Decoy-state protocol for quantum cryptography with four different intensities of coherent light

Xiang-Bin Wang*
IMAI Quantum Computation and Information Project, ERATO, JST, Daini Hongo White Bldg. 201, 5-28-3, Hongo, Bunkyo, Tokyo 133-0033, Japan
(Received 2 March 2005; published 20 July 2005)

We propose an efficient decoy-state protocol for practical quantum key distribution using coherent states. The protocol uses four intensities of different coherent light. A good final key rate is achieved by our protocol with typical parameters of existing practical setups, even with a very low channel transmittance.

DOI: 10.1103/PhysRevA.72.012322 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum key distribution(QKD) [1–3] has drawn much attention from scientists since it can help two remote parties to set up the unconditionally secure key [4–7]. However, there are still some limitations for QKD in practice. In particular, large channel loss seems to be the main challenge to the long-distance QKD with weak coherent states. If the perfect single-photon source were used in practice, large channel loss would not be a problem for the security because those lost pulses can be regarded as a vacuum [4]. Given a perfect single-photon source, Eve has to disturb the transmitted qubits if she wants to have some information about them. However, in practice, a perfect single-photon does not exist. Even an almost-perfect single-photon source is a difficult technique [8]. We normally use the weak coherent state. Theoretical results about secure QKD with an imperfect source has also been given [10]. There, the concept of "tagged" bits are used. Say, since the source is imperfect, Eavesdropper (Eve) is able to have full information of some of the bit values without causing any disturbance. In particular, the final key rate can be calculated by the formula [10]:

$$r = 1 - \Delta - H(t) - (1-\Delta)H[t/(1-\Delta)], \tag{1}$$

if we use a random classical CSS code [4] to distill the final key [10]. Here, t is the detected flipping error rate, Δ is the fraction of tagged bits [10] at Bob's side, i.e., the fraction for those counts in cases when Alice sends out a multiphoton pulse if we use coherent light. The functional $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$. From this formula we can see that, if Δ value is small, we can still have a good key rate. However, in practice, the channel can be rather lossy, say, the overall transmittance can be even less than 0.1%. This is to say, even we use an almost-perfect single photon source with only 1% of multiphoton pulses, it does not work unless we have a way to make tight verification of the upper bound of Δ. Trivial worst-case estimation does not work because here it is possible that all single-photon pulses have been lost, therefore the upper bound $\Delta = 1$ and the key rate is 0.

In a protocol using coherent light, all those bits carried by multiphoton pulses are regarded as tagged bits. Eve may split each of them, keep one of them, and send the remaining photons in each pulse to Bob, which is called the photon-number-splitting (PNS) attack. Therefore, we have to seek a way to overcome this [9].

A. Photon-number-splitting attack

The state of coherent light

$$|\mu e^{i\theta}\rangle = \sum_{n=0}^{\infty} \frac{\sqrt{\mu}e^{\mu/2}}{\sqrt{n!}} e^{in\theta}|n\rangle, \tag{2}$$

from a conventional laser is actually a mixed state of

$$\rho_u = \frac{1}{2\pi}\int_0^{2\pi} |\mu e^{i\theta}\rangle\langle\mu e^{i\theta}| \mathrm{d}\theta = \sum_n P_n(\mu)|n\rangle\langle n|, \tag{3}$$

and $P_n(\mu) = \mu^n e^{-\mu}/n!$, since the phase θ is unknown. (Even in the case where θ can be known, one can still randomize it.) Here, μ is a non-negative number. In practice, especially in doing long-distance QKD, the channel transmittance η can be rather small. An Eve may choose to first measure the photon number of each pulses. In measuring the photon number, Eve in principle does not necessarily destroy the bit value of the pulse. Given a multiphoton pulse, e.g., a two-photon pulse, she split it into two beams, with one beam containing one photon. She keeps one photon and sends the other to Bob through a highly transparent channel. After Alice and Bob announce the measurement, Eve measures the photon in the right basis. In such a way, to all those multiphoton pulses sent by Alice, Eve may have full information of their bit value without changing their bit values at all. This is completely different from the case with the single-photon source, where Eve has no way to obtain the information of bit values of the transmitted qubit without disturbing them. Note that by doing so, Eve does not change the total channel transmittance because she can in principle change the transmittance for different pulses as she likes. For example, she may choose to block all (or most of) single-photon pulses, split the multiphoton pulses, and send them through a less lossy channel. To Alice and Bob, the overall transmittance appears the same as that of their usual physical channel. In particular, if $\eta < (1-e^{-\mu}-\mu e^{-\mu})/\mu$, Eve in principle can have the full information of Bob's sifted key by the PNS attack [9] lossless channel.

Originally, the PNS attack has been investigated where Alice and Bob monitor only how many nonvacuum signals

*Email address: wang@qci.jst.go.jp

arise, and how many errors happen. However, it was then shown [11] that the simple-minded method does not guarantee the final security. It is shown [11] that in a typical parameter regime, nothing changes if one starts to monitor the photon number statistics as Eve can adapt her strategy to reshape the photon number distribution such that it becomes Poissonian again. It is not a trivial task to make unconditionally secure QKD even under possible PNS attack. Some possible ways have been raised to solve the issue [12–14]. One promisiong method is the so called decoy-state method proposed by Hwang [12].

B. Decoy-state method

A very important method with decoy states was then proposed by Hwang [12], where the *unconditional* verification of the multiphoton counting rate is given. The main idea is to use two different intensities of pulses. By observing the counting rate of the pulses of the larger intensity (the decoy state), one can verify the upper bound of Δ, the fraction of multiphoton counts at Bob's side for the pulses of less intensity (the signal pulses), given *whatever* type of Eve's action, including PNS attack.

From formula (1), we see that the value of Δ is crucial. Hwang's decoy-state method is so important because it gives a way to verify the upper bound of Δ and, consequently, it gives a way toward the unconditional security of QKD with coherent light. However, Hwang's initial protocol [12] does not give a sufficiently tight bound. If the intensity of decoy state is μ' and signal state is μ in Hwang's protocol, the verified upper bound of Δ in the normal case of no Eavesdropping is

$$\Delta = \frac{\mu e^{-\mu}}{\mu' e^{-\mu'}}. \tag{4}$$

For example, in the case of $\mu=0.3$, by Hwang's method, the optimized verified upper bound of Δ is 60.4%. As it has been mentioned [12,15], the decoy-state method can be combined with GLLP [10] to unconditionally distill the secure final key. With the value $\Delta=60.4\%$, the key rate can be rather low in practice [10]. In particular, formula (1) requires the bit-flip rate to be less than 2% for a larger-than-0 key rate, given that $\Delta=60.4\%$. This is a tough requirement in practice. A *tight* bound for Δ is needed in both the key rate and the threshold of flipping rates. Following Hwang's work [12], the decoy-state method was then further studied [15–20]. It is shown [15] that Hwang's idea can be also used to estimate the quantum bit error rate. However, the main protocol in [15] requires an infinite number of different intensities decoy states. This seems impractical. Prior to this, a review of PNS attack was given with some very shortly stated rough ideas for a possible solution [16]. However, no explicitly demonstrated result was given there [16]. For example, no explicit formula was given on the verified fraction of multiphoton counts. Neither were the effects of statistical fluctuation with only reasonably large number of pulses considered there. In particular, Ref. [16] suggests using two states, vacuum and very weak coherent states to verify the yield (counting rate) of single-photon pulses: ''On one hand, by using a vacuum as decoy state, Alice and Bob can verify the so called dark count rates of their detectors. On the other hand, by using a very weak coherent pulse as decoy state, Alice and Bob can easily lower bound the yield of single-photon pulses.'' If this idea is used, as it has been shown by us in Ref. [20], the intensity of the very weak coherent state must be less than the channel transmittance. Given the channel transmittance. Given the channel transmittance of $\eta=10^{-4}$ and the dark count rate $s_0=10^{-6}$, the number of counts caused by single-photon pulses is only 1/100 of the dark counts. Note that one must estimate the dark counts of the very weak coherent states rather precisely in order to make a meaningful verification of the counting rate of those single-pulses from the very weak coherent states. This is to say, we must limit the possible statistical fluctuation of dark counts to be around the order of 10^{-3} for a meaningful verification. For the unconditional security, we must be exponentially certain that the relative statistical fluctuation is less than $O(10^{-3})$ therefore we can deduce the dark counts for the very weak coherent state with the observed counting rate of the vacuum state. Such an exponential certainty requests at least 10^{14}pulses in one protocol. This is obviously too large to be realized by our existing technologies. It was then for the first time proposed and explicitly demonstrated by us [19] that one can actually make a rather tight verification of value of Δ even with three intensities of coherent light, with one of them being a vacuum. The three-intensity protocol raised by us is different from the previously proposed two-intensity idea [16] not only in using one more intensity, but also in jointly using the counting rates of all three intensities with nontrivial inequalities and simultaneous equations [20]. There [19], the effect of statistical fluctuation is also studied. However, the final key rate has not been calculated. In this paper, based on the protocol given in [19], we propose an improved protocol using four intensities of coherent light. We calculate the the final key rate for typical setups in practice, with the effect of statistical fluctuation being considered. A good key rate is demonstrated in comparison with the theoretically allowed maximal key rate. This paper is arranged as follows. In the next section, we present our protocol and show how it works, why we need four different intensities. Later, we calculate the final key rate of our protocol. We shall end this work with a summary.

II. PROTOCOL WITH FOUR INTENSITIES OF COHERENT LIGHT

We first state the main idea of this protocol. Alice shall use coherent pulses to carry the bit values. We can choose either the polarization space or the phase-coding method for bit values and measurement basis. The intensities of pulses have nothing to do with the bit values. The different intensities may help to verify the the upper bound of fraction of multiphoton counts Δ or lower bound of fraction of single-photon counts Δ_1. After the verification, the do the key distillation. As it has been shown in [19], to do a tight verification, three different intensities will be enough. However, in doing so, the intensities of coherent light cannot be chosen freely, while the final key rate is maximized at only one

value of intensity. To maximize the final key rate, we do the task in this way: We first estimate the lossy rate of the *physical channel*. According to this, we choose good values of intensities μ', μ. These, together with vacuum pulses, will give a very good verification of values Δ, Δ_1. Before the protocol is carried out, we can also expect the bit-flip rate of the channel and we choose another intensity μ_s which gives a maximum key rate given the bit-flip rate and Δ_1, according to the existing theoretical results [10]. After verification and error test, the verified values could be a bit different from the expected ones. However, in the normal case that there is no Eve, the verified values must be rather close to expected ones. In short, there will be four intensities of coherent light in our protocol, they are 0, μ, μ', μ_s. Alice shall randomize the order of all pulses. The first three intensities will be used for verification of of Δ_1 and error test. The last one, μ_s is the intensity of main signal pulses and will be used for final key distillation. Of course, μ, μ' can also be used for final key distillation, in case that the key rate is not zero for these two intensities.

A. Intensity and key rate

How to choose μ_s, the intensity of main signal pulses, is a problem. For clarity, we consider the perfect case where we can use true single-photon source to test the value of Δ_1 or Δ and use the coherent light for key distillation. Given all those single-photon pulses, Eve has no way to tell which ones are from the single-photon source and which ones are from the coherent light source. Consider s_1, the transmittance of single-photon pulse. There are two sets of single-photon pulses, the set of all those pulses from single-photon source (Set 1) and the set of all those single-photon pulses from coherent light (Set 0). Since Eve does not know which ones belongs to which set, we have

$$s_1(1) = s_1(0). \tag{5}$$

Here, $s_1(1)$ and $s_1(0)$ are the transmittance for single-photon pulses in Sets 1 and 0, respectively. After sending out all pulses, Alice announces which pulses belong to Set 1. In counting the number of counts caused by all pulses from Set 1, they shall know the value $s_1(1)$, therefore the value of $s_1(0)$. They can then calculate the value of Δ_1, Δ. (For simplicity we assume zero dark count here, at this moment.) In this way, they can verify Δ, Δ_1 explicitly, if we neglect the statistical fluctuation. For clarity, we consider the ideal case that Δ is known exactly, i.e., $\Delta = 1 - e^{-\mu_s}$. The dark count is zero and the channel transmittance is η. They use coherent states to generate the key. Suppose the tested QBER is t_1', and then they can upperbound the QBER of those single-photon states in signal pulses by

$$t_1 \leqslant (1 + \delta) t_1'. \tag{6}$$

They use coherent state with intensity μ_s to generate the key. According to Ref. [10], the overall key rate is

$$R = \eta \mu_s \{1 - 2H(t_1) - (1 - e^{-\mu_s})[1 - H(t_1)]\}. \tag{7}$$

They may choose an appropriate value μ_s to maximize R. For example, given $t_1 = 0$, maximized value is $R = \eta \mu_s e^{-\mu}$ at the point of $\mu_s = 1$. In this paper, we shall consider the typical case that the QBER is $t_1 = 0.03$ and for this value the TAMKR is

$$R_{\mathrm{TAMKR}} = 0.149\,\eta, \tag{8}$$

with $\mu_s = 0.572$. This is the theoretically allowed maximum key rate. This also shows that, given Δ and bit-flip rate, one can choose an appropriate value μ_s to maximize the key rate. We shall now consider the practical case where the single-photon source is not available and the dark count is nonzero, toward the goal of achieving a large key rate. Note that the value 0.572 does not always maximize the key rate, in practice, because we have different verified values of bit-flip rate and Δ.

B. Verification

One can use the method in Ref. [19] to verify various parameters. For simplicity, we denote those pulses produced in state $|\mu e^{i\theta}\rangle, |\mu' e^{i\theta}\rangle, |0\rangle$ as class Y_μ, $Y_{\mu'}$, and Y_0, respectively. The *counting rate* of *any* state ρ is defined as the probability that Bob's detector clicks whenever a state ρ is *sent out* by Alice. We *disregard* what state Bob may receive here. The *counting rate* is called the *yield* in other literature [12,15]. We use notations s_0, S_μ and $S_{\mu'}$ for the counting rates (yields) of a vacuum and class $Y_0, Y_\mu, Y_{\mu'}$, respectively. These three parameters are observed in the protocol itself. For convenience, we *always* assume $\mu' > \mu$; $\mu' e^{-\mu'} > \mu e^{-\mu}$. A coherent state of class Y_μ has the following convex form:

$$\rho_\mu = e^{-\mu}|0\rangle\langle 0| + \mu e^{-\mu}|1\rangle\langle 1| + c\rho_c \tag{9}$$

and $c = 1 - e^{-\mu} - \mu e^{-\mu} > 0$, $\rho_c = 1/c \Sigma_{n=2}^{\infty} P_n(\mu)|n\rangle\langle n|$. Similarly, a state in class $Y_{\mu'}$ is

$$\rho_{\mu'} = e^{-\mu'}|0\rangle\langle 0| + \mu' e^{-\mu'}|1\rangle\langle 1| + c\frac{\mu'^2 e^{-\mu'}}{\mu^2 e^{-\mu}}\rho_c + d\rho_d, \tag{10}$$

and $d = 1 - e^{-\mu'} - \mu' e^{-\mu'} - c\mu'^2 e^{-\mu'}/\mu^2 e^{-\mu} \geqslant 0$, ρ_d is a density operator. We shall use notations s_0, s_1,s_c,S_μ, $S_{\mu'}$, and s_d for the *counting rates* of state $|0\rangle\langle 0|$, $|1\rangle\langle 1|$, ρ_c, ρ_μ, $\rho_{\mu'}$, and ρ_d, respectively.

For security, we only consider the overall transmittance which is jointly determined by the channel loss and Bob's device loss [19]. Equations (9) and (10) lead to

$$S_{\mu'} = e^{-\mu'} s_0 + \mu' e^{-\mu'} s_1 + c\frac{\mu'^2 e^{-\mu'}}{\mu^2 e^{-\mu}} s_c + d s_d, \tag{11}$$

$$S_\mu = e^{-\mu} s_0 + \mu e^{-\mu} s_1 + c s_c. \tag{12}$$

Given that $s_d \geqslant 0$, Eq. (11) leads to

$$c s_c \leqslant \frac{\mu^2 e^{-\mu}}{\mu'^2 e^{-\mu'}}(S_{\mu'} - e^{-\mu'} s_0 - \mu' e^{-\mu'} s_1). \tag{13}$$

With the crude upper bound for s_c given by Eq. (13), we have the nontrivial lower bound for s_1 now:

TABLE I. Verification of transmittance of single-photon pulse. We need the pulses in class $Y_0, Y_\mu, Y_{\mu'}$ for verification. Class Y_μ or $Y_{\mu'}$ need 10^{10} pulses and Y_0 needs 4×10^9.

η	10^{-3}	10^{-3}	10^{-4}	10^{-4}
s_0	10^{-6}	2×10^{-7}	10^{-6}	2×10^{-7}
μ	0.1	0.1	0.22	0.1
μ'	0.27	0.26	0.48	0.35
s_1/η	0.958	0.969	0.821	0.922

$$s_1 \geqslant S_\mu - e^{-\mu}s_0 - cs_c > 0. \tag{14}$$

Therefore, tight values for s_c and s_1 can be obtained by solving the simultaneous constraints of Eq. (12) and inequality (13). There are two unknown parameters with two constraints. Parameters of s_c, s_1 can be solved analytically [19], and they are indeed very close to the true values in the normal case when there is no Eve.

C. Statistical fluctuation

The results above are only for the asymptotic case, i.e., we have assumed that pulses of the same states will be treated identically by (Eve's) channel, because no one knows which pulse of the state are from which class. In practice, this is not precisely true because the number of pulses are always finite therefore statistical fluctuations have to be considered. That is to say, Eve has a non-negligibly small probability to treat the pulses from different classes a little bit differently, even though the pulses have the same state. Mathematically, this can be stated by $s_\rho(\mu')=(1+r_\rho)s_\rho(\mu)$, and the real number r_ρ is the relative statistical fluctuation for counting rate of state ρ in different classes of pulses. Our task remains to verify a tight lower bound of s_1 and the probability that the real value of s_1 breaks the verified lower bound is exponentially close to 0. We shall use the primed notation for the counting rate for any state in class $Y_{\mu'}$ and the original notation for the counting rate for any state in class Y_μ. We convert Eqs. (12) and (13) to

$$\begin{cases} e^{-\mu}s_0 + \mu e^{-\mu}s_1 + cs_c = S_\mu, \\ cs'_c \leqslant \dfrac{\mu^2 e^{-\mu}}{\mu'^2 e^{-\mu'}}(S_{\mu'} - \mu' e^{-\mu'}s'_1 - e^{-\mu'}s'_0). \end{cases} \tag{15}$$

One should set $s'_x=(1-r_x)s_x$ for $x=1$, c and $s'_0=(1+r_0)s_0$ with $r_x>0$ to obtain the worst-case results. Consider the difference of counting rates for the same state from different classes, Y_μ and $Y_{\mu'}$. To make a faithful estimation, we require the probability to be less than $e^{-O(100)}$ for the failure of verification. With these settings, one can calculate the lower bound of s_1. The numerical results of some typical values of s_1 are listed in Table I.

III. FINAL KEY RATE

Now we calculate the final key rate. It is not likely to give the explicit formula with fluctuation being considered. We shall give the numerical results for typical parameter sets in practice. According to the transmittance of the physical channel, we first choose a reasonable value for μ, e.g., 0.1 or 0.22 and then find a good value μ' so that μ and μ' will help to verify a satisfactorily value of transmittance of single-photon pulses, s_1. According to s_1, we then choose the value μ_s so that the key rate of main signal states is maximized. In a real protocol, Alice is supposed to calculate these values according to the transmittance of physical channel *in advance*. Alice mixes all classes of pulses, sends them to Bob, and then verifies the value of the single-photon transmittance according to the counting rates of states of vacuum, μ and μ'. If the verified value of a single-photon counting rate is too much smaller than the expected value, they give up the protocol. Otherwise, they go on to distill the final key with the method stated in [10]. In order to compare the final key rate of our protocol with that of the ideal protocol, we need to estimate the QBER. For a fair comparison of the ideal protocol and our protocol, we assume the same channel and the same device for both protocols. The bit-flip part of the two protocols should be equal. The bound of phase-flip rate of our protocol should be larger than that in the ideal protocol, because here we have to assume all phase-flip errors have happened to the single-photon pulses. Our main task remaining is to estimate the upper bound of error rate of those single-photon pulses, i.e., e_1. We shall use the observed results in class Y_μ for the estimation of e_1 [15,21]. For such a goal, we first use

$$E_\mu = e + \frac{e^{-\mu}s_0(\mu)}{2S_\mu}, \tag{16}$$

where E_μ is the observed error rate of class Y_μ e is the actual error rate of those nonvacuum pulses and $s_0(\mu)$ is the rate of vacuum counts in class Y_μ. We shall first verify the value e, the true error rate to the nonvacuum pulses, and later we use the worst-case assumption that all of them have happened to the single-photon pulses. Note that E_μ is directly observed, while $s_0(\mu)$ is *derived* from observed counts of class Y_0. We have

$$(1+r_0)s_0 \geqslant s_0(\mu) \geqslant (1-r_0)s_0, \tag{17}$$

with a probability exponentially close to 1. The likely range for r_0 is, e.g., in the case of $\eta=10^{-6}$ with 4×10^9 pulses in class Y_0 is $[-1/2\sqrt{10}, 1/2\sqrt{10}]$. Therefore, we have a range for the value of e, whose upper bound is

$$\hat{e} \leqslant E_\mu - \left(1 - \frac{1}{2\sqrt{10}}\right)\frac{s_0}{2S_\mu} = e + \frac{s_0}{4\sqrt{10}S_\mu}. \tag{18}$$

Here, $\hat{e}$ is our estimated upper bound of actual error rate of nonvacuum pulses in class Y_μ. In the worst case, all of these flips could have happened to those single-photon pulses. We have

$$\hat{e}_1 = f * \left(E_\mu - \frac{s_0(\mu)}{2S_\mu}\right); f = \Delta_1^{-1}(\mu), \tag{19}$$

and $\hat{e}_1$ is the estimated upper bound of net flipping rate of single-photon pulses and $\Delta_1(\mu)=s_1/S_\mu$. In the normal case that there is no Eve., the observed value $S_\mu=1-e^{-\eta\mu}+S_0(\mu)$ therefore

$$\Delta_1(\mu)=\frac{\frac{s_1}{\eta}\cdot\eta\mu e^{-\mu}}{1-e^{-\eta\mu}+s_0(\mu)}\approx\frac{e^{-\mu}s_1}{\eta}/[1+s_0(\mu)/(\eta\mu)]. \tag{20}$$

We should choose the worst value of r_0 among its likely range so that $\hat{e}_1$ is maximized. We can also estimate the phase-flip error by using the data of class μ' in a similarly way.

As it has been shown in Ref. [21], in case of nonzero dark count, one can have a key rate formula even stronger than Eq. (1). Actually, for phase-flip part, one only needs to correct those phase-flip of single-photon pulses. Therefore the key rate for class Y_s is [21]:

$$R_s=S_{\mu_s}\left[\Delta_1(\mu_s)-H(E_s)-\Delta_1(\mu_s)H\left(f*\left(E_\mu-\frac{e^{-\mu}s_0}{2S_\mu}+\frac{r_0e^{-\mu}s_0}{2S_\mu}\right)\right)\right], \tag{21}$$

and $\Delta_1(\mu_s)=s_1/S_{\mu_s}$. In the normal case that there is no Eve., the observed value $S_{\mu_s}=1-e^{-\eta\mu}+S_0(\mu_s)$ therefore

$$\Delta_1(\mu_s)=\frac{\frac{s_1}{\eta}\cdot\eta\mu e^{-\mu_s}}{1-e^{-\eta\mu_s}+s_0(\mu_s)}\approx\frac{\frac{s_1}{\eta}\cdot\eta\mu e^{-\mu_s}}{\eta\mu_s+s_0(\mu_s)}. \tag{22}$$

In calculating $\Delta_1(\mu_s)$, since $\eta\mu_s$ is much larger than $s_0(\mu_s)$, we simply replace $s_0(\mu_s)$ by s_0. Note that the quantities S_{μ_s}, E_{μ_s}, and E_μ are directly observed in the protocol itself. Here, we use the averaged values in normal cases for these quantities to estimate the final key rate. Of course in a real protocol, the observed values could be a bit different from our assumed values; consequently, the key rate in a real protocol could be also a bit different. Normally, the observed value of S_{μ_s} must be around $1-e^{-\eta\mu_s}+s_0\approx\eta\mu_s+s_0$. E_s is the error rate of the main signal pulses. It should be dependent on both the net flipping rate of nonvacuum pulses and the dark count. If the net flipping rate of nonvacuum pulses is 3%, then the observed value for E_s must be around $E_s=0.03+s_0/2S_{\mu_s}$. Similarly, $E_\mu=0.03+s_0/2S_\mu$. Given all these, our formula for key rate is given by

$$R_s=S_{\mu_s}\left[\Delta_1(\mu_s)-H\left(0.03+\frac{s_0}{2S_{\mu_s}}\right)-\Delta_1(\mu_s)H\left(\left(0.03+\frac{(1-e^{-\mu})s_0}{2S_\mu}+\frac{e^{-\mu}r_0s_0}{2S_\mu}\right)f\right)\right]. \tag{23}$$

Here, we have assumed that the error rate of single-photon pulses in class Y_μ and class Y_s are equal for simplicity. We shall argue it later that this assumption does not change our main results. The key rate of the ideal protocol is

TABLE II. Final key rate, R. The last row is the ratio of key rate from main signal pulses and the theoretically allowed maximal value. We have assumed the QBER for signal states in the *Ideal protocol* is bounded by $t=3\%$. The number of pulses of in Y_s can be any number larger than 10^{10}. R_{TAMKR}: Theoretically allowed maximum key rate.

η, s_0	$10^{-3}, 10^{-6}$	$10^{-3}, 2\times10^{-7}$	$10^{-4}, 10^{-6}$	$10^{-4}, 2\times10^{-7}$
μ, μ'	0.1,0.27	0.1,0.26	0.22,0.45	0.1,0.35
$s_1(\mu_s)/\eta$	0.958	0.969	0.821	0.922
μ_s	0.548	0.555	0.452	0.532
R/R_{TAMKR}	87.0%	90.1%	42.0%	78.3%

$$R_0(\mu_x)=S_{\mu_x}\left[D_1(\mu_x)-H\left(0.03+\frac{s_0}{2S_{\mu_x}}\right)\right]-D_1(\mu_x)H\left[0.03+\left(\frac{s_0}{2(\eta+s_0)}\right)\right]. \tag{24}$$

and

$$D_1(\mu_x)=\frac{\eta\mu_xe^{-\mu_x}}{1-e^{-\eta\mu_x}+s_0}, \tag{25}$$

and the value μ_x is chosen to maximize the key rate in Eq. (24). We shall calculate $R_s/[\mathrm{Max}(R_0(\mu_x))]$ for the relative key rate. The key rates for class Y_s in various cases is listed in Table II. In our comparison, we have ignored the statistical fluctuation of the error rate, i.e., we have assumed the error rate of tested bits are equal to that of untested bits. This does not change our main result because we have only considered the *relative key rate*, i.e., the ratio of our protocol's key rate and the ideal protocol's key rate and the ideal protocol also has a fluctuation in error rate. Now, we consider a more restricted condition: The two protocols use the same number of test bits in error test. Consider the error values in Eqs. (23) and (24). We now assume the values of bit-flip rate and phase-flip rate in Eq. (24) are values *after* taken the statistical fluctuation, which is about 0.5% in our setting. Therefore the *bit-flip* rate in Eq. (23) remains the same because the fluctuation of this part is almost same with that in the ideal protocol. We only need to consider the change in *phase-flip* part of Eq. (23). Consider the worst specific setting of $\eta=10^{-4}$, $s_0=10^{-6}$ in Table II. Given such a setting, the *phase-flip* of our protocol is about two times of that of the ideal protocol. Therefore, its likely statistical fluctuation is almost two times of that ideal protocol, i.e., about 1%. (We have assumed that the number of single-photon pulse in class Y_μ in our protocol is equal to the number of pulses from perfect single-photon source in the ideal protocol.) But now, we have assumed the *phase-flip* value in Eq. (24) to be the one *after* taking the fluctuation, therefore we only need to raise the phase-flip value in our protocol by 0.5% for a new comparison. This will decrease the result of R/R_0 by only 5%. Even though we assume zero-statistical fluctuation for the ideal protocol, the net effect here is to raise the *bit-flip* rate by 0.5% and the *phase-flip* rate by 1% in our protocol, and a

fairly good key rate can still be obtained for our protocol with a very lossy channel.

IV. SUMMARY

In summary, we have proposed an efficient and feasible decoy-state protocol with four intensities to do QKD over very lossy channel. We have clearly demonstrated how it works efficiently in practice. That is, how it works with typical parameter sets in practice and with statistical fluctuations given only a reasonable number of total pulses. Our results show that, to improve the distance of secure QKD, reducing the rate of the dark count is crucially important. Raising the system repetition rate is also important because it reduces the possible relative statistical fluctuation. Our protocol with four different intensities of coherent states can be realized immediately by using current existing setups.

Note added: Several months after the initial presentation of Ref. [19] and this work (quant-ph/0411047), our 3-intensity protocol [19] was further studied in Ref. [22].

ACKNOWLEDGMENTS

I am grateful to Professor H. Imai for his long-term support. I thank Toshiyuki Shimono for his kind help with the numerical calculations. I thank W. Y. Hwang, N. Lükenhaus, K. Matsumoto, H.-K. Lo and many other colleagues for discussions. J. Kim for inviting me to KIAS where I did part of this job and H. W. Lee for inviting me to KAIST.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, UK, 2000).
[2] N. Gisin, G. Ribordy, W. Tittttel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002), and references therein.
[3] C. H. Bennett and G. Brassard, in *Proceedings IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175–802.
[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000), and references therein.
[5] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[6] D. Mayers, J. ACM **48**, 351 (2001); Its preliminary version appeared in *Advances in Cryptology-Proc. Crypto'96* Vol. 1109 of Lecture Notes in Computer Science, edited by N. Koblitz.
[7] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[8] E. Waks, C. Santori, and Y. Yamamoto, Phys. Rev. A **66**, 042315 (2002).
[9] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995); G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**,1330 (2000).
[10] H. Inamori, N. Lütkenhaus, and D. Mayers, e-print quant-ph/0107017; and D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[11] N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).
[12] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[13] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); M. Koashi, *ibid.* **93**, 120501 (2004).
[14] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004); A. Acin, N. Gisin, and V. Scarani, Phys. Rev. A **69**, 012309 (2004).
[15] H.-K. Lo, X.-F Ma, and K. Chen ⟨http://www.fields.utoronto.ca/programs/scientific/04-05/quantumIC/abstracts/lo.ppt;/lo. pdf⟩ Decoy state quantum key distribution (QKD); and also ⟨http://www.newton.cam.ac.uk/webseminars/pg+ws/2004/qisw01/0826/lo/⟩.
[16] H.-K. Lo, in *Proceedings of 2004 IEEE Int. Symp. on Inf. Theor.* (2004), p. 17.
[17] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[18] H. Kosaka *et al.*, Electron. Lett. **39**, 1199 (2003).
[19] X. B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[20] X. B. Wang, e-print quant-ph/0501143.
[21] X. B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[22] X. Ma, B. Qi, Z. Zhao, and H.-K. Lo, e-print quant-ph/0503005.