Photon-number-resolving decoy-state quantum key distribution

Qing-yu Cai[1,*] and Yong-gang Tan[1,2]
[1]*State Key Laboratory of Magnetic Resonances and Atomic and Molecular Physics, Wuhan Institute of Physics and Mathematics, The Chinese Academy of Sciences, Wuhan 430071, People's Republic of China*
[2]*Graduation University of Chinese Academy of Sciences, Beijing 100081, People's Republic of China*
(Received 30 March 2005; published 3 March 2006)

In this paper, a photon-number-resolving decoy-state quantum key distribution (QKD) scheme is presented based on recent experimental advancements. A new upper bound on the fraction of counts caused by multiphoton pulses is given, which seems *inherent* as long as weak coherent sources and high lossy channel are used. This implies that our scheme is optimal in long-distance QKD with weak coherent sources. We show that Eve's coherent multiphoton pulse (CMP) attack is more efficient than a symmetric individual attack when the quantum bit error rate is small, so that the CMP attack should be considered to ensure the security of the final key. Our results show that a *not-so-weak* pulse can be used to transmit the key. Optimal intensity of the laser source is presented which provides a 23.9 km increase in the transmission distance.

DOI: 10.1103/PhysRevA.73.032305 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD) is a physically secure method by which a private key can be created between two partners, Alice and Bob, who share a quantum channel and a public authenticated channel [1]. The key bits can then be used to implement a classical private key cryptosystem, or more precisely a *one-time pad* algorithm, to enable the partners to communicate securely. The best known QKD is the BB84 protocol published by Bennett and Brassward in 1984 [2], the reliability of which has been studied intensively [3–7].

Experimental BB84 QKD was demonstrated by many groups [8]. An optical BB84 QKD system includes the photon sources, quantum channels, single-photon detectors, and quantum random-number generators. In principle, optical quantum cryptography is based on the use of single-photon Fock states. However, perfect single-photon sources are difficult to realize experimentally. Practical implementations rely on weak laser pulses in which photon number distribution obeys Possionian statistics. Thus, a no-cloning principle is ineffective in the case of multiphoton pulses. If the quantum channel is high lossy, Eve can obtain full information on the final key by using photon-number- splitting (PNS) attack without being detected [9–13]. In [7], it has been shown that the secure final key of the BB84 protocol can be extracted from the sifted key at the asymptotic rate

$$R = (1 - \Delta) - H_2(e) - H_2(e + \Delta), \tag{1}$$

where e is the quantum bit error rate (QBER) found in the verification test and Δ is the fraction of counts caused by multiphoton pulses. This means that both the QBER e and the fraction of tagged signals Δ are important to generate the secure final key. It has been shown that Eve's PNS attack will be limited when Alice and Bob use the decoy-state protocols [14–20] or the nonorthogonal states scheme [21]. In the decoy-state protocols [14–20], an important assumption is that the detection apparatus cannot resolve the photon number of arriving signals. Recently, some photon-number-resolving detection apparatus were presented [22–24], especially the noise-free high-efficiency photon-number-resolving detectors [24]. Thus, a lower upper bound on the fraction of counts Δ is desired with the photon-number-resolving detectors. As a matter of fact, some of Eve's other attacks, such as the coherent multiphoton pulse (CMP) attack, should also be considered or else the security of the final key will be unreliable.

In this paper, we present a photon-number-resolving decoy state (PDS) quantum key distribution scheme based on recent experimental advancements. We show that the upper bound on the fraction of counts caused by multiphoton pulses is $1-e^{-\mu}$, no matter how high the channel loss is. We show that the CMP attack is more efficient than the symmetric individual (SI) attack. We present the optimal approach to generate the sifted key from the raw key. The optimal parameter of the intensity of the laser source is presented to generate the secure final key. This paper is organized as follows. We first introduce our PDS QKD scheme. Then we discuss Eve's CMP attack. Next, we present the optimal approach to generate the sifted key from the raw key and afterwords discuss how to select the optimal intensity of the laser source to generate the secure final key. Finally, we present our conclusions.

II. PHOTON-NUMBER-RESOLVING DECOY-STATE QUANTUM KEY DISTRIBUTION

At present, practical "single-photon" sources rely on weak laser pulses in which photon-number distribution obeys Possionian statistics. Most often, Alice sends to Bob a weak laser pulse in which she has encoded her bit. Each pulse is *a priori* in a coherent state $|\sqrt{\mu}e^{i\theta}\rangle$ of weak intensity. Since Eve and Bob have no information on θ, the state reduces to a mixed state $\rho=\int(\frac{d\theta}{2\pi})|\sqrt{\mu}e^{i\theta}\rangle\langle\sqrt{\mu}e^{i\theta}|$ outside Alice's laboratory. This state is equivalent to the mixture of the Fock state

*Electronic address: qycai@wipm.ac.cn

$\Sigma_n p_n|n\rangle\langle n|$, with the number n of photons distributed as Possionian statistics $p_n=p_\mu[n]=\mu^n e^{-\mu}/n!$. The source that emits pulses in coherent states $|\sqrt{\mu}e^{i\theta}\rangle$ is equivalent to the representation as below: With probability p_0, Alice does nothing; with probability $p_n(n>0)$, Alice encodes her bit in n photons. In order to gain Alice's encoding information, Eve first performs a nondemolition measurement to gain the photon number of the laser pulses. When she finds there is only one photon in the pulses, she may implement a symmetric individual (SI) attack on this qubit [12]. Otherwise, if there are two or more photons in the pulses, she may implement a PNS attack on Alice's qubit. In long-distance QKD, the channel transmittance η can be rather small. If $\eta<(1-e^{-\mu}-\mu e^{-\mu})/\mu$, Eve can gain full information on Bob's final key by using the PNS attack [11].

In order to detect Eve's PNS attack, Alice can introduce a decoy source μ' to ensure the security of their QKD. Since Bob's detection apparatus is sensitive to the photon-number, in the absence of Eve, photon-number distributions in Bob's detectors are also Poissonian (here, we assume that the dark counts rate r_{dark} in Bob's detectors is zero; we will discuss the realistic condition of that $r_{\text{dark}}>0$ later),

$$p_{\text{sig}}^{\text{loss}}[n]=\frac{(\eta\mu)^n}{n!}e^{(-\eta\mu)}, \tag{2}$$

$$p_{\text{dec}}^{\text{loss}}[n]=\frac{(\eta\mu')^n}{n!}e^{(-\eta\mu')}. \tag{3}$$

Without the decoy state, the necessary condition for Eve to implement her PNS attack without being detected is [11]

$$p_{\text{sig}}[n]\left(1-\sum_{i=0}^{n-1}f(n,i)\right)+\sum_{j=n+1}^{\infty}p_{\text{sig}}[j]f(j,n)\geqslant p_{\text{sig}}^{\text{loss}}[n], \tag{4}$$

where $f(m,k)$ is the probability that Eve forwards k photons to Bob and stores the other $m-k$ photons. In general, let us assume Eve implements the PNS attack P_n on Alice's pulses. Consider the case in which decoy states are used by Alice. Essentially, the idea of a decoy state is that [17]

$$P_n(\text{signal})=P_n(\text{decoy})=P_n, \tag{5}$$

$$e_n(\text{signal})=e_n(\text{decoy})=e_n. \tag{6}$$

In this case, Eve can implement her PNS attack without being detected if and only if

$$p_{\text{sig}}[n]\left(1-\sum_{i=0}^{n-1}f(n,i)\right)+\sum_{j=n+1}^{\infty}p_{\text{sig}}[j]f(j,n)=p_{\text{sig}}^{\text{loss}}[n], \tag{7}$$

$$p_{\text{dec}}[n]\left(1-\sum_{i=0}^{n-1}f(n,i)\right)+\sum_{j=n+1}^{\infty}p_{\text{dec}}[j]f(j,n)=p_{\text{dec}}^{\text{loss}}[n]. \tag{8}$$

Using the Taylor series, we can obtain that

$$f(n,i)=\binom{n}{i}\eta^i(1-\eta)^{n-i}, \tag{9}$$

$$f(j,n)=\binom{j}{n}\eta^n(1-\eta)^{j-n}. \tag{10}$$

Experimentally, these solutions just correspond to the case in which Eve blocks every photon with the probability $1-\eta$, i.e., Eve forwards every photon with probability η through her lossless channel [this can be realized by using a beam splitter (BS) with the reflection probability $1-\eta$ and the transmission probability η]. We will calculate the amount of information Eve can gain by using her PNS attack described by Eqs. (7) and (8) later.

III. COHERENT MULTIPHOTON PULSE ATTACK

From Eq. (1) we know that the rate of the secure final key is not only determined by the tagged counts but also by the QBER. That is, Eve may use some other eavesdropping schemes on the multiphoton pulses besides the PNS attack. Of course, these attacks will cause some QBER which could be detected in the verification test. A general attack scheme Eve may use is the coherent multiphoton pulses attack. Let us first review the SI attack to introduce the CMP attack. When a photon propagates from Alice to Bob, Eve can let a system of her choice, called a probe, interact with the photon. Eve can freely choose probe and the initial state. But her interaction must obey the laws of quantum mechanics. That is, her interaction must be described by a unitary operator. After the interaction, Eve forwards the photon to Bob. Eve will perform a measurement on her probe to draw Alice's encoding information after Alice announces the basis she used. This is Eve's SI attack scheme. In the case of a multiphoton pulse, Eve will let her probes interact with Alice's photons one-to-one. After Alice's announcements, Eve will perform a coherent measurement on her probes. We call this attack the CMP attack. In Eve's SI attack, if Alice sends a photon in the state $|\uparrow\rangle$, the result may be written as

$$U(|\uparrow\rangle|0\rangle)\rightarrow|X\rangle, \tag{11}$$

where $|X\rangle$ is the entangled state of the probe and the photon [25]. Likewise, we can obtain the state $|Y\rangle$, $|U\rangle$, and $|V\rangle$ corresponding to $|\downarrow\rangle$, $|\rightarrow\rangle$, and $|\leftarrow\rangle$, respectively. In the SI attack scheme, one can obtain that $|X\rangle=\sqrt{f}|\uparrow\rangle|\phi_\uparrow\rangle+\sqrt{e}|\downarrow\rangle|\theta_\uparrow\rangle$, $|Y\rangle=\sqrt{f}|\downarrow\rangle|\phi_\downarrow\rangle+\sqrt{e}|\uparrow\rangle|\theta_\downarrow\rangle$, $|U\rangle=\sqrt{f}|\rightarrow\rangle|\phi_\rightarrow\rangle+\sqrt{e}|\leftarrow\rangle|\theta_\rightarrow\rangle$, and $|V\rangle=\sqrt{f}|\leftarrow\rangle|\phi_\leftarrow\rangle+\sqrt{e}|\rightarrow\rangle|\theta_\leftarrow\rangle$, where f is the fidelity of the state and $f+e=1$. From the unitarity of the interaction, we have that $\langle\phi_\uparrow|\theta_\uparrow\rangle=\langle\phi_\downarrow|\theta_\downarrow\rangle=\langle\phi_\uparrow|\theta_\downarrow\rangle=\langle\phi_\downarrow|\theta_\uparrow\rangle=0$. It then follows from $\langle\phi_\uparrow|\phi_\downarrow\rangle=\cos\alpha$ that QBER$=[1-\cos\alpha]/2$. The maximal information Eve can gain is that

$$I_{\text{SI}}=1-h\left(\frac{1+2\sqrt{e-e^2}}{2}\right), \tag{12}$$

where $h(x)=-x\log_2 x-(1-x)\log_2(1-x)$ and e is QBER.

In Eve's CMP attack scheme, she attaches her probes with all photons in the multiphoton pulse one-to-one. She inter-

acts the probe-photon pair unitarily and then forwards the pulse to Bob. She measures the probes coherently after Alice's announcements. This can be described as

$$[U(|\uparrow\rangle|0\rangle)]^{\otimes n} \rightarrow |X\rangle^{\otimes n}, \tag{13}$$

where

$$[U(|\uparrow\rangle|0\rangle)]^{\otimes n} = \underbrace{U(|\uparrow\rangle|0\rangle)\cdots U(|\uparrow\rangle|0\rangle)}_{n},$$

and

$$|X\rangle^{\otimes n} = \underbrace{|X\rangle\cdots|X\rangle}_{n}.$$

Likewise, one can obtain $|Y\rangle^{\otimes n}$, $|U\rangle^{\otimes n}$, and $|V\rangle^{\otimes n}$. Suppose Alice announces that the $|\uparrow\rangle$, $|\downarrow\rangle$ basis has been used. It has

$$|X\rangle^{\otimes n} = (\sqrt{f}|\uparrow\rangle|\phi_\uparrow\rangle + \sqrt{e}|\downarrow\rangle|\theta_\uparrow\rangle)^{\otimes n}, \tag{14}$$

$$|Y\rangle^{\otimes n} = (\sqrt{f}|\downarrow\rangle|\phi_\downarrow\rangle + \sqrt{e}|\uparrow\rangle|\theta_\uparrow\rangle)^{\otimes n}. \tag{15}$$

Then the two density operators that Eve must distinguish are

$$\rho_\uparrow = \sum_{i=0}^{n} \frac{n! f^{n-i} e^i}{(n-i)!i!} |\phi_\uparrow\rangle^{\otimes n-i} |\theta_\uparrow\rangle^{\otimes i} (\langle\phi_\uparrow|)^{\otimes n-i} (\langle\theta_\uparrow|)^{\otimes i}, \tag{16}$$

$$\rho_\downarrow = \sum_{i=0}^{n} \frac{n! f^{n-i} e^i}{(n-i)!i!} |\phi_\downarrow\rangle^{\otimes n-i} |\theta_\downarrow\rangle^{\otimes i} (\langle\phi_\downarrow|)^{\otimes n-i} (\langle\theta_\downarrow|)^{\otimes i}. \tag{17}$$

The optimal information Eve can gain from these two states can be obtained as follows: Eve first performs the measurements on her probes. If her measurement results are that $|\phi_\uparrow\rangle^{\otimes n-i}|\theta_\uparrow\rangle^{\otimes i}$ (or $|\phi_\downarrow\rangle^{\otimes n-i}|\theta_\downarrow\rangle^{\otimes i}$), where $1 \leqslant i \leqslant n-1$, then Eve knows that her density operator is $\rho_\uparrow$ (or $\rho_\downarrow$) since $\langle\phi_\uparrow|\theta_\uparrow\rangle = \langle\phi_\downarrow|\theta_\downarrow\rangle = \langle\phi_\downarrow|\theta_\uparrow\rangle = \langle\phi_\downarrow|\theta_\uparrow\rangle = 0$. Only if the measurement results are $|\phi_\uparrow\rangle^{\otimes n}$, $|\theta_\uparrow\rangle^{\otimes n}$, $|\phi_\downarrow\rangle^{\otimes n}$, and $|\theta_\downarrow\rangle^{\otimes n}$ can Eve not distinguish her density operators. Suppose that Eve's measurement result is $|\phi_\uparrow\rangle^{\otimes n}$. From $\langle\phi_\uparrow|\phi_\downarrow\rangle = \cos\alpha$, we can obtain

$$(\langle\phi_\downarrow|\phi_\uparrow\rangle)^{\otimes n} = \cos^n\alpha, \tag{18}$$

i.e., the maximal probability that Eve can distinguish $\rho_\uparrow$ from $\rho_\downarrow$ correctly is that $(1+\sqrt{1-\cos^{2n}\alpha})/2$. Thus, the maximal information Eve can gain from her measurement results is

$$\begin{aligned} I_{\mathrm{CMP}}(n) &= 1 - \left[\sum_{i=1}^{n-1} \frac{n! f^{n-i} e^i}{(n-i)!i!} h(1) + f^n h\left(\frac{1+\sqrt{1-\cos^{2n}\alpha}}{2} \right) \right. \\ &\quad \left. + e^n h\left(\frac{1+\sqrt{1-\cos^{2n}\alpha}}{2} \right) \right] \\ &= 1 - (f^n + e^n) h\left(\frac{1+\sqrt{1-(1-2e)^{2n}}}{2} \right). \end{aligned} \tag{19}$$

That is, when Eve uses the CMP attack scheme, the optimal information she can gain is $I_{\mathrm{CMP}}(n)$. Suppose Eve interacts with n photons. If these n photons are from n independent qubits (qubits are uncorrelated since weak coherent sources are used), then the information Eve can gain is nI_{SI}. If these n photons are from a multiphoton pulse, then the information Eve can gain is $I_{\mathrm{CMP}}(n)$. When the QBER is small and the photon number n is not so big, we can gain that $I_{\mathrm{CMP}}(n) \geqslant nI_{\mathrm{SI}}$; see Fig. 1. In fact, most of the multiphoton pulses are two-photon pulses since weak coherent sources are used experimentally. Numerical solution shows that $I_{\mathrm{CMP}}(2) > 2I_{\mathrm{SI}}$ if $e \leqslant 0.11$, at which error correction can be implemented. That is, the CMP attack is more efficient than the SI attack when weak coherent sources are used [26].

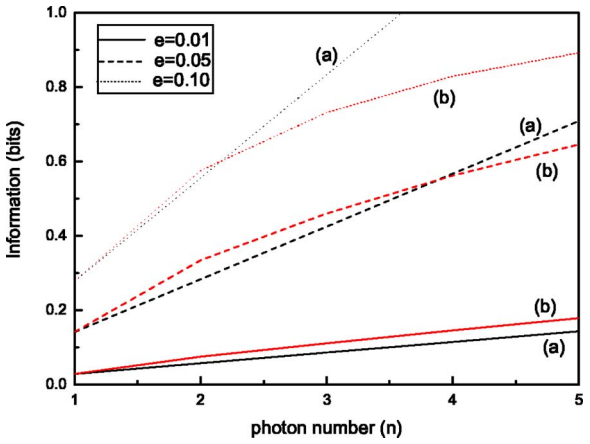

FIG. 1. (Color online) Information vs photon number. Information Eve can gain from n photons by using SI attack (a) is nI_{SI} since these n photons come from n uncorrelated photon pulses. If these n photons are from a multiphoton pulse, then information Eve can gain is $I_{\mathrm{CMP}}(n)$ (b). Numerical solution shows that $I_{\mathrm{CMP}}(2) > 2I_{\mathrm{SI}}$ when $e \leqslant 11\%$. And $I_{\mathrm{CMP}}(3) > 3I_{\mathrm{SI}}$ when $e \leqslant 6.8\%$. CMP attack is more efficient than SI attack when QBER is small.

IV. FROM RAW KEY TO SIFTED KEY

From the discussion above, we know that Eve can get more benefits from a multiphoton pulse than from the single-photon pulse. Since Bob's detection apparatus can resolve the photon number of an arriving pulse, Alice and Bob can discard all of the multiphoton pulses out of the raw key to generate the sifted key. Therefore, only the pulses detected in Bob's detectors as the single-photon pulses will be used to generate the sifted key. In this case, the fraction of counts caused by multiphoton pulses in the sifted key is

$$\Delta = \frac{\sum_{n=2}^{\infty} \mu^n e^{-\mu} \eta (1-\eta)^{n-1} n/n!}{\sum_{n=1}^{\infty} \mu^n e^{-\mu} \eta (1-\eta)^{n-1} n/n!} = 1 - e^{-\mu(1-\eta)}, \tag{20}$$

where

$$\lim_{\eta \rightarrow 0} \Delta = 1 - e^{-\mu}. \tag{21}$$

That is, the upper bound on the fraction of the count caused by multiphoton pulses is $\Delta_0 = 1 - e^{-\mu}$ no matter how high the channel losses are. This upper bound is approximate to μ when faint coherent sources are used. In order to gain the secure final key, a fraction $H_2(e)$ of the sifted key bits is sacrificed asymptotically to perform error correction and a fraction $H_2(e+\Delta_0)$ of the sifted key bits is sacrificed to perform privacy amplification [27]. After the correcting errors in

the sifted key, Alice and Bob can execute privacy amplification in two different strings, the sifted key bits arising from the untagged qubits and the sifted key bits arising from the tagged qubits. The worst case assumption is that the bit error rate is zero for tagged qubits [7]. Therefore, the secure final key can be extracted from the sifted key at the asymptotic rate

$$R \geqslant (1-\Delta_0) - H_2(e) - (1-\Delta_0)H_2\left(\frac{e}{1-\Delta_0}\right). \quad (22)$$

In our scheme, only "single-photon" pulses detected in Bob's detectors are used to generate the sifted key. If this "single-photon" pulse is a multiphoton pulse emitted from Alice, then we assume that it belongs to the tagged qubits. The other "single-photon" pulses detected in Bob's detectors are real single-photon pulses emitted from Alice. Thus, Eve's CMP attack can be ignored in our scheme.

V. PDS QKD WITH IMPERFECT PHOTON-NUMBER-RESOLVING DETECTORS

The resolving power of realistic photon-number-resolving detectors is finite. Suppose the photon-number-resolving power of the detectors is n_0. Let us assume that Eve can attack the photon pulses using PNS attack freely when the photon number of a pulse is bigger than n_0. In this case, additional information Eve can gain is that

$$\Delta' = \frac{\sum_{n=n_0+1}^{\infty} \mu^n e^{-\mu}/n!}{\sum_{n=1}^{\infty} \mu^n e^{-\mu}\eta(1-\eta)^{n-1}/(n-1)!}. \quad (23)$$

The particular resolving power of the detectors in [24] can go up to 10 photons or so (~8 eV), so that the quantity $\Delta' < \mu^{10}/10!$, which is negligible. In fact, Eve cannot get additional information from the pulses $n > n_0$ since decoy states were implemented and all of the multiphoton pulses detected in Bob's detectors were abandoned.

Another question involves dark counts from blackbody photons propagating through the optical fiber. Fortunately, these photons can be filtered well. Experimentally, a very good filter (40 dB out-of-band rejection, 10-nm-wide passband) would result in 0.05 Hz of background counts [28]. Suppose the pulse rate emitted from Alice is r_{pul} and the dark count rate is r_{dark} Hz. We can obtain that the *normalized* dark count rate d (dark counts per pulse) in Bob's detectors is $d \approx r_{\text{dark}}/r_{\text{pul}}\mu\eta$. The distribution of dark counts in Bob's detectors is

$$p_{\text{dark}}[n] = d^n. \quad (24)$$

Therefore, in experiment, Bob can obtain photon-number distribution of the laser pulse by subtracting the dark counts from the real counts. QBER e_{dark} caused by dark counts should be considered, especially in the long-distance QKD,

$$e = e_0 + e_{\text{dark}}, \quad (25)$$

where $e_{\text{dark}} = d/2$, and e_0 is caused by the imperfections of the optical setup [1].

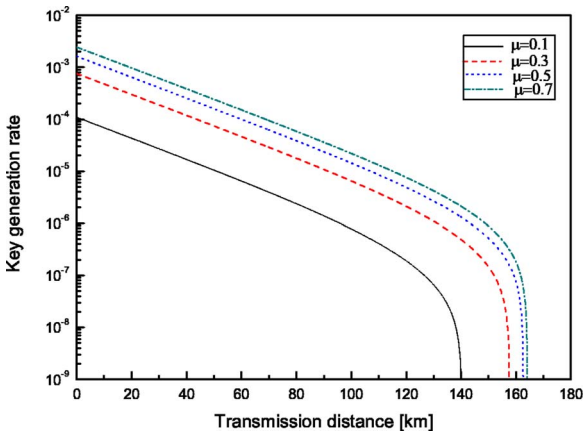

FIG. 2. (Color online) Rate of generating final key vs transmission distance. In order to be comparable, we use the parameters in [17,29] instead of [24]. When $\mu=0.1$, transmission distance is close to 140.2 km. Numerical solution shows that optimal intensity of laser source is $\mu \approx 0.78$ (transmission distance over 164.1 km). That is, a not-so-weak pulse can be used to transmit the key. Optimal intensity of the laser source provides a 23.9 km increase in the transmission distance. Transmission distance is stable to small perturbations to the optimal μ (up to 20% change of μ, less than 0.3% change of transmission distance). Here, we have verified that error correction is allowable for the maximal transmission distance.

VI. OPTIMAL INTENSITY OF THE LASER SOURCE TO GENERATE A SECURE FINAL KEY

In BB84, the rate of generating a raw key is approximate to $\frac{1}{4}\mu\eta$. Thus, the rate of generating a secure final key is approximate to $\frac{1}{4}\mu\eta R$. That is, the rate of generating the secure final key is approximate to R_f, where

$$R_f = \frac{1}{4}\mu\eta\left[(1-\Delta_0 - H_2(e) - (1-\Delta_0)H_2\left(\frac{e}{1-\Delta_0}\right)\right], \quad (26)$$

where $\Delta_0 = 1 - e^{-\mu}$. In practice, e and η are constants when the transmission distance is constant. Therefore, the only variable in R_f is μ. R_f reaches its maximum at the point $\partial R_f/\partial\mu = 0$. In this way, we can obtain the optimal parameter μ; see Fig. 2.

VII. DISCUSSION AND CONCLUSION

In [7], $\Delta \approx p_{\text{multi}}/\mu$, where p_{multi} is the probability of Alice's emitting a multiphoton signal. This is the worst situation where all the multiphoton pulses emitted by Alice will be received by Bob. In the prior decoy state QKD [14,15,17], it requires that $\mu' > \mu$. In [14,15,17], the upper bound on the fraction of counts caused by the multiphoton is $\Delta \leqslant \mu e^{-\mu}/\mu' e^{-\mu'}$. Only if $\mu = \mu'$ can the upper bound be reduced to μ [15]. In our scheme, μ is independent of μ' so that both signal pulse and decoy pulses can be used to generate the sifted key. Another difference is that all the pulses detected in Bob's detectors are discarded, so that Eve's CMP attack does not exist in our scheme. However, the CMP attack should be considered in [14,15,17] since it is more

efficient than the SI attack when QBER is small. Otherwise, the final key may be insecure.

In our scheme, from $\Delta=1-e^{-\mu(1-\eta)}$, we can conclude that the upper bound $\Delta_0=1-e^{-\mu}$ cannot be reduced as long as weak coherent sources and high lossy channel are used. Theoretically, we have to assume that Eve has a lossless channel. Experimentally, Eve can use a BS with transmission probability η to forward the photon to Bob through her lossless channel, which results in the same losses as the real channel. Therefore, this attack cannot be avoided when the channel Alice and Bob hold is lossy. Thus, the fraction $\Delta_0=1-e^{-\mu}$ seems "*inherent*" in the long-distance QKD with weak coherent sources and high lossy channel. This implies that our scheme is optimal as long as weak coherent sources and high lossy channel are used.

In summary, we have discussed the security of the practical BB84 QKD protocol with weak coherent sources, noises, and high losses. We have presented a PDS QKD scheme based on recent experimental advancements. The upper bound on the fraction of counts caused by multiphoton pulses is independent of the intensity of the decoy source so that both the signal pulses and decoy pulses can be implemented to generate the raw key after verifying the security of the QKD. We have shown that the CMP attack is more efficient than the SI attack. Finally, we have shown that a not-so-weak pulse can be used to transmit the key. Optimal μ is presented to improve the rate of generating the secure final key.

ACKNOWLEDGMENTS

We are grateful to D. Rosenberg for providing details of their experiment [24]. This work was supported by the National Natural Science Foundation of China under Grant Nos. 10447140 and 10504039. Y. T. also wishes to thank Ting-yun Shi and the National Natural Science Foundation of China (Grant No. 10374119).

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[3] D. Mayers, J. ACM **48**, 351 (2001).
[4] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, in *Proceedings of the Thirty-Second Annual ACM Symposium on the Theory of Computing*, Portland, OR (2000), pp. 715–724.
[5] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[7] D. Gottesman, H.-K. Lo, N. Lükenhaus, and J. Preskill, Quantum Inf. Comput. **5**, 325 (2004).
[8] C. H. Bennett, F. Bessette, G. Brassward, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992); for a review, please see Ref. [1] and references therein.
[9] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[10] H. P. Yuen, Quantum Semiclassic. Opt. **8**, 939 (1996).
[11] N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).
[12] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[13] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[14] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[15] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[16] X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).
[17] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[18] H.-K. Lo, in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)* (IEEE, Piscataway, NJ, 2004), p. 137.
[19] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[20] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt, e-print quant-ph/0503002.
[21] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004); C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Phys. Rev. A **72**, 032301 (2005); Chi-Hang F. Fung, K. Tamaki, and H.-K. Lo, e-print quant-ph/0510025.
[22] D. Achilles, C. Silberhorn, C. Sliwa, K. Banaszek, I. A. Walmsley, M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, J. Mod. Opt. **51**, 1499 (2004).
[23] E. Waks, K. Inoue, W. D. Oliver, E. Diamanti, and Y. Yamamoto, IEEE J. Sel. Top. Quantum Electron. **9**, 1502 (2003).
[24] D. Rosenberg, A. E. Lita, A. J. Miller, and S. W. Nam, Phys. Rev. A **71**, 061803(R) (2005).
[25] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[26] Some correlative works can be found in M. Curty and N. Lütkenhaus, Phys. Rev. A **69**, 042321 (2004); A. Niederberger, V. Scarani, and N. Gisin, *ibid.* **71**, 042316 (2005).
[27] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[28] Experimental data were obtained from D. Rosenberg (private communication). Perhaps we should assume that Eve can control the dark counts since Eve may change the wavelength of Alice's photon, which is more sensitive for Bob's detectors. However, Bob can add a filter in his laboratory to defeat Eve's attacks. At present, the bandwidth of optical devices is as narrow as 0.1–0.01 nm, which is comparable to the laser linewidth. An optical grating to filter out unwanted frequencies may be used in combination with such narrow bandwidth devices.
[29] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **19**, 3762 (2004).