Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources

Hong-Wei Li,[1,2] Shuang Wang,[1,*] Jing-Zheng Huang,[1] Wei Chen,[1,†] Zhen-Qiang Yin,[1,‡] Fang-Yi Li,[1] Zheng Zhou,[1] Dong Liu,[1] Yang Zhang,[1] Guang-Can Guo,[1] Wan-Su Bao,[2] and Zheng-Fu Han[1,§]

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

[2]*Zhengzhou Information Science and Technology Institute, Zhengzhou, 450004, China*

(Received 11 August 2011; published 14 December 2011)

It is well known that the unconditional security of quantum-key distribution (QKD) can be guaranteed by quantum mechanics. However, practical QKD systems have some imperfections, which can be controlled by the eavesdropper to attack the secret key. With current experimental technology, a realistic beam splitter, made by fused biconical technology, has a wavelength-dependent property. Based on this fatal security loophole, we propose a wavelength-dependent attacking protocol, which can be applied to all practical QKD systems with passive state modulation. Moreover, we experimentally attack a practical polarization encoding QKD system to obtain all the secret key information at the cost of only increasing the quantum bit error rate from 1.3 to 1.4%.

DOI: 10.1103/PhysRevA.84.062308 PACS number(s): 03.67.Dd, 03.67.Ac, 03.67.Hk

I. INTRODUCTION

Quantum-key distribution (QKD) is the art of sharing secret keys between two distant parties Alice and Bob. Since the proposal of the Bennett and Brassard 1984 QKD scheme (BB84) protocol [1], the unconditional security of the QKD protocol has attracted much attention. Lo and Chau [2] proved the unconditional security of the BB84 protocol with a quantum computer. Shor and Preskill [3] proved the unconditional security of the BB84 protocol by applying entanglement distillation and purification (EDP) technology. More recently, Renner [4] proved the unconditional security of the BB84 protocol by applying the quantum information theory method.

Whereas a security analysis model based on a perfect QKD protocol cannot be directly applied to practical QKD systems [5–7], Gottesman, Lo, Lükenhaus, and Preskill (GLLP) [8] analyzed the security of a practical QKD system and obtained the famous secret key rate formula GLLP. Combining their security analysis result with a decoy state method [9–11], a practical QKD system can be realized with a weak coherent source. But their security analysis cannot be applied to a practical QKD system with arbitrary imperfections [12,13], which may introduce side channel attacks. An imperfect phase modulator introducing a phase-remapping attack has been experimentally demonstrated [14]. An imperfect single-photon detector (SPD) introducing a detector blinding attack has also been proposed in Ref. [15], where it was demonstrated that an imperfect SPD can be fully remote controlled by utilizing especially tailored bright illumination. More recently, a dead time attack with an imperfect SPD has been proposed in Ref. [16], in which the eavesdropper can exploit the dead time effect of the imperfect SPD to gain almost all of the secret information without being discovered. Jain *et al.* [17] have proved that an inappropriately implemented calibration routine will introduce a fatal security loophole. All these results demonstrate that practical QKD device imperfections can lead to various types of attacks [18–23]. In current experimental realizations, the beam splitter (BS) has a wavelength-dependent property. Based on this imperfection, we propose a different type of attacking protocol. Our experimental demonstration shows that this strategy can effectively attack a practical passive modulated polarization-based QKD system without being discovered, where passive (active) modulation implies that Bob passively (actively) selects measurement bases. It should be noted that the attacking model also can be easily generalized to other passive modulated QKD systems.

Practical QKD systems can be divided into two parts, phase encoded and polarization encoded. In polarization-based QKD systems [24,25], Bob passively selects the measurement basis by the BS for convenient and high-speed modulation. More precisely, the 1×2 BS has one input port and two output ports (port 1 and port 2), and Bob can choose to measure the photon state either on a rectilinear basis if it passes through output port 1, or on a diagonal basis if it passes through output port 2. In the perfect case, the single-photon state will randomly select to pass through one output port of the BS. But the realistic BS is commonly made by fused biconical taper (FBT) technology [26], and the coupling ratio of the FBT BS is generally wavelength dependent. We made a BS with FBT technology in our experimental realization, and found that the coupling ratio is 0.5 in the 1550-nm wavelength, while the 1470- and 1290-nm sources have coupling ratios of 0.986 and 0.003, respectively. Interestingly, we can apply the 1470-nm (1290-nm) source to control the selection of the rectilinear basis (diagonal basis) on Bob's side. Using this loophole, we present that Eve can control Bob's measurement basis choice remotely at the cost of only increasing the quantum bit error rate (QBER) from 1.3 to 1.4%.

II. REALISTIC BEAM SPLITTER

The FBT BS is made by closing two or more bare optical fibers, fusing them in a high-temperature environment, and

*wshuang@ustc.edu.cn
†kooky@mail.ustc.edu.cn
‡yinzheqi@mail.ustc.edu.cn
§zfhan@ustc.edu.cn

drawing their two ends at the same time—then a specific biconic tapered waveguide structure can be formed in the heating area. The FBT BS can be used as the splitter or the coupler: It has the features of low insertion loss, good directivity, and low cost, so many of the commercial BS products are made by this technology. However, the coupling ratio of the FBT BS is wavelength dependent, and most types of FBT BSs work only in a limited wavelength range (limited bandwidth), where the coupling ratio of the BS is defined as $r = \frac{I_{\text{port1}}}{I_{\text{port1}}+I_{\text{port2}}}$, where I_{port1} (I_{port2}) is the output light intensity from BS's output port 1 (output port 2). A typical coupling ratio at the center wavelength provides optimal performance, but the coupling ratio varies periodically with wavelength changes. We manufactured a BS with FBT technology in our experimental realization, and found that it has a distinguishing wavelength-dependent characteristic; a detailed expression of this property is shown in Fig. 1.

We analyze the relationship between wavelength λ and coupling ratio r by using the coupling model given in Refs. [28,29]:

$$r = F^2 \sin^2\left(\frac{Cw}{F}\right), \tag{1}$$

where F^2 is the maximal power that is coupled, $C \propto \lambda^{2.5}$ is the coupling coefficient, and w is the heat source width. From Fig. 1, we find that the realistic BS has a perfect coupling ratio 0.5 with a 1550-nm laser diode (LD), in which case the BS can be regarded as a perfect QKD device. When we test it with 1290- and 1470-nm LDs, the coupling ratio changed to 0.003 and 0.986, respectively, which means that the 1290- and 1470-nm LDs will mainly pass through the BS's ports 2 and 1, respectively. Thus the realistic BS cannot be regarded as a perfect QKD device in the case where the wavelength of the LD is not 1550 nm. Combining this imperfection with multiwavelength sources, we show that Eve can acquire all the secret key information on Bob's side at very low cost [30].

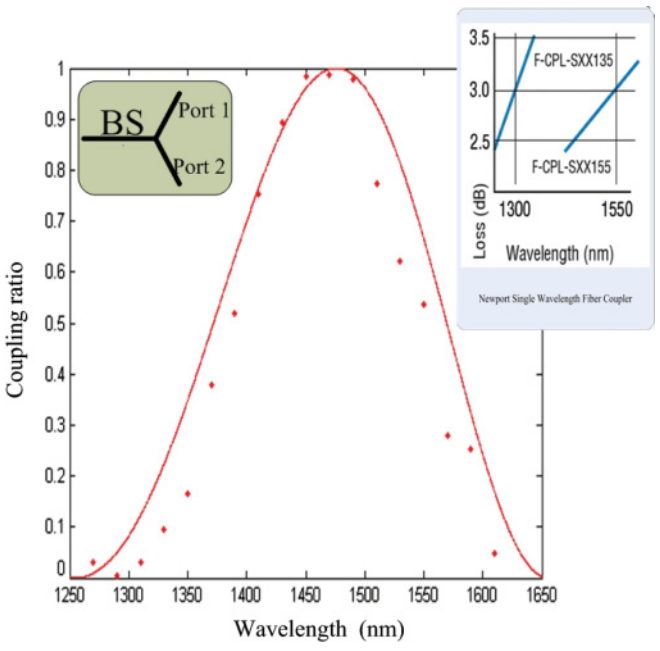

FIG. 1. (Color online) The relationship between the wavelength of the source and the coupling ratio. Here the red dot is the practical experimental result, and the red (gray) curve is the theoretical analysis result. The right-hand side (inset) is the single wavelength fiber coupler made by the Newport Corporation [27], the coupling ratio of which is also wavelength dependent.

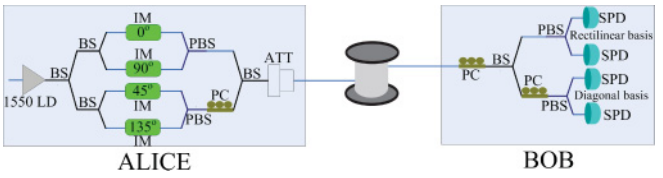

FIG. 2. (Color online) Schematic diagram of the polarization-based QKD system, where 1550 LD means Alice sends the quantum state with the 1550-nm source, BS is the beam splitter, PBS is the polarization beam splitter, IM is the intensity modulator, PC is the polarization controller, ATT is the attenuator, and SPD is the single-photon detector.

III. MODEL DESCRIPTION AND EXPERIMENTAL SETUP

The polarization-based QKD system with passive state modulation is depicted precisely in Fig. 2. After two cascaded BSs with an additional intensity modulation, four polarization states can be generated by a 1550-nm LD. More precisely, when Alice wants to transmit the prepared quantum state, the positive voltage will be added onto the matched intensity modulator (IM), and the negative voltage will be added onto the other IM, respectively. Thus only the single-photon state modulated by the positive voltage can be transmitted into the quantum channel. In the ideal polarization-based QKD experimental realization, one of the basic assumptions is that the photon state will pass through each output side with 50% probability. Actually, this perfect BS on Bob's side can be regarded as the random basis selector. Unfortunately, the coupling ratio of the realistic FBT BS is wavelength dependent, as illustrated above. Eve can adopt an intercept-and-resend strategy to attack practical polarization-based QKD systems, where Eve's detection setup in the quantum channel is the same as Bob's side. Applying her state measurement result, Eve will send the remodulated photon state to Bob. In this attacking protocol, the main difficulty for Eve is to find the appropriate LD with wavelengths λ_1 and λ_2, where λ_1 LD has a coupling ratio of $r_1 > 0.5$, and λ_2 LD has a coupling ratio of $r_2 < 0.5$. To attack the practical QKD system, Eve will send the remodulated quantum state with λ_1 (λ_2) LD to Bob, if she can get the detection result with a rectilinear basis $\{0°,90°\}$ (diagonal basis $\{45°,135°\}$).

We initially give a theoretical security analysis under the assumption that only the BS in the QKD system is imperfect. By considering that an intercept-and-resend strategy has been applied by Eve in the quantum channel, the final QBER (it is defined as Err) between Alice and Bob can be given by

$$\text{Err} = \frac{1}{4}\left(\frac{1-r_1}{2-(r_1+r_2)} + \frac{r_2}{r_1+r_2}\right); \tag{2}$$

this equation can be simply calculated with the probability tree of the state transformation as illustrated in Fig. 3. Utilizing Shor and Preskill's security analysis result with the perfect

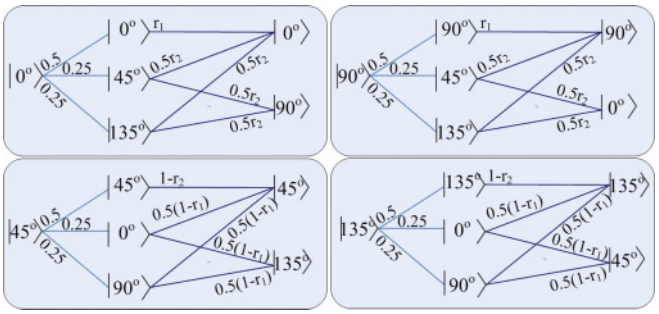

FIG. 3. (Color online) Probability tree of the state transformation. Alice sends the modulated quantum state to the quantum channel, Eve gets the state detection result with probability $p_1 \in \{0.25,0.25,0.5\}$ in the middle stage, and Bob saves his state detection result after the sifting protocol with probability $p_2 \in \{\frac{1}{2}r_1 + \frac{1}{4}r_2, \frac{1}{4}r_2\}$ or $\{\frac{1}{2}(1-r_2) + \frac{1}{4}(1-r_1), \frac{1}{4}(1-r_1)\}$ with different measurement bases.

QKD [3], Alice and Bob can distill the final secret key if the QBER introduced by the eavesdropper is lower than 11%. In the case where the coupling ratio and the wavelength have a strong correlation ($r_1 \to 1, r_2 \to 0$), Eve can get the full secret key bit even if the error rate is lower [31]. We note that no secret key can be established if the error rate is lower than Err between two legitimate parties. More interestingly, even zero QBER cannot generate any secret key with a full wavelength-dependent BS ($r_1 = 1, r_2 = 0$).

By using the analyzed realistic BS discussed above, a detailed setup of the attacking system is illustrated in Fig. 4. In this system, if Eve obtains a measurement result of 0 (1) with the rectilinear basis $\{0°,90°\}$, she will prepare the quantum state $|0°\rangle$ ($|90°\rangle$) again with the 1470-nm LD. Conversely, if she can obtain a detection result of 0 (1) with the diagonal basis $\{45°,135°\}$, she will prepare the quantum state $|45°\rangle$ ($|135°\rangle$) again with the 1290-nm laser diode, where $|45°\rangle = \frac{1}{\sqrt{2}}(|0°\rangle + |90°\rangle), |135°\rangle = -\frac{1}{\sqrt{2}}(|0°\rangle - |90°\rangle)$. We give a simple example: If Alice sends the quantum state $|0°\rangle$, and Eve obtains a detection result of $|0°\rangle$ in the rectilinear basis $\{0°,90°\}$ with a probability of 50%, then she will send the remodulated 1470-nm laser to the receiver Bob, since the 1470-nm laser can mainly pass through port 1 of the BS on Bob's side, and Bob can detect $|0°\rangle$ in the rectilinear basis with a 98.6% success probability. If Eve obtains the detection result in the diagonal basis $\{45°,135°\}$ with a probability of

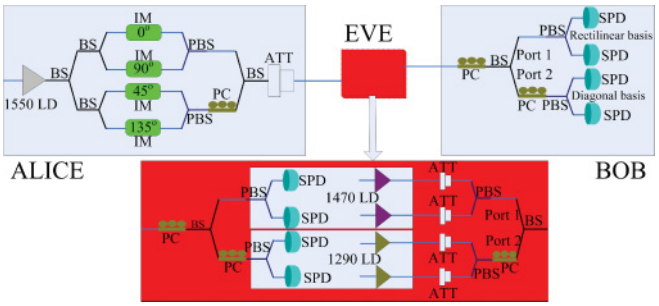

FIG. 4. (Color online) Attacking practical polarization-based QKD system. The red (dark gray) area is controlled by the eavesdropper Eve, who will utilize the intercept-and-resend strategy by applying the wavelength-dependent BS and multiwavelength sources.

50%, then she will send the remodulated 1290-nm laser to the receiver Bob, since the 1290-nm laser can mainly pass through port 2 of the BS on Bob's side, and Bob can obtain the detection result in the diagonal basis with a 99.7% success probability. Note that the detection efficiency of the practical SPD is also wavelength dependent, and we verified that the id 200 (The SPD produced by the Idquantique company) SPD [32] has detection efficiencies of 12.1%, 10.7%, and 5.0% by considering that the wavelengths of the source are 1550, 1470, and 1290 nm, respectively. To solve this problem, we will add different attenuations after the 1470- and 1290-nm LDs, and thus Bob can obtain a similar detection result with and without the eavesdropper.

Following the attacking model given above, we give the photon count result on Bob's side by considering two cases: without and with the eavesdropper. In the first case, Alice randomly sends the polarization state $\{|0°\rangle, |90°\rangle, |45°\rangle, |135°\rangle\}$ to the quantum channel. Considering that the practical single photon detection efficiency is 12.1% in the 1550-nm case, we can obtain an ∼1% effective detection result when the quantum channel has 10.79-dB attenuation. In our practical experimental realization without the eavesdropper, Alice sends 10^6 prepared quantum states, and then Bob obtains $\sim 10^4$ detection results, which are illustrated precisely in Fig. 5.

With the eavesdropper, Eve will apply a similar detection setup, but the channel attenuation between Alice and Eve is 0 dB—the reason for this is that Eve can utilize the lossless channel instead of the standard optical fiber. We give the detection result on Bob's side by considering that Eve sends 5×10^3 modulated quantum states (each pulse has two photons on average) to the quantum channel, where the channel loss between Eve and Bob is 3.3 and 0 dB in the 1470- and 1290-nm cases, respectively, and then Bob can obtain $\sim 5 \times 10^3$ effective detection results; detailed detection results are illustrated in

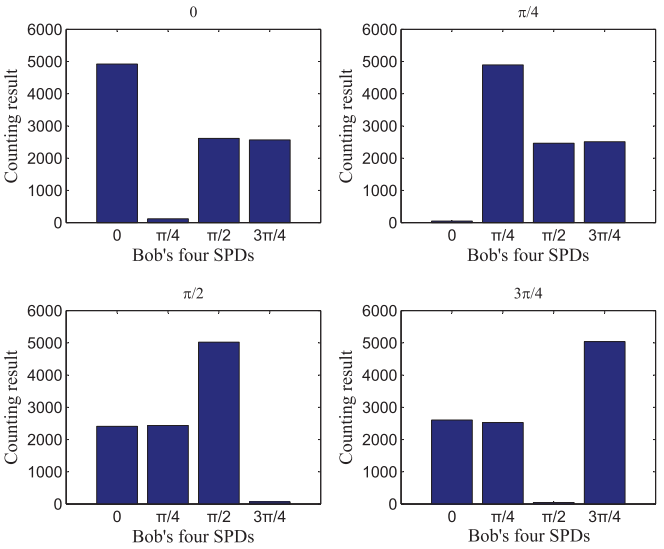

FIG. 5. (Color online) The detection result on Bob's side without the eavesdropper Eve. Alice sends four quantum states $\{|0°\rangle, |90°\rangle, |45°\rangle, |135°\rangle\}$ to the quantum channel with a 1550-nm LD, On Bob's side, he can obtain the correct detection result if the matched basis has been chosen. He will obtain the detection result with a 50% error rate if the unmatched basis has been chosen correspondingly.

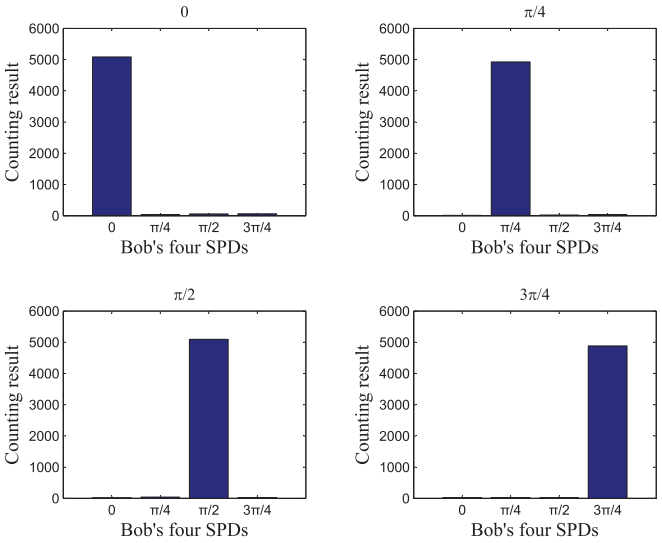

FIG. 6. (Color online) The detection result on Bob's side with the eavesdropper. Eve sends quantum states $\{|0^\circ\rangle,|90^\circ\rangle\}$ with a 1470-nm LD, and sends quantum states $\{|45^\circ\rangle,|135^\circ\rangle\}$ with a 1290-nm LD to the quantum channel. On Bob's side, he can only obtain a detection result in the rectilinear basis when the 1470-nm laser has been detected. Similarly, he can only obtain the detection result in the diagonal basis when the 1290-nm laser has been detected.

Fig. 6. Comparing different types of detection results, we find that Eve can remotely control Bob's basis selection only by changing the LD's wavelengths.

Based on this strategy, a polarization-based QKD system has been attacked in our practical experimental realization. Bob obtains a similar detection result with and without the eavesdropper. Similarly, the QBER between Alice and Bob only increases from 1.3 to 1.4%, and thus Eve can obtain almost all of the secret key information without being discovered.

IV. CONCLUSION

In conclusion, we propose a different type of strategy to attack the practical polarization-based QKD system by using a wavelength-dependent BS and multiwavelength sources. The eavesdropper Eve can control Bob's measurement basis with 100% success probability without reducing the receiver's expected detection rate or significantly increasing the bit error rate. Our results demonstrate that all practical devices require security inspection to avoid side channel attacks in practical QKD experimental realizations. We note that this attacking protocol cannot be avoided even if the wavelength filter was applied on Bob's side, since Eve only needs to increase the intensity of the light to attack Bob's detection setup. Meanwhile, we should also note that this attacking protocol can be avoided effectively by applying actively modulated phase encoding QKD systems [33–35].

ACKNOWLEDGMENTS

H.-W.L. thanks X.-B. Z for helpful discussions. We thank N. Jain for helpful comments and for bringing Ref. [17] to our attention. We also thank the anonymous referees for their efforts in reviewing this article, and providing much useful feedback that helped to improve the presentation of this study. This work was supported by the National Basic Research Program of China (Grants No. 2011CBA00200 and No. 2011CB921200), National Natural Science Foundation of China (Grant No. 60921091), National High Technology Research and Development Program of China (863 program) (Grant No. 2009AA01A349), and China Postdoctoral Science Foundation (Grant No. 20100480695).

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[2] Hoi-Kwong Lo and H. F. Chau, Science **283**(5410), 2050 (1999).
[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[4] R. Renner, e-print arXiv:quant-ph/0512258.
[5] S. Wang *et al.*, Opt. Lett. **35**, 2454 (2010).
[6] H. Takesue, E. Diamanti, C. Langrock, M. M. Fejer, and Y. Yamamoto, Opt. Express **14**, 9522 (2006).
[7] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).
[8] D. Gottesman, H.-K. Lo, N. Lükenhaus, and J. Preskill, Quant. Inf. Comput. **4**, 325 (2004).
[9] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[10] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[11] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[12] H-W. Li, Z-Q. Yin, Z-F. Han, W-S. Bao, and G-C. Guo, Quant. Inf. Comput. **10**, 771 (2010).
[13] H-W. Li, Z-Q. Yin, S. Wang, W-S. Bao, G-C. Guo, and Z-F. Han, Quant. Inf. Comput. **11**, 937 (2011).
[14] F. Xu, B. Qi and H. -K. Lo, New J. Phys. **12**, 113026 (2010).
[15] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[16] H. Weier, H. Krauss, M. Rau, M. Fuerst, S. Nauerth, and H. Weinfurter, New J. Phys. **13**, 073024 (2011).
[17] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. **107**, 110501 (2011).
[18] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73C82 (2007).
[19] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
[20] Y. Zhao, Chi-Hang Fred Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[21] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, J. Mod. Opt. **51**, 1267 (2004).

[22] V. Makarov and D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005).
[23] V. Scarani and C. Kurtsiefer, e-print arXiv:0906.4547.
[24] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan, Opt. Express **18**, 113 (2010).
[25] K. J. Gordon, V. Fernandez, P. D. Townsend, and G. S. Buller, IEEE J. Quantum Electron. **40**, 900 (2004).
[26] M. Eisenmann and E. Weidel, J. Lightwave Technol. **6**, 8588 (2010).
[27] [http://www.newport.com/].
[28] A. Ankiewicz, A. W. Snyder, and X. Zheng, J. Lightwave Technol. **4**, 1317 (1986).
[29] V. J. Tekippe, Fiber Integr. Opt. **9**, 97 (1990).
[30] In principle, the eavesdropper Eve is assumed to have unlimited computing and storage power when providing unconditional security to the ideal QKD protocol. Our attacking model shows that Eve only requires two practical different wavelength sources, which implies that the strategy lowers the cost but works more efficiently.
[31] Considering a strong correlation, the QBER between Alice and Bob is Err $\rightarrow$ 0. Bob obtains the rectilinear basis detection result with a probability $\frac{1}{2}(r_1 + r_2) \rightarrow \frac{1}{2}$, and then obtains the diagonal basis detection result with a probability $1 - \frac{1}{2}(r_1 + r_2) \rightarrow \frac{1}{2}$. Thus Eve's operation is detected without increasing unbalanced detection and QBER.
[32] [http://www.idquantique.com/].
[33] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).
[34] Z. F. Han, X. F. Mo, Y. Z. Gui, and G. C. Guo, Appl. Phys. Lett. **86**, 221103 (2005).
[35] X. F. Mo, B. Zhu, Z. F. Han, Y. Z. Gui, and G. C. Guo, Opt. Lett. **30**, 2632 (2005).