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

Shi-Hai Sun, Ming Gao, Mu-Sheng Jiang, Chun-Yan Li, Lin-Mei Liang*
Department of Physics, National University of Defense Technology, Changsha 410073, People’s Republic of China

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.

PACS numbers: 03.67.Hk, 03.67.Dd

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 [6,7]. 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 [0,π] with a phase modulator. In other words, Eve does not know how to spy the secret key, even if the source is not randomized or 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 θ ∈ [0, δ] and δ < 2π. 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 phase randomization assumption is the base of the decoy state method [14–22], 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 [22]. 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 θ ∈ [0, δ] and δ < 2π. Furthermore, we note that in most of the practical system [15–18], no active setup is used to randomize the phase of source. 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 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 phase randomization assumption is the base of the decoy state method [14–22], which is often used to defeat the PNS attack [23,24]. Thus, in the QKD system with decoy-state method, only the GLLP formula can be used.

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 phase randomization assumption is the base of the decoy state method [14–22], which is often used to defeat the PNS attack [23,24]. Thus, in the QKD system with decoy-state method, only the GLLP formula can be used.

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 [6,7]. 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 [0,π] with a phase modulator. In other words, Eve does not know how to spy the secret key, even if the source is not randomized or 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 θ ∈ [0, δ] and δ < 2π. 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 phase randomization assumption is the base of the decoy state method [14–22], which is often used to defeat the PNS attack [23,24]. Thus, in the QKD system with decoy-state method, only the GLLP formula can be used.

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 phase randomization assumption is the base of the decoy state method [14–22], which is often used to defeat the PNS attack [23,24]. Thus, in the QKD system with decoy-state method, only the GLLP formula can be used.
attack \cite{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 \cite{21,22}, since the vacuum state is used to estimate the gain and error rate of the background.

We note that in Ref. \cite{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 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 can not 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.

A. Plug-and-Play System

A simple diagram of a plug-and-play QKD system \cite{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 \(\phi = k\pi/2, k = 0, 1, 2, 3\). 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 \(\theta\) 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

\[
|\alpha e^{i(\theta+\theta')}\rangle_r |\alpha e^{i(\phi_\kappa^s+\theta')}\rangle_s,
\]

where \(\theta'\) is the phase induced by the birefringence of fiber. \(\alpha\) 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 \(\theta'\). Otherwise Eve can obtain more information by combining with the passive FM attack proposed by our group \cite{12}. Note that \(\theta'\) 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

\[
\rho = \int_0^{\delta} \frac{d\theta}{\delta} |\alpha e^{i(\phi_\kappa^s+\theta')}\rangle_r \langle \alpha e^{i(\phi_\kappa^s+\theta')}|,
\]

where \(\delta\) is range of random phase modulated by Alice. Here we assume \(\theta\) 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 \( \theta' \), 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 BS, signal pulse \( (s) \), reference pulse \( (r) \) and 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 randomly \( l \) with a phase \( \phi' = j\pi/2, j = 0, 1 \). Then \( s \) will interfere with \( l \) at BS and be detected by two photodiodes \( (Dc \text{ and } Dd) \).

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 \[25\] or implement the continuous variable quantum cryptography \[29\]. 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 (BS). Then the two output modes of BS, \( c \) and \( d \), will reach two photodiodes \( (Dc \text{ and } Dd) \) respectively. The measured output signal of homodyne detection is determined by the difference of \( Dc \text{ and } Dd \), which is given by 31

\[ i \propto \sqrt{n_i}(a_s e^{-i\phi'} + a_s^+ e^{i\phi'}) = \sqrt{2n_i}x, \]

where \( n_i \) is the average photon number of the local pulse, \( a_s \) is the annihilation operator of signal pulse, \( \phi' \) is the difference of phase between signal pulse and local pulse. Here we assume the local pulse is 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

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

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

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

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

where \( \mu_s = |\alpha|^2 \) is the average photon number of signal pulse, \( \phi = \phi'_s - \phi'_l \) is the difference of phase modulated by Eve and Alice, \( \theta \in [0, \delta] \) is the random phase modulated by Alice. \( \lambda \) and \( \kappa \) 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 priori information about \( \theta \) excepting that \( \theta \in [0, \delta] \), thus Eq.\(3\) should be rewritten as

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

Fig.\(2\) shows the theoretical probability distribution of \( x \) when the total phase shifts \( \phi \) are 0, \( \pi/2 \), \( \pi \) and \( 3\pi/2 \). It shows clearly that measured result of the homodyne detection can be used to distinguish 0 and \( \pi \) by setting a suitable threshold value. For example, Eve can set two threshold value \( X_+ \geq 0 \) and \( X_- \leq 0 \). When the measured quadrature amplitude \( x \geq X_+ \), Eve judge that \( \phi = 0 \); when \( x \leq X_- \), Eve judge that \( \phi = \pi \). But when \( X_- < x < X_+ \), Eve can’t give a judgement about the phase. Although Eve can’t distinguish the four phases deterministically, it is easy to check that, the conditional probability that Eve 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 the measured outcome \( x \) satisfies \( x \geq X_+ \) or \( x \leq X_- \).

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

Remark one: 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 doesn’t monitor the intensity of $s$ and $r$ respectively in most practical QKD systems. Thus Eve only needs to ensure the total of them entering Alice’s zone, denoted as $n_{si}$, is unchanged, but no needs to keep the intensities of both $s$ and $r$ to be the same as their expected values respectively. In other words, Eve can change the proportion of average photon number between signal pulse and reference pulse (denoted as $n_s$ and $n_r$ respectively), but keeps $n_s + n_r = n_{si}$ constant. In the following, we let $n_s = \beta n_{si}$ and $n_r = (1 - \beta)n_{si}$. Note that, if Alice monitors the intensity of signal pulse and reference pulse at the same time, Eve can’t 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 two: Note that only $s$ will be modulated by Alice, thus Eve should increase the coefficient $\beta$ to maximize her information. The maximal value of $\beta$ 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 $(1 - \beta_{max})n_{si}$ 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. In this case, Alice doesn’t 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, thus $n_s = n_{si}$. Therefore, the intensity of signal pulse outgoing Alice’s zone is $\mu_s = \gamma n_s = \gamma n_{si}$, where $\gamma$ 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 $\phi^e_j = j\pi/2, j = 0, 1$. Then she sets two threshold value $X^e_+$ and $X^e_-$. Simply, we consider the symmetrical case that $X^e_+ = -X^e_- \equiv X^e_{th}$ in this paper. When $x \geq X^e_{th}$, Eve judges that the phase modulated by Alice is the same as her, thus she resends a state with phase $\phi^e_+ + \pi$ to Bob. When $-X^e_{th} \leq x \leq X^e_{th}$, 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 judgement. 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 Eve uses the different basis with Alice. Here a valid outcome means the measured outcome $x$ of Eve satisfies $x \geq X^e_{th}$ or $x \leq -X^e_{th}$. Generally speaking, the larger Eve sets $X^e_{th}$, 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 $\phi_a^e = 0$. According to Eq. (9), when Eve modulates the local pulse with a phase $\phi_a^e = 0$, the probability that she obtains a valid outcome are given by

$$P^+_0 = \frac{1}{\pi^2 \delta^2 \kappa^2} \int_{-X_{th}}^{X_{th}} dx \int_0^\delta d\theta \exp[-2(x - \sqrt{\mu_s} \cos(\theta))^2/\kappa^2],$$

(7a)

$$P^-_0 = \frac{1}{\pi^2 \delta^2 \kappa^2} \int_{-\infty}^{-X_{th}} dx \int_0^\delta d\theta \exp[-2(x - \sqrt{\mu_s} \cos(\theta))^2/\kappa^2],$$

(7b)

Obviously, when Eve obtains $x \geq X_{th}$, she will not induce any error. But when Eve obtains $x \leq -X_{th}$, 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 $\phi_a^e = \pi/2$, then the probability that she obtains a valid outcome are given by

$$P^+_0 = \frac{1}{\pi^2 \delta^2 \kappa^2} \int_{-X_{th}}^{X_{th}} dx \int_0^\delta d\theta \exp[-2(x + \sqrt{\mu_s} \sin(\theta))^2/\kappa^2],$$

(8a)

$$P^-_0 = \frac{1}{\pi^2 \delta^2 \kappa^2} \int_{-\infty}^{-X_{th}} dx \int_0^\delta d\theta \exp[-2(x + \sqrt{\mu_s} \sin(\theta))^2/\kappa^2].$$

(8b)

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

$$e = \frac{P^-_0 + [P^+_{\pi/2} + P^-_{\pi/2}]/2}{P^+_0 + P^-_0 + P^+_{\pi/2} + P^-_{\pi/2}}.$$

(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:

$$P_{post} = (P^+_0 + P^-_0 + P^+_{\pi/2} + P^-_{\pi/2})/2.$$

(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 $X_{th}$ and $\delta$. As expected, for given $\delta$, the higher the threshold value $X_{th}$ is 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 $X_{th} = 2$ and $X_{th} = 1.5$ respectively. At the same time, the smaller the range of partially random phase $\delta$ is, the lower the error rate will be. For example, when Eve sets $X_{th} = 2$, the error rate is 8.01%, 9.21% and 12.65% for $\delta = \pi/5$, $\delta = \pi/4$ and $\delta = \pi/3$ respectively. According to Eq. (8), the error rate induced by Eve will depend on the intensity of signal pulse $\mu_s$, which is shown in Fig. 3 (part (b)). For example, when Eve sets $X_{th} = 2$ and $\delta = \pi/6$, the error rate will be 6.06%, 9.21% and 18.65% for $\mu_s = 0.5, 0.3, 0.1$ respectively. In other words, if Eve wants to keep the error rate is smaller than 20%, she only needs to set $X_{th} = 1.02$ 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 Eve obtains an unambiguous result that $x \geq X_{th}$ or $x \leq -X_{th}$. Although Eve can send vacuum state to Bob when she obtains the ambiguous result that $-X_{th} < x < X_{th}$, she should ensure that the expected count rate of Bob is unchanged. In other words, Eve should ensure that the equation that $P_{post} \eta_{Bob} \mu_E = \mu_a \eta_a \eta_{Bob}$ holds. Here $\eta_{Bob}$ is the transmittance of Bob’s setups. $\eta_a = 10^{-10/10}$ is the transmittance of channel. $\mu_E$ is the intensity of pulse sent
Although the one decoy state is not optimal for Alice to estimate the final secret key rate, Eve still can spy the attack for a given length of channel. For example, if the length of channel between Alice and Bob is 50 km, the equivalent length of channel for a given channel length when Eve sends a single photon state to Bob, which means $\mu_E = 1$ and the detection efficiency of Bob $\eta_{Bob}$ is not compensated. Part(b) shows the case that $\mu_E = 1/\eta_{Bob}$, which means that Eve compensates totally Bob’s detection efficiency $\eta_{Bob}$ by sending a strong pulse to Bob.

to Bob by Eve. Here we assume that Eve can send a strong pulse to Bob to compensate $\eta_{Bob}$, which means $\mu_E = 1/\eta_{Bob}$. Therefore, the maximal value of $X_{th}$ is determined by the transmittance of channel between Alice and Bob. The equivalent length of channel for a given $X_{th}$ is given by

$$l = -\frac{10}{a} \log_{10}[\min\{1, \mu_E P_{post}/\mu_s\}],$$

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

Fig. 4 shows the equivalent length of channel changes with $X_{th}$ and $\delta$. It shows clearly that our attack is valid even 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 the practical QKD systems with the WCS, the decoy state method should be used to beat the PNS attack. In this section, we will 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 $\mu$ and $\nu$ ($\mu > \nu > 0$) respectively. Then they estimate the lower bound for the yield of single photon state, $Y_1^L$, and the upper bound for error rate of single photon state, $\epsilon_1^U$, which are given by the Eq.(41) of Ref. [22]:

$$Y_1^L = \frac{\mu}{\mu - \nu} [Q_\nu e^{\nu} - Q_\mu e^{\nu \mu^2}],$$

$$\epsilon_1^U = \frac{E_\nu Q_\nu e^{\nu}}{Y_1^L e^{\nu}},$$

where $Q_\mu$ and $Q_\nu$ are the gain of the signal state and the decoy state, $E_\nu$ is the error rate of the decoy state, $e_0 = 1/2$ is the error rate of 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]:

$$R \geq q\{-Q_\mu f(E_\nu)H_2(E_\nu) + Q_1^L [1 - H_2(\epsilon_1^U)]\},$$

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. $Q_1^L = \mu e^{-\nu}Y_1^L$ is the gain of single photon state, $E_\nu$ is the error rate of the signal state.

Note that, in the decoy state method, Eve can’t 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

$$Q_\mu = \eta_{Bob}Q_{\mu} + (1 - \eta_{Bob})Y_0,$n

$$E_\nu Q_\nu = \eta_{Bob}Q_{\nu}^\prime + (1 - \eta_{Bob})Y_0 e_0,$$

$$E_\nu Q_{\nu}^\prime = \eta_{Bob}Q_{\nu}^\prime + (1 - \eta_{Bob})Y_0 e_0,$$

where $Y_0$ is the dark count of Bob’s single photon detector, $e_0 = 0.5$ is the error rate of dark count. Under our attack, $E_\nu$ and $E_\nu^\prime$ are given by Eq.(14), $Q_\mu'$ and $Q_{\nu}^\prime$ are given by Eq.(10).

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

$$L_{eq} = -\frac{10}{a} \log_{10}[\min\{1, \frac{Q_\mu}{\mu E_{post}}\}],$$

where $Q_\mu$ is the gain of signal state. Here the equivalent length is used to ensure the gain of signal state under our attack is same as Bob’s expectancy.
FIG. 5: (Color online) 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. We set $\mu = 0.48$ and $\nu = 0.05$ according to the decoy state theory and the experimental parameters of GYS, 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 $\eta_{Bob} = 0.045$. 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 $\delta$, but the difference is much small. Thus we just draw the equivalent length for $\delta = 17^\circ$ in the figure.

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. For example, when $\delta = 17^\circ$, the key rate is positive if Eve sets $X_{th} > 1.37$, but in fact no secret key can be generated in this range, since Eve’s intercept-and-resend attack is an entanglement breaking channel. Fig. 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 $X_{th} = 1.4$, the key rate will be positive and the equivalent length of channel is about 50.83 km.

Note that, in the simulation of Fig. 5 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 Fig. 5 we show the key rate changes with the two parameters $\lambda$ and $\kappa$ which are used to characterize the imperfections of Eve’s homodyne detector. It shows clearly that our attack is still valid even the homodyne detector of Eve is imperfect. In Fig. 5 we also draw the equivalent length of channel with the same parameters as that of key rate. It shows clearly that even the length of channel between Alice and Bob is short, our attack is still valid.

In Fig. 5 we also show 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 signal state and decoy state ($\mu$ and $\nu$) to maximize the key rate. For example, in the experimental parameters of Gobby-Yuan-Shield (GYS), the optimal $\mu$ and $\nu$ are 0.48 and 0.036 when the length of channel between Alice and Bob is 50km. 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+weak decoy state method, in which Alice sends three kinds of pulses to Bob, the signal state, the decoy state. 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 signal state and decoy state ($\mu$ and $\nu$) to maximize the key rate. For example, in the experimental parameters of Gobby-Yuan-Shield (GYS), the optimal $\mu$ and $\nu$ are 0.48 and 0.036 when the length of channel between Alice and Bob is 50km. 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+weak decoy state method, in which Alice sends three kinds of pulses to Bob, the signal state, the decoy state. 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 signal state and decoy state ($\mu$ and $\nu$) to maximize the key rate. For example, in the experimental parameters of Gobby-Yuan-Shield (GYS), the optimal $\mu$ and $\nu$ are 0.48 and 0.036 when the length of channel between Alice and Bob is 50km. 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.
state and the vacuum state. The main reason is that Eve may obtain valid outcome with a high probability, even Alice sends a vacuum state. Thus the gain of vacuum state will be much larger than the dark count of 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 the one decoy state method is used by Alice and Bob. In the end of this paper, we give some discussions about 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 QKD (CV-QKD) scheme. In the CV-QKD, Bob also uses the homodyne detection to measure the signal pulse, thus he can reconstruct the probability distribution of signal pulse and then discover the existence of Eve. Furthermore, due to the same reason as the CV-QKD, our attack is also invalid for the BB84 QKD system with pulse homodyne detection, which is proposed and demonstrated by Hirano et al.

Second, in this paper, we assume that Eve only changes the random phase of source which is a global phase, but not remaps 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 to maximize her information.

Third, in 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 40GHz. Thus our attack is valid even for the high-speed QKD system. Further, a well-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 GHz QKD system can also be used in our attack to ensure the interferometer of Eve 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 the practical situation. 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. Specially, the numerical simulation shows that our attack is immune to the one decoy state method in some parameter regime. Therefore, the legitimate parties should consider our attack carefully, when they use the WCS to implement the BB84 protocol.

VII. ACKNOWLEDGEMENT

This work is supported by the National Natural Science Foundation of China, Grant No. 61072071. S.H. Sun 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(5), 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. Fred Fuang, 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. Fred Fuang, B. Qi, K. Tanaki, and H.-K. Lo, Phys. Rev. A 75, 032314 (2007).
[11] P.-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. 5(6), 431 (2007).
[14] Y. Zhao, B. Qi, and H. -K. Lo, Appl. Phys. Lett. 90, 044106 (2007).
[15] http://www.idquantique.com/scientific-
Here we means that it is hard for Alice to monitor the
degree of random phase using current QKD system. Of
course, if she adds additional optical and electrical se-
tups, she can do this easily. For example, she can estab-
lish one interferometer to measure the visibility of pulses.
If the visibility is zero, the phase of pulse is randomized
totally. Otherwise, it is just partially randomized. There-
fore, if our attack is taken into account, Alice must re-
design her system to monitor carefully the random phase.

Here \( \lambda = \sqrt{T \eta P D V} \), where \( T \) is the loss of optical
setups, \( \eta P D \) is the quantum efficiency (QE) of pho-
diode, \( V \) is the visibility of interference. Thus the
crucial imperfection of homodyne detection is the QE
of 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 Hamam-
matsu: http://jp.hamamatsu.com/products/sensor-
ssd/pd128/pd129/pd130/G8370-81/index_en.html).
Furthermore, \( \kappa \) is determined by the excess noise of
the signal and the phase error. But, as the best of our
knowledge, we only find one experimental result that
\( \kappa = 1.1 \) which is given by Ref.[31]. However, it does not
matter, theoretically, Eve can make a perfect homodyne
detection with \( \lambda = \kappa = 1 \).

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).

P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J.
Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nord-
holt, New J. Phys. 8 193 (2006).

C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys.
Lett. 84, 3762 (2004).

W. -Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).

H. -K. Lo, X. -F. Ma, and K. Chen, Phys. Rev. Lett. 94,
230504 (2005).

X. -B. Wang, Phys. Rev. Lett. 94, 230503 (2005).

B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev.
A 72, 012326 (2005).

G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sander,
Phys. Rev. Lett. 85, 1330 (2000).

Here we means that it is hard for Alice to monitor the
degree of random phase using current QKD system. Of
course, if she adds additional optical and electrical se-
tups, she can do this easily. For example, she can estab-
lish one interferometer to measure the visibility of pulses.
If the visibility is zero, the phase of pulse is randomized
totally. Otherwise, it is just partially randomized. There-
fore, if our attack is taken into account, Alice must re-
design her system to monitor carefully the random phase.

A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zhiden,
and N. Gisin, Apple. Phys. Lett. 70, 793 (1997)

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

U. Leonhardt, Measuring the Quantum State of Light
(Cambridge, University Press, Cambridge, 1997).

T. Symul, D. J. Alton, S. M. Assad, et al., Phys. Rev. A
76. 030303(R) (2007).

J. Lodewyck, T. Debuisschert, et al., Phys. Rev. Lett.
98. 030503 (2007).

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

K. Vogel and H. Risken, Phys. Rev. A 40, 2847 (1989).

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