doi:10.3788/gzxb20154402.0227001

法拉第镜不完善对连续变量量子密钥分发系统的影响

杨荣桓,何广强

(上海交通大学 电子工程系,区域光纤通信网与新型光通信系统国家重点实验室,上海 200240)

摘 要:采用连续变量量子密钥分发的纠缠模型,在反向协商情况下,研究法拉第镜不完善对系统安全密钥速率的影响.结果表明,不完善的法拉第镜会降低系统实际的密钥速率,并且降低安全通信距离,且随着法拉第镜失偏角度的增大而增大.此外,使用大的调制方差,可以降低法拉第镜不完善对系统的影响.

关键词:量子通信,量子光学,量子理论计算机仿真,量子密码,量子理论计算

中图分类号:TN913.7,TN918 **文献标识码**:A **文章编号**:1004-4213(2015)02-0227001-5

The Influence of Faraday Mirror′s Imperfection in Continuous Variable Quantum Key Distribution System

YANG Rong-huan, HE Guang-qiang

(*State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai* 200240, *China*)

Abstract: The influence of imperfect Faraday mirror on secret key rate of continuous variable quantum key distribution system in reverse reconciliation is considered with theoretical analysis and numerical simulation. It takes entanglement based scheme. It′s found that Faraday mirror′s imperfection reduces the secret key rate and transmission distance of system. The impact increases if the imperfection turns more serious. Besides it finds using great modulation variance can reduce the impact of Faraday mirror significantly.

Key words: Quantum communication; Quantum optics; Quantum theory computer simulation; Quantum cryptography; Quantum theory computation

OCIS Codes: 270.5565, 270.5568, 060.5565

0 Introduction

Continuous Variable Quantum Key Distribution (CVQKD), as a secure communication scheme between two legitimate parties Alice and Bob, attracts many attentions. In theory, CVQKD has been proven to be unconditionally secure[1], but in practical system researchers find that the security of CVQKD is depend on whether the components are perfect or not. Recent years some researchers spend amount of time picking loopholes of practical system and repairing them to guarantee the security of system. Some imperfections of practical system are pointed out[2], such as modulation method. In theory we always take perfect Gaussian modulation while we use discrete Gaussian modulation in experiment due to hardware limitations. The wavelength dependent feature of beam splitter and LO without monitoring also open loopholes for Eve[3-5]. In discrete variable quantum key distribution, many possible attacks have been proposed. Recently, some

Foundation item: The National Natural Science Foundation of China (No. 61102053)

First author: YANG Rong-huan(1989—), male, M. S. degree, mainly focuses on quantum key distribution and quantum stream cipher. Email:yax2008@sjtu.edu.cn

Supervisor(Contact author): HE Guang-qiang (1977—), male, associate professor, Ph. D degree, mainly focuses on quantum key distribution, quantum entanglement and nonlinear optics. Email:gqhe@sjtu.edu.cn

Received: Jul. 2, 2014; **Accepted**: Sep. 28, 2014

research has found the imperfection of Faraday Mirror (FM) will reduce the security of discrete variable QKD. Passive Faraday-mirror attack to the practical two-way QKD system is put forward[6]. The security and secret key rate of practical CVQKD system depend on the performance of its components. Using imperfect components will degrade its security and secret key rate as stated above.

The paper finds the imperfection of FM will lead to the loss of secret key rate and transmission distance of CVQKD system. Part of secret key is wasted which could be attained if perfect FM is used in system. It presents the analysis model with imperfect FM, which is more rigorous. Besides, some suggestions to reduce the FM′s impact are proposed, such as increasing V properly if the modulator and funds are available, or using FM with rotation angle closed to 45° as far as possible.

1 The accuracy of Faraday mirror′s rotation angle

Fig. 1 is the layout of CVQKD system[7-8], where LD is laser diode, BS is beam splitter, AM is amplitude modulation, PM is phase modulation, PBS is polarization beam splitter, FM is Faraday mirror, solid line is Local Oscillator (LO) path and dotted line is signal path respectively. Firstly, Alice prepares a series of coherent states centered on $X_S \in \{Q_S, P_S\}$, and then he sends these coherent states to Bob through a quantum channel. $Q_S \in N(0, V_S)$, $P_S \in N(0, V_S)$, N is Gaussian distribution. The initial mode prepared by Alice can be depicted as $\hat{X}_A = X_S + \hat{X}_N$. $\hat{X}_A \in \{\hat{Q}_A, \hat{P}_A\}$ describes the coherent state after modulation and $\hat{X}_N \in \{\hat{Q}_N, \hat{P}_N\}$ describes the vacuum state. Hence, the variance of $\hat{X}_A$ is defined as V by $V = V_S + 1$.

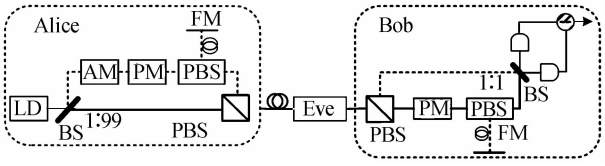

Fig. 1 Scheme of CVQKD

After amplitude modulation and phase modulation, signal passes the FM. It will make the signal′s polarization angle to rotate an angle twice as large as the rotation angle of FM. In theory, it′s supposed the initial polarization angle of LO and signal is 0° and the rotation angle of FM is 45°. Hence, after passing FM, the polarization angle of signal is 90°, which is vertical with the LO. And at the PBS, signal and LO can be put together without influencing each other. But limited by manufacturing technology, the practical rotation angle of Faraday mirror is not 45°, which induces some problems.

To simplify calculation, we just consider FM with practical rotation angle $45°-\theta$. After passing FM, the polarization angle of signal rotates $90° - 2\theta$. If the polarization angles of signal and LO are orthogonal, they can all pass through the PBS. If FM has imperfection, when they pass PBS, LO can all pass through the PBS but signal can′t do this, as the arrow B shows in Fig. 2. It represents the actual polarization angle of signal when signal passes PBS, and the arrow A represents the supposed polarization angle of signal in ideal situation. The included angle of them is 2θ.

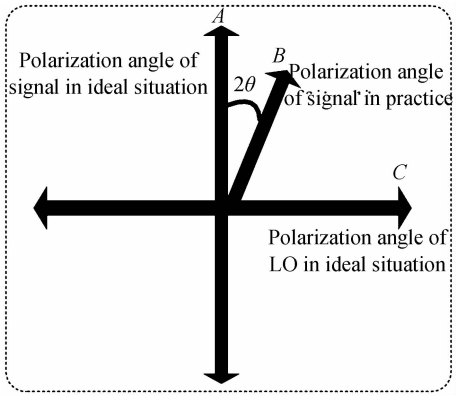

Fig. 2 The practical polarization angle of signal when passing PBS

For subsequent calculations, it′s necessary to introduce $\hat{a}$ and $\hat{a}^{\dagger}$, the annihilation and creation operator of the light state after Alice modulates the signal. We just consider $\hat{a}_H \neq 0$ and $\hat{a}_V = 0$, where the subscripts H and V label the horizontal and vertical polarization modes.

The Jones matrix of practical FM is as follows[6].

$$\boldsymbol{F}_M(\theta) = \begin{bmatrix} \cos(45°-\theta) & \sin(45°-\theta) \\ -\sin(45°-\theta) & \cos(45°-\theta) \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \cos(45°-\theta) & -\sin(45°-\theta) \\ \sin(45°-\theta) & \cos(45°-\theta) \end{bmatrix} = \begin{bmatrix} \sin 2\theta & -\cos 2\theta \\ -\cos 2\theta & -\sin 2\theta \end{bmatrix} \tag{1}$$

then

$$\begin{bmatrix} \hat{a}'_H \\ \hat{a}'_V \end{bmatrix} = \boldsymbol{F}_M(\theta) \begin{bmatrix} \hat{a}_H \\ \hat{a}_V \end{bmatrix} = \begin{bmatrix} \sin 2\theta \hat{a}_H - \cos 2\theta \hat{a}_V \\ -\cos 2\theta \hat{a}_H - \sin 2\theta \hat{a}_V \end{bmatrix} = \begin{bmatrix} \sin 2\theta \hat{a}_H \\ -\cos 2\theta \hat{a}_H \end{bmatrix} \tag{2}$$

$\hat{a}'_H$ and $\hat{a}'_V$ are the horizontal and vertical polarization modes after passing FM. $\hat{a}'_V$ can all pass through PBS into the quantum channel due to the special structure of PBS, but $\hat{a}'_H$ can′t do this. Hence, $\hat{a}'_V = -\cos 2\theta \hat{a}_H$. Using complex conjugate relations, $\hat{a}'^{\dagger}_V = -\cos 2\theta \hat{a}^{\dagger}_H$. Because of $\hat{n} = \hat{a}^{\dagger}\hat{a}$, so when leaving

PBS, the photon number is

$$\hat{n}' = (-\cos 2\theta)\hat{a}_H^\dagger(-\cos 2\theta)\hat{a}_H = \cos^2 2\theta \hat{a}_H^\dagger \hat{a}\hat{a}_H \quad (3)$$

If FM is perfect with $\theta=0°$, the photon number in ideal situation is

$$\hat{n}_0 = \hat{a}_H^\dagger \hat{a}_H = \frac{\hat{n}'}{\cos^2 2\theta} \quad (4)$$

And the variance of signal is

$$V' = \frac{\langle \hat{X}^2 + \hat{P}^2 \rangle}{2N_0} = \langle \hat{a}_V' \hat{a}_V'^\dagger + \hat{a}_V'^\dagger \hat{a}_V' \rangle = \cos^2 2\theta \langle \hat{a}_H \hat{a}_H^\dagger + \hat{a}_H^\dagger \hat{a}_H \rangle \quad (5)$$

where N_0 is the variance of vacuum state, $\hat{X}$ and $\hat{P}$ are the quadrature of coherent state. If $\theta=0°$, the variance of signal in ideal situation is

$$V = \langle \hat{a}_H \hat{a}_H^\dagger + \hat{a}_H^\dagger \hat{a}_H \rangle = \frac{V'}{\cos^2 2\theta} \quad (6)$$

After estimating channel parameters, the probability distribution of X_A' is a Gaussian distribution with $N(0,V')$, and $X_A \sim N(0,V) = N(0,V'/\cos^2 2\theta)$. V' is the modulation variance after Alice and Bob estimate the channel parameter (the variance of signal when it leaves Alice), and V is the variance of signal after Alice modulates the signal. If FM is perfect with rotation angle 45°, signal can all pass through PBS and V' will be equal to V, which is the hypothesis of theoretical model in recent years. But now it needs to be corrected with our model. X_A is the quadrature of coherent state after modulation, and X_A' is the quadrature of coherent state after passing PBS.

2 Analysis of secret key rate in reverse reconciliation

Fig. 3 is the entanglement based scheme of CVQKD which is widely used for theoretical analysis[9]. Mode B_0 and mode A are an EPR pair with $V'=V\cos^2 2\theta$. Mode E_0 and mode E_2 are also an EPR pair with variance N. $\hat{X}B_0$, $\hat{X}E_0$ are the quadrature of mode B_0 and E_0.

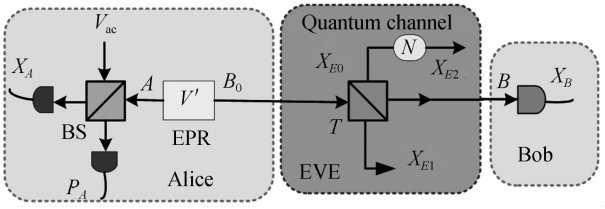

Fig. 3 Entanglement based scheme of CVQKD

$\hat{X}_B$ can be get from $\hat{X}_{B_0}$ and $\hat{X}_{E_0}$.

$$\hat{X}B = \sqrt{T}\hat{X}_{B_0} + \sqrt{1-T}\hat{X}_{E_0} \quad (7)$$

The variance of mode B is as follows.

$$V_B = TV' + (1-T)N \quad (8)$$

The conditional variance is defined as follows.

$$V_{X|Y} = V(X) - \frac{|\langle XY \rangle|^2}{V(Y)} \quad (9)$$

The conditional variance $V_{B|A}$, from Eq. (8) and Eq. (9), is as follows.

$$V_{B|A} = T + (1-T)N \quad (10)$$

After getting V_B and $V_{B|A}$, the mutual information between Alice and Bob can be attained.

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|A}} \quad (11)$$

The Holevo bound obtained by Eve can be calculated by using entangling cloner model[10-11], and then the secret key rate shared by Alice and Bob can be get. From Fig. 3, we can get

$$\hat{X}_{E_1} = \sqrt{T}\hat{X}_{E_0} - \sqrt{1-T}\hat{X}_{B_0} \quad (12)$$

Thus, the variance of mode E_1 is given by

$$V_{E_1} = (1-T)V' + TN \quad (13)$$

And from Eq. (9) and Eq. (13) the conditional variance $V_{E_1|A}$ can be calculated as

$$V_{E_1|A} = (1-T) + TN \quad (14)$$

Hence, Eve's covariance matrix can be obtained as follows.

$$\boldsymbol{\gamma}_E(V',V') = \begin{pmatrix} \gamma_{E_1} & \sigma_{E_1E_2}^{\mathrm{T}} \\ \sigma_{E_1E_2} & \gamma_{E_2} \end{pmatrix} = \begin{pmatrix} V_{E_1}I & Z_{E_1E_2}\sigma_Z \\ Z_{E_1E_2}\sigma_Z & NI \end{pmatrix} \quad (15)$$

where $\boldsymbol{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\boldsymbol{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $Z_{E_1E_2} = \sqrt{T(N^2-1)}$. $\sigma_{E_1E_2}$ is the covariance matrix between mode E_1 and mode E_2.

Before analyzing secret key rate of CVQKD, it's necessary to introduce two mode Gaussian states[12]. The covariance matrix of two-mode Gaussian states is a 4×4 matrix which can be depicted as $\boldsymbol{\sigma} = \begin{pmatrix} A & C^{\mathrm{T}} \\ C & B \end{pmatrix}$. A and B, 2×2 matrixes, are the reduced states of system A and system B, while C is the classic association between A and B. The symplectic eigenvalue of σ can be get from Eq. (16)

$$\lambda\pm = \sqrt{\frac{\Delta\sigma \pm \sqrt{\Delta\sigma^2 - 4\det\sigma}}{2}} \quad (16)$$

where det means the determinant of matrix, $\Delta\sigma = \det A + \det B + 2\det C$.

Hence, using Eq. (15) and Eq. (16), the symplectic eigenvalue λ_1, λ_2 of $\boldsymbol{\gamma}_E(V',V')$ is easy to attain. So the von Neumann entropy of Eve's state is given by

$$S(E) = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) \quad (17)$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$.

$\boldsymbol{\gamma}_E^{\hat{X}_B}$ can be obtained by the conditional covariance matrix

$$\boldsymbol{\gamma}_E^{\hat{X}_B} = \boldsymbol{\gamma}_E - \sigma_{E_1E_2B}^{\mathrm{T}}(X\boldsymbol{\gamma}_B X)^{MP}\sigma_{E_1E_2B} \quad (18)$$

where $\boldsymbol{X} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\sigma_{E_1E_2B} = (Z_{E_1B}I, Z_{E_2B}\sigma_Z)$, $Z_{E_1B} = \sqrt{T(1-T)}(N-V')$, $Z_{E_2B} = \sqrt{1-T}\sqrt{N^2-1}$.

$\boldsymbol{\gamma}_E^{\hat{X}_B}$ can be depicted as follow format.

$$\boldsymbol{\gamma}_{E^n}^{\hat{X}_B}=\begin{pmatrix}\boldsymbol{F} & \boldsymbol{H}^{\mathrm{T}}\\ \boldsymbol{H} & \boldsymbol{G}\end{pmatrix} \tag{19}$$

where $\boldsymbol{F}=\begin{bmatrix}V_{E_1}-\dfrac{Z_{E_1B}^2}{V_B} & 0\\ 0 & V_{E_1}\end{bmatrix}$, $\boldsymbol{G}=\begin{bmatrix}N-\dfrac{Z_{E_2B}^2}{V_B} & 0\\ 0 & N\end{bmatrix}$,

$\boldsymbol{H}=\begin{bmatrix}Z_{E_1E_2}-\dfrac{Z_{E_1B}Z_{E_2B}}{V_B} & 0\\ 0 & -Z_{E_1E_2}\end{bmatrix}$.

Using Eq. (16), the symplectic eigenvalue λ_3, λ_4 of $\gamma_{E^n}^{\hat{X}_B}$ can bet get. Hence, the von Neumann entropy is as follows.

$$S(E|B)=G\left(\frac{\lambda_3-1}{2}\right)+G\left(\frac{\lambda_4-1}{2}\right) \tag{20}$$

Finally, the mutual information between Bob and Eve, from Eq. (17) and Eq. (20), is as follows.

$$\chi_{BE}=S(E)-S(E|B) \tag{21}$$

So the secret key rate for reverse reconciliation is given by

$$R^{\triangleleft}=I_{AB}-\chi_{BE} \tag{22}$$

The loss of secret key rate is defined as follows.

$$R_{\mathrm{loss}}^{\triangleleft}=R^{\triangleleft}(V)-R^{\triangleleft}(V') \tag{23}$$

$R^{\triangleleft}(V)$ is the secret key rate with perfect FM, $R^{\triangleleft}(V')$ is the secret key rate with imperfect FM, and $R_{\mathrm{loss}}^{\triangleleft}$ means the difference between $R^{\triangleleft}(V)$ and $R^{\triangleleft}(V')$.

First, the secret key rate with perfect FM and that with imperfect FM are analyzed. $\theta=5°$, $V=2$ and $N=1$ are used in the following computation. From Fig. 4, $R^{\triangleleft}(V)$ is greater than $R^{\triangleleft}(V')$. The dotted line is $R_{\mathrm{loss}}^{\triangleleft}$, the loss due to using imperfect FM. The result shows Faraday mirror′s imperfection will reduce the secret key rate.

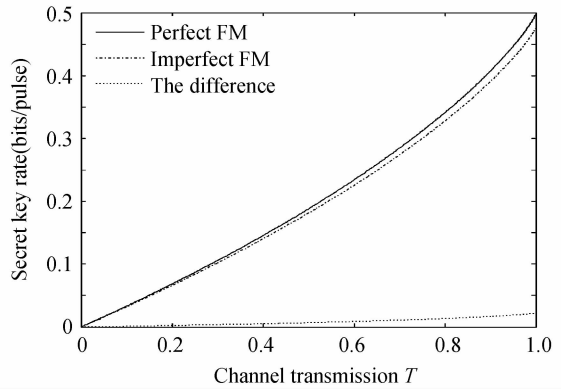

Fig. 4 The secret key rate with perfect FM and that with imperfect FM

The transmission distance and transmission efficiency have such relationship $T=10^{-\alpha L/10}$, where $\alpha=0.2$ dB/km. If we use imperfect FM, the transmission distance will be cut short. To get the same secret key rate 0.1, the transmission distance with imperfect FM is almost $1km$ less than that with perfect FM as point A and point B show in Fig. 5, which can′t be neglected in project. We use $\theta=5°$, $V=1.8$ and $N=1$ in Fig. 5.

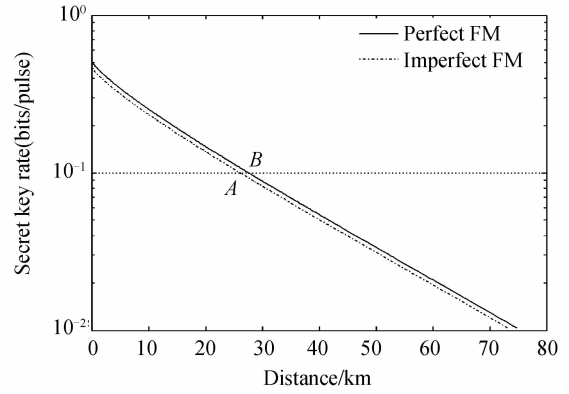

Fig. 5 Transmission distance with perfect FM and that with imperfect FM

Then, the relationship between the secret key rate and modulation variance is discussed. From Fig. 6, $R_{\mathrm{loss}}^{\triangleleft}$ will become less if V becomes greater. When V is 500 and $T<0.8$, $R_{\mathrm{loss}}^{\triangleleft}$ is nearly zero as the fourth curve shows. Hence, $R_{\mathrm{loss}}^{\triangleleft}$ is inversely proportional to V and proportional to T. When T is little, the influence of imperfect FM is little, and when V is great, the influence of imperfect FM is little. Hence, in practical experiments, great modulation variance is suggested. But the modulation variance is limited by the photoelectric modulator, which is finite. The influence can′t be removed by increasing V without limitation. The first curve is the secret key rate loss while using imperfect FM and $V=2$. Then we use $V=10$, the second curve, the secret key rate loss is less than the former. This shows the modulation variance value is more importance than FM′s precision. It is because modulator is more adjustable, which can range from 2 to 500. But the range of FM′s rotation angle is only from 40° to 45°.

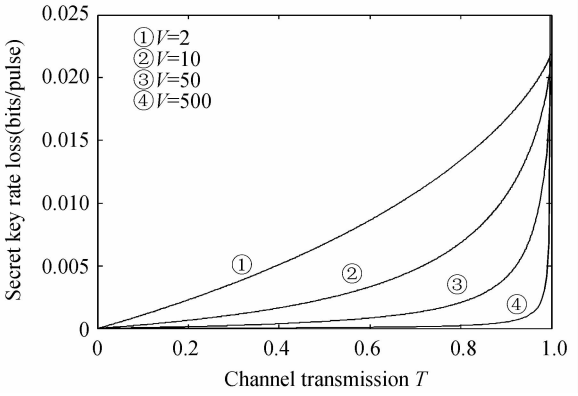

Fig. 6 The loss of secret key rate with different modulation variances $\theta=5°$

Last, how the size of FM′s rotation angle affects secret key rate is discussed. From the result, the secret key rate is inversely proportional to θ. When θ becomes greater and $T>0.4$, the secret key rate that Alice and Bob attain becomes less as shown in Fig. 7.

To look more obviously, the curves, from $T=0.5$ to $T=0.6$, are enlarged as shown in the illustration of Fig. 7, which clearly proves the conclusion.

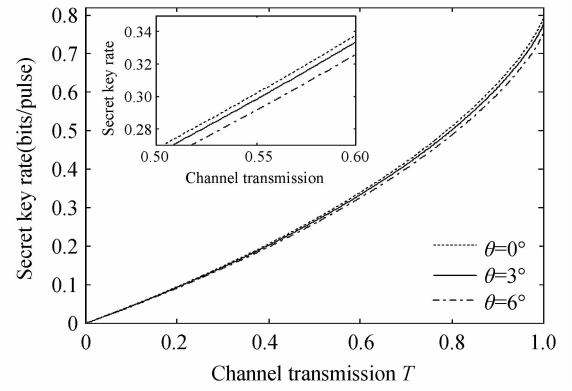

Fig. 7 The secret key rate when FM has different rotation angles $V=3$

The situation of secret key rate with imperfect FM in direct reconciliation is almost the same as that in reverse reconciliation. Hence, it's not necessary to repeat once again.

3 Conclusion

It's shown that using FM with imperfection in practical system will reduce the secret key rate which can be reached with perfect FM. It's suggested to consider the FM's rotation angle in the theoretical model as part 3 shows, which will make the analytic model more rigorously. The influence of FM can be reduced if the modulation variance is great, such as $V=500$ or the transmission distance is long. This is suggestions to get higher secret key rate. Firstly, using FM with rotation angle closed to 45° as far as possible. Using photoelectric polarization controller to change the signal's polarization angle is also a choice. Secondly, as soon as the communication system is set up, Alice had better to detect the practical rotation angle of FM which can provide data to correct the modulation variance. If not considering the FM's imperfection, Alice and Bob will be surprised to find the communication system can't attain the secret key rate which is designed in laboratory. Thirdly, it's advised to use great modulation variance in practical system if modulator allows.

Reference

[1] GROSSHANS F. Collective attacks and unconditional security in continuous variable quantum key distribution[J]. *Physical Review Letters*, 2005, **94**(2): 020504.

[2] JOUGUET P, KUNZ-JACQUES S, DIAMANTI E, *et al*. Analysis of imperfections in practical continuous-variable quantum key distribution[J]. *Physical Review A*, 2012, **86**(3): 02309.

[3] HUANG Jing-zheng, WEEDBROOK C, YIN Zhen-qiang, *et al*. Quantum hacking of a continuous variable quantum key distribution system using a wavelength attack[J]. *Physical Review A*, 2013, **87**(6): 062329.

[4] MA Xiang-chun, SUN Shi-hai, JIANG Mu-sheng, *et al*. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol [J]. *Physical Review A*, 2013, **87**(5): 052309.

[5] MA Xiang-chun, SUN Shi-hai, JIANG Mu-sheng, *et al*. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems [J]. *Physical Review A*, 2013, **88**(2): 022339.

[6] SUN Shi-hai, JIANG Mu-sheng, LIANG Lin-mei. Passive Faraday mirror attack in a practical two-way quantum-key-distribution system[J]. *Physical Review A*, 2011, **83**(6): 062331.

[7] FOSSIER S, DIAMANTI E, DEBUISSCHERT T, *et al*. Field test of a continuous-variable quantum key distribution prototype[J]. *New Journal of Physics*, 2009, **11**: 045023.

[8] JOUGUET P, KUNZ-JACQUES S, LEVERRIER A, *et al*. Experimental demonstration of long-distance continuous-variable quantum key distribution [J]. *Nature Photonics*, 2013, **7**: 378-381.

[9] LODEWYCK J, BLOCH M, GARCíA-PATRóN R, *et al*. Quantum key distribution over 25 *km* with an all-fiber continuous-variable system[J]. *Physical Review A*, 2007, **76**(4): 042305.

[10] WEEDBROOK C, PIRANDOLA S, LLOYD S, *et al*. Quantum cryptography approaching the classical limit[J]. *Physical Review Letters*, 2010, **105**(110501): 1-4.

[11] WEEDBROOK C, PIRANDOLA S, RALPH C T. Continuous-variable quantum key distribution using thermal states[J]. *Physical Review A*, 2012, **86**(2): 022318.

[12] SERAFINI A, ILLUMINATI F, SIENA S D. Symplectic invariants, entropic measures and correlations of Gaussian states[J]. *Journal of Physics B*, 2004, **37**(02): L21-L28.