ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理 Chinese Physics B

Attacking a high-dimensional quantum key distribution system with wavelength-dependent beam splitter

Ge-Hai Du(杜舸海), Hong-Wei Li(李宏伟), Yang Wang(汪洋), Wan-Su Bao(鲍皖苏)

Citation: Chin. Phys. B . 2019, 28(9): 090301 . **doi:** 10.1088/1674-1056/28/9/090301
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Temperature effects on atmospheric continuous-variable quantum key distribution

Shu-Jing Zhang(张淑静), Hong-Xin Ma(马鸿鑫), Xiang Wang(汪翔), Chun Zhou(周淳), Wan-Su Bao(鲍皖苏), Hai-Long Zhang(张海龙)

Chin. Phys. B . 2019, 28(8): 080304 . **doi:** 10.1088/1674-1056/28/8/080304

Research on co-propagation of QKD and classical communication by reducing the classical optical power

Ru-Shi He(何如适), Mu-Sheng Jiang(江木生), Yang Wang(汪洋), Ya-Hui Gan(甘亚辉), Chun Zhou(周淳), Wan-Su Bao(鲍皖苏)

Chin. Phys. B . 2019, 28(4): 040303 . **doi:** 10.1088/1674-1056/28/4/040303

Demonstration of a cold atom beam splitter on atom chip

Xiaojun Jiang(蒋小军), Xiaolin Li(李晓林), Haichao Zhang(张海潮), Yuzhu Wang(王育竹)

Chin. Phys. B . 2016, 25(8): 080311 . **doi:** 10.1088/1674-1056/25/8/080311

A new bipartite entangled state describing the parametric down-conversion process and its applications in quantum optics

Meng Xiang-Guo, Wang Ji-Suo, Zhang Xiao-Yan

Chin. Phys. B . 2012, 21(10): 100305 . **doi:** 10.1088/1674-1056/21/10/100305

Four-mode coherent-entangled state and its application

Li Hong-Qi, Ren Ting-Qi, Zhang Yun-Hai, Xu Xing-Lei

Chin. Phys. B . 2012, 21(1): 010305 . **doi:** 10.1088/1674-1056/21/1/010305

Attacking a high-dimensional quantum key distribution system with wavelength-dependent beam splitter*

Ge-Hai Du(杜舸海)[1,2], Hong-Wei Li(李宏伟)[1,2,†], Yang Wang(汪洋)[1,2], and Wan-Su Bao(鲍皖苏)[1,2,‡]

[1] *Henan Key Laboratory of Quantum Information and Cryptography, PLA SSF IEU, Zhengzhou* 450001, *China*

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

(Received 16 May 2019; revised manuscript received 18 June 2019; published online 23 August 2019)

The unconditional security of quantum key distribution (QKD) can be guaranteed by the nature of quantum physics. Compared with the traditional two-dimensional BB84 QKD protocol, high-dimensional quantum key distribution (HD-QKD) can be applied to generate much more secret key. Nonetheless, practical imperfections in realistic systems can be exploited by the third party to eavesdrop the secret key. The practical beam splitter has a correlation with wavelength, where different wavelengths have different coupling ratios. Using this property, we propose a wavelength-dependent attack towards time-bin high-dimensional QKD system. What is more, we demonstrate that this attacking protocol can be applied to arbitrary d-dimensional QKD system, and higher-dimensional QKD system is more vulnerable to this attacking strategy.

Keywords: high-dimensional quantum key distribution, beam splitter, wavelength attack

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/ab343c

1. Introduction

Quantum key distribution (QKD)[1,2] is a novel routine of sharing secret key between two distant parties (called Alice and Bob) in the presence of an eavesdropper Eve. The unconditional security of QKD protocol is guaranteed by the nature of quantum physics, which has been proved via different methods.[3–5] Some experimental demonstrations are also carried out and advances are achieved.[6–9] However, practical devices may be imperfect by comparing with the ideal protocol. For example, an imperfect phase modulator may be remote controlled by an eavesdropper Eve and introduce a phase remapping attack.[10,11] For practical single photon detectors (SPDs), detection efficiency mismatch between several SPDs would introduce time-shift attack[12] or faked state attack.[13–15] One single SPD may also be blinded by bright illumination and controlled by Eve.[16–20] Recently, the avalanche-transition region of SPD has also been utilized to hack the QKD system.[21] But not only that, the imperfections in real devices may open security loopholes and be utilized by Eve to get secret key information.

High-dimensional quantum key distribution (HD-QKD),[22–26] which is an expansion to common qubit-based QKD, is capable of encoding multiple bits on one single photon and has many advantages such as high photon information efficiency (PIE) and strong tolerance to channel noise. So HD-QKD has attracted much attention since its proposal. Ali-Khan *et al.*[27] put forward the first HD-QKD protocol based on time–energy entanglement but did not prove its security. Afterwards, Mower *et al.*[28] proved the security of time–energy entanglement-based HD-QKD against collective attack using dispersive optics. Zhang *et al.*[29] applied decoy-state method[30–32] to HD-QKD to defeat photon-number-splitting (PNS) attack[33,34] and proved its security against collective attacks. The security of decoy-state HD-QKD against collective attacks[35] and coherent attacks[36] in the finite-key scenario has also been established. However, the practical HD-QKD system may have imperfect devices, which can be utilized by the eavesdropper to get the final secret key.

In Ref. [37], the fiber beam splitter (BS) was discovered to possess a wavelength-dependent property. Making use of this property, Eve has the ability to control the outputs of the fiber beam splitter and then remotely control Bob's measurement basis choice. Utilizing this security loophole, a polarization-encoded BB84 QKD system was attacked successfully. Subsequently, Huang *et al.*[38,39] and Ma *et al.*[40] independently extended this so-called wavelength attack to practical continuous-variable QKD (CV-QKD) systems, regardless of whether Bob employs intensity monitoring. Afterwards, few investigations about wavelength attack have been constructed.

In this work, we apply wavelength attack towards HD-QKD system. We take four-dimensional time-bin HD-QKD system for example.[41] The eavesdropper Eve can control the measurement bases by just choosing two certain wavelengths, then she can apply the man-in-the-middle attack to get the final secret key. We calculate the final quantum bit error rate intro-

*Project supported by the National Key Research and Development Program of China (Grant No. 2016YFA0302600) and the National Natural Science Foundation of China (Grant No. 61675235).

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

‡Corresponding author. E-mail: bws@qiclab.cn

© 2019 Chinese Physical Society and IOP Publishing Ltd

duced by this attack and design a concrete implementation on a practical time-bin HD-QKD system. We also demonstrate that this attacking strategy is universally applicable towards any d-dimensional QKD system and higher-dimensional QKD system is more vulnerable to this attack.

The rest of this paper is organized as follows. In Section 2, we present a brief introduction on time-bin HD-QKD system and wavelength-dependent beam splitter. In Section 3, we demonstrate how to perform wavelength attack on time-bin HD-QKD system and calculate the quantum bit error rate caused by this attack. Some further discussion is put forward in Section 4 and conclusions are summarized in Section 5.

2. Preliminary

2.1. Time-bin HD-QKD system

Without loss of generality, we take four-dimensional time-bin HD-QKD system for example.[41] The schematic diagram of time-bin HD-QKD system is depicted in Fig. 1. Alice employs a 1550-nm source to create time-bin states and phase states in time series with probabilities of 0.90 and 0.10, respectively. Time-bin states are denoted as $|t_n\rangle$, where $n = 0, \ldots, d-1$. Phase states which are the discrete Fourier transforms of time-bin states are denoted as

$$|f_n\rangle = \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} \exp\left(\frac{2\pi i n m}{d}\right) |t_m\rangle, \quad n = 0, \ldots, d-1. \quad (1)$$

Both states are illustrated in Fig. 1(a). Here, time-bin states are used to generate secret key and phase states are used to monitor the presence of Eve. As shown in Fig. 1(b), after the propagation through a fiber quantum channel, a 90/10 beam splitter directs 90% of the incident quantum states to the temporal basis measurement device and 10% to the phase basis measurement device. The time-bin states are measured using single-photon counting detectors and translated into time-of-arrival data. States $|t_0\rangle$, $|t_1\rangle$, $|t_2\rangle$, and $|t_3\rangle$ correspond to 00, 01, 10, and 11 bit codes, respectively. For phase state measurement, after two cascaded time-delay interferometers,[41,42] emergence of the central time-bin from detector D_n corresponds to the incidence of the phase state $|f_n\rangle$. There will be a 1/4 probability of detection when a state is prepared and measured in different bases. After all states are transferred, Alice and Bob announce their basis choices and then perform classical data postprocessing. If the quantum bit error rate (QBER) is lower than the permitted value, a string of secret key can be distilled.

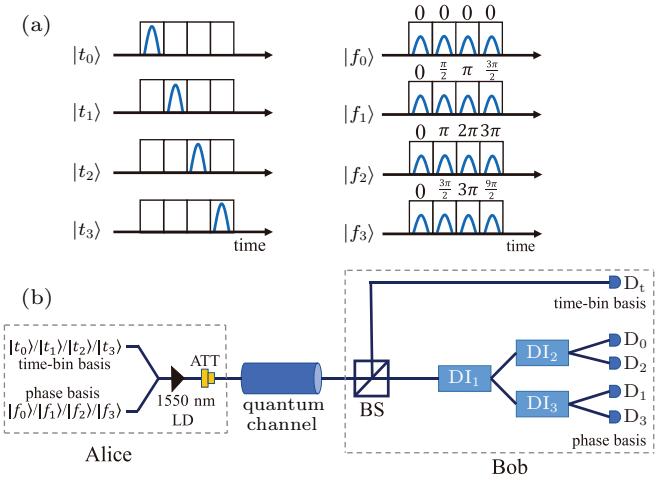


Fig. 1. Schematic daigram of four-dimensional time-bin HD-QKD system. (a) Representation of time-bin states (left) and phase states (right). (b) Experimental setup of time-bin HD-QKD system. 1550-nm LD means that Alice prepares signals with 1550-nm laser diode, ATT is the attenuator which is used to attenuate the light to single-photon level, BS is the beam splitter, DI_1, DI_2, and DI_3 are delay-line interferometers which are used to direct different phase states to the corresponding detectors, D_t and D_0, D_1, D_2, D_3 are single-photon detectors which are used to detect time-bin states and phase states, respectively. See more details in Ref. [41].

2.2. Wavelength-dependent beam splitter

For a general beam splitter (BS), it has one input port and two output ports. In the perfect situation, the incident single photon will pass through one output port randomly. This type of BS plays the role of a passive random basis selector in QKD systems. However, in a realistic setup, the fiber BS is manufactured by fused biconical taper (FBT) technology.[43] The coupling ratio (defined as $r = I_{\text{port1}}/(I_{\text{port1}} + I_{\text{port2}})$, $I_{\text{port1}}/I_{\text{port2}}$ is the intensity of the output light from output port 1/output port 2) of the BS has a strong correlation with wavelength. As a result, the BS only works in a limited range of wavelengths. Li *et al.*[37] made a common FBT BS and demonstrated that the coupling ratio is 0.5 for 1550-nm wavelength, while 0.986 and 0.003 for 1470-nm and 1290-nm wavelengths, respectively. Utilizing 1470-nm and 1290-nm laser sources, they successfully carried out wavelength attack towards a polarization-based BB84 QKD system.

3. Wavelength attack towards time-bin HD-QKD system

With regard to time-bin HD-QKD system mentioned above, the coupling ratio of BS is 0.90 for 1550 nm. In this protocol, the 90/10 beam splitter directs 90% of the incident photons out of output port 1 to temporal basis measurement device. The other 10% are directed out of output port 2 to phase-basis measurement device. To attack this system via wavelength attack, Eve's measurement setup is the same as Bob's. After measuring the state sent from Alice, Eve prepares a new state with a certain wavelength which has a different coupling ratio according to her measurement result. Af-

terwards, Eve sends this remodulated state to Bob. More precisely, Eve will send remodulated photon state with λ_1 (λ_2) source if her measurement result occurs at temporal (phase) basis measurement device side. That is to say there is a requirement that λ_1 and λ_2 photons pass through the BS from output port 1 and output port 2, respectively. Furthermore, the coupling ratios r_1 and r_2 which correspond to wavelengths λ_1 and λ_2 should satisfy $r_1 > 0.9$ and $r_2 < 0.9$. It is much more likely that λ_1 photon passes from output port 1 and λ_2 photon from output port 2 if r_1 and r_2 have large deviations from 0.9. Then this attack is more likely to be realized. In the practical setup, it is not difficult to find two wavelengths which satisfy $r_1 > 0.9$ and $r_2 < 0.9$ since FBT-fabricated beam splitter always has a wavelength-dependent property.[39]

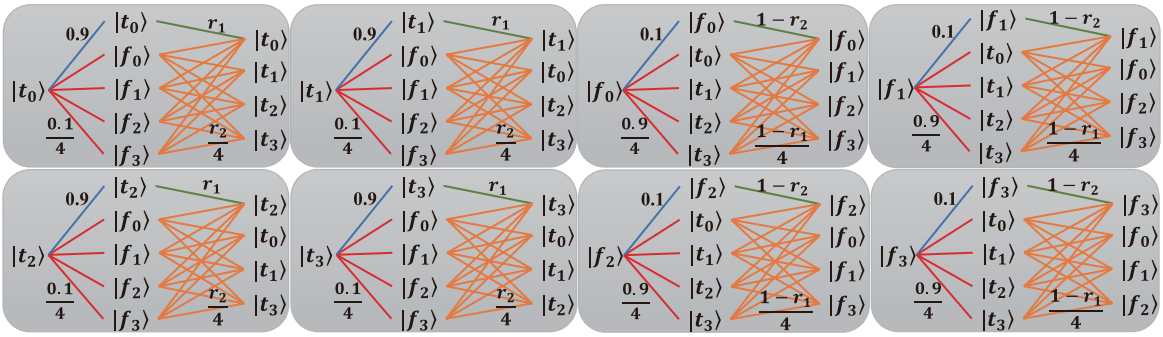


Fig. 2. Probability tree of the state transformation. Alice sends the prepared photon state to the quantum channel, Eve gets the detection result with probability $p_1 \in \{0.9, 0.1/4, 0.1/4, 0.1/4, 0.1/4\}$ or $\{0.1, 0.9/4, 0.9/4, 0.9/4, 0.9/4\}$ in the middle stage, then Bob preserves his detection result after the sifting protocol with probability $p_2 \in \{0.9r_1 + (0.1/4)r_2, (0.1/4)r_2, (0.1/4)r_2, (0.1/4)r_2, (0.1/4)r_2\}$ or $\{0.1(1-r_2) + (0.9/4)(1-r_1), (0.9/4)(1-r_1), (0.9/4)(1-r_1), (0.9/4)(1-r_1), (0.9/4)(1-r_1)\}$ with different measurement bases. Different colors represent different probabilities.

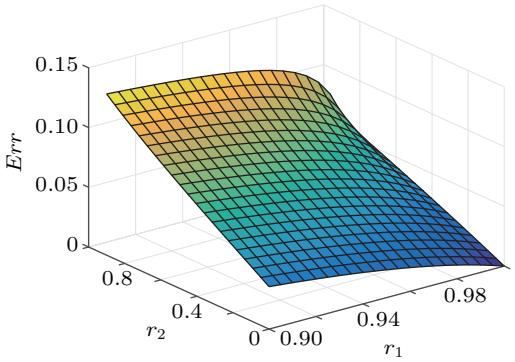


Fig. 3. The final QBER as a function of coupling ratios r_1 and r_2 where r_1 and r_2 are coupling ratios corresponding to wavelengths λ_1 and λ_2.

Considering that wavelength attack has been carried out by Eve to time-bin HD-QKD system with the assumption that only the beam splitter is imperfect, the final quantum bit error rate (QBER) is given by

$$Err = \frac{1}{10}\left[\frac{27r_2}{36r_1 + 4r_2} + \frac{27(1-r_1)}{36(1-r_1) + 4(1-r_2)}\right]; \quad (2)$$

this error rate value can be intuitively obtained by the probability tree of the state transformation as shown in Fig. 2. Using the analysis results in Ref. [44], Alice and Bob can obtain secret key if the QBER introduced by Eve is lower than 18.9%. As illustrated in Fig. 3, when r_1 is just a little more than 0.9 and r_2 is a little less than 0.9, the QBER reaches the maximal Err value 13.5%, lower than the maximal tolerable QBER value. Hence, Alice and Bob will not discover Eve's existence. In the asymptotic case where $r_1 \to 1$ and $r_2 \to 0$, the QBER is much lower and Eve can get much more secret key even the full secret key bit. We should notice that even zero QBER can distill no secret key in the extreme case where $r_1 = 1$ and $r_2 = 0$. What is more, since the tolerable QBER for four-dimensional time-bin QKD system is 18.9% (compared to 11% for BB84), the presence of Eve is more difficult to discover. This potential threat is detrimental to time-bin HD-QKD system.

Utilizing the analysis above, a detailed schematic diagram of this attacking model is illustrated in Fig. 4. If Eve gets a detection result of 00/01/10/11 with the temporal basis $\{|t_0\rangle, |t_1\rangle, |t_2\rangle, |t_3\rangle\}$, she will prepare the photon state $|t_0\rangle/|t_1\rangle/|t_2\rangle/|t_3\rangle$ again with the λ_1 source. Conversely, if she obtains an emergence from detector D_n, she will prepare the photon state $|f_n\rangle$ again with the λ_2 source, where

$$|f_0\rangle = \frac{1}{2}(|t_0\rangle + |t_1\rangle + |t_2\rangle + |t_3\rangle),$$
$$|f_1\rangle = \frac{1}{2}(|t_0\rangle + \mathrm{i}|t_1\rangle - |t_2\rangle - \mathrm{i}|t_3\rangle),$$
$$|f_2\rangle = \frac{1}{2}(|t_0\rangle - |t_1\rangle + |t_2\rangle - |t_3\rangle),$$
$$|f_3\rangle = \frac{1}{2}(|t_0\rangle - \mathrm{i}|t_1\rangle - |t_2\rangle + \mathrm{i}|t_3\rangle).$$

For instance, if Alice sends the quantum state $|t_0\rangle$, then Eve gets a detection result of $|t_0\rangle$ in the temporal basis $\{|t_0\rangle, |t_1\rangle, |t_2\rangle, |t_3\rangle\}$ with a probability of 90%, then she will prepare a remodulated quantum state $|t_0\rangle$ using a λ_1 source to the receiver Bob, since the λ_1 wavelength laser can mainly pass through output port 1 of the BS on Bob's side, and Bob can detect $|t_0\rangle$ in the temporal basis with a $(100r_1)\%$ success probability. Conversely, if Eve gets a detection result in the phase basis $\{|f_0\rangle, |f_1\rangle, |f_2\rangle, |f_3\rangle\}$ with a probability of 10%,

then she will prepare a remodulated quantum state using a λ_2 source to the receiver Bob, since the λ_2 wavelength laser can pass through output port 2 of the BS on Bob's side with a probability less than 90%, and Bob can get the detection result in the phase basis with a $[100(1-r_2)]\%$ success probability. It is worth noting that in the realistic setup, the detection efficiency of the single photon detector also has a correlation with wavelength, leading to different detection counts on Bob's side. Then, Bob will realize an eavesdropper's existence. To settle this problem, we can just add different attenuations after λ_1 and λ_2 sources, hence Bob can get a similar amount of detection results with and without the eavesdropper. Therefore, the wavelength attack is insusceptible to detection efficiency distinction.

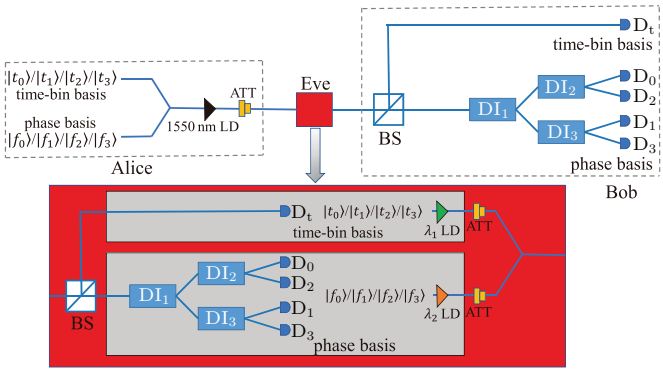


Fig. 4. Attacking time-bin HD-QKD system. The red area is controlled by the eavesdropper Eve.

4. Discussion

We consider wavelength attack towards arbitrary d-dimensional QKD system where the BS has an arbitrary coupling ratio r. In the d-dimensional QKD system, Alice prepares two sets of mutually unbiased bases $\{A|A_0,A_1,A_2,\ldots,A_{d-1}\}$ and $\{B|B_0,B_1,B_2,\ldots,B_{d-1}\}$ which satisfy

$$\begin{aligned}&\langle A_i|A_j\rangle^2=\delta_{ij},\\&\langle B_i|B_j\rangle^2=\delta_{ij},\\&\langle A_i|B_j\rangle^2=\frac{1}{d},\quad i,j=0,1,2,\ldots,d-1.\end{aligned}\tag{3}$$

A-basis states and B-basis states are prepared with probabilities of p and $1-p$ $(0<p<1)$, respectively. After the propagation through a quantum channel, a $r/(1-r)$ beam splitter $(0<r<1)$ directs $(100r)\%$ of the incident quantum states to A-basis measurement setup and $[100(1-r)]\%$ to B-basis measurement setup. When Eve carries out the wavelength attack by an intercept-and-resend strategy, her measurement setup is the same as Bob's. What she also needs are two certain wavelengths λ_1 and λ_2 for which the coupling ratios are r_1 and r_2, satisfying $r_1>r$ and $r_2<r$. Similar to the discussion in Section 2, we can calculate the final QBER by the probability tree of the state transformation as shown in Fig. 5. The final QBER is given by

$$\begin{aligned}Err=&\frac{d-1}{d}[p\frac{(1-r)r_2}{(1-r)r_2+rr_1}\\&+(1-p)\frac{r(1-r_1)}{r(1-r_1)+(1-r)(1-r_2)}].\end{aligned}\tag{4}$$

Substituting $d=2$, $p=0.50$, $r=50\%$ (classical BB84 protocol) or $d=4$, $p=0.90$, $r=90\%$ (four-dimensional time-bin HD-QKD system mentioned above) into Eq. (4), we can obtain QBER results which accord with those in Ref. [37] and Eq. (2).

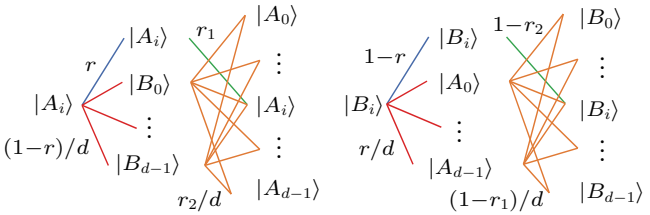


Fig. 5. Probability tree of the state transformation for arbitrary d-dimensional QKD system.

From Eq. (4), we can make out that wavelength attack is a universal attack strategy towards arbitrary d-dimensional QKD systems. As long as the final QBER is lower than the tolerable value, two legitimate parties will not be conscious of the presence of an eavesdropper, and Eve can acquire almost all of the secret key information. Eve can achieve this goal just in virtue of two certain wavelength sources.

Furthermore, we discuss the relationship between the dimension d and the coupling ratio r_i. Considering the general case of unbiased-basis-selection, the preparation probability and coupling ratio of Bob's BS both equal 0.5. Then, equation (4) turns into

$$Err=\frac{d-1}{2d}\left(\frac{r_2}{r_1+r_2}+\frac{1-r_1}{2-r_1-r_2}\right).\tag{5}$$

As illustrated in Fig. 6, for the sake of quantum bit error rate lower than the maximal tolerable value, there are requirements on both r_1 and r_2.

As a further discussion, we study the requirement for coupling ratios under different dimensions. For simplicity, we just suppose that we can find two wavelengths which satisfy $r_1+r_2=1$. In reality, it is not easy to find two wavelengths exactly satisfy this assumption. Besides, even though this assumption is not satisfied, wavelength attack can also be settled successfully. Here, we just make this simplified assumption for intuitional illustration. Similar results can be achieved even if without this assumption by further calculation. Then, equation (5) turns into

$$Err=\frac{d-1}{d}(1-r_1).\tag{6}$$

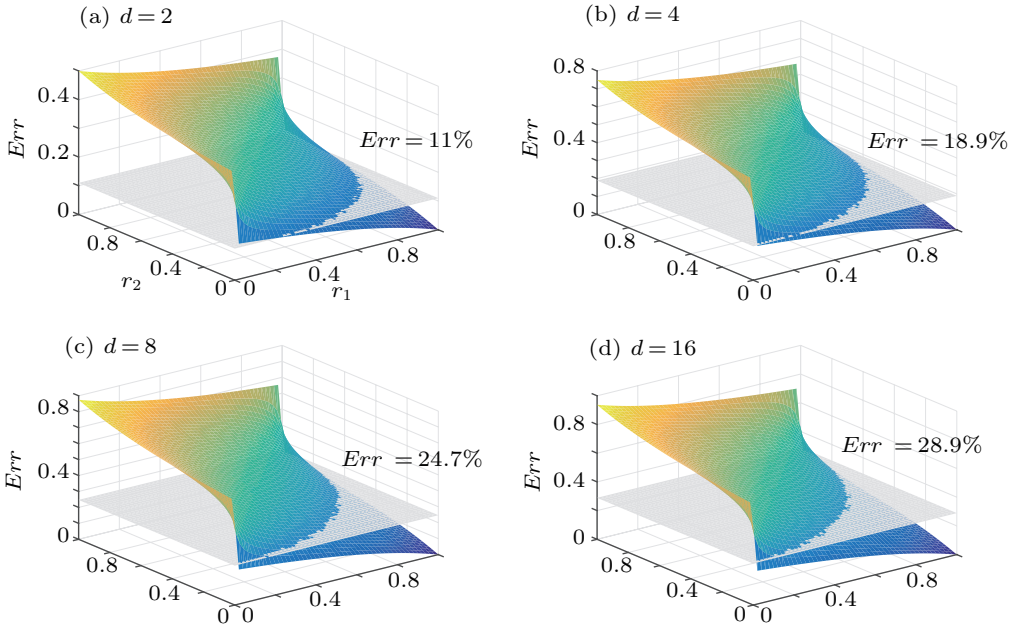


Fig. 6. Relationship between quantum bit error rate and coupling ratios. For dimensions $d=2$, 4, 8, 16 [panels (a)–(d)], only data points (r_1, r_2) satisfying Err value less than the maximal tolerable error rate (11%, 18.9%, 24.7%, 28.9%)[44] can guarantee successful wavelength attack.

To cover her presence, Eve should guarantee that the QBER value is lower than the maximal tolerable error rate. Therefore, r_1 should be larger than a certain value. Here, we calculate the maximal tolerable error rate by employing the security analysis in Ref. [44]. The secret key rates for different dimensions are given by $R_d = \log_2 d - 2H(e)$, where

$$H(x) = -x\log_2\frac{x}{d-1} - (1-x)\log_2(1-x).$$

When error rate e reaches the maximal tolerable value, the secret key rate reaches 0. As illustrated in Fig. 7, we can figure out that for different dimensions, the requirements for r_1 differ. For two-dimensional QKD system, for the sake of hiding Eve's attack, the coupling ratio r_1 should be larger than 0.78. With increasing the dimension d, the requirement for r_1 decreases. When d reaches 16, this requirement is only 0.6917. When d approaches infinity, the maximal tolerable QBER is 50% which corresponds to the r_1 value of 0.5, then the QKD system will be entirely insecure. Therefore, we can infer that higher-dimensional QKD system is more vulnerable to wavelength attack. Although HD-QKD is more robust against channel noise, it is sensitive to wavelength attack.

Last but not least, we would mention the resistance of QKD systems with different basis choice methods towards wavelength attack. We again take four-dimensional time-bin HD-QKD system mentioned above for example. This system adopts biased basis choice,[45] *i.e.*, the preparation probabilities of two bases are unequal. Here biased ratio (defined as $q_A = p_A/(p_A+p_B)$, p_A, and p_B are preparation probabilities) and coupling ratio are both selected as 0.90. As shown in Eq. (2) and Fig. 3, the QBER introduced by wavelength attack is no more than 13.5%. Even though Eve performs a simple intercept-and-resend attack, r_1 and r_2 are both 0.90. Substituting $r_1 = r_2 = 0.90$ into Eq. (2), we find that the QBER is just 13.5%, still less than the maximal tolerable QBER value. Therefore, Eve's presence is hard to detect. Then, we consider unbiased basis choice ($p = r = 0.5$), the QBER becomes

$$Err = \frac{3}{8}\left(\frac{r_2}{r_1+r_2} + \frac{1-r_1}{2-r_1-r_2}\right)$$

according to Eq. (4). Thus, the maximal QBER when Eve performs wavelength attack is 37.5% (r_1 is a little more than 0.50 and r_2 is a little less than 0.50), much more than security threshold value (18.9%). If so, Alice and Bob can realize Eve's attacking behavior. By comparison, we can find that systems with biased basis choice are more vulnerable to wavelength attack, although biased basis choice is conducive to generate more secret key. By calculation, our analysis results apply to any dimension.

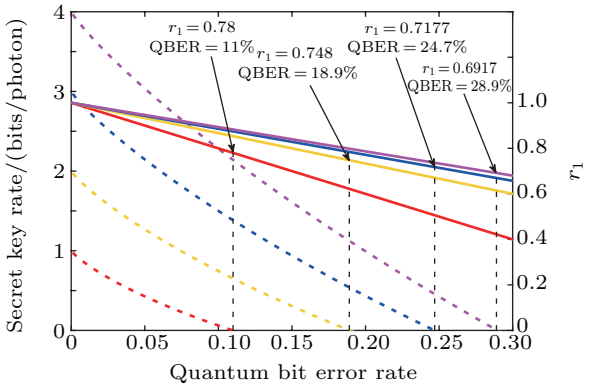


Fig. 7. The relationship between the requirement for coupling ratio and QBER. Full lines represent relationships between coupling ratio and QBER while dotted lines denote secret key rates in infinite-key scenario. Colors red, yellow, blue, and purple correspond to dimensions $d=2$, 4, 8, and 16, respectively.

5. Conclusion

In summary, we successfully carry out wavelength attack towards time-bin high-dimensional QKD system by utilizing the imperfection of fiber beam splitter. The eavesdropper Eve can obtain secret key information without increasing the quantum bit error rate. Our results also demonstrate that wavelength attack is a universal attacking strategy towards arbitrary d-dimensional QKD systems. Furthermore, we demonstrate that higher-dimensional QKD system is more vulnerable to wavelength attack. Meanwhile, we should also note that this type of attacking protocol can be avoided by applying actively modulated QKD systems. Measurement-device-independent QKD (MDI-QKD) is also immune to wavelength attack.

References

[1] Bennett C H and Brassard G 1984 *Proceddings of the IEEE International Conference on Computers, Systems and Signal Processing*, 1999, Bangalore, India (IEEE, New York, 1984) p. 175

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[3] Lo H K and Chau H F 1999 *Science* **283** 2050

[4] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[5] Renner R 2005 Security of quantum key distribution, Ph. D. Dissertation (Zurich: Swiss Federal Institute of Technology Zurich)

[6] Wang S, He D Y, Yin Z Q, Lu F Y, Cui C H, Chen W, Zhou Z, Guo G C and Han Z F 2019 *Phys. Rev. X* **9** 021046

[7] Cui C H, Yin Z Q, Wang R, Chen W, Wang S, Guo G C and Han Z F 2019 *Phys. Rev. Appl.* **11** 034053

[8] Wu S H, Li Y, Feng L P, Zeng X L, Li W, Qiu J F, Zuo Y, Hong X B, Yu H, Chen R, Giles I P and Wu J 2018 *Opt. Lett.* **43** 2130

[9] He D Y, Wang S, Chen W, Yin Z Q, Qian Y J, Zhou Z, Guo G C and Han Z F 2017 *Appl. Phys. Lett.* **110** 111104

[10] Fung C H F, Qi B, Tamaki K and Lo H K 2006 *Phys. Rev. A* **75** 032314

[11] Xu F H, Qi B and Lo H K 2010 *New J. Phys* **12** 113026

[12] Qi B, Fung C H F, Lo H K and Ma X F 2005 *Quantum Inf. Comput.* **7** 0073

[13] Qi B, Fung C H F, Zhao Y, Ma X F, Tamaki K, Chen C and Lo H K 2007 *Quantum Communications and Quantum Imaging V* **6710** 730

[14] Makarov V and Hjelme D R 2005 *J. Mod. Opt.* **52** 691

[15] Makarov V, Anisimov A and Skaar J 2007 *Phys. Rev. A* **74** 022313

[16] Makarov V and Skaar J 2008 *Quantum Inf. Comput.* **8** 622

[17] Makarov V 2012 *New J. Phys.* **11** 065003

[18] Lydersen L, Akhlaghi M K, Majedi A H, Skaar J and Makarov V 2011 *New J. Phys.* **13** 113042

[19] Gerhardt I, Liu Q, L-Linares A, Skaar J, Kurtsiefer C and Makarov V 2010 *Nat. Commun.* **2** 349

[20] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686

[21] Huang A, Sajeed S, Chaiwongkhot P, Soucarros M, Legré M and Makarov V 2016 *IEEE J. Quantum Electron.* **52** 8000211

[22] Qian Y J, He D Y, Wang S, Chen W, Yin Z Q, Guo G C and Han Z F 2018 *Phys. Rev. Appl.* **10** 064062

[23] Zhang L, Silberhorn C and Walmsley I A 2008 *Phys. Rev. Lett.* **100** 110504

[24] Tittel W, Brendel J, Zbinden H and Gisin N 2000 *Phys. Rev. Lett.* **84** 4737

[25] Mafu M, Dudley A, Goyal S, Giovannini D, McLaren M, Padgett M J, Konrad T, Petruccione F, Lütkenhaus N and Forbes A 2014 *Phys. Rev. A* **88** 032305

[26] Wang S, Yin Z Q, Chen W, He D Y, Song X T, Li H W, Zhang L J, Zhou Z, Guo G C and Han Z F 2015 *Nat. Photon.* **9** 832

[27] Chau H F, Yin Z Q, Wang S, Chen W and Han Z F 2019 *Quantum Inf. Proc.* **18** 138

[28] Ali-Khan I, Broadbent C J and Howell J C 2007 *Phys. Rev. Lett.* **98** 060503

[29] Mower J, Desjardins P, Shapiro J H and Englund D R 2012 *Phys. Rev. A* **87** 062322

[30] Zhang Z S, Mower J, Englund D R, Wong F N and Shapiro J H 2014 *Phys. Rev. Lett.* **112** 120506

[31] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

[32] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[33] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[34] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330.

[35] Lütkenhaus N and Jahma M 2002 *New J. Phys.* **4** 44

[36] Bao H Z, Bao W S, Wang Y, Zhou C and Chen R K 2016 *J. Phys. A: Math. Theor.* **49** 205301

[37] Niu M Y, Xu F H, Furrer F and Shapiro J H 2016 *Phys. Rev. A* **94** 052323

[38] Li H W, Wang S, Huang J Z, Chen W, Yin Z Q, Li F Y, Zhou Z, Liu D, Zhang Y, Guo G C, Bao W S and Han Z F 2011 *Phys. Rev. A* **84** 062308

[39] Huang J Z, Weedbrook C, Yin Z Q, Wang S, Li H W, Chen W, Guo G C and Han Z F 2013 *Phys. Rev. A* **87** 062329

[40] Huang J Z, Kunz-Jacques S, Jouguet P, Weedbrook C, Yin Z Q, Wang S, Chen W, Guo G C and Han Z F 2014 *Phys. Rev. A* **89** 4

[41] Ma X C, Sun S H, Jiang M S and Liang L M 2013 *Phys. Rev. A* **87** 052309

[42] Islam N T, Lim C C W, Cahall C, Kim J and Gauthier D J 2017 *Sci. Adv.* **3** e1701491

[43] Islam N T, Cahall C, Aragoneses A, Lezama A, Kim J and Gauthier D J 2017 *Phys. Rev. Appl.* **7** 044010

[44] Eisenmann M and Weidel E 1991 *J. Lightwave Technol.* **9** 853

[45] Sheridan L and Scarani V 2010 *Phys. Rev. A* **82** 030301

[46] Lo H K, Chau H F and Ardehali M 2005 *J. Cryptology* **18** 133