Partially random phase attack to the practical two-way quantum-key-distribution system

Shi-Hai Sun, Ming Gao, Mu-Sheng Jiang, Chun-Yan Li, and Lin-Mei Liang[*]

Department of Physics, National University of Defense Technology, Changsha 410073, People's Republic of China

(Received 30 November 2011; published 7 March 2012)

Phase randomization is a very important assumption in the Bennett-Brassard 1984 quantum key distribution (QKD) system with a weak coherent source. Thus an active phase modulator is needed to randomize the phase of source. However, it is hard to check whether the phase of source is randomized totally or not in practical QKD systems. In this paper a partially random phase attack is proposed to exploit this imperfection. Our analysis shows that Eve can break the security of a two-way QKD system by using our attack, even if an active phase randomization is adopted by Alice. Furthermore, the numerical simulation shows that in some parameter regimes, our attack is immune to the one-decoy-state method.

DOI: 10.1103/PhysRevA.85.032304 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum key distribution (QKD) [1] admits two remote parties, known as Alice and Bob, to establish an unconditional secret key; even the eavesdropper (Eve) has unlimited power admitted by the quantum mechanics. The unconditional security of QKD has been proved in theory for both the ideal system [2,3] and the practical system [4,5] based on some assumptions. However, the practical QKD system is imperfect. Strictly speaking, any deviation between the standard security analysis and the practical QKD system can be exploited by Eve to attack the practical system [6–12]. Therefore, in order to guarantee the unconditional security of the final key generated by the practical system, the legitimate parties must survey the practical QKD system carefully and close these loopholes.

In the standard security analysis for the Bennett-Brassard 1984 (BB84) QKD system with a weak coherent source (WCS), an important assumption is that the phase of source has been randomized totally. Thus, in the view of Eve, the state sent by Alice is a mixed state of all number states. However, in a practical QKD system, the phase information of source might be accessible to Eve [13]. In order to remove the phase randomization assumption from the standard security analysis, Lo and Preskill have proved the security of BB84 protocol using the WCS with nonrandom phase. But their proof is at the price of the secret key rate and the maximal security distance is very short [13]. Thus the best choice for the legitimate parties is to actively randomize the WCS phase, which can be implemented by modulating a totally random phase $\theta \in [0,2\pi]$ with a phase modulator [14]. In fact, in most practical QKD systems [15–18], including the commercial system produced by Id Quantique [15], the legitimate parties assume the phase of source has been randomized totally, and thus they use the Gottensman-Lo-Lütkenhaus-Preskill (GLLP) formula [4] but not the results of Ref. [13] to estimate the key rate. Specifically, the phase randomization assumption is the base of the decoy-state method [19–22], which is often used to defeat the photon number splitting (PNS) attack [23,24]. Thus, in the QKD system with decoy-state method, only the GLLP formula can be used.

However, in practical situations, it is a hard task for the legitimate parties to check whether the phase of source has been randomized totally or not [25]. In the latter, we will show that even if an active *phase modulator* is used by the legitimate parties to randomize the phase of source, Eve can change the range of random phase by using the imperfection of the phase modulator so that it is just partially randomized. Here *partially random* means that the range of random phase modulated by Alice is smaller than 2π. In other words, the random phase $\theta \in [0,\delta]$ and $\delta < 2\pi$. Furthermore, we note that in most of the practical system [15–18], no active setup is used to randomize the phase of source. We think there may be two reasons: (1) When Alice actively randomizes the source, an additional active setup is needed which will increase the complexity of the QKD system. (2) More importantly, within the best of our knowledge, until now there is not an effective attack strategy to exploit the phase information of WCS. In other words, Eve does not know how to spy the secret key, even if the source is not randomized or just partially randomized.

In this paper, we propose a partially random phase (PRP) attack to break the security of the practical two-way QKD system using WCS. Then a simple intercept-and-resend attack strategy and experimental arrangement within current technology are proposed to spy the secret key. Our analysis shows that 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 [19–22] which is often used to defeat the PNS attack [23,24]. Therefore, the legitimate parties should consider our attack carefully when they use the WCS to implement the BB84 protocol. However, note that we only claim that our attack is immune to the one-decoy-state method in some parameter regimes, but we do not claim that our attack is completely immune to the decoy-state method. In fact, our attack can be defeated by the two-decoy-state (weak + vacuum) method [21,22], since the vacuum state is used to estimate the gain and error rate of the background.

We note that in Ref. [13], Lo and Preskill have proposed a simple attack to exploit the nonrandom phase of source. However, our attack performs better than their attack at least

[*] nmliang@nudt.edu.cn

in two aspects. First, in their attack Eve performs the positive operator valued measure (POVM) belonging to the photon number state space to distinguish the key bit, which cannot be implemented within current technology. Our attack needs only a homodyne detector, which can be implemented within current technology. Second, in their attack Eve needs to know the exact phase of source, which corresponds to the case that the source is not randomized. But our attack is valid as long as the source is partially randomized. Therefore, the legitimate parties do not need to consider their attack, especially in practical situations, but they must consider our attack and monitor their system carefully.

The paper is organized as follows: In Sec. II we introduce how to exploit the imperfection of a partially random phase to break the security of the cryptosystem. In Sec. III we introduce an intercept-and-resend attack with our PRP attack and then analyze the error rate induced by our attack. In Sec. IV we show that our attack is immune to the one-decoy-state method which can be used to defeat the PNS attack. In Sec. V we provide some discussion regarding our attack. Finally, in Sec. VI we give a brief summary of this paper.

II. PRP ATTACK

In this section, we first introduce the *plug-and-play* QKD system briefly. Then we discuss how to exploit the partially random phase of source to spy the secret key.

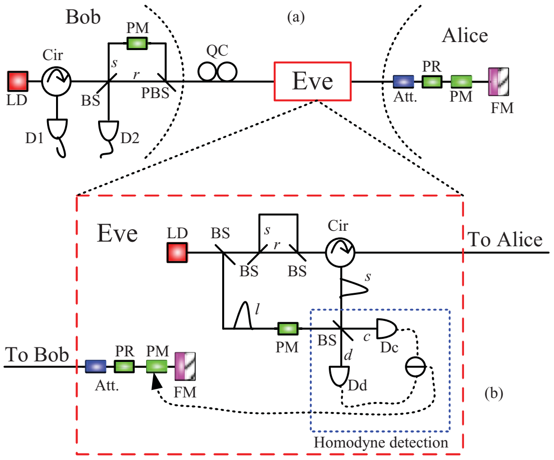

FIG. 1. (Color online) A simple diagram of the *Plug-and-Play* QKD system [26] and Eve's experimental arrangement. LD: laser diode; Cir: circulator; BS: 50:50 beam splitter; PBS: polarization beam splitter; Att., attenuator; PM: phase modulator; PR: phase randomizer; FM: Faraday mirror; QC: quantum channel; D1 and D2: single photon detectors (SPDs); Dc and Dd: photodiode. Note that in the commercial system of Id Quantique, there is not PR [15]. Part (a) shows the practical QKD system. Part (b) shows Eve's experimental arrangement. 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.

A. Plug-and-play system

A simple diagram of a *plug-and-play* QKD system [26] without Eve is shown in Fig. 1(a). A strong pulse sent by Bob's laser will be divided into two parties by a 50:50 beam splitter (BS), noted as a signal pulse (s) and reference pulse (r). When the two pulses arrive at Alice's zone, Alice encodes her information on the signal pulse by modulating a phase $\phi_k^a = k\pi/2, k = 0,1,2,3$. In order to ensure the global phase of pulse is totally random, Alice modulates a random phase $\theta \in [0,\delta]$ on both s and r. Note that θ should be random on each pulse of the laser, but it must be the same for both s and r of each pulse. Then the two pulses will be attenuated to a single photon level and sent back to Bob. Thus the two outgoing pulses from Alice's zone can be written as

$$|\alpha e^{i(\theta+\theta')}\rangle_r |\alpha e^{i(\phi_k^a+\theta+\theta')}\rangle_s, \tag{1}$$

where θ' is the phase induced by the birefringence of fiber. α is real and $|\alpha|^2$ is the average photon number of s and r. Here we assume the Faraday mirror (FM) is perfect in the QKD system; thus the birefringence of fiber can be compensated successfully with a global phase θ'. Otherwise Eve can obtain more information by combining with the passive FM attack proposed by our group [12]. Note that θ' is a fixed value and can be compensated by Eve, and thus we assume $\theta' = 0$ in this paper. Therefore the practical state sent by Alice is given by

$$\rho = \int_0^\delta \frac{d\theta}{\delta} |\alpha e^{i(\phi_k^a+\theta)}\rangle\langle\alpha e^{i(\phi_k^a+\theta)}|, \tag{2}$$

where δ is range of random phase modulated by Alice. Here we assume θ follows the uniform distribution on $[0,\delta]$. For the three cases that the phase is nonrandomized, partially randomized, and totally randomized, $\delta = 0$, $0 < \delta < 2\pi$, and $\delta = 2\pi$, respectively. Note that in Eq. (2) we consider only the signal pulse and ignore the reference pulse, since only the signal pulse is modulated by Alice.

Here we remark that if Alice does not actively randomize the phase of source or she thinks that Eve may know the phase of source exactly, she must use the method given by Ref. [13] to estimate the key rate. However, the security analysis of Ref. [13] can only be used for short-distance quantum cryptography. Thus, generally speaking, Alice should use an active setup to randomize the phase of source in the long-distance quantum cryptography. However, in the practical QKD system, it is a hard task for the legitimate parties to check whether the phase is really totally randomized or not. In fact, if Alice and Bob do not check carefully that the phase is truly random, then the range of random phase can be controlled by Eve so that it is just partially randomized ($\delta < 2\pi$). For example, in the two-way QKD system, since the phase modulator has a finite response time, Eve can control the practical phase modulated on the pulse by shifting the arrival time of the signal pulse to the rising or falling edge of the phase modulator. It is known as a phase remapping attack, which was proposed by Fung *et al.* in theory [10] and then demonstrated by Xu *et al.* in experiment [11]. Thus the practical phase modulated on the source will be lower than the expected phase of Alice, if Eve shifts the arrival time of the pulse. For instance, Alice wants to modulate a random phase θ', but the practical phase modulated on the source is $\theta < \theta'$.

Therefore, in the practical QKD system, the range of random phase modulated by Alice can be controlled by Eve so that the pulse is just partially modulated ($\delta < 2\pi$).

B. PRP imperfection

We have shown that the random phase can be controlled by Eve so that it is just partially modulated. In the following, we will show how Eve can exploit this imperfection to spy the secret key.

Since Alice admits the pulse into and out of her zone in the two-way system, it is easy for Eve to set her experimental arrangement to load our attack, which is shown in Fig. 1(b). The strong pulse sent by Eve's laser will be divided into three parts by two BSs, a signal pulse (s), a reference pulse (r), and a local pulse (l). Then Eve sends s and r to Alice and keeps l in her own hand. When the pulse is modulated by Alice and resent back to Eve, Eve modulates l randomly with a phase $\phi_j^e = j\pi/2, j = 0,1$. Then s will interfere with l at the BS and be detected by two photodiodes (Dc and Dd).

Here Eve uses a homodyne detector to analyze Alice's information. The homodyne detection is a well-established quantitative method to measure the quadrature-amplitude operator of the signal field [27,28] or implement the continuous variable quantum cryptography [29,30]. A simple illustration of the homodyne detection is shown in Fig. 1(b). The signal pulse (s) and the local pulse (l) interfere at a 50:50 beam splitter. Then the two output modes of BS, c and d, will reach the two photodiodes, Dc and Dd, respectively. The measured output signal of homodyne detection is determined by the difference of Dc and Dd, which is given by [31]

$$i \propto \sqrt{n_l}\langle a_s e^{-i\phi'} + a_s^\dagger e^{i\phi'}\rangle \equiv \sqrt{2n_l}x, \tag{3}$$

where n_l is the average photon number of the local pulse, a_s is the annihilation operator of the signal pulse, and ϕ' is the difference of phase between the signal pulse and the local pulse. Here we assume the local pulse is a strong coherent state. x is known as the normalized quadrature amplitude of the signal. Generally speaking, x takes a random value for each pulse due to the quantum fluctuations. Theoretically, the probability of x is given by integrating the Wigner distribution [32], which is given by

$$P(x,\theta') = \int_{-\infty}^{\infty} W(x\cos\theta' - p\sin\theta', x\sin\theta' + p\cos\theta')dp, \tag{4}$$

where $W(q,p)$ is the Wigner function in $p-q$ space.

It is easy to check that when the signal pulse is a coherent state, the probability distribution of x is given by [31,33]

$$P(x,\phi,\theta) = \sqrt{\frac{2}{\pi\kappa^2}}\exp\{-2[x-\lambda\sqrt{\mu_s}\cos(\phi+\theta)]^2/\kappa^2\}, \tag{5}$$

where $\mu_s = |\alpha|^2$ is the average photon number of the signal pulse, $\phi = \phi_k^a - \phi_j^e$ is the difference of phase modulated by Eve and Alice, and $\theta \in [0,\delta]$ is the random phase modulated by Alice. λ and κ are two parameters that characterize the imperfection of homodyne detection [31,34]. When the homodyne is perfect, $\lambda = \kappa = 1$. According to Eq. (2), Eve has no prior information about θ, except that $\theta \in [0,\delta]$; thus Eq. (5) should be rewritten as

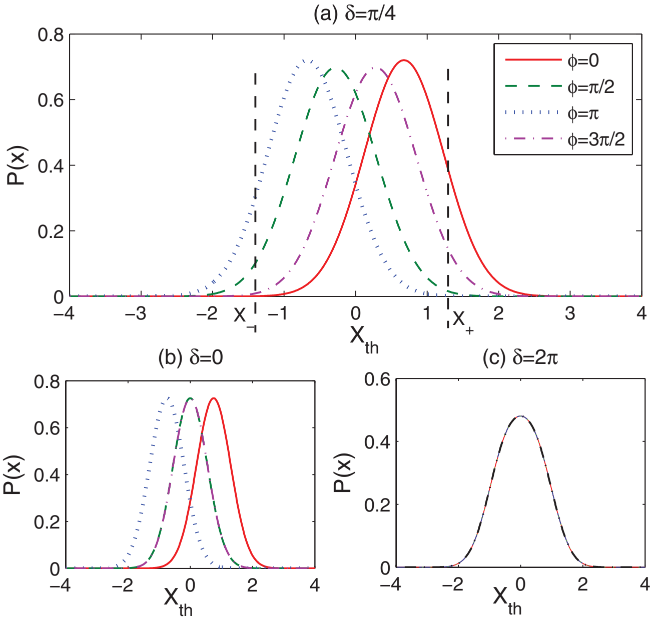

FIG. 2. (Color online) The theoretical probability distribution of the quadrature amplitude when the total phase shifts are 0, $\pi/2$, π, and $3\pi/2$. We show the three cases where the source has not been randomized ($\delta = 0$), is partially randomized ($\delta = \pi/4$), and totally randomized ($\delta = 2\pi$). Here we set $\lambda = 0.75$ and $\kappa = 1.1$ due to the experimental results of Ref. [31]. X_+ and X_- are two threshold values used to distinguish 0 and π from the set $\{0,\pi/2,\pi,3\pi/2\}$.

$$P(x,\phi) = \int_0^\delta \frac{d\theta}{\delta}\sqrt{\frac{2}{\pi\kappa^2}}\exp\{-2[x-\lambda\sqrt{\mu_s}\cos(\phi+\theta)]^2/\kappa^2\}. \tag{6}$$

Figure 2 shows the theoretical probability distribution of x when the total phase shifts ϕ are 0, $\pi/2$, π, and $3\pi/2$. It shows clearly that the measured result of the homodyne detection can be used to distinguish 0 and π by setting a suitable threshold value. For example, Eve can set two threshold values $X_+ \geqslant 0$ and $X_- \leqslant 0$. When the measured quadrature amplitude $x \geqslant X_+$, Eve can judge that $\phi = 0$; when $x \leqslant X_-$, Eve judges that $\phi = \pi$. But when $X_- < x < X_+$, Eve cannot give a judgment about the phase. Although Eve cannot distinguish the four phases deterministically, it is easy to see that the conditional probability that Eve will obtain a valid outcome given that $\phi = 0$ or $\phi = \pi$ can be much larger than that of $\phi = \pi/2$ and $\phi = 3\pi/2$. Here, a valid outcome means that the measured outcome x satisfies $x \geqslant X_+$ or $x \leqslant X_-$.

Obviously, the smaller the probability that Eve makes a wrong judgment, the larger μ_s is. Here, *wrong judgement* means Eve obtains X_+ (or X_-), but the state sent by Alice is not $\phi = 0$ (or $\phi = \pi$). In order to maximize Eve's information for a given system, we make two remarks about the optimal intensity of the signal pulse (μ_s) that is accessible for Eve.

Remark 1. Generally speaking, Alice will monitor the power of light coming into her zone; thus Eve should set the intensity of light sent to Alice carefully. However, note the fact that Alice does not monitor the intensity of s and r, respectively, in most practical QKD systems. Thus Eve needs only to ensure that the total of them entering Alice's zone, denoted as n_a^i, is unchanged but does not need to keep the intensities of both s and r the same as their expected values. In other words, Eve can change the proportion of average photon number between the signal pulse and reference pulse (denoted as n_s and n_r, respectively) but keeps $n_s + n_r = n_a^i$ constant. In the following, we let $n_s = \beta n_a^i$ and $n_r = (1-\beta)n_a^i$. Note that if Alice monitors the intensity of the signal pulse and reference pulse at the same time, Eve cannot change the proportion between n_s and n_r. Then Eve must keep the intensity of n_s and n_r unchanged, which means $\beta = 1/2$.

Remark 2. Note that only s will be modulated by Alice; thus Eve should increase the coefficient β to maximize her information. The maximal value of β that can be set by Eve, denoted as $\beta_{\max}$, depends on the way that Alice and Bob synchronize their clock in the practical QKD system. Generally speaking, there are two ways to synchronize the clock of Alice and Bob. One way is that Alice triggers her setups according to the arrival time of r. Thus $(1-\beta_{\max})n_a^i$ is the minimal intensity of r that can trigger Alice's setups, which depends on the efficiency of Alice's photodiode. The other way is that Alice synchronizes her clock with Bob according to another optical or electric signal, such as the wavelength division multiplexing [35]. In this case, Alice does not know whether r arrives at her zone or not. Thus Eve can block the reference pulse and only send s to Alice, which means $\beta_{\max} = 1$. In this paper we assume that Alice and Bob use the second way to synchronize their clock, and thus $n_s = n_a^i$. Therefore, the intensity of signal pulse outgoing Alice's zone is $\mu_s = \gamma n_s = \gamma n_a^i$, where γ is the transmittance of Alice's attenuator.

III. INTERCEPT-AND-RESEND ATTACK WITH PRP

We show that the partially random phase of source may leave a loophole for Eve to spy the secret key. Generally speaking, when an imperfection is found by Eve, she can combine all imperfections of the system and take advantage of all attack strategies to maximize her information of the key. However, we only consider a simple intercept-and-resend attack in this paper, which clearly shows that the generated key will be compromised due to the partially random phase.

According to the analysis above, we can consider the following attack: Eve intercepts all the pulse from Alice and measures the quadrature amplitude (x) of the signal pulse with the experimental arrangement of Fig. 1(b). In order to judge Alice's phase information, Eve modulates the local pulse randomly and equiprobably with one of the two phases $\phi_j^e = j\pi/2, j = 0,1$. Then she sets the two threshold values X_+ and X_-. Simply, we consider the symmetrical case that $X_+ = -X_- \equiv X_{\rm th}$ in this paper. When $x \geqslant X_{\rm th}$, Eve judges that the phase modulated by Alice is the same as hers, and thus she resends a state with phase ϕ_j^e to Bob. When $x \leqslant -X_{\rm th}$, Eve judges that the difference of phase modulated by Alice and her is π, and thus she resends a state with phase $\phi_j^e + \pi$ to Bob. When $-X_{\rm th} \leqslant x \leqslant X_{\rm th}$, 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.

Obviously, sometimes Eve may make a wrong judgment. However, it is easy to check that when Eve uses the same basis as Alice, the probability that Eve obtains a valid outcome is much higher than that when Eve uses a different basis with Alice. Here a valid outcome means that the measured outcome x of Eve satisfies $x \geqslant X_{\rm th}$ or $x \leqslant -X_{\rm th}$. Generally speaking, the larger Eve sets $X_{\rm th}$, the lower the error rate. But, at the same time, the probability that Eve obtains a valid outcome will decrease. Thus Eve should make a tradeoff between the error rate and efficiency when she loads her attack in a practical situation.

In order not to be discovered, Eve should ensure that the error rate induced by her attack is smaller than the tolerable threshold value of Alice and Bob. In the following, we analyze the error rate induced by Eve's attack and show that Eve can load our attack without being discovered by the legitimate parties. Without loss of generalization, we assume that the phase modulated by Alice is $\phi_0^a = 0$. According to Eq. (6), when Eve modulates the local pulse with a phase $\phi_0^e = 0$, the probability that she obtains a valid outcome is given by

$$P_0^+ = \sqrt{\frac{2}{\pi\delta^2\kappa^2}}\int_{X_{\rm th}}^{\infty}dx\int_0^{\delta}d\theta\,\exp\{-2[x-\sqrt{\mu_s}\cos(\theta)]^2/\kappa^2\}, \tag{7a}$$

$$P_0^- = \sqrt{\frac{2}{\pi\delta^2\kappa^2}}\int_{-\infty}^{-X_{\rm th}}dx\int_0^{\delta}d\theta\,\exp\{-2[x-\sqrt{\mu_s}\cos(\theta)]^2/\kappa^2\}. \tag{7b}$$

Obviously, when Eve obtains $x \geqslant X_{\rm th}$, she will not induce any error, but when Eve obtains $x \leqslant -X_{\rm th}$, she will induce an error event with a probability up to 1. At the same time, Eve may modulate the local pulse with a phase $\phi_1^e = \pi/2$. Then the probability that she obtains a valid outcome is given by

$$P_{\pi/2}^+ = \sqrt{\frac{2}{\pi\delta^2\kappa^2}}\int_{X_{\rm th}}^{\infty}dx\int_0^{\delta}d\theta\exp\{-2[x+\sqrt{\mu_s}\sin(\theta)]^2/\kappa^2\}, \tag{8a}$$

$$P_{\pi/2}^- = \sqrt{\frac{2}{\pi\delta^2\kappa^2}}\int_{-\infty}^{-X_{\rm th}}dx\int_0^{\delta}d\theta\,\exp\{-2[x+\sqrt{\mu_s}\sin(\theta)]^2/\kappa^2\}. \tag{8b}$$

Obviously, she will induce an error event with a probability of 1/2 for this case, no matter which outcome is obtained by her. Therefore, the error rate induced by Eve can be written as

$$e = \frac{P_0^- + (P_{\pi/2}^+ + P_{\pi/2}^-)/2}{P_0^+ + P_0^- + P_{\pi/2}^+ + P_{\pi/2}^-}. \tag{9}$$

Here we assume Eve modulates randomly 0 or $\pi/2$ with equal probability. Since the four states sent by Alice are symmetrical, the total error rate induced by Eve's attack is the same as Eq. (9). At the same time, the probability that Eve obtains a valid outcome is given by

$$P_{\rm post} = (P_0^+ + P_0^- + P_{\pi/2}^+ + P_{\pi/2}^-)/2. \tag{10}$$

The error rate induced by our attack is shown in Fig. 3. It shows clearly that when the phase of source is just partially random, the generated key will be compromised. In part (a) we show that the error rate changes with $X_{\rm th}$ and δ. As expected,

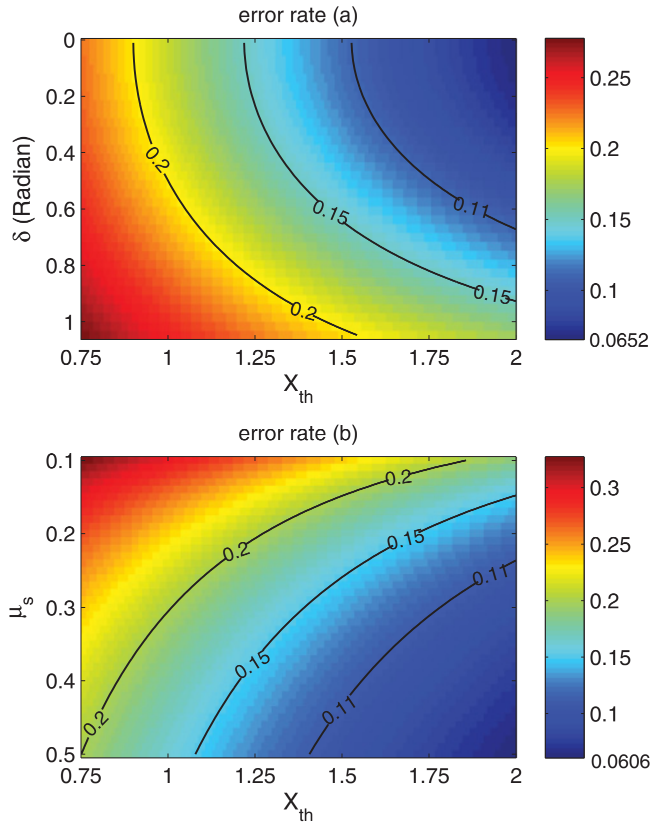

FIG. 3. (Color online) The error rate induced by Eve. In the simulations, we set $\lambda = 0.75$ and $\kappa = 1.1$ due to the experimental results of Ref. [31]. Part (a) shows the error rate changes with X_{th} and δ for given $\mu_s = 0.3$. Part (b) shows the error rate changes with X_{th} and μ_s for given $\delta = \pi/6$. In the figure, we also draw the contour line for $e = 11\%, 15\%$, and 20%.

for a given δ, the higher the threshold value X_{th} set by Eve, the lower the error rate will be. For example, when $\delta = \pi/6$ and $\mu_s = 0.3$, the error rate is 9.21% and 13.79% for $X_{\text{th}} = 2$ and $X_{\text{th}} = 1.5$, respectively. At the same time, the smaller the range of partially random phase δ, the lower the error rate will be. For example, when Eve sets $X_{\text{th}} = 2$, the error rate is 8.01%, 9.21%, and 12.65% for $\delta = \pi/8$, $\delta = \pi/6$, and $\delta = \pi/4$, respectively. According to Eq. (6), the error rate induced by Eve will depend on the intensity of signal pulse μ_s, which is shown in Fig. 3(b). For example, when Eve sets $X_{\text{th}} = 2$ and $\delta = \pi/6$, the error rate will be 6.06%, 9.21%, and 18.65% for $\mu_s = 0.5, 0.3$, and 0.1, respectively. In other words, if Eve wants to keep the error rate smaller than 20%, she only needs to set $X_{\text{th}} = 1.02$ for $\mu_s = 0.3$, but X_{th} will increase to 1.86 for $\mu_s = 0.1$.

According to the analysis above, we know that Eve can reduce the error rate induced by her attack by increasing the threshold value X_{th}. However, the higher X_{th} is, the lower the chance that Eve will obtain an unambiguous result such as $x \geqslant X_{\text{th}}$ or $x \leqslant -X_{\text{th}}$. Although Eve can send a vacuum state to Bob when she obtains the ambiguous result that $-X_{\text{th}} < x < X_{\text{th}}$, she should ensure that the expected rate count of Bob is unchanged. In other words, Eve should ensure that the equation $P_{\text{post}}\eta_{\text{Bob}}\mu_E = \mu_s\eta_c\eta_{\text{Bob}}$ holds. Here η_{Bob} is the transmittance of Bob's setups. $\eta_c = 10^{-al/10}$ is the transmittance of channel, and μ_{E} is the intensity of pulse sent to Bob by Eve. Here we assume that Eve can send a strong pulse to Bob to compensate η_{Bob}, which means $\mu_{\text{E}} = 1/\eta_{\text{Bob}}$. Therefore, the maximal value of X_{th} is determined by the transmittance of the channel between Alice and Bob. The equivalent length of channel for a given X_{th} is given by

$$l = -\frac{10}{a}\log_{10}[\min(1, \mu_{\text{E}}P_{\text{post}}/\mu_s)], \tag{11}$$

where we assume the channel is fiber, $a = 0.21$ dB/km is the typical loss of fiber, and P_{post} is given by Eq. (10).

Figure 4 shows the equivalent length of channel changes with X_{th} and δ. It shows clearly that our attack is valid even though the channel distance of Alice and Bob is very short. It can be explained as the maximal X_{th} that Eve can set for a given length of channel. Note that the error rate induced by Eve is determined by X_{th}. Thus it also can be explained as the minimal error rate induced by our attack for a given length of channel. For example, if the length of channel between Alice and Bob is 50 km, the maximal X_{th} that Eve can set is 1.97 when $\delta = \pi/6$ and $\mu_s = 0.3$; thus the minimal error rate induced by Eve is 9.36%.

IV. ONE-DECOY-STATE METHOD

It is well known that in practical QKD systems with the WCS, the decoy-state method should be used to beat the PNS attack. In this section we show that if Alice and Bob use the one-decoy-state method to estimate the final secret key rate, Eve still can spy the secret key using our attack in some parameter regime. Although the one-decoy state is not optimal for Alice and Bob, it is still adopted in some experimental systems [17,36].

In the one-decoy-state method, Alice will send two kinds of pulses with different intensities to Bob, the signal state and the decoy state, whose average photon number are denoted as μ and ν ($\mu > \nu > 0$), respectively. Then they estimate the lower bound for the yield of single-photon state Y_1^L and the upper bound for the error rate of the single-photon state e_1^U, which are given by Eq. (41) of Ref. [22]:

$$Y_1^L = \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2}\right), \tag{12a}$$

$$e_1^U = \frac{E_\nu Q_\nu e^\nu}{Y_1^L \nu}, \tag{12b}$$

where Q_μ and Q_ν are the gain of the signal state and the decoy state, E_μ is the error rate of the decoy state, and $e_0 = 1/2$ is the error rate of the background. Note that Alice and Bob will think that the phase of source has been randomized totally (in fact, it is just partially randomized); thus they will use the GLLP formula to estimate the key rate, which is given by [4]

$$R \geqslant q\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1^L[1 - H_2(e_1^U)]\}, \tag{13}$$

where $q = 1/2$ with the standard BB84 protocol, $f(e) = 1.22$ is the bidirectional error correction efficiency, $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon information entropy, $Q_1^L = \mu e^{-\mu}Y_1^L$ is the gain of the single-photon state, and E_μ is the error rate of the signal state.

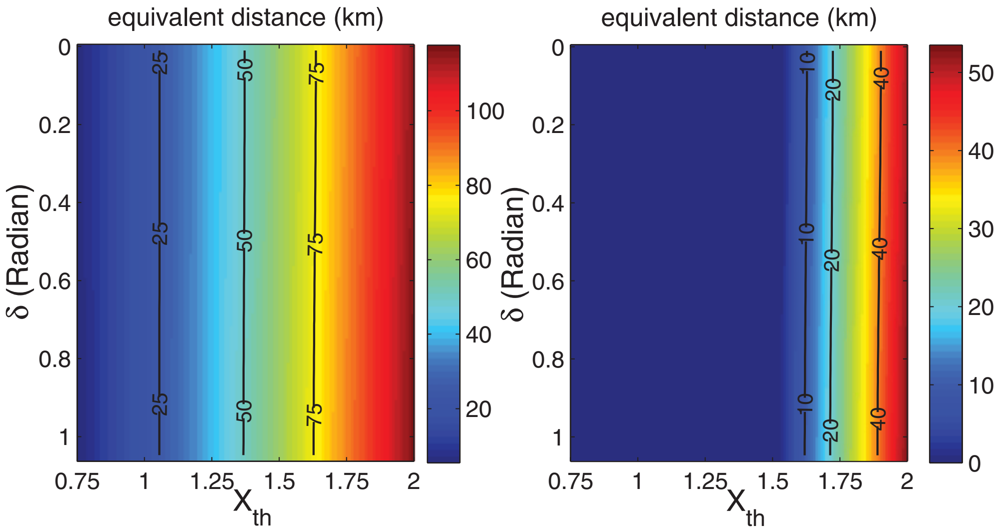

FIG. 4. (Color online) The equivalent length of channel that Eve can load her attack successfully for a given X_{th}. Here we assume the channel is fiber and $\mu_s = 0.3$. In the simulations, we set $\eta_{\text{Bob}} = 0.045$, $\lambda = 0.75$, and $\kappa = 1.1$ due to the experimental result of [18,31]. Part (a) shows the equivalent distance when Eve sends a single photon state to Bob, which means $\mu_E = 1$, and the detection efficiency of Bob η_{Bob} is not compensated. Part (b) shows the case that $\mu_E = 1/\eta_{\text{Bob}}$, which means that Eve totally compensates Bob's detection efficiency η_{Bob} by sending a strong pulse to Bob.

Note that in the decoy-state method, Eve cannot distinguish the signal state and the decoy state. Thus we assume Eve sends a single-photon state to Bob when she obtains a valid measurement outcome. Thus the gain and error rate of Bob for the signal state and the decoy state are given by

$$\begin{aligned} Q_\mu &= \eta_{\text{Bob}} Q'_\mu + (1-\eta_{\text{Bob}})Y_0, \\ E_\mu Q_\mu &= \eta_{\text{Bob}} Q'_\mu E'_\mu + (1-\eta_{\text{Bob}})Y_0 e_0, \\ Q_\nu &= \eta_{\text{Bob}} Q'_\nu + (1-\eta_{\text{Bob}})Y_0, \\ E_\nu Q_\nu &= \eta_{\text{Bob}} Q'_\nu E'_\nu + (1-\eta_{\text{Bob}})Y_0 e_0, \end{aligned} \tag{14}$$

where Y_0 is the dark count of Bob's single-photon detector, and $e_0 = 0.5$ is the error rate of dark count. Under our attack, E'_μ and E'_ν are given by Eq. (9), and Q'_μ and Q'_ν are given by Eq. (10).

By substituting these parameters into Eq. (13), it is easy to estimate the key rate under our attack, which is shown in Fig. 5. Here we also show the equivalent length of channel between Alice and Bob, which is given by

$$L_{\text{eq}} = -\frac{10}{a}\log_{10}\left[\min\left(1, \frac{Q_\mu}{\mu\eta_{\text{Bob}}}\right)\right], \tag{15}$$

where Q_μ is the gain of signal state. Here the equivalent length is used to ensure that the gain of signal state under our attack is the same as Bob's expectancy.

The numerical simulations show clearly that Eve can ensure that the key rate between Alice and Bob is still positive by setting a suitable threshold value. For example, when $\delta = 17^\circ$, the key rate is positive if Eve sets $X_{\text{th}} > 1.37$, but in fact, no secret key can be generated in this range, since Eve's intercept-and-resend attack is an entanglement-breaking channel [10,37]. Figure 5 also shows clearly that our attack can be implemented successfully even if the distance of channel between Alice and Bob is short. For example, if Eve sets $X_{\text{th}} = 1.4$, the key rate will be positive and the equivalent length of the channel is about 50.83 km.

Note that in the simulation of Fig. 5, we assume that the homodyne detector of Eve is perfect. Although Eve can make a perfect homodyne detector in theory, a practical Eve is still

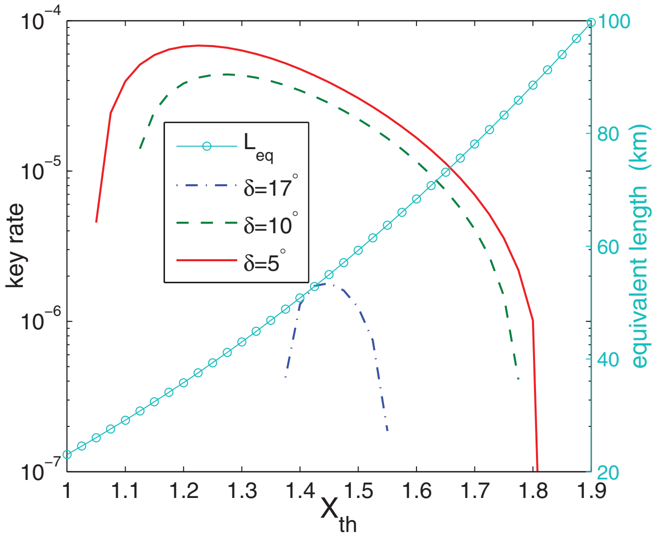

FIG. 5. (Color online) The key rate between Alice and Bob at various threshold values X_{th}. Here the legitimate parties use the one-decoy-state method to estimate the key rate. Here we set $\mu = 0.48$ and $\nu = 0.05$ according to the decoy-state theory [22] and the experimental parameters of GYS [18], 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, and 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 very small. Thus we draw just the equivalent length for $\delta = 17^\circ$ in the figure.

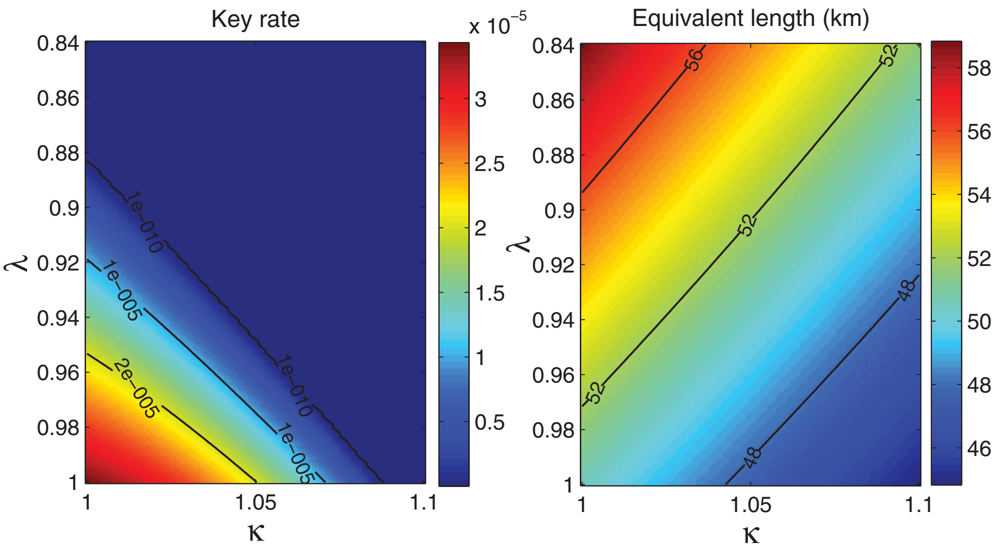

FIG. 6. (Color online) The key rate between Alice and Bob changes with the parameters that characterize the imperfection of homodyne detection. In the simulation, we also use the experimental parameters of GYS (see Fig. 5) and set $\mu = 0.48$ and $\nu = 0.05$. Here we assume the partially randomized phase is $\delta = 10^\circ$ and Eve sets $X_{\rm th} = 1.4$. The point where $\lambda = \kappa = 1$ represents a perfect homodyne detector. In the figure we also draw the equivalent length of channel when Eve sets $X_{\rm th} = 1.4$.

imperfect. In Fig. 6 we show the key rate changes with the two parameters λ and κ, which are used to characterize the imperfections of Eve's homodyne detector. It shows clearly that our attack is still valid, even if the homodyne detector of Eve is imperfect. In Fig. 6 we also draw the equivalent length of channel with the same parameters as that of the key rate. This clearly shows that even if the length of channel between Alice and Bob is short, our attack is still valid.

In Fig. 7 we also show that the key rate changes with the intensity of signal state and decoy state. Generally speaking, for a given practical QKD system, the legitimate parties will optimize the intensity of the signal state and decoy state (μ and ν) to maximize the key rate. For example, in the experimental parameters of Gobby-Yuan-Shield (GYS), the optimal μ and ν are 0.48 and 0.036, respectively, when the length of channel between Alice and Bob is 50 km. However, under these parameters, the final key rate is still positive under our attack, but in fact no secret key can be generated. In other words, when our attack is taken into account, the estimated optimal parameters that are unaware of our attack may be not secret. Thus, in a practical system, the legitimate parties must set their experimental parameters carefully.

Here we remark that although our attack is immune to the one-decoy-state method, it can be defeated by the vacuum +

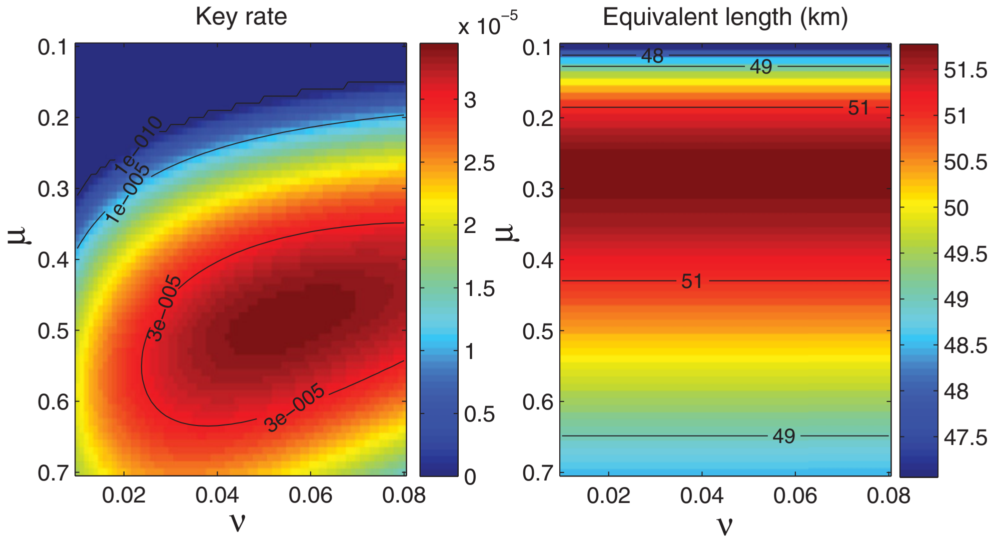

FIG. 7. (Color online) The key rate changes with the intensity of signal state and decoy state. In the simulation, we assume the homodyne detector is perfect and Eve sets $X_{\rm th} = 1.4$. Here the partially randomized phase is set at $\delta = 10^\circ$. The equivalent length is also drawn in the figure to show that our attack is valid, even in the short-distance QKD system.

weak-decoy-state method, in which Alice sends three kinds of pulses to Bob—the signal state, the decoy state, and the vacuum state. The main reason is that Eve may obtain a valid outcome with a high probability, even if Alice sends a vacuum state. Thus the gain of the vacuum state will be much larger than the dark count of the single photon detector (SPD), and then can be found by Alice and Bob.

V. DISCUSSION

We have shown that our attack can be used by Eve to break the security of a practical QKD system with WCS, even if the one-decoy-state method is used by Alice and Bob. At the end of this paper we discuss our attack.

First, it has shown that our attack can beat the BB84 QKD system with WCS and SPD. However, it is invalid for the continuous variable (CV) QKD scheme. In the CVQKD, Bob also uses homodyne detection to measure the signal pulse; thus he can reconstruct the probability distribution of the signal pulse and then discover the existence of Eve. Furthermore, due to the same reason as for the CVQKD, our attack is also invalid for the BB84 QKD system with pulse homodyne detection, which is proposed and demonstrated by Hirano [31] *et al.*

Second, in this paper we assume that Eve changes only the random phase of source, which is a global phase, but does not remap the bit phase, which is a relative phase. In other words, in the analysis above, we assume the states sent by Alice are still the standard BB84 states. Strictly speaking, Eve also can change the bit phase. Then Eve can combine our attack with the phase remapping attack [10,11] to maximize her information.

Third, in a high-speed QKD system, Eve needs a high-speed homodyne detector to detect the signal pulse. It seems an experimental challenge to implement our attack. In fact, the speed of some commercial homodyne detectors produced by Picometrix can reach 40 GHz [38]. Thus our attack is valid even for the high-speed QKD systems. Furthermore, a highly stable interferometer is needed to ensure that the local pulse and signal pulse can interfere at the BS. Thus Eve must compensate the phase shift of fiber induced by the environment. In fact, the feedback method developed in the gigahertz QKD system [16] can also be used in our attack to ensure that Eve's interferometer is very stable.

VI. SUMMARY

For the BB84 QKD protocol, phase randomization is a very important assumption in the standard security analysis. However, it is a hard task to check whether the phase of source is randomized totally or not in practical situations. In fact, Eve can control the range of random phase so that it is just partially randomized.

In this paper we proposed a partially random phase attack to spy the secret key. Our results show that if the phase of source is partially randomized, the error rate induced by our attack 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 the secret key generated by a practical QKD system will be compromised. Specifically, the numerical simulation shows that our attack is immune to the one-decoy-state method in some parameter regimes. Therefore, the legitimate parties should consider our attack carefully when they use the WCS to implement the BB84 protocol.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China, Grant No. 61072071. S.H.S. is supported by the Hunan Provincial Innovation Foundation for Postgraduates, Grant No. CX2010B007, and the Fund of Innovation, Graduate School of NUDT, Grant No. B100203.

[1] C. H. Bennett and G. Brassard, *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, Science **283**, 2050 (1999).
[3] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[4] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[5] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).
[6] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[7] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[8] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[9] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
[10] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007).
[11] F.-H. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).
[12] S.-H. Sun, M.-S. Jiang, and L.-M. Liang, Phys. Rev. A **83**, 062331 (2011).
[13] H.-K. Lo and J. Preskill, Quantum Inf. Comput. **7**, 431 (2007).
[14] Y. Zhao, B. Qi, and H.-K. Lo, Appl. Phys. Lett. **90**, 044106 (2007).
[15] [http://www.idquantique.com/scientific-instrumentation/clavis2-qkd-platform.html].
[16] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, Opt. Express **19**, 10387 (2011).
[17] P. A. Hiskett, D. Rosenherg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, New J. Phys. **8**, 193 (2006).
[18] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[19] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[20] H.-K. Lo, X.-F. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[21] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[22] X.-F. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[23] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).

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

[25] Here we mean that it is hard for Alice to monitor the degree of random phase using the current QKD system. Of course, if she adds additional optical and electrical setups, she can do this easily. For example, she can establish one interferometer to measure the visibility of pulses. If the visibility is zero, the phase of pulse is totally randomized. Otherwise, it is just partially randomized. Therefore, if our attack is taken into account, Alice must redesign her system to carefully monitor the random phase.

[26] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997)

[27] H. P. Yuen and V. W. S. Chan, Opt. Lett. **8**, 177 (1983).

[28] U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge University Press, Cambridge, UK, 1997).

[29] T. Symul, D. J. Alton, S. M. Assad, A. M. Lance, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. A **76**, 030303(R) (2007).

[30] J. Lodewyck, T. Debuisschert, R. Garcia-Patron, R. Tualle-Brouri, N. J. Cerf, and P. Grangier, Phys. Rev. Lett. **98**, 030503 (2007).

[31] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Phys. Rev. A **68**, 042331 (2003).

[32] K. Vogel and H. Risken, Phys. Rev. A **40**, 2847 (1989).

[33] S. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[34] Here $\lambda = \sqrt{T\eta_{PD}}V$, where T is the loss of optical setups, η_{PD} is the quantum efficiency (QE) of photodiode, and V is the visibility of interference. Thus the crucial imperfection of homodyne detection is the QE of the photodiode. Although the QE is just 0.84 in the experiment of Ref. [31], the QE of Hamamatsu's new product can approach 0.9 (see the website of Hamamatsu: [http://jp.hamamatsu.com/products/sensor-ssd/pd128/pd129/pd130/G8370-81/index_en.html]). Furthermore, κ is determined by the excess noise of the signal and the phase error, but to the best of our knowledge, we find only one experimental result where $\kappa = 1.1$, which is given by Ref. [31]. However, it does not matter theoretically, Eve can make a perfect homodyne detection with $\lambda = \kappa = 1$.

[35] A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K. I. Yoshino, S. Miki, B. Baek, Z. Wang *et al.*, Opt. Express **16**, 11354 (2008).

[36] Y. Zhao, B. Qi, X.-F. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).

[37] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[38] [http://www.picometrix.com/pico-products/hsor-datatables.asp].