Front. Phys., 2014, 9(5): 613–628
DOI 10.1007/s11467-014-0420-6

REVIEW ARTICLE

Security analysis on some experimental quantum key distribution systems with imperfect optical and electrical devices

Lin-Mei Liang (梁林梅)[1,2,†], **Shi-Hai Sun** (孙仕海)[1], **Mu-Sheng Jiang** (江木生)[1], **Chun-Yan Li** (李春燕)[1]

[1] *Department of Physics, National University of Defense Technology, Changsha 410073, China*

[2] *State Key Laboratory of High Performance Computing, National University of Defense Technology, Changsha 410073, China*

Corresponding author. E-mail: [†] *nmliang@nudt.edu.cn*

Received December 9, 2013; accepted March 20, 2014

In general, quantum key distribution (QKD) has been proved unconditionally secure for perfect devices due to quantum uncertainty principle, quantum noncloning theorem and quantum nondividing principle which means that a quantum cannot be divided further. However, the practical optical and electrical devices used in the system are imperfect, which can be exploited by the eavesdropper to partially or totally spy the secret key between the legitimate parties. In this article, we first briefly review the recent work on quantum hacking on some experimental QKD systems with respect to imperfect devices carried out internationally, then we will present our recent hacking works in details, including passive faraday mirror attack, partially random phase attack, wavelength-selected photon-number-splitting attack, frequency shift attack, and single-photon-detector attack. Those quantum attack reminds people to improve the security existed in practical QKD systems due to imperfect devices by simply adding countermeasure or adopting a totally different protocol such as measurement-device independent protocol to avoid quantum hacking on the imperfection of measurement devices [Lo, *et al.*, Phys. Rev. Lett., 2012, 108: 130503].

Keywords quantum key distribution, quantum cryptography, quantum hacking

PACS numbers 03.67.Hk, 03.67.Dd

Contents

1 Introduction

Quantum key distribution (QKD), such as the Bennett-Brassard 1984 (BB84) protocol [1], makes use of quantum principle to share secure key between two remote parties due to quantum uncertainty principle, quantum noncloning theorem and quantum nondividing principle. Although the unconditional security of QKD has been proved for both the ideal system [2, 3] and the practical system [4, 5] in past years, some imperfections existed in the system are ignored, which may open some back doors for the eavesdropper (Eve) to spy the secret key. Strictly speaking, any deviation between the standard security analysis and the QKD system based on practical

Frontiers of Physics

devices can be exploited by Eve to obtain more information. Thus it is important to do research on the QKD system carefully and close these loopholes to guarantee the unconditional security of the final key.

Generally speaking, a complete QKD system consists of three main parts: sender, optical channel and receiver. The sender, Alice, has apparatus such as laser, phase modulators or polarization controllers to encode key information, the receiver, Bob, has single photon detectors, phase modulators or polarization controllers to decode key information. In the standard security proof of QKD, it is always based on the assumption that the apparatus in Alice and Bob are perfect and the optical channel is controlled by Eve. However, there always exist imperfections in the practical apparatus of both Alice and Bob, which may cause security loopholes and can be exploited by Eve. In fact, some potential loopholes have been discovered.

As far as Alice is concerned, strictly speaking, BB84 protocol requires Alice uses a single photon source (SPS) to carry her key information. Note that SPS is very important for quantum communication and have been researched widely in theory and experiment [6–10], at the same time, some QKD protocols based on SPS (or entangled photon source), in which the legitimate parties can use quantum repeaters to prolong the transmission distance, have been proposed [11–14]. However, SPS is unavailable now, thus the weak coherent source (WCS) is often used in most experimental systems. Although the distance of QKD with WCS cannot be prolonged by using quantum repeaters, it is still a good method within one or two hundred kilometers before ideal single photon source or near single photon source are available. The WCS will send multi-photon pulses with nonzero probability, then Eve can obtain all the key information by using the photon-number-splitting (PNS) attack [15–18] unless the optical channel between Alice and Bob is lossless. Luckily, the decoy state method [19–22] is proposed to defeat the PNS attack, which has been considered as the best way to defeat the PNS attack, and widely applied in some QKD systems [23–27]. Note that an important assumption in the decoy state method is that Alice and Bob must know the probability distribution of photon number of the source, but this assumption may not hold in some situations, for example, in the plug-and-play QKD system, the source is totally controlled by Eve, thus she can change the probability distribution of photon-number to maximize her information, which is known as "untrusted source problem" [28–30]. At the same time, there exist both random errors and statistical fluctuations of light intensity, which will compensate the unconditional security of final key [31–34]. Furthermore, the side channel of source will leak some information to Eve, for example, in some QKD systems based on polarization encoding, Alice uses four laser diodes to generate the four linear polarizations of BB84 protocol. However, the pulses emitted from the four laser diodes are not perfectly indistinguishable in their spatial, spectral or temporal properties, then Eve can exploit these properties [35]. Finally, note that in the standard BB84 protocol, the difference of phase of two states is $\pi/2$, but it can be much smaller than $\pi/2$ in some situations, which is known as phase remapping attack [36, 37].

When the pulses arrive at Bob's side, he randomly chooses one of two bases to decode the key information, and then detect the pulses with two or four single photon detectors (SPD). However, in some situations, both the base of Bob and the responding of the SPD can be partially or totally controlled by Eve. For example, the transmission rate of beam splitter, used by Bob to passively choose the measurement base, may depend on the wavelength of light, then Eve can control the measurement base of Bob with a multi-wavelength source [38]. Generally speaking, Bob needs two or four SPDs to record the pulse from Alice, but the efficiency of these detectors does not perfectly match, which also can be exploited by Eve to implement the time-shift attack [39–41]. Much worse, the SPDs of Bob can be blinded by bright light, then Eve can totally control the response of these detectors and obtain all the information about the final key, which have been demonstrated in experiment [42–44].

Excepting the imperfection of physical devices, the imperfection existed in the preparation processing also can be exploited by Eve, for example, Jain *et al.* had proposed and demonstrated a device calibration attack by deceiving a channel length calibration routine [45]. Here note that although we pay attention to the discrete variable QKD system based on BB84 protocol in the article, Eve also can implement quantum hacking for the continuous variable QKD system, which is alternative to the discrete variable QKD and have been demonstrated by many groups [46–48]. For example, the wavelength attack by exploiting the wavelength-dependent property of a beam splitter in Bob side [49, 50], and the local oscillator intensity attack by using the intensity fluctuation of local oscillator pulses [51].

In order to bridge the gap between theory and practice, the legitimate parties have two approaches. First, they analyze the imperfection of these systems, and then modify the QKD protocol or system to remove the existence of Eve. Although it cannot discover all the loopholes existed in the system, it is helpful to enhance the security of QKD systems based on current technology. Sec-

ond, they use the device-independent QKD (DI-QKD) to exclude all the imperfections of practical apparatus. *Full* DI-QKD [52, 53] is impractical within current technology, since it requires a single photon detector with near unity efficiency. Recently, *measurement-* DI-QKD (MDI-QKD) [54–57] was proposed by Lo *et al.* and then demonstrated by some groups [58–60], which remove all the detection loopholes, but it requires two-photon interference. In this article, as examples, we review on our recent works, following the first approach, about quantum hacking and defence on some experimental QKD system, including passive faraday mirror attack [61], partially random phase attack [62], wavelength-selected photon-number-splitting attack [63], frequency shift attack [64], and single-photon-detector attack [65].

2 Passive faraday mirror attack

In the QKD system based on long distance fiber, the major difficulty is to maintain the stability and compensate the birefringence of fiber. In order to overcome this problem, Muller *et al.* proposed an interesting *plug-and-play* scheme [66], which can compensate the birefringence of fiber automatically. A simple diagram of the *plug-and-play* scheme is shown in Fig. 1(a), in which Bob sends a strong reference pulse to Alice, then Alice encodes her information to the reference pulse, attenuates it to single photon level, and sends it back to Bob. Due to the faraday mirror (FM), the birefringence of fiber is

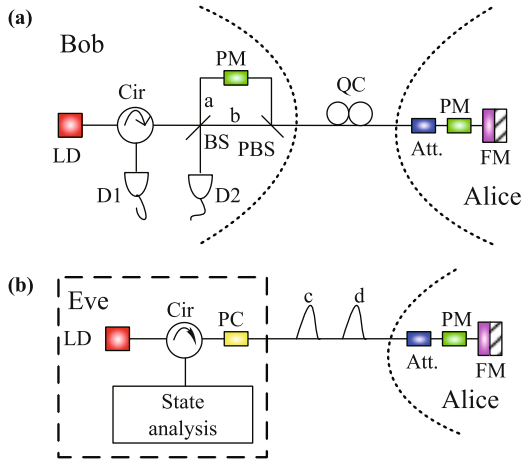

Fig. 1 The simple diagram of plug-and-play system [66] and Eve's attack scheme. LD: Laser diode, Cir: Circulator, BS: Beam splitter, PBS: Polarization beam splitter, Att.: Attenuator, PM: Phase modulator, FM: Faraday mirror, QC: Quantum channel, D1 and D2: Single photon detectors, PC: Polarization controller. Part (a) shows the plug-and-play system without Eve. Part (b) shows Eve's PFM attack strategy. In the diagram, we only show how Eve analyzes the information of Alice. c and d are two time modes sent to Alice by Eve and we assume only mode c is modulated by Alice. Reproduced from Ref. [61].

automatically compensated in this system. However, the practical FM is imperfect, which will not only introduce additional quantum bit error rate (QBER) but also leave a loophole for Eve to spy the secret key. In fact, a passive faraday mirror (PFM) attack based on the imperfection of FM is proposed by our group [61]. Our analysis shows that, if the FM is imperfect, the dimension of Hilbert space spanned by the four states of Alice is three instead of two. Thus Eve can distinguish these states with a set of POVM operators belonging to three dimension space, which will reduce the QBER induced by her attack.

2.1 PFM attack

Now we give a brief review of the PFM attack, the detail information about this attack is given in Ref. [61]. The FM is a combination of a θ faraday rotator and an ordinary mirror, thus the Jones matrix of FM can be written as

$$FM(\theta) = -\begin{pmatrix} \sin(2\varepsilon) & \cos(2\varepsilon) \\ \cos(2\varepsilon) & -\sin(2\varepsilon) \end{pmatrix} \equiv FM(\varepsilon) \qquad (1)$$

where $\varepsilon = \pi/4 - \theta$ is the deviation angle of the practical FM. It is easy to check that when $\varepsilon = 0$ ($\theta = \pi/4$), the following equation always holds, which is given by

$$T(-\theta') \cdot FM(45^\circ) \cdot T(\theta') = \mathrm{e}^{\mathrm{i}(\varphi_o+\varphi_e)} FM(45^\circ) \qquad (2)$$

where $T(\theta')$ and $T(-\theta')$ are the Jones matrices of birefringence medium when the photon travels forward and backward the quantum channel. Thus, the polarization of the outgoing state is always orthogonal to that of the incoming state, regardless of the input polarization state and the birefringence medium. However, the practical FM is imperfect, which means $\varepsilon \neq 0$, for example, in the center wavelengths 1550 nm and 1310 nm, the maximal rotation angle tolerance is 1° (at 23°C) for the popular FM produced by *Newport* [67] and *General Photonics* [68]. Thus we only consider the case that $|\varepsilon| \leqslant 1^\circ$ in the following.

In fact, when FM is imperfect, it will not only increase QBER, but also leave a loophole for Eve. Then, the states sent by Alice are not the standard BB84 state, noted as $|\phi_k\rangle = (\mathrm{e}^{\mathrm{i}k\pi/2}|c\rangle + |d\rangle)/\sqrt{2}$, but four new states that can be written as

$$|\Phi_k\rangle = \frac{1}{\sqrt{2}}\{\sin(2\varepsilon)\mathrm{e}^{\mathrm{i}2k\delta}|cH\rangle + \cos(2\varepsilon)\mathrm{e}^{\mathrm{i}k\delta}|cV\rangle + \sin(2\varepsilon)|dH\rangle + \cos(2\varepsilon)|dV\rangle\} \qquad (3)$$

where δ is the difference of phase of Alice's states. In the standard BB84 protocol, $\delta = \pi/2$, but the plug-and-play system will suffer from the phase remapping attack [36, 37], then δ can be much smaller than $\pi/2$. It is easy to

check that, when $\varepsilon \neq 0$, the dimension of Hilbert space spanned by the four new states of Eq. (3) is three.

The attack is shown in Fig. 1(b), Eve can intercepts Alice's pulses and measure them with five POVM operators $\{M_{\rm vac}, M_i | i = 0, 1, 2, 3\}$ which satisfy the condition that $M_{\rm vac} + \sum_{i=0}^{3} M_i = I$. When Eve obtains the outcome corresponding to M_i, she resends $|\phi_i\rangle$ to Bob, otherwise, she sends a vacuum state to Bob. Note that the dimension of M_i and $M_{\rm vac}$ is three instead of two in our attack.

Since the four new states are also linearly dependent, Eve may introduce some errors. However, the QBER introduced by Eve can be much smaller than the inherent QBER of practical systems. The QBER between Alice and Bob induced by Eve's attack, and the probability that Eve obtains an valid outcome successfully are given by

$$\mathrm{e}^B = \frac{\sum_{k=0}^{3}\sum_{j=0,j\neq k}^{3} P(j|k)}{\sum_{k=0}^{3}\sum_{j=0}^{3} P(j|k)} = \frac{\sum_{i=0}^{3} \mathrm{Tr}(M_i L_i)}{\sum_{i=0}^{3} \mathrm{Tr}(M_i \rho)} \tag{4a}$$

$$P_{\rm succ}^{E} = \frac{1}{4}\sum_{i=0}^{3} \mathrm{Tr}(M_i \rho) \tag{4b}$$

where the valid outcome means that Eve obtains outcome corresponding to M_i but not $M_{\rm vac}$, and

$$L_i = \frac{1}{2}\rho_{i+1} + \rho_{i+2} + \frac{1}{2}\rho_{i+3} \tag{5a}$$

$$\rho = \rho_0 + \rho_1 + \rho_2 + \rho_3 \tag{5b}$$

$$P(j|k) = \sum_{i=0}^{3} |\langle\phi_j|\phi_i\rangle|^2 \mathrm{Tr}(M_i \rho_k) \tag{5c}$$

$$\rho_k = |\Phi_k\rangle\langle\Phi_k| \tag{5d}$$

Therefore, in order to find the optimal strategy for Eve, she needs to solve the optimization program with two penalty functions, which can be written as

$$\begin{aligned} &\min \quad \mathrm{e}^B \quad \text{and} \quad \max \quad P_{\rm succ}^{E} \\ &\text{subject to} \quad M_i \geqslant 0, \quad M_{\rm vac} \geqslant 0, \\ &\qquad M_{\rm vac} + \sum_{i=0}^{3} M_i = I \end{aligned} \tag{6}$$

where $M_i \geqslant 0$ and $M_{\rm vac} \geqslant 0$ mean the matrix M_i and $M_{\rm vac}$ are positive. In fact Eve cannot obtain the optimal value of the two penalty functions simultaneously, which will be shown in the following. Thus we consider e^B as the major object and $P_{\rm succ}^{E}$ as a minor one.

2.2 Suboptimal measurement strategy of Eve and numerical simulations

Although the optimal strategy of Eve is given by the solution of Eq. (6), it is hard to solve this optimization program. Thus, here we use the method introduced by Fung *et al.* [36], and consider the following suboptimal strategy for Eve. First, instead of distinguishing the four states of Alice, here Eve only distinguishes ρ_0 from $\{\rho_1, \rho_2, \rho_3\}$ and ρ_3 from $\{\rho_0, \rho_1, \rho_2\}$. It means that, Eve sets $M_1 = M_2 = 0$. Furthermore, Eve uses the following POVM operators to measure the states of Alice, which are given by

$$\begin{aligned} M_0 &= x\rho^{-1/2}|C_0\rangle\langle C_0|\rho^{-1/2} \\ M_3 &= x\rho^{-1/2}|C_3\rangle\langle C_3|\rho^{-1/2} \end{aligned} \tag{7}$$

where $|C_0\rangle$ or $|C_3\rangle$ is the eigenvector of matrix $\rho^{-1/2}L_0\rho^{-1/2}$ or $\rho^{-1/2}L_3\rho^{-1/2}$ corresponding to the minimal un-zero eigenvalue λ_0 or λ_3, x is the maximal real number that ensure the matrix $M_{\rm vac} = I - M_0 - M_3$ is positive. Obviously, $\{M_{\rm vac}, M_0, M_3\}$ are positive and sum to the identity, thus they are valid POVM operators.

The QBER between Alice and Bob induced by Eve's attack is shown in Fig. 2. It shows QBER introduced by Eve can be not only lower than 20% which is the maximally tolerable QBER in the BB84 protocol under the two-way post-processing [69, 70], but also lower than 11% which is the maximal tolerable QBER for the BB84 protocol under the collective attack and one-way post-processing [71]. It is interesting that, when δ is given, the QBER induced by Eve is almost constant. In fact, e^B is constant in order of $o(\varepsilon)$, thus it is not represented in the figure.

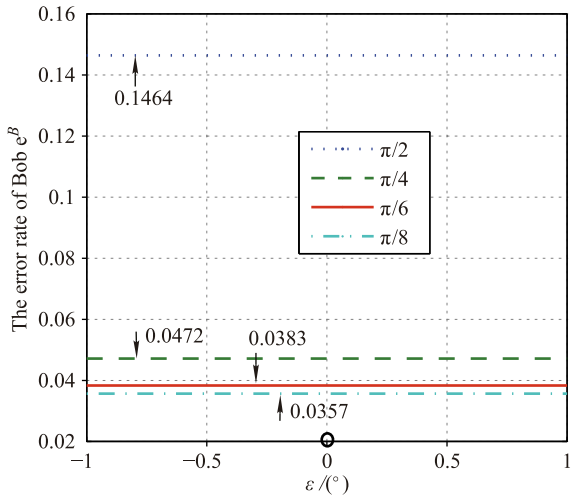

Fig. 2 The error rate of Bob changes with ε for given δ. Note that the special point that $\varepsilon = 0$ is unconsidered in our simulation, since FM is perfect in this point. Reproduced from Ref. [61].

3 Partially random phase attack

Phase randomization of source is an important assump-

tion in the standard security analysis of BB84 protocol [72–75], especially for the decoy state method [19–22]. However, in QKD systems, this assumption may not hold, especially for the plug-and-play QKD system in which the source is totally controlled by Eve, and for the systems that no active randomization setups are used.

Here we introduce the partially random phase (PRP) attack proposed by our group [62], which shows that if the phase of source is just partially randomized, the error rate induced by Eve can be lower than the tolerable threshold value of error rate, whereas the same range of error rate has been proved secure if the legitimate parties are unaware of our attack. Thus when our attack is taken into account, the secret key rate will be compromised. Specifically, the numerical simulations show that, in some parameter regime, our attack is immune to the one-decoy-state method [21].

3.1 PRP attack

The diagram of the PRP attack is shown in Fig. 3. Eve intercepts Alice's signal pulses and measures them with a homodyne detector. Note that, in the plug-and-play system, Alice sends two coherent pulse $|\alpha e^{i\theta}\rangle_r|\alpha e^{i(\phi_k^a+\theta)}\rangle_s$ to Bob, here $s(r)$ is signal (reference) pulse, α is real and $|\alpha|^2$ is the average photon number, $\phi_k^a = k\pi/2, k = 0, 1, 2, 3$ is the encoding phase of Alice, θ is the global phase which should be a random phase belonging $[0, \delta]$. Therefore, according to the measurement theory, the probability distribution of the measurement result (x) of the homodyne detection can be written as [79, 80]:

$$P(x,\phi) = \int_0^{\delta} \frac{\mathrm{d}\theta}{\delta}\sqrt{\frac{2}{\pi\kappa^2}} \times \exp[-2(x-\lambda\sqrt{\mu_s}\cos(\phi+\theta))^2/\kappa^2] \quad (8)$$

where $\mu_s = |\alpha|^2$, $\phi = \phi_k^a - \phi_j^e$ is the difference of phase modulated by Eve and Alice, λ and κ are two parameters that characterize the imperfection of homodyne detection [79].

Figure 4 shows the theoretical probability distribution of x when ϕ are 0, $\pi/2$, π and $3\pi/2$. It shows Eve can use the following attack: she first intercepts all the pulse from Alice and randomly modulates one of the two phase $\phi_j^e = j\pi/2, j = 0, 1$ on the local pulse, then she measures the quadrature amplitude (x) of the signal pulse with a homodyne detector. Finally, she sets two threshold value X_+ and X_- to judge Alice's information. Simply, we consider the symmetrical case that $X_+ = -X_- \equiv X_{th}$. When $x \geqslant X_{th}$, Eve judges that the phase modulated by Alice is the same as her, thus she resends a state with phase ϕ_j^e to Bob. When $x \leqslant -X_{th}$, Eve judges that the difference of phase modulated by Alice and her is π, thus she resends a state with phase $\phi_j^e + \pi$ to Bob. When $-X_{th} \leqslant x \leqslant X_{th}$, she blocks this pulse and resends a vacuum state to Bob. Note that these invalid judgements will not affect our attack, since the channel between Alice and Bob is lossy.

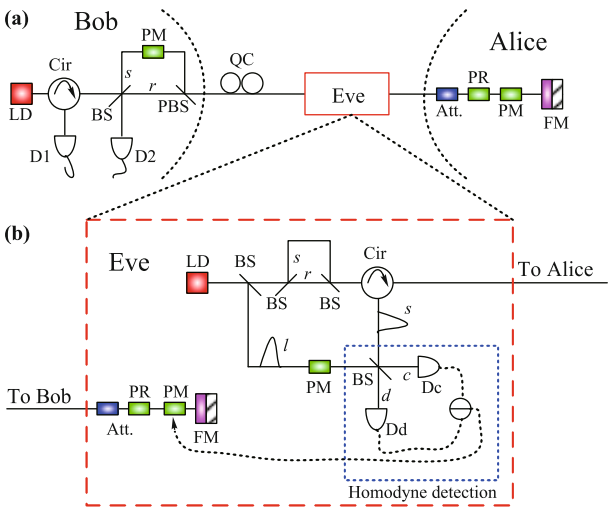

Fig. 3 A simple diagram of the PRP attack. Eve intercepts the pulse from Bob and sends a faked pulse to Alice. When the faked pulse is modulated by Alice and returns to Eve, Eve measures it and modulates a phase on Bob's pulse according to her measurement results. Then she resends Bob's pulse to Bob. Note that in our attack Eve uses the homodyne detection but not SPD to detect Alice's information. Reproduced from Ref. [62].

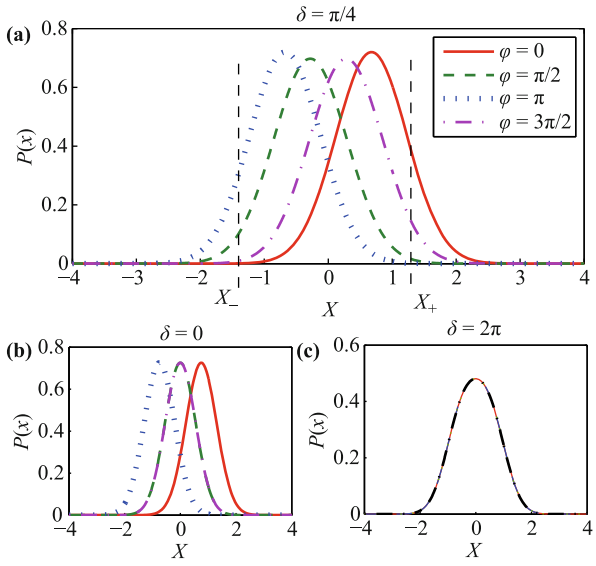

Fig. 4 The theoretical probability distribution of x when ϕ are 0, $\pi/2$, π and $3\pi/2$. In the figure, we show the three case that the source has been unrandomized ($\delta = 0$), partially randomized ($\delta = \pi/4$) and totally randomized ($\delta = 2\pi$). Here we set $\lambda = 0.75$ and $\kappa = 1.1$ due to the experimental results of Ref. [79]. X_+ and X_- are two threshold values used to distinguish 0 and π from the set $\{0, \pi/2, \pi, 3\pi/2\}$. Reproduced from Ref. [62].

The further calculations show that the error rate induced by Eve and the probability that Eve obtains a valid outcome can be written as

$$e = \{P_0^- + [P_{\pi/2}^+ + P_{\pi/2}^-]/2\}/(2P_{\text{post}}) \tag{9a}$$

$$P_{\text{post}} = (P_0^+ + P_0^- + P_{\pi/2}^+ + P_{\pi/2}^-)/2 \tag{9b}$$

where

$$P_0^+ = \int_{X_{th}}^{\infty} \mathrm{d}x P(x,0), \quad P_0^- = \int_{-\infty}^{-X_{th}} \mathrm{d}x P(x,0)$$

is the valid count rate of Eve when $\phi_0^e = 0$, and

$$P_{\pi/2}^+ = \int_{X_{th}}^{\infty} \mathrm{d}x P(x,\pi/2)$$

$$P_{\pi/2}^- = \int_{-\infty}^{-X_{th}} \mathrm{d}x P(x,\pi/2)$$

is the case for $\phi_1^e = \pi/2$.

The error rate induced by our attack is shown in Fig. 5. It shows clearly that when the phase of source is just partially random, the generated key will be compromised. Part (a) shows that the error rate changes with X_{th} and δ. Part (b) shows the error rate changes with μ_s.

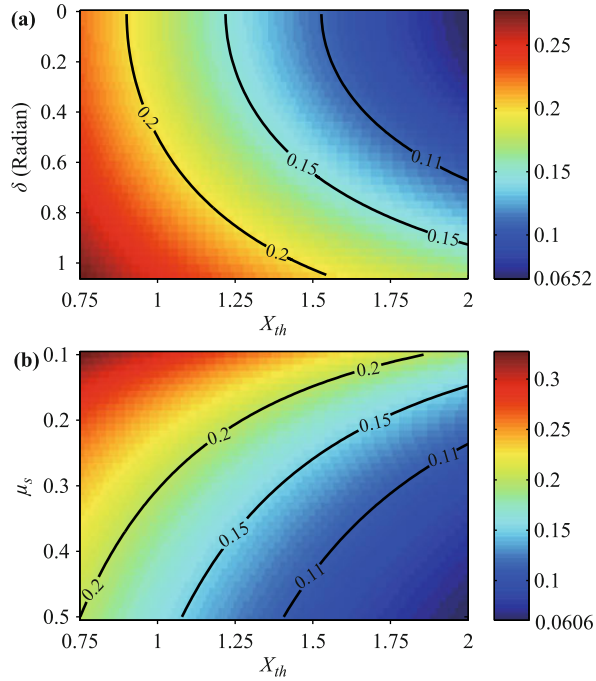

Fig. 5 The error rate induced by Eve. In the simulations, we also set $\lambda = 0.75$ and $\kappa = 1.1$. **(a)** shows the error rate changes with X_{th} and δ for given $\mu_s = 0.3$. **(b)** shows the error rate changes with X_{th} and μ_s for given $\delta = \pi/6$. In the figure, we also draw the contour line for $e = 11\%, 15\%, 20\%$. Reproduced from Ref. [62].

3.2 PRP attack to the one decoy state method

Decoy state method is often used in the QKD system with WCS to beat the PNS attack, thus here we show that, if Alice and Bob use the one decoy state method [21], our attack is still valid. Although the one decoy state is not optimal for Alice and Bob, it is still adopted in some experimental systems [26, 77]. Furthermore, we assume Eve sends a single photon state to Bob, when she obtains a valid measurement outcome, since she does not distinguish the signal state and decoy state. Thus the gain and error rate of Bob for the signal state and the decoy state are given by

$$Q_\mu = \eta_{\text{Bob}} Q'_\mu + (1 - \eta_{\text{Bob}}) Y_0 \tag{10a}$$

$$E_\mu Q_\mu = \eta_{\text{Bob}} Q'_\mu E'_\mu + (1 - \eta_{\text{Bob}}) Y_0 e_0 \tag{10b}$$

$$Q_\nu = \eta_{\text{Bob}} Q'_\nu + (1 - \eta_{\text{Bob}}) Y_0 \tag{10c}$$

$$E_\nu Q_\nu = \eta_{\text{Bob}} Q'_\nu E'_\nu + (1 - \eta_{\text{Bob}}) Y_0 e_0 \tag{10d}$$

where Y_0 is the dark count of Bob's single photon detector, $e_0 = 0.5$ is the error rate of dark count, η_{Bob} is the transmittance of Bob's setups. Under the PRP attack, E'_μ and E'_ν are given by Eq. (9a), Q'_μ and Q'_ν are given by Eq. (9b).

Then according to the decoy state method [21], we can estimate the key rate under the PRP attack, which is shown in Fig. 6. Here we also show the equivalent length of channel between Alice and Bob, which is given by

$$L_{eq} = -\frac{10}{a} \log_{10}[\min\{1, \frac{Q_\mu}{\mu \eta_{\text{Bob}}}\}] \tag{11}$$

where Q_μ is the gain of signal state. Here the equivalent

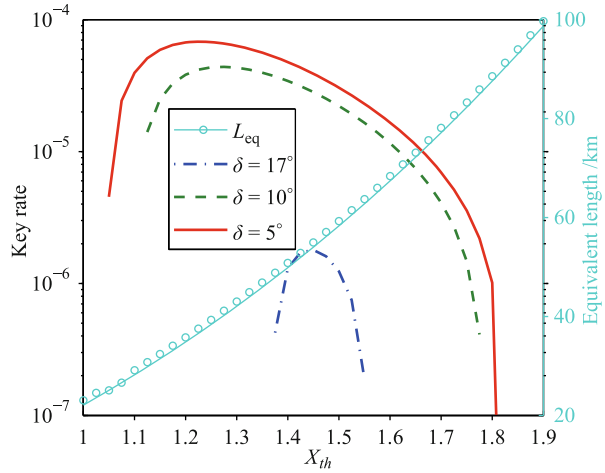

Fig. 6 The key rate between Alice and Bob at various threshold value X_{th}. Here the legitimate parties use the one decoy state method to estimate the key rate. Here we set $\mu = 0.48$ and $\nu = 0.05$ according to the decoy state theory [21] and the experimental parameters of GYS [78], which are laser $\lambda = 1550$ nm at 2 MHz, dark count rate $Y_0 = 1.7 \times 10^{-6}$, fiber loss 0.21 dB/km, Bob's quantum efficiency $\eta_{\text{Bob}} = 0.045$. In the simulation, we assume the homodyne detector of Eve is perfect, which means $\lambda = \kappa = 1$. Strictly speaking, the equivalent length will change with δ, but the difference is much small. Thus we just draw the equivalent length for $\delta = 17°$ in the figure. Reproduced from Ref. [62].

length is used to ensure the gain of signal state under our attack is the same as Bob's expectancy. The numerical simulations show clearly that, Eve can ensure the key rate between Alice and Bob is still positive by setting a suitable threshold value. Note that, here we assume the homodyne detector of Eve is perfect. Although Eve can make a perfect homodyne detector in theory, a practical Eve is still imperfect. In fact, our analysis shows that even if the homodyne detector is imperfect, the PRP attack is still valid in some parameters regime [62].

4 Wavelength-selected photon-number-splitting attack

In the decoy state QKD system, an important assumption is that the signal state and the decoy state are indistinguishable for Eve. However, in QKD systems, the assumption is invalid in some situations, then the security of decoy state method will be compromised. Actually, a wavelength-selected PNS (W-PNS) is proposed [63] by our group to break the security of decoy state *plug-and-play* QKD systems by exploiting the imperfection of the intensity modulator (IM) that used to generate the signal state and the decoy state. Our analysis shows that Eve can use our attack to determinately distinguish the signal state and decoy state, then the security of decoy state method is broken.

4.1 Frequency shift of waveguide-based Mach–Zehnder-type electro-optic intensity modulator

In the decoy state method, an IM is used by Alice to generate the signal state and the decoy state. Here we take the weak+vacuum decoy state method [21] as an example, in which three kinds of pulses, the signal state, the decoy state, and the vacuum state, with different intensities are used, whose intensities are denoted as μ, ν and 0 respectively. Usually, the waveguide-based Mach–Zehnder-type electro-optic IM (EOIM) works as following: Alice modulates the intensities of the decoy state and the vacuum state but do not change that of the signal state [see Fig. 7(a)], then their intensities are modulated to a proportion of $0 : \nu : \mu$, finally, a fixed attenuator is used to attenuate them to their own intensity level.

According to the principle of IM, when an input field with amplification E_0 and frequency ω_0 is coupled in the EOIM, and a driving voltage $V_\nu(t)$ is modulated on the EOIM, the output field can be written as

$$E(t) = \frac{1}{2}E_0 e^{i\omega_0 t}[e^{i(\gamma_1 V_\nu(t)+\varphi_{01})} + e^{i(\gamma_2 V_\nu(t)+\varphi_{02})}] \quad (12)$$

where γ_1 and γ_2 (φ_{01} and φ_{02}) are the voltage-to-phase

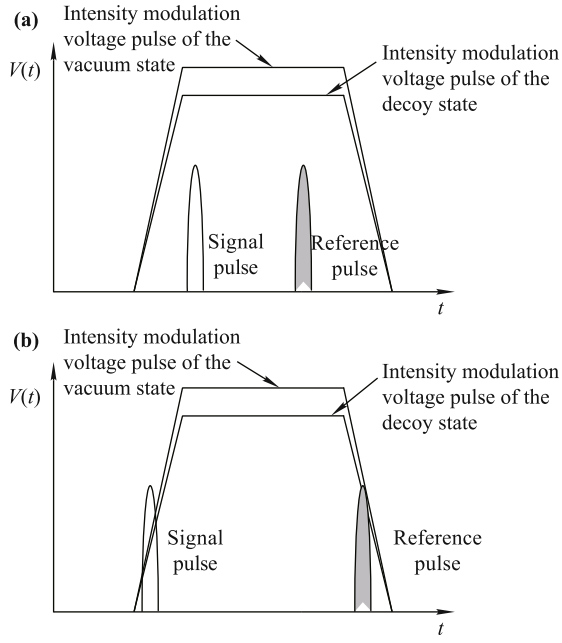

Fig. 7 **(a)** Intensity modulator (IM) are acting to have pure intensity modulation of the vacuum state and the decoy state; **(b)** Eve time shifts the light pulse to introduce a frequency shift to the decoy state during intensity modulation. Reproduced from Ref. [63].

conversion coefficient (static phase) for the two arms of EOIM. In the general decoy state mthod, $V_\nu(t)$ is a constant when the electron-optical (EO) effect happens in the lithium niobate waveguides, thus the IM only changes the intensity of light pluse without introducing any side channel. However, in some situations, $V_\nu(t)$ can change with time. In fact, in most of systems, Alice does not monitor the arrival times of light pulse, thus Eve can time shift the light pulse during the device calibration routine, so that the light pulse will arrive at the IM at the rising edge of driving voltage of IM [see Fig. 7(b)]. Without loss of generalization, we assume $V_\nu(t) = V_0 + kt$. If the EOIM is "X-cut" device (that is $\gamma_1 = -\gamma_2$), and no DC bias voltage is applied, then Eq. (12) can be rewritten as

$$E(t) = \frac{1}{2}E_0 e^{i\omega_0 t}[e^{i\gamma_1(kt+\gamma_1 V_0)} + e^{-i\gamma_1(kt+V_0)}] \quad (13)$$

Eq. (13) shows that the frequency of the light pulses has been changed with a shift of $\pm\omega_m = \pm\gamma_1 k$. Note that Eve begins the time shift during the device calibration routine, Alice will calibrate her devices to get the required intensities and phases, even though Eve has performed the time shift. Thus we have assumed here that the phase modulation and intensities of the signal state, decoy state and vacuum state are not impacted by time shift.

4.2 W-PNS attack

Briefly speaking, the W-PNS attack [63] works as follow-

ing: i) Eve performs time shift to introduce frequency shift to the decoy state; ii) Eve distinguishes the signal state and decoy state and by using wavelength division multiplex (WDM) technology; iii) Eve performs the PNS attack on the signal state and the decoy state respectively. Here we remark that, since the the intensity of vacuum state is 0, Eve does not need to do anything on it. Furthermore, since only the decoy state is attenuated by the EOIM, the frequency of the signal state is unchanged, and the frequency shift is only introduced on the decoy state. Therefore, Eve can distinguish the signal state and the decoy state by using WDM.

Note that, in the weak+vacuum decoy state method, the key rate is estimated by the experimental results of the total gain (and error rate) of signal state, decoy state and vacuum state, noted as Q_μ, Q_ν, Y_0 (and E_μ, E_ν, e_0) respectively. Thus, in order not to be discovered, Eve should keep these parameters unchanged under her attack. Here we consider the PNS attack as following: Eve picks out one photon from the multi-photon pulses, then she attenuates the single-photon pulses and multi-photon pulses with different transmission rates, and lastly transmits them to Bob with a lossless channel. Thus Eve should ensure the following equations hold, which is given by

$$Y_0 + k_\nu \eta_{\mathrm{Bob}} p_{\nu 1} + \sum_{n=2}^{\infty} p_{\nu n}[1-(1-T_\nu \eta_{\mathrm{Bob}})^{n-1}] = Q_\nu \tag{14a}$$

$$Y_0 + k_\mu \eta_{\mathrm{Bob}} p_{\mu 1} + \sum_{n=2}^{\infty} p_{\mu n}[1-(1-T_\mu \eta_{\mathrm{Bob}})^{n-1}] = Q_\mu \tag{14b}$$

where η_{Bob} is the transmission rate of Bob's side. T_ν and T_μ (k_ν and k_μ) are the channel transmission rate of multi-photon pulse (single photon pulse) for decoy state and signal state, which belong to $[0,1]$ and are controlled by Eve. In order to maximize her information, Eve needs to set k_ν and k_μ as smaller as possible. Therefore, take the signal state as example, when

$$\sum_{n=2}^{\infty} p_{\mu n}[1-(1-\eta_{\mathrm{Bob}})^{n-1}] \leqslant Q_\mu \tag{15}$$

Eve can set $T_\mu = 1$ and k_μ is given by Eq. (14b). Oppositely, when

$$\sum_{n=2}^{\infty} p_{\mu n}[1-(1-\eta_{\mathrm{Bob}})^{n-1}] \geqslant Q_\mu \tag{16}$$

Eve can set $k_\mu = 0$ and T_μ is given by Eq. (14b). Furthermore, the similar results can be deduced for the decoy state. Therefore, when W-PNS attack is performed, the real gain and error rate of single photon pulse for the signal state is given by

$$Q_1 = p_{\mu 1}(Y_0 + k_\mu \eta_{\mathrm{Bob}}) \tag{17a}$$

$$e_1 = \frac{e_0 Y_0 + e_{\mathrm{detector}} k_\mu \eta_{\mathrm{Bob}}}{Y_0 + k_\mu \eta_{\mathrm{Bob}}} \tag{17b}$$

According to the decoy state method [9–22], the key rate between Alice and Bob under W-PNS attack is given by

$$R_{\mathrm{Bob}} = q\{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1-H_2(e_1)]\} \tag{18}$$

And the key rate leaked to Eve is given by

$$R_{\mathrm{Eve}} = R - R_{\mathrm{Bob}}, \quad \text{when } R_{\mathrm{Bob}} > 0 \tag{19a}$$

$$R_{\mathrm{Eve}} = R, \quad \text{when } R_{\mathrm{Bob}} \leqslant 0 \tag{19b}$$

where R is the key rate between Alice and Bob when Eve is absent [21].

Figure 8 has shown an example of the efficiency of W-PNS attack, which clearly shows that R_{Eve} can be larger than 0 when channel length between Alice and Bob is larger than 13.6 km, specially when channel length is larger than 24.6 km [corresponds to the situation of Eq. (19b)], Eve can get full information ($R_{\mathrm{Eve}} = R$).

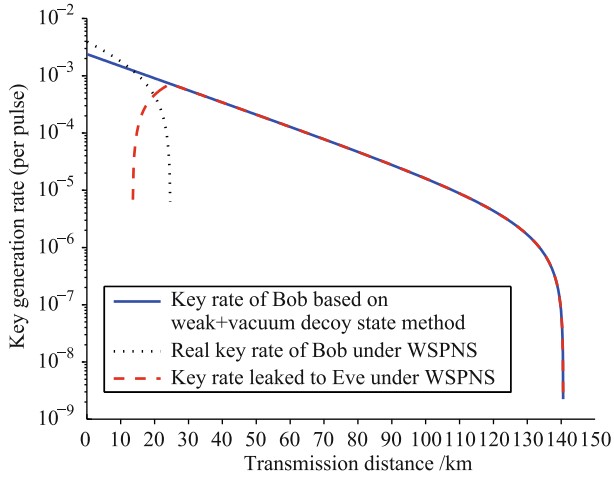

Fig. 8 The efficiency of W-PNS attack when determinately distinguishing the decoy state and the signal state. Here we set $\mu = 0.48$, $\nu = 0.05$ which are the optimal values under the experimental parameters of GYS [78]. The solid line shows the key rate of Bob when Eve is absent, with a maximal secure distance of 140.55 km. The dotted line shows the real key rate of Bob under W-PNS attack, with a maximal secure distance of only 24.6 km. The dashed line shows the key rate leaked to Eve under W-PNS attack. When the transmission distance is larger than 24.6 km, Eve can get full information, which shows the strong capability of our attack. Reproduced from Ref. [63].

5 Frequency shift attack

In long distance QKD system, birefringence of fiber is the major problem to maintain the stability of systems, then *plug-and-play* QKD system [66] is proposed and widely

used in some QKD systems [75–81], in which the birefringence is compensated automatically. Since Alice allows signals to go in and out of her device, this system will suffer from the phase-remapping attack [36, 37], in which Eve shifts the arriving time of signal pulse from the constant acting range of the phase modulation voltage to its rising edge, then the signal states encoded by Alice are no longer the standard BB84 states, which will give more information to Eve. The analysis shows that the QBER introduced by the phase remapping attack can be lower than 20%, which is the security limit of BB84 protocol with two-way postprocessing [69, 70].

However, if the one-way postprocessing, with maximal tolerable QBER 11% [71], is used, the phase-remapping attack is not valid any more, since the legitimate parties can discover the existence of Eve by estimating the QBER. Thus, in order not to be discovered, Eve should ensure that the QBER introduced by her is lower than a reasonable level. In fact, we find that the phase-rampping attack can be improved by using the frequency shift (FS) attack proposed by our group [64]. Our analysis shows that, by exploiting the same imperfection of the phase remapping attack, Eve can distinguish the quantum state of Alice without any detectable error, then she can obtain full information about the final key.

5.1 Frequency shift of $LiNbO_3$ waveguide phase modulator

In most QKD systems based on phase encoding, a $LiNbO_3$ waveguide phase modulator (PM) is used to encode random bits. However, the PM will introduce frequency shift instead of pure phase modulation under certain conditions, which will introduce a side channel for Eve.

In the *plug-and-play* QKD system [see Fig. 1(a)], when the pulses from Bob pass through the PM of Alice at the constant acting range of the modulation voltage and undergoes proper modulation [see Fig. 9(a)], one of the four phases, noted as $\varphi_n = n\pi/2$ $(n = 0, 1, 2, 3)$, are modulated on the signal state. Thus the output light field after PM can be written as

$$E_n(t) = E_0 e^{i(\omega_0 t + \frac{n}{2}\gamma V_\pi + \varphi_s)} = E_0 e^{i(\omega_0 t + \varphi_n)} \tag{20}$$

where, $\gamma = \pi/V_\pi$ is the voltage-to-phase conversion coefficient of the PM, V_π is the half-wave voltage of the PM, φ_s is the static phase for the PM and is set to zero for simplicity and without loss of generality. In Eq. (20), the modulation voltage for the PM is a constant when the EO effect happens in the $LiNbO_3$ waveguide during time τ, so that the modulation phase φ_n is also constant, which corresponds to pure phase modulation and fits the assumption in the security proofs.

However, in most of *plug-and-play* QKD systems, Alice does not monitor the arrival times of light pulses. Thus Eve can shift the arriving time of light pulse at the PM, so that the electro-optic effect will happen at the rising edge of phase modulation voltage [see Fig. 9(b)] and something unexpected will happen. Assuming that the driving voltages of PM is $V_n(t) = k_n t + V_{n0}$, then Eq. (20) can be rewritten as

$$E_n(t) = E_0 e^{i[(\omega_0 + \frac{n\gamma V_\pi}{2\Delta t})t + \theta_n]} \tag{21}$$

where Δt is the rise time of modulation voltages for Alice's PM. The frequency of these signal states can be written as

$$\nu_n = \frac{\omega_n}{2\pi} = \nu_0 + \frac{n}{4\Delta t} \tag{22}$$

with a frequency difference of $\Delta\nu = \frac{1}{4\Delta t}$.

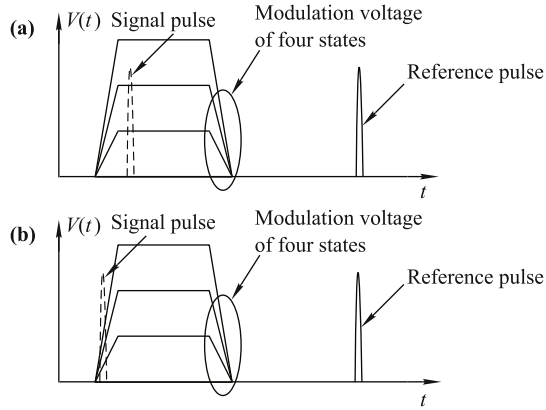

Fig. 9 **(a)** The signal pulse passes through Alice's phase modulator at the constant acting range of the modulation voltage and undergoes proper modulation; **(b)** Eve time shifts the light pulse to introduce a frequency shift to the signal pulse. Reproduced from Ref. [64].

The modulation voltage of $LiNbO_3$ waveguide PM used in current QKD systems has rise time Δt ranging from 1 ns to 10 ns (see Ref. [37]), which will introduce a $\Delta\nu$ ranging from 0.025 GHz to 0.25 GHz. Therefore, the four signal states sent by Alice under Eve's time shift can be distinguished by wavelength measurement, which can be exploited by Eve to perform the FS attack to beat the "*plug-and-play*" QKD systems.

5.2 FS attack

The brief idea of our FS attack scheme is shown in Fig. 10. Eve intrudes the quantum channel and sends two strong laser pulses (the fake signal pulse and the fake reference pulse) to Alice. But in order to introduce frequency shift to the fake signal states, Eve has shifted

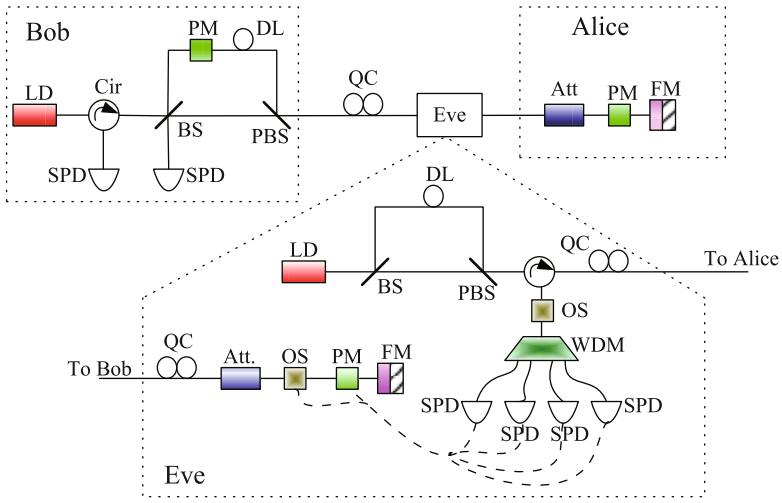

Fig. 10 A schematic diagram of the frequency shift attack. DL: Delay line; SPD: Single photon detector. WDM: Wavelength division multiplexer; OS: Optical switch; other abbreviations are the same as those in Fig. 1. Reproduced from Ref. [64].

the time difference of the fake signal pulse and the fake reference pulse by the delay line (DL). Then Alice attenuates the fake pulses to single-photon level, and sends them back to Eve. Eve uses an optical switch (OS) to block the reference pulses and a wavelength division multiplexer (WDM) to distinguish the four fake signal states and detects them by single photon detector (SPD) respectively. If Eve's SPDs have detected a single photon with frequency ν_n, she modulates the signal pulse from Bob with phase φ_n. Otherwise, she blocks the pulse by an OS and resends a vacuum state to Bob.

Usually, the spectrum of a light pulse with a finite line width can be treated as Gaussian type. Thus the spectrums of these signal states can be written as

$$f_n(\nu) = \frac{1}{\sqrt{2\pi}\sigma} \mathrm{e}^{-\frac{(\nu_n-\nu)^2}{2\sigma^2}} \tag{23}$$

where ν_n is the central frequency of each signal state. If we have known the 3dB line width of the light pulses $\delta\nu$, the standard deviation σ can be determined as follows

$$\sigma = \frac{\delta\nu}{2\sqrt{2\ln 2}} \approx 0.425\delta\nu \tag{24}$$

Based on Eq. (23), the four signal states can be distinguished by WDM with a suitable threshold coefficient. For example, Eve can set that each port of the WDM exports photons with frequency located in range of $\nu_n \pm \alpha_{th}\Delta\nu$, where α_{th} is the threshold coefficient for frequency selection. Then she can judge which phase has been encoded to the photon by Alice when corresponding SPD clicks. However, considering the characteristic of Gaussian wavepacket, Eve can never distinguish the four signal states without error, since overlapped frequency will always exist for different signal states, which will introduce an additional QBER to Bob's raw key. Note that the probability that a signal pulse is encoded with phase φ_i while Eve judges it as φ_j is given by

$$P_{i|j} = \int_{\nu_0+j\Delta\nu-\alpha_{th}\Delta\nu}^{\nu_0+j\Delta\nu+\alpha_{th}\Delta\nu} f_i(\nu)\mathrm{d}\nu \tag{25}$$

Thus the additional QBER introduced by Eve can be given by

$$QBER = \frac{\frac{3}{4}P_{1|0} + P_{2|0} + \frac{1}{4}P_{3|0}}{P_{0|0} + \frac{6}{4}P_{1|0} + P_{2|0} + \frac{1}{2}P_{3|0}} \tag{26}$$

Obviously, with a certain α_{th}, the QBER introduced by Eve is determined by $\delta\nu$ and $\Delta\nu$, specially, it increases with $\delta\nu/\Delta\nu$. Therefore, to reduce the QBER introduced by Eve, narrow line width is required for the light pulses sent by Eve.

As a matter of fact, not only narrow line width but also narrow pulse width are required for Eve's light pulses. In order to guarantee that the whole EO effect of all photons is carried out at the rising edge of phase modulation voltage, the pulse width of the light (δt) and the rising edge of phase modulation voltage (Δt) should satisfy $\Delta t - \tau \gg \delta t$, where τ is the duration of EO effect happening in the $LiNbO_3$ waveguide.

Fortunately, when Eve use gate-mode SPDs with gate width $\Delta t - \tau$ and carefully synchronize them to detect only those photons whose EO effect is carried out completely at the rising edge of phase modulation voltage, the requirement of narrow pulse width is unessential. Thus Eve can set

$$\Delta t - \tau = \beta_{th}\delta t \tag{27}$$

where β_{th} is the pulse width setting coefficient.

However, if the pulse width is limited, the bandwidth is finite, which denotes that Eve cannot simultaneously set the line width and the pulse width arbitrarily. When considering transform limited laser pulse (the best choice for Eve), we have time-bandwidth product (TBP) $\delta t \delta \nu = const \equiv q$ (where $q = 0.4412$ for transform limited Gauss pulse). Considering Eq. (26), Eq. (27) and $\Delta\nu = \frac{1}{4\Delta t}$, we get

$$\delta\nu/\Delta\nu = \frac{4q\beta_{th}}{1-\tau/\Delta t} \tag{28}$$

Figure 11 shows the QBER introduced by our attack changes with α_{th} and β_{th}, using Eq. (26) and Eq. (28). Obviously, the smaller the threshold coefficient α_{th} and β_{th} set by Eve, the lower the QBER will be. Thus Eve can reduce QBER introduced by her attack by decreasing the threshold coefficient α_{th} and β_{th}. Of course, the lower α_{th} and β_{th} are, the smaller the probability that Eve obtains a useful detection, which will lower the transmittance of the quantum channel. However, if the optical losses of Eve's receiver are small and can be neglected and detection efficiencies of Eve's SPDs are unity, Eve can set appropriate β_{th} and α_{th} to get a QBER always lower than 0.1% for a quantum channel longer than 5 km, which is undetectable compared with the QBER caused by the dark count of Bob's SPDs. That is, Eve can perform the FS attack against "*plug-and-play*" QKD systems to get full information without introducing detectable QBER.

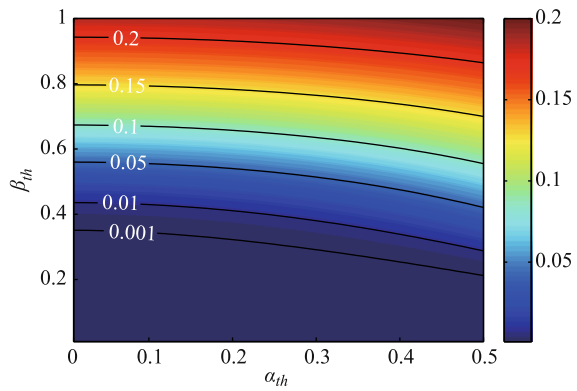

Fig. 11 The QBER introduced by Eve changing with α_{th} and β_{th} based on Eq. (26) and Eq. (28). Here we set the rise time Δt is 6 ns due to the experimental result of [37], and $\tau = \frac{L_{EO}}{c/n_L} = 0.2508$ ns since L_{EO} is about 35 mm in current PM with low half-wave voltage, $c = 3 \times 10^8$ m/s, and $n_L = 2.15$. Reproduced from Ref. [64].

6 Single photon detection attack

As an alternative scheme of the discrete variable QKD (DV-QKD) which has been demonstrated with high repetition rate and long distance, the continuous variable QKD (CV-QKD) is proposed and demonstrated [46–48] which has two advantages: the source is very easy to make, and the efficiency of homodyne detector is very high.

In view of the experimental side, the scheme that application of the homodyne detection on the phase coding four-state protocol [27, 82–84] provides the simplest CV-QKD scheme. Although this scheme is secure for the ideal system [84], there exists inherent loss in the QKD system, and the single photon detection (SPD) attack proposed by our group [44] show that it will not only raise the inherent QBER of system but also compromise the security of final key.

The CV-QKD protocol runs as follows [79]: Alice randomly sends one of the four coherent states $\{|\alpha e^{ik\pi/2}\rangle\}$ to Bob, here $k = 0, 1, 2, 3$ and α is positive real number. The coherent state is the eigenstate of the annihilation operator $\hat{a}$ of the light field. Then Bob randomly measures one of the two quadratures $\{\hat{x}_1, \hat{x}_2\}$. Here, $\hat{x}_1 + i\hat{x}_2 = \hat{a}$, thus $[\hat{x}_1, \hat{x}_2] = i/2$. After the communication, Alice announces the basis used by her, when Bob uses the correct-basis, they keep the pulse, otherwise, they discard the pulse. Here we say a pulse is correct-basis means that Bob measures $\hat{x}_1$ when Alice sends $|\pm\alpha\rangle$ and Bob measures $\hat{x}_2$ when Alice sends $|\pm i\alpha\rangle$. For all the correct-basis pulses, Bob sets two threshold values $x_+ > 0$ and $x_- < 0$ to judge the bit value of Alice. In the symmetric case, he can set $x_+ = -x_- = x_0$. We assume Alice regards $\{|\alpha\rangle, |i\alpha\rangle\}$ as bit 0 and $\{|-\alpha\rangle, |-i\alpha\rangle\}$ as bit 1. Thus when Bob measures $x > x_0$, he sets his bit is 0, when $x < -x_0$, he sets his bit is 1, otherwise, he has an inconclusive result.

The simple diagram of the experimental arrangement is shown in Fig. 12(a). And it is easy to check that the probability that Bob obtains a conclusive result is given by

$$P_{\text{post}}^{\text{absence}} = \frac{1}{2}\{erfc[\sqrt{2}(x_0 + \sqrt{\eta\mu_a})] + erfc[\sqrt{2}(x_0 - \sqrt{\eta\mu_a})]\} \tag{29}$$

where $erfc(x)$ is the error function. Therefore, the inherent QBER of Bob, in the absence of Eve, is given by

$$E_{\text{Bob}}^{\text{absence}} = \frac{1}{2P_{\text{post}}^{\text{absence}}} erfc[\sqrt{2}(x_0 + \sqrt{\eta\mu_a})] \tag{30}$$

Eq. (30) shows clearly that the inherent QBER of system is determined by x_0, μ_a and η. Although Alice can choose x_0 and μ_a carefully to ensure that the system provides higher security, the loss of channel and homodyne detection is unavoidable. The QBER for different communication distance is shown in Fig. 13. It shows clearly that the loss of channel raise the inherent QBER

of system quickly. Therefore, it may give some space to hide the existence of Eve. In fact, in next section, we will show that Eve can break the security of system in some parameter regime.

The experimental arrangement of Eve is shown in Fig. 12(b). Eve first intercepts the pulse from Alice, then she randomly and equally modulates the local pulse with one of two phase (0 and $\pi/2$). Then local pulse and signal

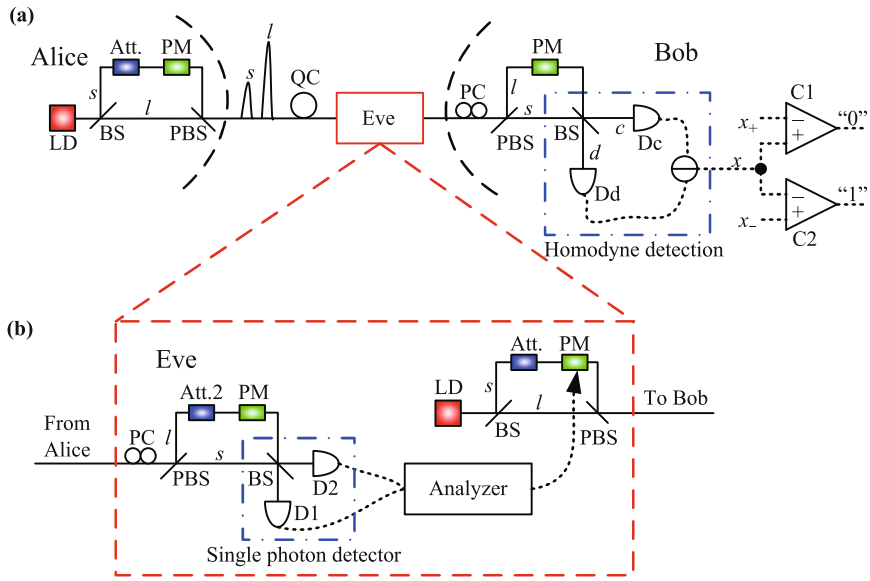

Fig. 12 The simple diagram of quantum cryptosystem with pulsed homodyne detector and Eve's experimental arrangement. x_+ and x_- are two threshold values set by Bob to judge the bit value of Alice. Generally speaking, he can set $x_+ = -x_- = x_0$. **(a)** shows the general cryptosystem. **(b)** shows Eve's experimental arrangement. Eve intercepts the pulse from Alice and sends a faked pulse to Bob according to her measurement results. Reproduced from Ref. [65].

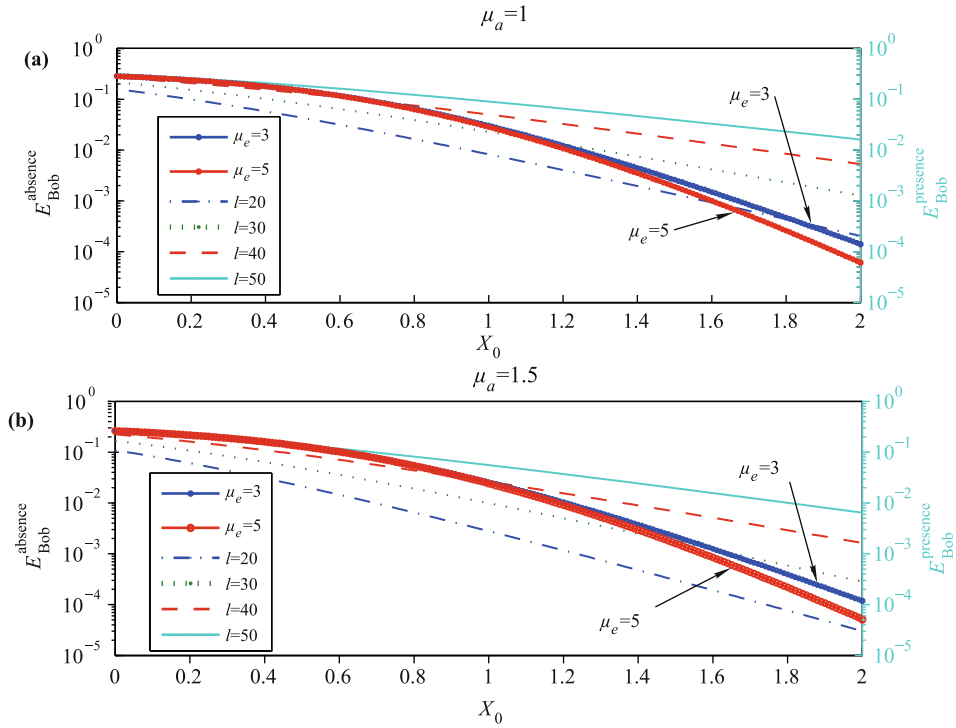

Fig. 13 The bit error rate of Bob changes with the threshold value set by Bob. The dashed lines are the QBER in the absence of Eve for different communication distance. The solid lines are the QBER in the presence of Eve. μ_e is the intensity of pulse sent by Eve. l is the distance of channel whose unit is km. We assume the channel between Alice and Bob is fiber, thus $\eta_c = 10^{-al/10}$ ($a = 0.21$ dB/km is the typical loss of fiber). In the simulations, we set $\eta_{Bob} = 0.6636$ according to the experimental result of Ref. [79]. At the same time, we assume the SPD of Eve is perfect, which means $Y_0 = 0$ and $\epsilon = 1$. Reproduced from Ref. [65].

pulse will interfere at the BS and be detected by two SPDs. Note that the intensity of local pulse is much larger than that of signal pulse, thus Eve should attenuate the intensity of local pulse to maximize the visibility of interference. If Eve obtains a valid result, she resends a faked state to Bob according to her measurement result, for example, if Eve modulates 0, she resends $|\alpha\rangle$ (or $|-\alpha\rangle$) to Bob when D1 (or D2) clicks, if Eve modulates $\pi/2$, she resends $|\mathrm{i}\alpha\rangle$ (or $|-\mathrm{i}\alpha\rangle$) to Bob when D1 (or D2) clicks. Here valid result means that only one SPD clicks. If both of D1 and D2 click or neither of them click, Eve resends a vacuum state to Bob.

Obviously, Eve's attack will disturb the original state sent by Alice. If we take the state $|\alpha\rangle$ as example, the state in the presence of Eve will be transformed as

$$\begin{aligned}|\alpha\rangle\langle\alpha| \to \rho' = {} & P_0^{\mathrm{co}}|\alpha_e\rangle\langle\alpha_e| + P_1^{\mathrm{co}}|-\alpha_e\rangle\langle-\alpha_e| \\ & + P_0^{\mathrm{inco}}|\mathrm{i}\alpha_e\rangle\langle\mathrm{i}\alpha_e| + P_1^{\mathrm{inco}}|-\mathrm{i}\alpha_e\rangle\langle-\mathrm{i}\alpha_e| \\ & + P_{\mathrm{vac}}|0\rangle\langle 0| \end{aligned} \tag{31}$$

where $|\alpha_e|^2$ is the intensity of pulse sent by Eve, and P_0^{co} and P_1^{co} (P_0^{inco} and P_1^{inco}) are the probabilities that Eve resends $|\alpha\rangle$ and $|-\alpha\rangle$ ($|\mathrm{i}\alpha\rangle$ and $|-\mathrm{i}\alpha\rangle$), P_{vac} is the probability that Eve resends a vacuum state to Bob. Thus, as a result, the probability that Bob obtains conclusive result in the presence of Eve is given by

$$\begin{aligned} P_{\mathrm{post}}^{\mathrm{presence}} = {} & \frac{1}{2}(P_0^{\mathrm{co}} + P_1^{\mathrm{co}})\{erfc[\sqrt{2}(x_0 + \sqrt{\mu_e})] \\ & + erfc[\sqrt{2}(x_0 - \sqrt{\mu_e})]\} \\ & + (P_0^{\mathrm{inco}} + P_1^{\mathrm{inco}} + P_{\mathrm{vac}})erfc(\sqrt{2}x_0) \end{aligned} \tag{32}$$

where we set $\mu_e = \eta_{\mathrm{Bob}}|\alpha_e|^2$, since Eve can send a strong pulse to compensate the loss of Bob's optical setups and the efficiency of homodyne detector. And the QBER in the presence of Eve can be written as

$$\begin{aligned} E_{\mathrm{Bob}}^{\mathrm{presence}} = {} & \frac{1}{2P_{\mathrm{post}}^{\mathrm{presence}}}\{P_0^{\mathrm{co}} erfc[\sqrt{2}(x_0 + \sqrt{\mu_e})] \\ & + P_1^{\mathrm{co}} erfc[\sqrt{2}(x_0 - \sqrt{\mu_e})] \\ & + (P_0^{\mathrm{inco}} + P_1^{\mathrm{inco}} + P_{\mathrm{vac}})erfc(\sqrt{2}x_0)\} \end{aligned} \tag{33}$$

The QBER in the presence of Eve is shown in Fig. 13. It shows clearly that the QBER induced by Eve can be lower than the QBER induced by the loss of system in some parameter regime, in which the security of final key will be compromised. In other words, the legitimate parties must set their experimental parameters carefully to remove the existence of Eve.

Here we review the SPD attack proposed by our group. According to the analysis described above, it is known that the security of final key will be compromised in some parameter regimes, when our attack is taken into account. Our attack can be classified as an intercept-and-resend attack, but Eve uses SPDs to read out Alice's information, instead of using a homodyne detection system. In fact, our attack can perform better than the simultaneous measurement attack (SMA) proposed by Namiki and Hirano in Ref. [84], in which Eve equivalently splits the signal pulse into two parts with a 50:50 beam splitter, and measures $\widehat{x}_1$ of one part and $\widehat{x}_2$ of the other part. Finally, we remark that Bob can discover the existence of Eve by reconstructing the probability density of his measurement result. The detail information about the comparing and the countermeasure are given in Ref. [65].

7 Conclusions and perspectives

Although QKD is unconditionally secure for perfect systems, there exist some imperfections for the practical optical and electrical setups, which can be exploited by Eve to partially or totally steal the secret key. Thus the security of QKD systems must be carefully reexamined, otherwise its security will be compromised. There exist two approaches to implement this task. First, the legitimate parties do research on the QKD system and discover the potential loophole, then they modify the system to ensure that Eve cannot exploit this loophole. Second, the legitimate parties replace the BB84 protocol with the device-independent QKD (DI-QKD) protocol, in which the detailed information about the setups of Alice and Bob is not needed. However, the *full* DI-QKD is impractical within current technology. Even if MDI-QKD has been implemented in experiments, it requires the source of Alice and Bob is perfect. Thus the first approach is still an important way to guarantee the security of QKD system within current technology.

In this article, we review five quantum attack schemes proposed by our group, such as passive faraday mirror attack, partially random phase attack, wavelength-selected photon-number-splitting attack, frequency shift attack, and single photon detection attack. All of these attacks show that Eve can exploit the imperfection of systems to spy parts of secret key without being discovered by the legitimate parties. Thus Alice and Bob must carefully modify their system to monitor the existence of Eve, and the countermeasures of these attacks are also discussed in our paper [61–65]. The goal of those attack proposed in our group is to remind people of designing more secure QKD protocols.

Acknowledgements This work was supported by the National Natural Science Foundation of China under Grant No. 61072071. L. M. Liang was supported by Program for NCET. S. H. Sun was

supported by the National Natural Science Foundation of China under Grant No. 11304391.

References and notes

1. C. H. Bennett and G. Brassard, Quantum Cryptography: Public key distribution and coin tossing, in: *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York), 1984, pp 175–179
2. H. K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science*, 1999, 283(5410): 2050
3. P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, *Phys. Rev. Lett.*, 2000, 85(2): 441
4. D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, *Quant. Inf. Comput.*, 2004, 4(5): 325
5. H. Inamori, N. Lütkenhaus, and D. Mayers, Unconditional security of practical quantum key distribution, *Eur. Phys. J. D*, 2007, 41(3): 599
6. M. Davanco, J. R. Ong, A. B. Shehata, A. Tosi, I. Agha, S. Assefa, F. Xia, W. M. J. Green, S. Mookherjea, and K. Srinivasan, Telecommunications-band heralded single photons from a silicon nanophotonic chip, *Appl. Phys. Lett.*, 2012, 100(26): 261104
7. J. S. Neergaard-Nielsen, B. M. Nielsen, H. Takahashi, A. I. Vistnes, and E. S. Polzik, High purity bright single photon source, *Opt. Express*, 2007, 15(13): 7940
8. F. Hargart, C. A. Kessler, T. Schwarzbäck, E. Koroknay, S. Weidenfeld, M. Jetter, and P. Michler, Electrically driven quantum dot single-photon source at 2 GHz excitation repetition rate with ultra-low emission time jitter, *Appl. Phys. Lett.*, 2013, 102(1): 011126
9. M. M. Müller, A. Kölle, R. Löw, T. Pfau, T. Calarco, and S. Montangero, Room-temperature Rydberg single-photon source, *Phys. Rev. A*, 2013, 87(5): 053412
10. S. Deshpande and P. Bhattacharya, An electrically driven quantum dot-in-nanowire visible single photon source operating up to 150 K, *Appl. Phys. Lett.*, 2013, 103(24): 241117
11. A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.*, 1991, 67(6): 661
12. F. G. Deng and G. L. Long, Secure direct communication with a quantum one-time pad, *Phys. Rev. A*, 2004, 69(5): 052319
13. G. L. Long, F. G. Deng, C. Wang, X. H. Li, K. Wen, and W. Y. Wang, Quantum secure direct communication and deterministic secure quantum communication, *Front. Phys. China*, 2007, 2(3): 251
14. F. G. Deng and G. L. Long, Controlled order rearrangement encryption for quantum key distribution, *Phys. Rev. A*, 2003, 68(4): 042315
15. B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, *Phys. Rev. A*, 1995, 51(3): 1863
16. G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Limitations on practical quantum cryptography, *Phys. Rev. Lett.*, 2000, 85(6): 1330
17. N. Lütkenhaus and M. Jahma, Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack, *New J. Phys.*, 2002, 4: 44
18. W. T. Liu, S. H. Sun, L. M. Liang, and J. M. Yuan, Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution, *Phys. Rev. A*, 2011, 83(4): 042326
19. W. Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, *Phys. Rev. Lett.*, 2003, 91(5): 057901
20. H. K. Lo, X. F. Ma, and K. Chen, Decoy state quantum key distribution, *Phys. Rev. Lett.*, 2005, 94(23): 230504
21. X. F. Ma, B. Qi, Y. Zhao, and H. K. Lo, Practical decoy state for quantum key distribution, *Phys. Rev. A*, 2005, 72(1): 012326
22. X. B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, *Phys. Rev. Lett.*, 2005, 94(23): 230503
23. C. Z. Peng, J. Zhang, D. Yang, W. B. Gao, H. X. Ma, H. Yin, H. P. Zeng, T. Yang, X. B. Wang, and J. W. Pan, Experimental long-distance decoy-state quantum key distribution based on polarization encoding, *Phys. Rev. Lett.*, 2007, 98(1): 010505
24. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. Rarity, A. Zeilinger, and H. Weinfurter, Experimental demonstration of free-space decoy-state quantum key distribution over 144 km, *Phys. Rev. Lett.*, 2007, 98(1): 010504
25. D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. Lita, S. Nam, and J. Nordholt, Long-distance decoy-state quantum key distribution in optical fiber, *Phys. Rev. Lett.*, 2007, 98(1): 010503
26. Y. Zhao, B. Qi, X. F. Ma, H. K. Lo, and L. Qian, Experimental quantum key distribution with decoy states, *Phys. Rev. Lett.*, 2006, 96(7): 070502
27. 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, Decoy-state quantum key distribution with polarized photons over 200 km, *Opt. Express*, 2010, 18(8): 8587
28. Y. Zhao, B. Qi, and H. K. Lo, Quantum key distribution with an unknown and untrusted source, *Phys. Rev. A*, 2008, 77(5): 052327
29. X. Peng, H. Jiang, B. J. Xu, X. F. Ma, and H. Guo, Experimental quantum-key distribution with an untrusted source, *Opt. Lett.*, 2008, 33(18): 2077

30. B. J. Xu, X. Peng, and H. Guo, Passive scheme with a photon-number-resolving detector for monitoring the untrusted source in a plug-and-play quantum-key-distribution system, *Phys. Rev. A*, 2010, 82(4): 042301
31. X. B. Wang, Decoy-state quantum key distribution with large random errors of light intensity, *Phys. Rev. A*, 2007, 75(5): 052301
32. X. B. Wang, C. Z. Peng, and J. W. Pan, Simple protocol for secure decoy-state quantum key distribution with a loosely controlled source, *Appl. Phys. Lett.*, 2007, 90(3): 031110
33. X. B. Wang, L. Yang, C. Z. Peng, and J. W. Pan, Decoy-state quantum key distribution with both source errors and statistical fluctuations, *New J. Phys.*, 2009, 11(7): 075006
34. X. B. Wang, C. Z. Peng, J. Zhang, L. Yang, and J. W. Pen, General theory of decoy-state quantum cryptography with source errors, *Phys. Rev. A*, 2008, 77(4): 042311
35. S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, Information leakage via side channels in freespace BB84 quantum cryptography, *New J. Phys.*, 2009, 11(6): 065001
36. C. H. F. Fung, B. Qi, K. Tamaki, and H. K. Lo, Phase-remapping attack in practical quantum-key-distribution systems, *Phys. Rev. A*, 2007, 75(3): 032314
37. F. H. Xu, B. Qi, and H. K. Lo, Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, *New J. Phys.*, 2010, 12(11): 113026
38. H. W. Li, S. Wang, J. Z. Huang, W. Chen, Z. Q. Yin, F. Y. Li, Z. Zhou, D. Liu, Y. Zhang, G. C. Guo, W. S. Bao, and Z. F. Han, Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multi-wavelength sources, *Phys. Rev. A*, 2011, 84(6): 062308
39. Y. Zhao, C. H. Fung, B. Qi, C. Chen, and H. K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, *Phys. Rev. A*, 2008, 78(4): 042333
40. V. Makarov, A. Anisimov, and J. Skaar, Effects of detector efficiency mismatch on security of quantum cryptosystems, *Phys. Rev. A*, 2006, 74(2): 022313
41. V. Makarov and J. Skaar, Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols, *Quant. Inf. Comput.*, 2008, 8(6–7): 0622
42. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, *Nat. Photonics*, 2010, 4(10): 686
43. V. Makarov, Controlling passively quenched single photon detectors by bright light, *New J. Phys.*, 2009, 11(6): 065003
44. N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Device calibration impacts security of quantum key distribution, *Phys. Rev. Lett.*, 2011, 107(11): 110501
45. I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, *Nat. Commun.*, 2011, 2: 349
46. C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, *Rev. Mod. Phys.*, 2012, 84(2): 621
47. B. Qi, L. L. Huang, L. Qian, and H. K. Lo, Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers, *Phys. Rev. A*, 2007, 76(5): 052323
48. Z. Zhang and P. L. Voss, Security of a discretely signaled continuous variable quantum key distribution protocol for high rate systems, *Opt. Express*, 2009, 17(14): 12090
49. X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol, *Phys. Rev. A*, 2013, 87(5): 052309
50. J. Z. Huang, C. Weedbrook, Z. Q. Yin, S. Wang, H. W. Li, W. Chen, G. C. Guo, and Z. F. Han, Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack, *Phys. Rev. A*, 2013, 87(6): 062329
51. X. C. Ma, S. H. Sun, M. S. Jiang, and L. M. Liang, Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems, *Phys. Rev. A*, 2013, 88(2): 022339
52. A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-independent security of quantum cryptography against collective attacks, *Phys. Rev. Lett.*, 2007, 98(23): 230501
53. S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, *New J. Phys.*, 2009, 11(4): 045021
54. H. K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, *Phys. Rev. Lett.*, 2012, 108(13): 130503
55. K. Tamaki, H.K. Lo, C.H. F. Fung, and B. Qi, Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw, *Phys. Rev. A*, 2012, 85(4): 042307
56. X. F. Ma and M. Razavi, Alternative schemes for measurement-device-independent quantum key distribution, *Phys. Rev. A*, 2012, 86(6): 062319
57. S. H. Sun, M. Gao, C. Y. Li, and L. M. Liang, Practical decoy-state measurement-device-independent quantum key distribution, *Phys. Rev. A*, 2013, 87(5): 052329
58. Y. Liu, T. Y. Chen, L. J. Wang, H. Liang, G. L. Shentu, J. Wang, K. Cui, H.L. Yin, N.L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.Z. Peng, Q. Zhang, and J.W. Pan, Experimental measurement-device-independent quantum key distribution, *Phys. Rev. Lett.*, 2013, 111(13): 130502
59. A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks, *Phys. Rev. Lett.*, 2013, 111(13): 130501

60. Z. Y. Tang, Z. F. Liao, F. H. Xu, B. Qi, L. Qian, and H. K. Lo, Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution, arXiv: 1306.6134, 2013
61. S. H. Sun, M. S. Jiang, and L. M. Liang, Passive Faraday-mirror attack in a practical two-way quantum-key-distribution system, *Phys. Rev. A*, 2011, 83(6): 062331
62. S. H. Sun, M. Gao, M. S. Jiang, C. Y. Li, and L. M. Liang, Partially random phase attack to the practical two-way quantum-key-distribution system, *Phys. Rev. A*, 2012, 85(3): 032304
63. M. S. Jiang, S. H. Sun, C. Y. Li, and L. M. Liang, Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states, *Phys. Rev. A*, 2012, 86(3): 032310
64. M. S. Jiang, S. H. Sun, C. Y. Li, and L. M. Liang, Frequency shift attack on "plug-and-play" quantum key distribution systems, *J. Mod. Opt.*, 2014, 61(2): 147
65. S. H. Sun, M. S. Jiang, and L. M. Liang, Single-photon-detection attack on the phase-coding continuous-variable quantum cryptography, *Phys. Rev. A*, 2012, 86(1): 012305
66. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "Plug and play" systems for quantum cryptography, *Appl. Phys. Lett.*, 1997, 70(7): 793
67. http://www.newport.com/Fiber-Optic-Faraday-Rotator-Mirrors/835750/1033/catalog.aspx
68. http://www.generalphotonics.com
69. H. F. Chau, Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate, *Phys. Rev. A*, 2002, 66(6): 060302 (R)
70. K. S. Ranade and G. Alber, Asymptotic correctability of Bell-diagonal quantum states and maximum tolerable bit-error rates, *J. Phys. A*, 2006, 39(7): 1701
71. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.*, 2009, 81(3): 1301
72. H. K. Lo and J. Preskill, Security of quantum key distribution using weak coherent states with Nonrandom phases, *Quant. Inf. Comput.*, 2007, 5(6): 431
73. Y. Zhao, B. Qi, and H. K. Lo, Experimental quantum key distribution with active phase randomization, *Appl. Phys. Lett.*, 2007, 90(4): 044106
74. S. H. Sun and L. M. Liang, Experimental demonstration of an active phase randomization and monitor module for quantum key distribution, *Appl. Phys. Lett.*, 2012, 101(7): 071107
75. http://www.idquantique.com/scientific-instrumentation/clavis2-qkd-platform.html
76. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, et al., Field test of quantum key distribution in the Tokyo QKD Network, *Opt. Express*, 2011, 19(11): 10387
77. P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, Long-distance quantum key distribution in optical fibre, *New J. Phys.*, 2006, 8(9): 193
78. C. Gobby, Z. L. Yuan, and A. J. Shields, Quantum key distribution over 122 km of standard telecom fiber, *Appl. Phys. Lett.*, 2004, 84(19): 3762
79. T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Quantum cryptography using pulsed homodyne detection, *Phys. Rev. A*, 2003, 68(4): 042331
80. S. Braunstein and P. van Loock, Quantum information with continuous variables, *Rev. Mod. Phys.*, 2005, 77(2): 513
81. http://www.magiqtech.com
82. D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, High rate, long-distance quantum key distribution over 250 km of ultralow loss fibres, *New J. Phys.*, 2009, 11(7): 075003
83. P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, Quantum key distribution and 1 Gbps data encryption over a single fibre, *New J. Phys.*, 2010, 12(6): 063027
84. R. Namiki and T. Hirano, Security of quantum cryptography using balanced homodyne detection, *Phys. Rev. A*, 2003, 67(2): 022308