Effect of electromagnetic disturbance on the practical QKD system in the smart grid*

Li Fang-Yi(李芳毅)[a)b)], Wang Dong(王 东)[a)b)], Wang Shuang(王 双)[a)b)†], Li Mo(李 默)[a)b)], Yin Zhen-Qiang(银振强)[a)b)‡], Li Hong-Wei(李宏伟)[a)b)], Chen Wei(陈 巍)[a)b)], and Han Zheng-Fu(韩正甫)[a)b)]

[a)] *Key Laboratory of Quantum Information, University of Science and Technology of China, Chinese Academy of Sciences, Hefei* 230026, *China*

[b)] *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*

(Received 29 April 2014; revised manuscript received 30 May 2014; published online 10 October 2014)

To improve the security of the smart grid, quantum key distribution (QKD) is an excellent choice. The rapid fluctuations on the power aerial optical cable and electromagnetic disturbance in substations are two main challenges for implementation of QKD. Due to insensitivity to birefringence of the channel, the stable phase-coding Faraday–Michelson QKD system is very practical in the smart grid. However, the electromagnetic disturbance in substations on this practical QKD system should be considered. The disturbance might change the rotation angle of the Faraday mirror, and would introduce an additional quantum bit error rate (QBER). We derive the new fringe visibility of the system and the additional QBER from the electromagnetic disturbance. In the worst case, the average additional QBER only increases about 0.17% due to the disturbance, which is relatively small to normal QBER values. We also find the way to degrade the electromagnetic disturbance on the QKD system.

Keywords: Faraday mirror, electromagnetic disturbance, quantum key distribution, quantum bit error rate, smart grid

PACS: 42.50.Ex **DOI:** 10.1088/1674-1056/23/12/124201

1. Introduction

The electrical grid delivers electricity from power plants to the society, and plays an important role in our daily life. With the development of information technology, the new smart grid uses two-way flows of electricity and information to create an automated and distributed advanced energy delivery network.[1] The security and reliability of the communication infrastructures are essential for electric power systems. Although the most effective solution is using encryption techniques, it is difficult to achieve the desired security in practice. On one hand, the encryption techniques based on unproven mathematical assumptions become vulnerable in the face of new computer technologies. On the other hand, the refresh rate of keys is too slow.

Quantum key distribution (QKD) provides us with a real-time way to distribute unconditionally secure keys through public channels, based on the laws of quantum theory.[2] Any eavesdropping attempts can be detected in the QKD procedure.[3] QKD would be a prime candidate to solve the key distribution problem in cryptography. Combining QKD with one-time pad encryption which has been proven to be information-theoretically secure would offer us the highest secure communication. Or, employing QKD, we can fast refresh keys in Advanced Encryption Standard (AES) to enhance its security. Therefore, QKD might be an excellent choice to improve the security of the smart grid.

In this paper, we first explore the practical QKD system in the smart grid, and find that the stable Faraday–Michelson QKD system is recommendable. Then, the electromagnetic disturbance in substations on this practical QKD system is considered, we recalculate the fringe visibility, and get the expression of additional quantum bit error rate (QBER) from electromagnetic disturbance. Finally, we assess the effect of electromagnetic disturbance on the QKD system using the numerical simulation method.

2. The practical QKD system in the smart grid

The electric power special optical cable is the new and important transmission medium for communication in the smart grid.[4] Now the coverage rate of optical fiber in 220 kV and 110 kV substations has already exceeded 90%. So the ideal transmission medium for QKD in the smart grid is optical fiber. However, there are two major challenges when we implement QKD: complex and open environment of the aerial optical cable, and strong electromagnetic disturbance in substations. Facing these challenges, the protocol, coding

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61101137, 61201239, 61205118, and 11304397) and the National Basic Research Program of China (Grants No. 2013CB338002).

†Corresponding author. E-mail: wshuang@ustc.edu.cn

‡Corresponding author. E-mail: yinzheqi@mail.ustc.edu.cn

© 2014 Chinese Physical Society and IOP Publishing Ltd

method, and implementation system are things we should consider.

Many QKD protocols have been proposed and realized in the past two decades. Among these protocols, BB84[5] is the first and also the most popular QKD protocol, and its security has been rigorously proven.[6] In the original BB84 proposal, the key was encoded on the polarizations of photons, but then it was extended to the phases of photons, polarization, and phase are two equivalent coding methods. But in the power aerial optical cable, the complex and open atmosphere, such as temperature changes, thermal gradients, vibration caused by wind, and electromagnetic field, leads to rapid and random vibrations of polarization. In order to counter the fluctuations on the power aerial optical cable channel, the Faraday–Michelson QKD system[7] that implements BB84 protocol with phase coding method is recommended. This type of QKD system is insensitive to the polarization disturbance,[7–9] and has been successfully demonstrated in telecommunication fiber networks.[10–12] Hence the practical QKD system in the smart grid is the Faraday–Michelson QKD system.

The simplified diagram of a Faraday–Michelson QKD system is shown in Fig. 1. The main part is two asymmetric Faraday–Michelson interferometers (FMI), one of which consists of one 50:50 beam splitter (BS), one phase modulator (PM), and two Faraday mirrors (FM). Two arms of the FMI are named short arm and long arm, respectively. The arm with PM is the long arm, and the other is the short one. Through controlling PM to modulate $(\{0,\pi\},\{\pi/2,3\pi/2\})$ four phases, the BB84 protocol is implemented in the Faraday–Michelson QKD system. FM is the core unit of the Faraday–Michelson QKD system. It is composed of a 45°-Faraday rotator and a mirror, the reflected state of polarization (SOP) is orthogonal with the original signal. We can write the Jones matrix of FM as

$$\mathrm{FM}(45^\circ) = -\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{1}$$

FM is a conventional optical unit used to automatically compensate polarization disturbance in optical fiber. Through theory analysis, the fringe visibility of an ideal Faraday–Michelson QKD system is independent of the channel, and equals 1.[7] It means that the Faraday–Michelson QKD system is immune to the fluctuations on the power aerial optical cable channel.

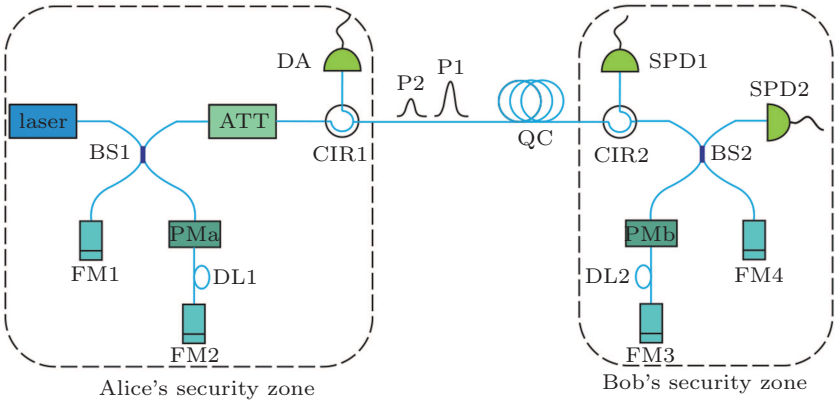


Fig. 1. (color online) Schematic diagram of the Faraday–Michelson QKD system. L: laser diode; BS: 50:50 beam splitter; FM: Faraday mirror; PM: phase modulator; DL: delay line; ATT: attenuator; CIR: circulator; QC: quantum channel; SPD: single-photon detector.

3. Electromagnetic disturbance on FM

Although the Faraday–Michelson QKD system can passively compensate the fluctuations on the power aerial optical cable channel, there is another challenge for the QKD system. The QKD terminals used for key distribution are placed in the substations, and the strong electromagnetic disturbance on the QKD system should be considered. Here we focused on the electromagnetic disturbance on the optical part of the QKD system. FM is the most likely optical unit to be disturbed, since the ambient electromagnetic field would affect its internal magnetic field, and change the rotation angle. Jones matrix of FM under strong electromagnetic disturbance is rewritten as

$$\mathrm{FM}(\boldsymbol{B}) \equiv \mathrm{FM}(45^\circ + \varepsilon) = -\begin{bmatrix} \sin 2\varepsilon & \cos 2\varepsilon \\ \cos 2\varepsilon & -\sin 2\varepsilon \end{bmatrix}, \tag{2}$$

where the outside electromagnetic disturbance represents as $\boldsymbol{B}$, and ε is the change of rotation angle caused by electromagnetic disturbance. Considering the internal magnetic field and outside electromagnetic disturbance, the value of $|\varepsilon|$ is less than 1°. FM_1 and FM_2 are in the same FMI, which is placed in one substation, hence FM_1 and FM_2 are affected by the same electromagnetic disturbance ε_a. Analogously, the disturbance on FM_3 and FM_4 is denoted as ε_b.

Since the rotation angle is not equivalent to 45° any more, the compensation action of FM would be weakened, and the

fringe visibility of the Faraday–Michelson QKD system will be less than 1. The electromagnetic disturbance would eventually introduce an additional optical background quantum bit error rate (QBER).

4. Additional QBER from electromagnetic disturbance

Let S_a, S_b (L_a, L_b) denote Jones matrices of the short (long) arms belonging to Alice's and Bob's FMI, respectively. Matrices of two PMs in FMIs are PM_a and PM_b. QC represents the Jones matrix of the quantum channel connecting Alice and Bob. The superscripts "$\rightarrow$" and "$\leftarrow$" mark the forward and backward matrices, respectively. For example, $\overrightarrow{S_a}$ denotes the transformation matrix of the short arm in Alice's FMI, the direction is from BS_1 to FM_1, while the direction of $\overleftarrow{S_a}$ is from FM_1 to BS_1. Thus the overall transformation matrices of the two interference pulses are denoted as follows:

$$\begin{aligned}&\text{Pulse } S_a+L_b: \left(\overleftarrow{L_b}\cdot\overleftarrow{PM_b}\cdot FM_3\cdot\overrightarrow{PM_b}\cdot\overrightarrow{L_b}\right)\\&\quad\cdot\overrightarrow{QC}\cdot\left(\overleftarrow{S_a}\cdot FM_1\cdot\overrightarrow{S_a}\right),\\&\text{Pulse } L_a+S_b: \left(\overleftarrow{S_b}\cdot FM_4\cdot\overrightarrow{S_b}\right)\cdot\overrightarrow{QC}\\&\quad\cdot\left(\overleftarrow{L_a}\cdot\overleftarrow{PM_a}\cdot FM_2\cdot\overrightarrow{PM_a}\cdot\overrightarrow{L_a}\right),\end{aligned}\tag{3}$$

where pulse S_a+L_b denotes the interference pulse that propagates along the short arm of Alice's FMI and then along the long arm of Bob's FMI; Pulse L_a+S_b denotes the interference pulse that propagates along the long arm of Alice's FMI and then along the short arm of Bob's FMI.

The optical unit between BS and FM in the short arm is the normal single mode fiber (SMF), and in the long arm is SMF and PM. The Jones matrix of SMF that can be equivalent to the one of an ellipse delayer, is given by

$$\overrightarrow{R}=\begin{bmatrix}P & -Q^*\\ Q & P^*\end{bmatrix},\tag{4}$$

while, in the inverse direction, the Jones matrix is given by

$$\overleftarrow{R}=\begin{bmatrix}P & -Q\\ Q^* & P^*\end{bmatrix},\tag{5}$$

where $P=\cos(\delta/2)+\mathrm{i}\cos(2\alpha)\sin(\delta/2)$, and $Q=\mathrm{i}\sin(2\alpha)\sin(\delta/2)$, α is the rotation angle between the equivalent fast axis and the x axis of the reference frame, δ is the phase difference between the equivalent fast and slow axes of the SMF, and the PM only introduces phase information φ. In this way, elements in expression (3) could be written as

$$\begin{aligned}T_1 &\equiv \overleftarrow{S_a}\cdot FM_1\cdot\overrightarrow{S_a}\\&=\overleftarrow{R_1}(\alpha_1,\delta_1)\cdot FM(45^\circ+\varepsilon_a)\cdot\overrightarrow{R_1}(\alpha_1,\delta_1),\\T &\equiv \overrightarrow{QC}=\overrightarrow{R}(\alpha,\delta),\end{aligned}$$

$$\begin{aligned}T_3 &\equiv \overleftarrow{L_b}\cdot\overleftarrow{PM_b}\cdot FM_3\cdot\overrightarrow{PM_b}\cdot\overrightarrow{L_b}\\&=\overleftarrow{R_3}(\alpha_3,\delta_3)\cdot FM(45^\circ+\varepsilon_b)\cdot\overrightarrow{R_3}(\alpha_3,\delta_3)\cdot\mathrm{e}^{\mathrm{i}\varphi_b};\end{aligned}\tag{6}$$

and

$$\begin{aligned}T_2 &\equiv \overleftarrow{L_a}\cdot\overleftarrow{PM_a}\cdot FM_2\cdot\overrightarrow{PM_a}\cdot\overrightarrow{L_a}\\&=\overleftarrow{R_2}(\alpha_2,\delta_2)\cdot FM(45^\circ+\varepsilon_a)\cdot\overrightarrow{R_2}(\alpha_2,\delta_2)\cdot\mathrm{e}^{\mathrm{i}\varphi_a},\\T_4 &\equiv \overleftarrow{S_b}\cdot FM_4\cdot\overrightarrow{S_b}\\&=\overleftarrow{R_4}(\alpha_4,\delta_4)\cdot FM(45^\circ+\varepsilon_b)\cdot\overrightarrow{R_4}(\alpha_4,\delta_4).\end{aligned}\tag{7}$$

Suppose the input Jones vector of Alice's FMI is $E_{in}=(\cos\beta,\ \sin\beta\,\mathrm{e}^{\mathrm{i}\gamma})^{\mathrm{T}}$, the output of Bob's FMI can be expressed as

$$E_{out}=\frac{\sqrt{\sigma}}{4}\left(T_3\cdot T\cdot T_1\cdot\mathrm{e}^{\mathrm{i}\varphi_b}+T_4\cdot T\cdot T_2\cdot\mathrm{e}^{\mathrm{i}\varphi_a}\right)E_{in},\tag{8}$$

where σ is the overall loss. Then the power of the interference output is given by

$$P_{out}=E_{out}^{+}\cdot E_{out}=\frac{\sigma}{8}\left[1+\sqrt{A^2+B^2}\cos\left(\varphi_a-\varphi_b+\Theta\right)\right],\tag{9}$$

where $\Theta=\arctan(B/A)$. Although there are many parameters in this equation, α_j and δ_j ($j=1,2,3,4$) can be considered as constants, and also β and γ, because the environments of two FMIs and the laser diode are relatively stable. A and B are the functions of parameters α, δ, ε_a and ε_b. The concrete expressions of A and B are very complex, we do not present them here.

Then, the fringe visibility of the Faraday–Michelson QKD system can be deduced as follows:

$$\eta\equiv\frac{P_{out}^{max}-P_{out}^{min}}{P_{out}^{max}+P_{out}^{min}}=\sqrt{A^2+B^2}.\tag{10}$$

Finally, the additional optical background QBER caused by electromagnetic disturbance is given by

$$\mathrm{QBER}_{add}\equiv\frac{1-\eta}{2}=\frac{1-\sqrt{A^2+B^2}}{2}.\tag{11}$$

From the last two equations, as a result of the electromagnetic disturbance in the smart grid, the fringe visibility of the Faraday–Michelson QKD system is not equivalent to 1 any more, and becomes a function of the birefringence of the quantum channel, which leads to the increment of optical background QBER of the QKD system.

5. Numerical simulation of the additional QBER

Using the numerical simulation method, we can get the value of the additional QBER, and assess whether stable QKD is feasible. The SOP of pulses generated by the laser diode is good linear polarized light, here is assumed to be horizontally polarized, $E_{in}=(1,\ 0)^{\mathrm{T}}$. The constant values of α_j and δ_j ($j=1,2,3,4$) are ($\alpha_1=0.12\pi,\delta_1=1.56\pi$), ($\alpha_2=0.25\pi,\delta_2=1.12\pi$), ($\alpha_3=0,\delta_3=0.72\pi$), and ($\alpha_4=0.35\pi,\delta_4=0.36\pi$), the same as in Ref. [13].

5.1. Additional QBER versus random variations of QC

Due to the complex and open environment of the aerial optical cable, the birefringence of characteristic of QC changes randomly, the SOP of output light of QC varies randomly, and the corresponding additional QBER also varies as the random variation of QC.

The fiber used as QC in the aerial optical cable is SMF, whose Jones matrix is given by Eq. (4). In order to simulate the random variation of QC with time, the random walking model[14]

$$X(t+\Delta t) = X(t) + \xi + k\Delta X \tag{12}$$

is used, where X denotes α or δ in Eq. (4), $k\Delta X$ is the correction term for memory effect in variation process, and $\Delta X = X(t) - X(t-\Delta t)$. For α, ξ_α is a uniform random number in $[-\pi/50, \pi/50]$, $k_\alpha = 0.35$. For δ, ξ_δ is a uniform random number in $[-\pi/30, \pi/30]$, $k_\delta = 0.85$.

We use the Stokes parameters to show the variation of birefringence of the fiber. The Stokes parameters of the output light from the fiber is given by

$$\begin{aligned} S_1 &= E_S^+ \cdot \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot E_S, \\ S_2 &= E_S^+ \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot E_S, \\ S_3 &= E_S^+ \cdot \begin{bmatrix} 0 & \mathrm{i} \\ -\mathrm{i} & 0 \end{bmatrix} \cdot E_S, \end{aligned} \tag{13}$$

where E_S denotes the output light from the fiber, and equals $\overrightarrow{R}_F \cdot (1, 0)^T$ if the input light is supposed to be horizontal, $\overrightarrow{R}_F$ is the Jones matrix of the fiber. To estimate the electromagnetic disturbance effects on QKD, the values of ε_a and ε_b from electromagnetic disturbance are set to maximum, $\varepsilon_a = 1^\circ$, and $\varepsilon_b = -1^\circ$.

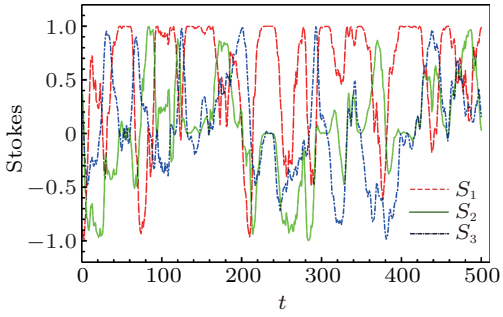


Fig. 2. (color online) Variations of normalized Stokes parameters of QC with time.

The numerical simulation results are shown in Fig. 2 and Fig. 3. Three lines in Fig. 2 stand for three normalized Stokes parameters. Figure 3 gives us the intuitive sense of the effects from electromagnetic disturbance, the variation of QBER means electromagnetic disturbance on FM weakens compensation of birefringence fluctuations in the power aerial optical cable. However, the maximum value of the additional QBER is just around 0.3%.

5.2. The average additional QBER

The additional QBER in Fig. 3 is the instantaneous value, but the average value is more suitable for accessing effects from electromagnetic disturbance on the Faraday–Michelson QKD system. The average additional QBER can be written as

$$\overline{\mathrm{QBER}}_{\mathrm{add}} = \frac{1}{\pi^2} \int_0^{\pi/2} \int_0^{2\pi} \mathrm{QBER}_{\mathrm{add}} \, \mathrm{d}\alpha \, \mathrm{d}\delta. \tag{14}$$

Now the average additional QBER is the function of ε_a and ε_b.

The average values of the additional QBER from electromagnetic disturbance are shown in Fig. 4. Without electromagnetic disturbance, in this case $\varepsilon_a = \varepsilon_b = 0$, of course, the value of $\overline{\mathrm{QBER}}_{\mathrm{add}}$ reaches minimum 0. Then, with electromagnetic disturbance increase, corresponding to increase of $|\varepsilon_a|$ and $|\varepsilon_b|$, the average additional QBER also increases. We also find that the increments of $\overline{\mathrm{QBER}}_{\mathrm{add}}$ are different, the case that ε_a and ε_b have the same direction (the same positive or negative) increases slower than the case that ε_a and ε_b have the opposite direction (one positive and the other negative). This result offers us one way to degrade the electromagnetic disturbance on the QKD system, by changing the placement direction of QKD systems to keep ε_a and ε_b in the same direction. It is also the reason why we chose $\varepsilon_a = 1^\circ$ and $\varepsilon_b = -1^\circ$ in last subsection to simulate the additional QBER, and the value of $\overline{\mathrm{QBER}}_{\mathrm{add}}$ reaches maximum 0.17%, which is relatively small to normal QBER values.

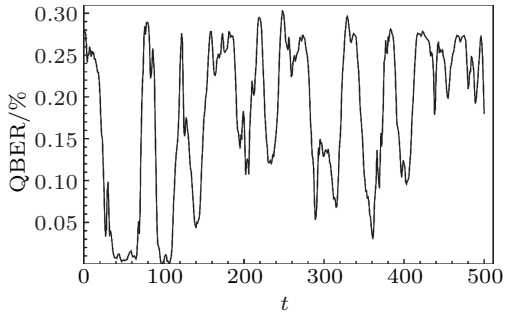


Fig. 3. Variation of the additional QBER: $\mathrm{QBER}_{\mathrm{add}}$ with time.

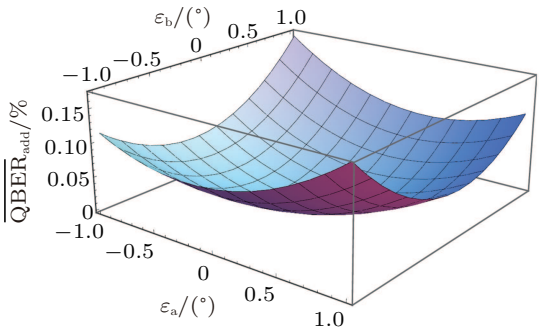


Fig. 4. (color online) Relationship between the average additional QBER: $\overline{\mathrm{QBER}}_{\mathrm{add}}$ and electromagnetic disturbance ε_a, ε_b.

6. Conclusion

In summary, we have analyzed the effect of electromagnetic disturbance on the Faraday–Michelson QKD system in the smart grid. In order to adapt the rapid and random fluctuations on the power aerial optical cable, the stable Faraday–Michelson QKD system is recommended, but the electromagnetic disturbance in substations on this practical QKD system should be considered. The disturbance might change the rotation angle of the Faraday mirror, and would introduce an additional QBER. Through recalculating the fringe visibility of the Faraday–Michelson QKD system under electromagnetic disturbance, we get the expression of additional QBER which is a function of the birefringence of the channel. Furthermore, we numerically simulate the instantaneous and average additional QBERs. From results of numerical simulations, we not only find the way to degrade the electromagnetic disturbance on the QKD system, but also conclude that the additional QBER from electromagnetic disturbance is relatively small. These positive results show the potential of QKD for secure applications in the smart grid.

References

[1] http://en.wikipedia.org/wiki/Electrical_grid

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

[3] Li H W, Yin Z Q, Wang S, Bao W S, Guo G C and Han Z F 2011 *Chin. Phys. B* **20** 100306

[4] Chen X. 2009 *Telecommunications for Electric Power System* **1** 16

[5] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* **175** 8

[6] Scaraniv, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301

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

[8] Yin Z Q, Han Z F, Chen W, Xu F X, Wu Q L and Guo G C 2008 *Chin. Phys. Lett.* **25** 3547

[9] Zhang Y, Wang S, Yin Z Q, Chen W, Liang W Y, Li H W, Guo G C and Han Z F 2012 *Chin. Phys. B* **21** 100307

[10] Chen W, Han Z F, Zhang T, Wen H, Yin Z Q, Xu F X, Wu Q L, Liu Y, Zhang Y, Mo X F, Gui Y Z, Wei G and Guo G C 2009 *IEEE Photon. Tech. Lett.* **21** 575

[11] Xu F X, Chen W, Wang S, Yin Z Q, Zhang Y, Liu Y, Zhou Z, Zhao Y B, Li H W, Liu D, Han Z F and Guo G C 2009 *Chin. Sci. Bull.* **54** 2991

[12] Wang S, Chen W, Yin Z Q, Zhang Y, Zhang T, Li H W, Xu F X, Zhou Z, Yang Y, Huang D J, Zhang L J, Li F Y, Liu D, Wang Y G, Guo G C and Han Z F 2010 *Opt. Lett.* **35** 2454

[13] Zeng Z M, Zhang X M, Feng H, Jin S J and An Y 2012 *Optics and Precision Engineering* **20** 468 (in Chinese)

[14] Knill O 2009 *Probability Theory and Stochastic Processes with Applications* (New Delhi: Overseas Press India Private Limitied) pp. 164–167

[15] Liao Y B 2003 *Polarization Optics* (Beijing: Science Press) pp. 55–56 (in Chinese)