Analysis of Faraday–Michelson quantum key distribution system with unbalanced attenuation

Xiaotian Song (宋萧天)[1,2], Hongwei Li (李宏伟)[1,2*], Chunmei Zhang (张春梅)[1,2], Dong Wang (王 东)[1,2], Shuang Wang (王 双)[1,2], Zhenqiang Yin (银振强)[1,2], Wei Chen (陈 巍)[1,2], and Zhengfu Han (韩正甫)[1,2]**

[1]*Key Laboratory of Quantum Information, CAS, University of Science and Technology of China, Hefei 230026, China*

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

[*]*Corresponding author: lihw@mail.ustc.edu.cn;* [**]*corresponding author: yinzheqi@mail.ustc.edu.cn*

Received July 5, 2014; accepted October 24, 2014; posted online January 5, 2015

Quantum key distribution (QKD) is a major research topic because it provides unconditional security. Unfortunately, many imperfections remain in QKD's experimental realization. The Faraday–Michelson (FM) QKD system is proposed to eliminate these imperfections using polarization. However, the long arm's phase modulator (PM) has an unexpected insertion loss, meaning that the state sent is no longer perfect. In this letter, we propose an alternative FM-QKD system structure, and analyze the security and key generation rate in comparison with the original system via different analysis methods. We find an obvious key rate improvement when the PM insertion loss is not extremely small.

OCIS codes: 270.5565, 270.5568.
doi: 10.3788/COL201513.012701.

Quantum key distribution (QKD)[1] allows two certificated parties, known here as Alice and Bob, to share secret keys, which have unconditional security based on the laws of quantum mechanics, as has been proved in several ways in the literature[2,3]. However, in reality, these imperfect setups cannot work in exactly the same way as that described in the protocol, meaning that the operation may not be completely secure. At present, QKD has become a very hot research topic[4,5] and most QKD operations use the BB84 protocol, which is generally based on either phase or polarization coding[6–10]. The original phase coding-based QKD[11,12] scheme uses an unbalanced Mach–Zehnder interferometer, but it is very unstable because the birefringence in the fiber makes the polarization very complex; therefore, the Faraday–Michelson (FM) QKD system[12] was proposed. As described in Ref. [12], a Faraday mirror's Jones matrix can be given by

$$\mathrm{FM}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ -1 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}=\begin{bmatrix}0 & -1\\ -1 & 0\end{bmatrix}.$$

Finally, we can get the visibility of the system as 1, which means that the polarization problem can be solved.

In an ideal FM-QKD system, the phase modulator (PM) in the long arm has no insertion loss, and the states that Alice sends are the BB84 states, while in reality, the PM causes more losses in the long arm, which result in imperfect BB84 states. In this case, we must find another way to confirm the security of the method other than the GLLP[13] formula. Similar to the assumption used in our previous work[14], in which we find that the real-life states that Alice sends can be assumed to be perfect BB84 states combined with a unitary transformation. More interestingly, we can place the PM outside the interference ring, which has no corresponding imperfect state preparation problem. Finally, we analyze the final key generation rate, first with infinite decoy states, and then with the vacuum, decoy, and signal states.

A schematic diagram of the FM system is shown in Fig. 1.

From Fig. 1, the weak coherent states that Alice prepared in the long arm and the short arm can be given as follows:

Long arm:

$$|a\rangle_{\mathrm{l}}=e^{-\frac{|a|^2}{2}}\sum_{n=0}^{\infty}\frac{a^n}{\sqrt{n!}}|n\rangle_{\mathrm{l}}, \tag{1}$$

$$a=\sqrt{\mu}e^{i(\theta+\varphi)}. \tag{2}$$

Short arm:

$$|\beta\rangle_{\mathrm{s}}=e^{-\frac{|\beta|^2}{2}}\sum_{n=0}^{\infty}\frac{\beta^n}{\sqrt{n!}}|n\rangle_{\mathrm{s}}, \tag{3}$$

$$\beta=\sqrt{\nu}e^{i\theta}, \tag{4}$$

where $|a\rangle_{\mathrm{l}}, |\beta\rangle_{\mathrm{s}}$ represent the weak coherent state of the long and short arms, respectively. $|n\rangle_{\mathrm{l}}, |n\rangle_{\mathrm{S}}$ represent the n photon state in the long and short arms, respectively. μ is the mean photon number of the long arm while ν is the mean photon number of the short arm. We consider the loss of the PM on both sides to be the same, and this loss can be set as r. We can therefore find that $\nu = r^2\mu$, $e^{i\theta}$ is random but uniform at both sides, $e^{i\varphi}$ is the modulated phase by PM in the

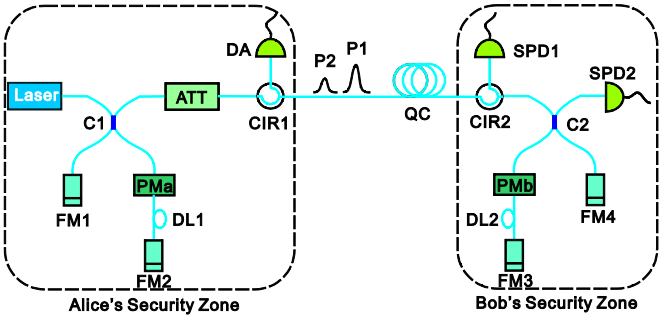

Fig. 1. QKD system with FM interferometer.

long arm. Using the method given by Lo *et al.*[15], the single-photon state sent by Alice can be given by

$$\frac{1}{\sqrt{\mu+\nu}}\left(\sqrt{\mu}|1\rangle+e^{i\varphi}\sqrt{\nu}|0\rangle\right), \tag{5}$$

where φ can be 0, 0.5π, π, and 1.5π which refer to the four states emitted by Alice. Here we can clearly see that these are no longer the perfect BB84 states, so we cannot simply use the GLLP.

For simplicity, we assume that the state emitted by Alice is the perfect BB84 state, whereas the unbalanced loss at Alice's side is all controlled by Eve, who is a third party, and then the upper bound of the final single-photon detection rate can be estimated by

$$P10^{\frac{-aL}{10}}P_{\mathrm{A}}P_{\mathrm{B}}=2\mu e^{-2\mu}10^{\frac{-aL}{10}}\frac{\mu+\nu}{2\mu}\frac{\nu}{\mu+\nu}$$

$$=\nu e^{-2\mu}10^{\frac{-aL}{10}}, \tag{6}$$

where P is the probability of the single photon emitted by Alice, α is the loss efficiency of the fiber, L is the length of the quantum channel. P_{A} and P_{B} are the pass efficiencies of Alice and Bob, respectively. Our previous work[14] shows that the practical state in Eq. (5) is as secure as the perfect BB84 state, which means that every effective click of the avalanche photodiode can generate a secret key. In this analysis, it was proved that the practical state is equal to the perfect BB84 state combined with a unitary transformation. The virtual setup is shown in Fig. 2.

The form of the unitary transformation is

$$U|0\rangle_{\mathrm{l}}|0\rangle_{\mathrm{s}}|0\rangle_{\mathrm{A}}=|0\rangle_{\mathrm{l}}|0\rangle_{\mathrm{s}}|0\rangle_{\mathrm{A}},$$

$$U|0\rangle_{\mathrm{l}}|1\rangle_{\mathrm{s}}|0\rangle_{\mathrm{A}}=|0\rangle_{\mathrm{l}}|1\rangle_{\mathrm{s}}|0\rangle_{\mathrm{A}},$$

$$U|1\rangle_{\mathrm{l}}|0\rangle_{\mathrm{s}}|0\rangle_{\mathrm{A}}=\frac{\sqrt{\nu}}{\sqrt{\mu}}|1\rangle_{\mathrm{l}}|0\rangle_{\mathrm{s}}|0\rangle_{\mathrm{A}}+\frac{\sqrt{\mu-\nu}}{\sqrt{\mu}}|0\rangle_{\mathrm{l}}|0\rangle_{\mathrm{s}}|1\rangle_{\mathrm{A}},$$

$$U|n\rangle_{\mathrm{l}}|m\rangle_{\mathrm{s}}|0\rangle_{\mathrm{A}}=|n\rangle_{\mathrm{l}}|m\rangle_{\mathrm{s}}|0\rangle_{\mathrm{A}},m+n\geq 2, \tag{7}$$

where $|0\rangle_{\mathrm{A}},|1\rangle_{\mathrm{A}}$ are mutually orthogonal states in Alice's system and unknown to Alice. Then, we can show that the state emitted by the virtual source with a unitary transformation is the same as that of the practical FM-QKD system with

$$\tilde{\mu}=2\mu,$$

$$\tilde{P}=\frac{\mu+\nu}{2\mu},$$

$$\tilde{p}_1=\frac{(\mu+\nu)e^{-(\mu+\nu)}}{\tilde{P}},$$

$$\tilde{p}_0=e^{-(\mu+\nu)}-e^{-(\mu+\nu)}-e^{-(\mu+\nu)}\left(\frac{\mu+\nu}{\tilde{P}}-(\mu+\nu)\right),$$

$$\tilde{p}_n=e^{-(\mu+\nu)}\frac{(\mu+\nu)^n}{n!}, \tag{8}$$

where $\tilde{\mu}$ is the mean number of the virtual source, $\tilde{P}$ is the pass efficiency of the single-photon state, and $\tilde{p}_n$ denotes the probability distribution of the n-photon state of the virtual source. When we assume that this unitary transformation is controlled by Eve, we can easily see that the security of the virtual source is the same as that of the practical QKD. Based on this analysis, we can show that the upper bound of the single-photon detection rate is

$$\tilde{p}_1\tilde{P}10^{\frac{-aL}{10}}P_B=(\mu+\nu)e^{-(\mu+\nu)}.10^{\frac{-aL}{10}}.\frac{\nu}{\mu+\nu}$$

$$=\nu e^{-(\mu+\nu)}10^{\frac{-aL}{10}}. \tag{9}$$

We can clearly see that this has improved the secret key rate by a factor of $e^{\mu-\nu}$. In addition to the improvement offered in the theory, we also have some ideas with regard to the practical system. First, we can simply add another PM with the same loss to the short arm, and then the single-photon state is the ideal BB84

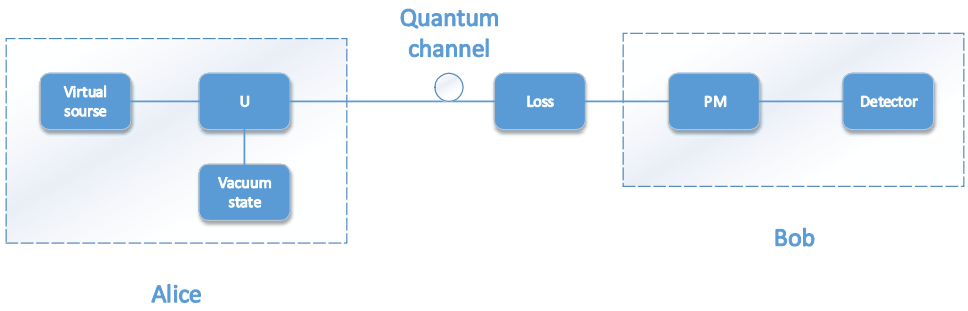

Fig. 2. Virtual setup of the QKD with a virtual source and a unitary transformation.

state. In this case, we can show that the upper bound of the single-photon detection rate is

$$P_1 10^{\frac{-aL}{10}} P_A' P_B' = \nu e^{-2\mu} 10^{\frac{-aL}{10}}. \quad (10)$$

This is just the same as Eq. (6), which is exactly lower than the virtual source.

In our method, we then put the PM outside the FM interference ring (the detailed setup of which can be shown in Fig. 3 and with the calculation of Eq. (10), it can also solve the polarization problem), so that the state emitted by Alice is the perfect BB84 state, and the loss at Bob's side is no longer r^2 as described before, but is simply r because the light passes through the PM only once. We can therefore easily obtain the upper bound of the single-photon detection rate as

$$P_1 10^{\frac{-aL}{10}} P_A'' P_B'' = 2\mu e^{-2\mu} 10^{\frac{-aL}{10}} \cdot \frac{\nu''}{2\mu}$$

$$= \nu'' e^{-2\mu} 10^{\frac{-aL}{10}}, \quad (11)$$

where $P_A'' = 1$ is the pass efficiency at Alice's side, while $P_B'' = \frac{\nu''}{2\mu}$ is the pass efficiency at Bob's side, and $\nu'' = r\mu = \sqrt{\mu\nu}$.

When compared with Eq. (9), we can see that it performs differently with different losses in the PM.

We consider the infinite decoy states and calculate the lower bound of the secret key rate in the four different cases. First, we can get the functions

$$\eta = P_A P_B 10^{\frac{-aL}{10}} \eta_D,$$

$$Y_1 = Y_0 + \eta,$$

$$e_1 = \frac{e_0 Y_0 + e_{Det}\eta}{Y_1},$$

$$Q_k = Y_0 + 1 - e^{-\eta k},$$

$$E_k = \frac{\frac{1}{2}Y_0 + e_{Det}(1 - e^{-\eta k})}{Q_k},$$

$$R \geq \frac{1}{2}(Y_1 P_1 (1 - h(e_1)) - Q_k h(E_k)), \quad (12)$$

where η_D is the detector efficiency, Y_0 is the dark count rate, Y_1 is the yield of the single-photon state, e_{Det} is the detection error rate, κ is the mean number of the state emitted by Alice, Q_κ is the gain of the photon state, E_κ is the error rate of the photon state, P_1 is the probability of the single-photon state, e_1 is the error rate of the single-photon state, and h is the binary Shannon information function.

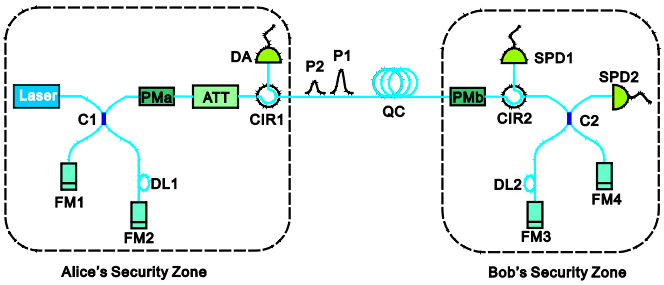

Fig. 3. FM-QKD system with PM out of the interference ring.

In the first case, we can consider the perfect scenario. The second case is based on the virtual source (we call this the VS case). In the third case, we consider the unbalanced attenuator to be controlled by Eve, which is the same as the case where we add another attenuator to the short arm (we call this the ACE case). The fourth case is where the PM is placed outside the interference ring (we call this the PMO case). The parameters in these cases can be given as follows:

In the first case,

$$k = 2\mu, P_1 = 2\mu e^{-2\mu}, P_A = 1, P_B = \frac{1}{2}.$$

In the second case,

$$k = \mu + \nu, P_1 = (\mu + \nu)e^{-(\mu+\nu)}, P_A = 1, P_B = \frac{\nu}{\mu + \nu}.$$

In the third case,

$$k = 2\mu, P_1 = 2\mu e^{-2\mu}, P_A = 1, P_B = \frac{\nu}{2\mu}.$$

In the fourth case,

$$k = 2\mu, P_1 = 2\mu e^{-2\mu}, P_A = 1, P_B = \frac{\nu''}{2\mu}.$$

The results of the simulation are given in Fig. 4 with different values of the insertion loss of the PM, which is represented by r. The mean photon number is 0.6 and the other parameters are referred to as the GYS parameters[16]. From these results, we can see that for the different PM insertion losses, the final key generation rate of the perfect scenario is undoubtedly the best, while that of the ACE case is the worst. However, the other two situations do show different performances under the different insertion loss conditions. When the insertion loss is $\sqrt{2/3}$, the VS case has a higher final key generation rate (Fig. 4(a)). However, as the insertion loss increases to $\sqrt{1/2}$, the two key generation rate curves have a crossing point (Fig. 4(b)). When the transmission distance is shorter than the distance to the crossing point, the PMO case has the higher key generation rate, and when the transmission distance is longer than the distance to the crossing point, the VS case has the better rate. As we expected, the PMO case produces a better performance when the insertion loss of the PM increases to $\sqrt{1/3}$ (Fig. 4(c)).

We analyze the lower bound of the secret key rate using the vacuum, decoy, and signal states[17–21] in the four different cases described above.

First, we can obtain the lower bound of Y_1 and the upper bound of e_1 from

$$\eta = P_A P_B 10^{\frac{-aL}{10}} \eta_D,$$

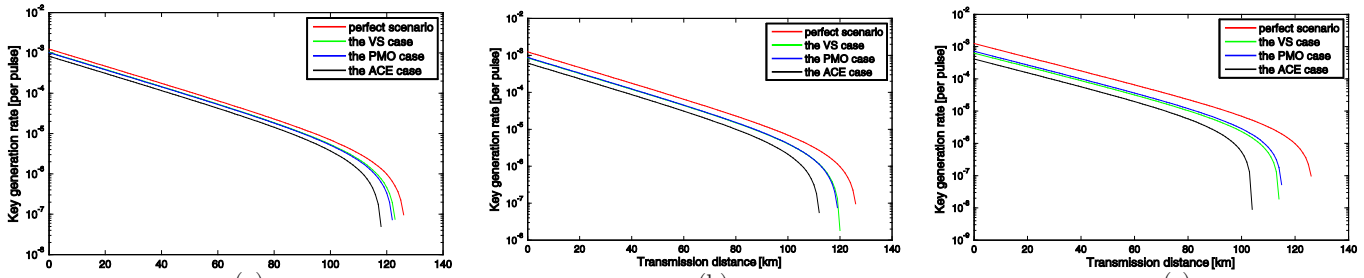

Fig. 4. Simulation results of the infinite decoy states: (a) $r^2 = 2/3$, (b) $r^2 = ½$, and (c) $r^2 = 1/3$.

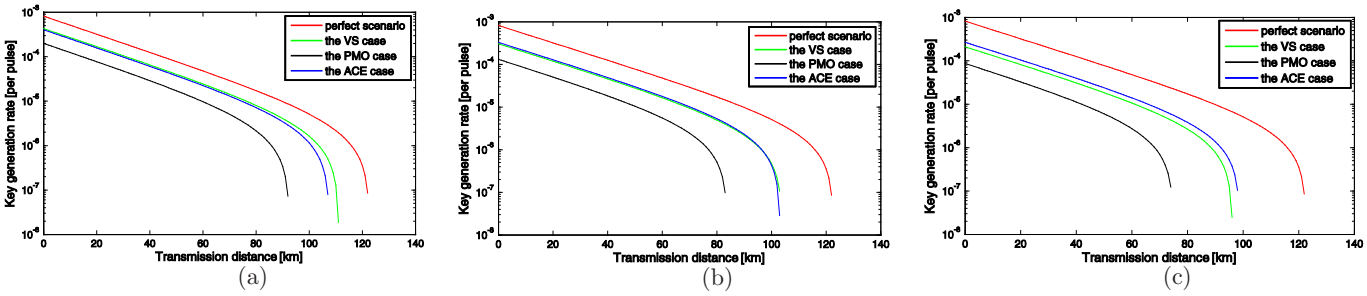

Fig. 5. Simulation results of the vacuum, decoy, and signal states (a) $r^2 = 1/4$, (b) $r^2 = 1/6$, and (c) $r^2 = 1/9$.

$$Q_k = Y_0 + 1 - e^{-\eta k},$$

$$E_k = \frac{\frac{1}{2}Y_0 + e_{\mathrm{Det}}(1 - e^{-\eta k})}{Q_k},$$

$$Y_1 \geq Y_1^{L,v_1,v_2} = \frac{\mu}{\mu v_1 - \mu v_2 - v_1^2 + v_2^2}\left(Q_{v_1}e^{v_1} - Q_{v_2}e^{v_2} - \frac{v_1^2 - v_2^2}{\mu^2}(Q_\mu e^\mu - Y_0^L)\right),$$

$$Y_0^L = \max\left\{\frac{v_1 Q_{v_2} e^{v_2} - v_1 Q_{v_2} e^{v_2}}{v_1 - v_2}, 0\right\},$$

$$e_1 \leq \frac{E_{v_1}Q_{v_1}e^{v_1} - E_{v_2}Q_{v_2}e^{v_2}}{(v_1 - v_2)Y_1^{L,v_1,v_2}}, \tag{13}$$

where the variables are the same as in Eq. (12).

The mean photon numbers of the three states that we use are 0, 0.2, and 0.6 and the other parameters are the same as those of the infinite decoy states. We can get the final key generation rate of the system with the decoy state using

$$R \geq \frac{1}{2}(Y_1 P_1(1 - h(e_1)) - Q_k h(E_k)). \tag{14}$$

The simulation result is as we expected, where the VS case and the PMO case are better than the case in which the unbalanced loss is controlled by Eve and worse than the perfect scenario. In addition, this situation is the same as the infinite decoy states situation. When the insertion loss of the PM is $\sqrt{1/4}$ (Fig. 5(a)), the VS case has better performance, and as the insertion loss increases, the crossing point occurs at approximately $\sqrt{1/6}$ (Fig. 5(b)). Figure 6 shows the relation between the transmission length and the insertion loss when the VS and the PMO cases have the same secure key rate, so that when the insertion loss is $\sqrt{1/9}$ (Fig. 5(c)) the PMO case has a higher key generation rate, and higher insertion losses lead to greater advantages for the PMO case.

In conclusion, we propose a new type of FM-QKD system with the PM located outside the interference ring. We compare the transmission distance and the

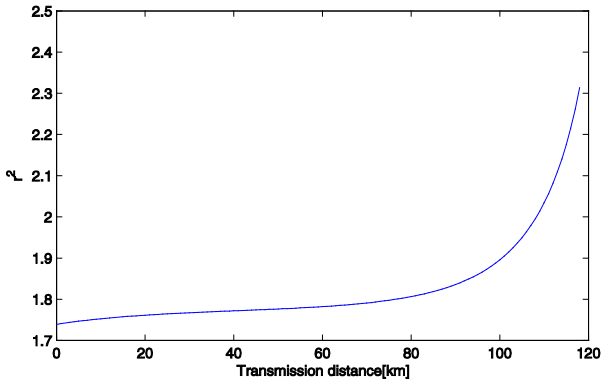

Fig. 6. Relation between the transmission length and insertion loss when VS and PMO cases have te same secure key rate.

key generation rate with those of other experimental setups. The comparison results show that in the practical QKD, higher insertion losses in the PM lead to better performance levels with our method. However, when the PM is outside the interference ring, we will require accurate electronics technology to distinguish between the two pulses outside the ring and apply different phase modulation voltages to the PM.

This work was supported by the National Natural Science Foundation of China (Nos. 61101137, 61201239, 61205118, and 11304397) and the China Postdoctoral Science Foundation (No. 2013M540514).

References

1. C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* 175 (1984).
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. Q. C. Sun, W. L. Wang, Y. Liu, F. Zhou, J. S. Pelc, M. M. Fejer, C. Z. Peng, X. F. Chen, X. Ma, Q. Zhang, and J. W. Pan, Laser Phys. Lett. **11,** 085202 (2014).
5. F. Xu, H. Xu, and H. K. Lo, Phys. Rev. A **89,** 052333 (2014).
6. Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, New J. Phys. **11,** 045019 (2009).
7. M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, Opt. Express **104,** 051123 (2014).
8. S. Wang, W. Chen, J. F. Guo, Z. Q. Yin, H. W. Li, Z. Zhou, G. C. Guo, and Z. F. Han, Opt. Lett. **37,** 1008 (2012).
9. Z. Zhao, Y. Luo, Z. Zhao, and H. Long, Chin. Opt. Lett. **9,** 032702 (2011).
10. F. Tang and B. Zhu, Chin. Opt. Lett. **11,** 090101 (2013).
11. Z. F. Han, X. F. Mo, Y. Z. Gui, and G. C. Guo, Appl. Phys. Lett. **86,** 221103 (2005).
12. X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui, and G. C. Guo, Opt. Lett. **30,** 2632 (2005).
13. D. Gottesman, H. K. Lo, N. Lukenhaus, and J. Preskill, Quant. Inf. Comput. **4,** 325 (2004).
14. H. K. Lo and J. Preskill, "Phase randomization improves the security of quantum key distribution," Quant-ph. 0504209 (2005).
15. H. W. Li, Z. Q. Yin, Z. F. Han, W. S. Bao, and G. C. Guo, Quant. Inf. Comput. **10,** 771 (2010).
16. X. Ma, B. Qi, Y. Zhao, and H. K. Lo, Phys. Rev. A **72,** 012326 (2005).
17. C. Gobby, Z. L. Yuan, and J. Shields, Appl. Phys. Lett. **84,** 3762 (2004).
18. H. K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94,** 230504 (2005).
19. X. B. Wang, Phys. Rev. Lett. **94,** 230503 (2005).
20. Z. Q. Yin, Y. B. Zhao, Z. W. Zhou, Z. F. Han, and G. C. Guo, Phys. Rev. A **77,** 062326 (2008).
21. Z. Q. Yin, Z. F. Han, F. W. Sun, and G. C. Guo, Phys. Rev. A **76,** 014304 (2007).