secret key rate. $r = 1, \Sigma = \frac{1}{4}$.

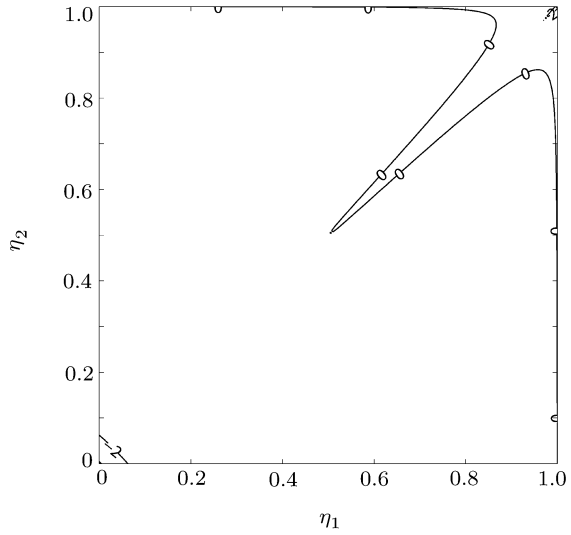


**Fig.4.** The contour line of secret key rate. $r = 5, \Sigma = \frac{1}{4}$.

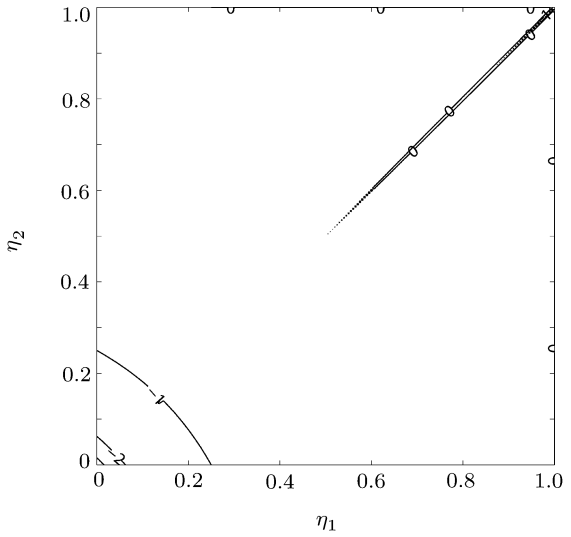


**Fig.5.** The contour line of secret key rate. $r = 10, \Sigma = \frac{1}{4}$.

According to expressions (10) and (11), the theoretical secret key rate is as follows:

$$\begin{aligned} \Delta I =&I(\text{Alice},\text{Bob}) - I_{\max}(\text{Alice},\text{Eve}) \\ =&\frac{1}{2}\log_2\frac{1+\text{SNR}(\text{Alice},\text{Bob})}{1+\text{SNR}_{\max}(\text{Alice},\text{Eve})}. \end{aligned} \quad (12)$$

According to expression (12), the analytical expression of $\Delta I$ is very prolix, so we present a numerical solution of $\Delta I$ in order to explain the relationship between $\Delta I$ and $\eta_1, \eta_2$ and then plot the contour line of secret key rate $\Delta I$.

### 3.3. Discussion

From Figs.2–9, we can see that the smaller the squeezed factor $r$ is, the more the secret key rate $\Delta I$ depends on $\eta_1$ than $\eta_2$. If $r = 0$, then $\Delta I > 0$ when $\eta_1 > 0.5$, while $\Delta I$ is unrelated to $\eta_2$. This can be explained by the fact that $r = 0$ implies that modes $\hat{a}_5$ and $\hat{a}_4$ are unentangled and independent of each other, and only mode $\hat{a}_5$ carries useful information. So $\Delta I$ depends only on $\eta_1$. Modes $\hat{a}_3$ and $\hat{a}_4$ become more and more related with $r$ increasing. If Eve does not exist ($\eta_1 = \eta_2 = 1$), the secret key rate $\Delta I = I(\text{Alice}, \text{Bob}) = \log_2\left(1+\frac{2\Sigma^2}{\mathrm{e}^{-2r}}\right)$ becomes larger with $r$ increasing. On the other hand, Eve can take advantage of the entanglement correlation to eavesdrop Alice's information, Figs.2–9 show that the security region becomes smaller and smaller with $r$ increasing. So increasing $r$ can improve the channel capacity $I(\text{Alice}, \text{Bob}) = \log_2\left(1+\frac{2\Sigma^2}{\mathrm{e}^{-2r}}\right)$ without Eve. In addition, when $r$ increases, Eve is more easily detected by applying the entanglement parameter $F_\mathrm{b}$ between $\hat{a}_3$ and $\hat{a}_4$[21]although the secure region becomes smaller. Entanglement parameter $F$[21] describes the entanglement degree of the entangled beams. If $r$ becomes larger, the entanglement degree is higher. Thus $F$ is smaller. So Alice can calculate the initial $F_\mathrm{a}$ between $\hat{a}_3$ and $\hat{a}_4$, then statistically calculates the entanglement parameter $F_\mathrm{b}$ between $\hat{a}'_8 = \hat{a}_8 - m$ and $\hat{a}_9$ through a reconciliation process. Eve can be easily detected by comparing $F_\mathrm{a}$ with $F_\mathrm{b}$.

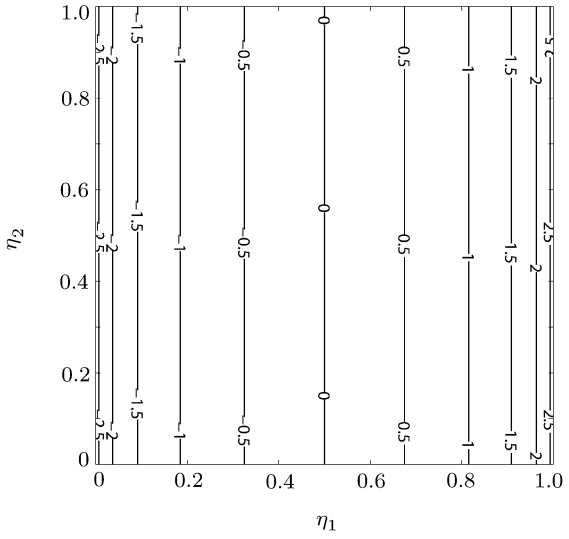


**Fig.6.** The contour line of secret key rate. $r = 0, \Sigma = 10$.

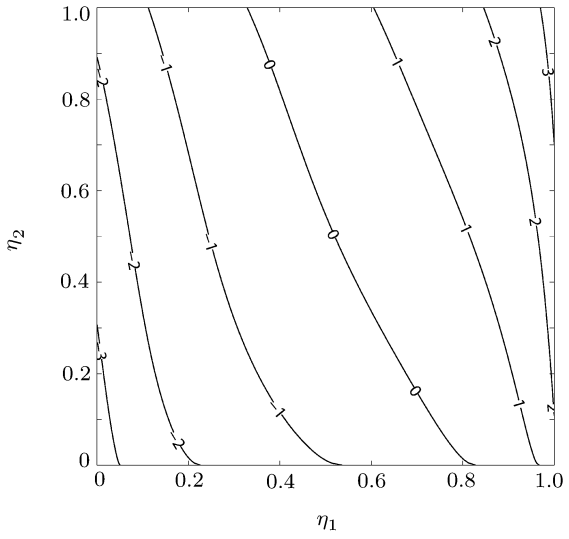


**Fig.7.** The contour line of secret key rate. $r = 1, \Sigma = 10$.

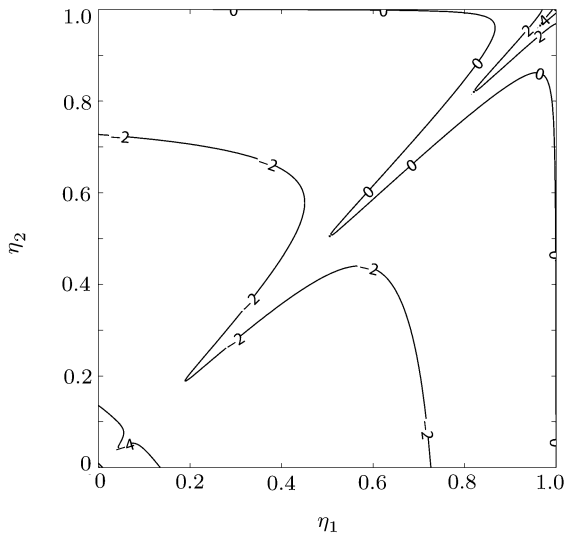


**Fig.8.** The contour line of secret key rate. $r = 5, \Sigma = 10$.

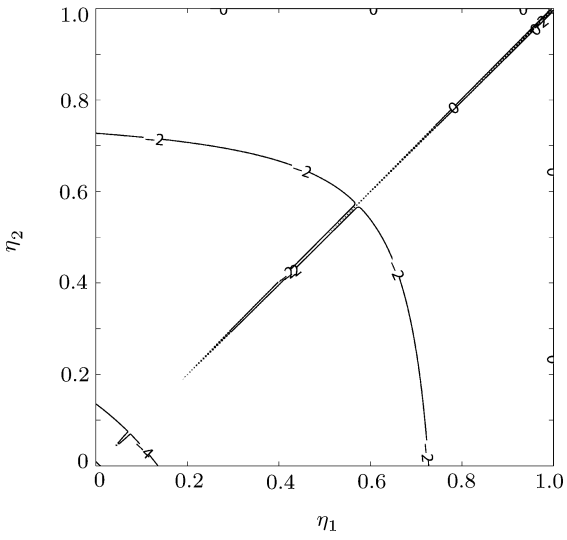


**Fig.9.** The contour line of secret key rate. $r = 10, \Sigma = 10$.

Reference [29] investigates the symmetrical beam splitter attack against QKD by using two-mode squeezed states, i.e. by assuming the transmission parameter of beam splitter to be 0.5. The results show that the scheme is secure against the symmetrical beam splitter attack. The more general attack is the optimal beam splitter, for which Eve can select the optimal transmission parameter as the attack parameter according to the quantum channel parameters $\eta_1$ and $\eta_2$. By the optimal attack, Eve can obtain the maximal information about Alice's message for the same disturbance level. In this paper, the analytical expression of the optimal beam splitter parameter is provided. The analytical results show that the proposed scheme is still secure for an appropriate quantum channel region, and it is also secure against a more powerful optimal beam splitter.

# 4. Conclusion

The analytical expression of the optimal beam splitter parameter against QKD using two-mode squeezed states is provided in this paper by applying the Shannon information theory. And the theoretical secret key rate after error correction and privacy amplification is given in terms of the squeezed factor and channel parameters. The results show that the two-mode squeezed state QKD is secure against an optimal beam splitter attack. When the squeezed factor $r$ increases, Eve can be easily detected, but the security region become smaller.

# References


[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Chen J J, Han Z F, Zhao Y B, Gui Y Z and Guo G C 2007 *Acta Phys. Sin.* **56** 5 (in Chinese)
[3] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2007 *Chin. Phys.* **16** 277
[4] Zheng L M, Wang F Q and Liu S H 2007 *Acta Phys. Sin.* **56** 2180 (in Chinese)
[5] Lo H K and Chau H F 1999 *Science* **283** 2050
[6] Shor P W and Preskill J 2000 *Phy. Rev. Lett.* **85** 441
[7] Mayers D 2001 *Journal of the ACM* **48** 351
[8] Cai Q Y and Tan Y G 2006 *Phys. Rev.* A **73** 032305
[9] Koashi M 2004 *Phys. Rev. Lett.* **93** 120501
[10] Scarani V, Acín A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[11] Stucki D, Brunner N, Gisin N, Scarani V and Zbinden H 2005 *Appl. Phys. Lett.* **87** 194108
[12] Takesure H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 *Nature Photonics* **1** 343
[13] Ralph T C 1999 *Phys. Rev.* A **61** 010303(R)
[14] Hillery M 2000 *Phys. Rev.* A **61** 022309
[15] Reid M D 2000 *Phys. Rev.* A **62** 062308
[16] Gottesman D and Preskill J 2001 *Phys. Rev.* A **63** 022309
[17] Cerf N J, Lévy M and VanAssche G 2001 *Phys. Rev.* A **63** 052311
[18] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[19] Silberhorn C, Korolkova N and Leuchs G 2002 *Phys. Rev. Lett.* **88** 167902
[20] Grosshans F, Assche G Van, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* (London) **421** 238
[21] He G Q, Zhu J and Zeng G H 2006 *Phys. Rev.* A **73** 012314
[22] Su X L, Jing J T, Pan Q and Xie Ch D 2006 *Phys. Rev.* A **74** 062305
[23] He G Q and Zeng G H 2006 *Chin. Phys.* **15** 1284
[24] He G Q and Zeng G H 2006 *Commun. Theor. Phys.* **46** 61
[25] Braunstein S L and Loock P v 2005 *Rev. Mod. Phys.* **77** 513 and reference therein
[26] Schrödinger E 1935 *Proc. Cambridge Phil. Soc.* **32** 446
[27] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[28] Grosshans F, Cerf N J, Wenger J, Tualle-Brouri R and Grangier Ph 2003 *Quantum information and Computation* **3** 535
[29] He G Q, Yi Z, Zhu J and Zeng G H 2007 *Acta Phys. Sin.* **56** 6427 (in Chinese)
[30] Shannon C E 1948 *Bell. Syst. Tech. J.* **27** 623
[31] Maurer U M 1993 *IEEE Trans. Inf. Theory* **39** 733