# Decoy-state quantum key distribution with large random errors of light intensity

Xiang-Bin Wang*
*Department of Physics, Tsinghua University, Beijing 100084, China*
*and JST, 4-1-8 Honcho, Kawaguchi-shi, Satima 332-0012, Japan*
(Received 19 September 2006; published 2 May 2007)

We show how to do decoy-state quantum key distribution efficiently with large random errors in the intensity control. We present a theorem for efficiently calculating the lower bound of single-photon counts with many undetermined parameters. In the calculation of the single-photon counts of our protocol, the linear terms of the intensity fluctuation disappear and only the quadratic terms take effect. Given that the intensity fluctuation is upper bounded by ±5%, ±10%, and ±15%, the verified lower bound of the percentage of untagged bits from our protocol is as large as 99.7%, 99.0%, and 97.9% of that from an ideal protocol where the light intensity is exactly controlled.

DOI: 10.1103/PhysRevA.75.052301 PACS number(s): 03.67.Dd, 42.81.Gs, 03.67.Hk

## I. INTRODUCTION

Recently, some proposals have been made for implementing quantum key distribution (QKD) [1–3] securely with existing technologies [4–11]. The decoy-state method [4–8] seems to be very promising: it only requires a random switch of the intensity of coherent-state pulses (light pulses directly from a laser device) among a few values. Different from the earlier results [12], which used only one intensity of coherent light, the decoy-state method is unconditionally secure under any attack, including the so-called photon-number-splitting (PNS) attack [12–14]. By the separate theoretical results of Inamori, Lütkenhaus, and Mayers (ILM) and Gottesman, Lo, Lütkenhaus, and Preskill (GLLP) [15], QKD can be done securely even if Alice uses an imperfect source, provided that the upper bound of the fraction of tagged bits (those raw bits caused by multiphoton pulses from Alice) or the lower bound of the fraction of single-photon counts is known. The decoy-state method can be used to verify such bounds faithfully and efficiently.

Decoy-state QKD has been implemented in a number of experiments [16–20]. Very recent experiments have demonstrated a QKD distance longer than 100 km [17–19] and a very stable, remarkable key rate over a distance of more than 20 km [20], with one-way quantum communication only. All these indicate that decoy-state QKD will be practically useful. However, the existing theory of the decoy-state method assumes the exact intensity of each light pulse. As a continuous variable, the intensity of a coherent-state light pulse cannot be controlled exactly in principle. A very important problem in practical QKD is how to use the decoy-state method efficiently, given the inexact control of the pulse intensity. In this paper, we study this problem and we find that, if the intensity error of each pulse is random, the decoy-state method can work efficiently even when there are large intensity errors. This paper is arranged as follows. After a brief background review of decoy-state QKD in the next section, we show in Sec. III how to verify the fraction of single-photon counts by the decoy-state method when there are random intensity fluctuations in the decoy and signal pulses, if the averaged intensity is bounded in a small range. A simple method to verify the bounds of the averaged intensity is presented in Sec. IV. We then evaluate the efficiency of our method in Sec. V. A discussion of the applicability of our protocol is given in Sec. VI. The paper ends with concluding remarks in Sec. VII. Detailed derivations of some formulas used in Sec. III are given in the Appendix.

## II. BACKGROUND REVIEW

To have a clear picture, we would like first to consider an analogy here. We want to distill out pure water from raw water by heating. For security, we have to heat the raw water for a sufficiently long time so that all poisonous constituents in the raw water are removed. The heating time is dependent on the amount of poison in the raw water. The ILM-GLLP result says that if the amount of poisonous constituents in the raw water is given, then we know the heating time needed to remove all harmful constituents, and the remaining water is pure. For security, we need only the upper bound of the poisonous constituents. Suppose the true amount is $\hat{\Delta}$ and this requires a heating time $\tilde{t}$. If we overestimate the amount as $\Delta \geqslant \tilde{\Delta}$, we shall use a longer heating time $t \geqslant \tilde{t}$. We can regard it as two-stage heating: first, heat the water for time $\tilde{t}$ and then take additional heating for an interval $t-\tilde{t}$. Since at time $\tilde{t}$ the water is pure already, it is still pure with any additional heating. This ILM-GLLP result itself does not show how to verify the amount of poisonous constituents in the raw water. If we overestimate the amount too much, we need too long a heating time and then all the raw water may be evaporated and we obtain nothing finally; if we underestimate the amount then we are worrying that the raw water is insufficiently heated and the remaining water after heating is still impure. The "decoy-state method" in this analog is to *faithfully* and *tightly* verify the upper bound of poisonous constituents in the raw water. The verified amount is always larger than the true amount for any type of raw water, and the verified amount is normally only a little bit larger than the true value.

Now we come back to the theory of QKD with an imperfect source. We start from the theoretical result of ILM and

*Electronic address: xbwang@mail.tsinghua.edu.cn

 

GLLP [15]. The elementary concept there is the so-called tagged bits, of which Eve can have full information without causing any disturbance. In the case that Alice uses an imperfect source, those raw bits caused by multiphoton pulses from Alice are regarded as tagged bits, because Eve in principle can have full information of their bit values without causing any disturbance if she uses a PNS attack. The ILM-GLLP results [15] show that, even if Alice has used an imperfect source, a secure final key can be distilled if one knows the upper bound of the tagged bits. There are two important features of the ILM-GLLP results [15]. First, the key distillation does not need information about which raw bits are tagged. Second, the key distillation does not need an exact value for the fraction of tagged bits. The only information needed is the upper bound of the fraction of tagged bits among all those initial bits. In particular, the final key rate is given by [15]

$$R = 1 - \Delta - H(t) - (1-\Delta)H\left(\frac{t}{1-\Delta}\right), \tag{1}$$

where $\Delta$ is the upper bound of the fraction of tagged bits, $t$ is the quantum bit-flip rate (QBER), and $H(t)=-t\log_2 t-(1-t)\log_2(1-t)$. There are two tasks in the final key distillation, error correction and privacy amplification. Formula (1) shows that after the error correction, which consumes $H(t)$ of raw bits, is done, $q=\Delta+(1-\Delta)H(t/(1-\Delta))$ bits must then be used in privacy amplification to guarantee security. Suppose the true value of the fraction of tagged bits is $\hat{\Delta}\leqslant\Delta$. If we knew the exact value $\hat{\Delta}$, we would need to consume only $\tilde{q}=\hat{\Delta}+(1-\hat{\Delta})H(t/(1-\hat{\Delta}))$ of raw bits in the privacy amplification in order to obtain a secure final key $\tilde{\mathcal{K}}$. But we do not know the precise value $\hat{\Delta}$; what is used is the upper bound value $\Delta$ in doing the privacy amplification. This means that if we replace the precise value $\hat{\Delta}$ by a larger value $\Delta$, we shall consume more than the needed amount of raw bits in the privacy amplification and the final key $\mathcal{K}$ is shorter than $\tilde{\mathcal{K}}$. Equivalently, the whole privacy amplification can be virtually divided into two stages. In stage 1, $\tilde{q}$ raw bits have been consumed and the key $\tilde{\mathcal{K}}$ is obtained. In stage 2, $q-\tilde{q}$ raw bits are consumed for a further privacy amplification and the final key $\mathcal{K}$ is obtained. Since $\tilde{\mathcal{K}}$ is secure already, additional privacy amplification to a secure key is also secure. Therefore $\mathcal{K}$ is secure. This means that any overestimation of the amount of tagged bits is secure. However, too much overestimation will decrease the key rate or even lead to a zero final key. For example, if we trivially assume $\Delta=1$, this is a correct upper bound but the key rate will be zero. Before the decoy-state method was proposed, one had no other choice but to trivially assume that all those multiphoton pulses caused counts at Bob's side. This would overestimate the $\Delta$ value drastically with increase in the distance of QKD. The necessary condition for a secure QKD is $\Delta<1$. Consider a coherent state of intensity $x$ (with phase randomization)

$$\hat{\rho}_x = \sum_{n=0}^{\infty} \frac{e^{-x}x^n}{n!}|n\rangle\langle n|. \tag{2}$$

Suppose the channel transmittance is $\eta$ and the constant intensity $x=\mu$ is used by Alice for all pulses. The total counts of Bob's detector are given by

$$1 - e^{\eta\mu} + d_B \approx \eta\mu + d_B \approx \eta\mu \tag{3}$$

if the dark count rate $d_B$ of Bob's detector is very small. For security, we need

$$\eta\mu > e^{-\mu}\mu^2/2 \tag{4}$$

if we trivially assume that all those multiphoton pulses have caused counts at Bob's side. This requires $\eta>\mu e^{-\mu}/2$. Note that Eve could also control the instantaneous detection efficiency of Bob's detector. Suppose the average detection efficiency of Bob's detector is $\xi_B$ and the light intensity decreases by one-half over every 15 km, then $\eta=2^{-L/15}\xi_B$, given the QKD distance $L$. The secure distance is then limited by

$$L < -15\log_2(e^{-\mu}\mu\xi_B^{-1}/2). \tag{5}$$

This shows that the secure distance decreases with increasing intensity $\mu$. If $\mu\geqslant 0.1$ and $\xi_B\leqslant 10\%$, the secure distance is shorter than 20 km. One can raise the secure distance by decreasing $\mu$; however, this demands better detection technology [21] because otherwise the quantum bit-flip rate will be too large due to the dark count. Also, the key rate will be low if $\mu$ is too small.

The central task of the decoy-state method is to verify the $\Delta$ value faithfully and tightly. For security, the verification should be faithful so that the verified value $\Delta$ should never be smaller than the true value of the fraction of tagged bits, whatever is Eve's channel. For efficiency, the verified $\Delta$ value should be only a little larger than the true value in the normal case when there is no Eve.

If one uses coherent states, information about the upper bound of the tagged bits (multiphoton counts) is equivalent to information about the lower bound of the fraction of single-photon counts $\Delta_1$. The ILM-GLLP result has then been improved [26] and a higher key rate formula is given based on the the lower bound of the fraction of single-photon counts

$$R = \Delta_1 + \Delta_0 - H(t) - \Delta_1 H(t_1), \tag{6}$$

where $\Delta_1$ and $\Delta_0$ are the lower bounds of the fraction of single-photon counts, and vacuum counts respectively, and $t_1$ is the upper bound of the QBER of those single-photon pulses. Recently, the result has been further improved by Koashi [27].

In this paper, we shall study only how to verify the lower bound of the fraction of single-photon counts instead of the upper bound of the fraction of tagged bits hereafter. We shall call those raw bits caused by single-photon pulses sent from Alice untagged bits.

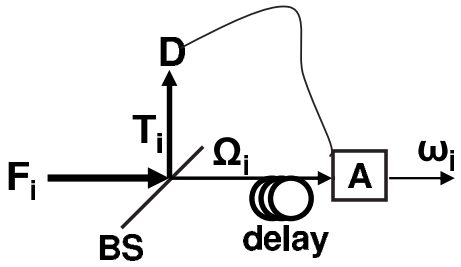


FIG. 1. Single-shot feedforward control of the intensity of each individual light pulse. BS, beam splitter; $D$, detector; $A$, attenuator. The attenuator offers instantaneous attenuation controlled by the measurement outcome of $D$. Since there could be random errors in the measurement outcome and attenuation, there are random errors in the outcome light pulse $\omega_i$.

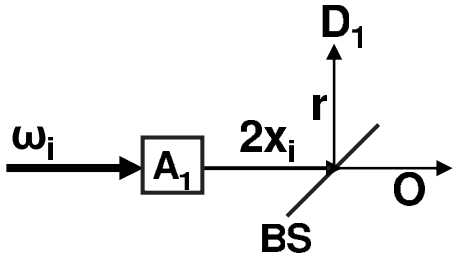


FIG. 2. Our proposed setup for decoy-state QKD. $D1$, low-efficiency detector; $A1$, constant attenuation; BS, 50:50 beam splitter. The transmitted light (pulse $O$) is sent to Bob and the reflected light (pulse $r$) is detected by Alice. The intended intensity of pulse $x_i$ can be either $\mu$ or $\mu'$ as required by the three-intensity decoy-state protocol. By observing the number of counts of $D1$, the bound values of the *averaged* intensity of output pulses can be determined tightly.

## III. THREE-INTENSITY DECOY-STATE METHOD WITH RANDOM INTENSITY FLUCTUATIONS

The counting rate of any state $\rho$ is defined as the probability that Bob's detector counts whenever Alice sends out a pulse of state $\rho$. If Alice sends out $N$ pulses of state $\rho$ and Bob observes $n$ counts, the counting rate of state $\rho$ is $S=n/N$. In general, given a source producing independent pulses of mixed states,

$$\rho = a_1|1\rangle\langle 1| + (1-a_1)\tilde{\rho}, \tag{7}$$

if the lower bound of the counting rate of the single-photon state ($|1\rangle\langle 1|$) is known to be $s_1$, the $\Delta_1$ value of this source is $a_1 s_1/S$. Note that in such a case $S$ can be directly observed in the experiment. In the following we shall consider only how to verify $s_1$. In the protocol, Alice uses three types of pulse, vacuum pulses, decoy pulses of supposed intensity $\mu$, and signal pulses of supposed intensity $\mu' > \mu$ (and $\mu' < 1$). For simplicity of presentation we shall also call these three types of pulses three classes: $Y_0$, $Y$, and $Y'$ for the vacuum pulses, the decoy pulses, and the signal pulses, respectively. At each time, Alice chooses a pulse randomly from one class and sends it to Bob. More explicitly, we assume that at each time, the probabilities of using a vacuum pulse (a pulse from $Y_0$), a decoy pulse, and a signal pulse is $p_0$, $p_\mu$, and $p_{\mu'}$, respectively ($p_{\mu'} > p_\mu > p_0, p_0+p_\mu+p_{\mu'}=1$).

We shall assume that the intensity fluctuation of each individual pulse is random. This is possible if we use some specially designed schemes to generate the pulses. For example, consider a scheme where Alice controls the intensity of each decoy pulse and signal pulse by the single-shot feedforward method as shown in Fig. 1. Each time she first produces a strong father pulse $F_i$ whose intensity is not controlled exactly. This pulse is then split into two daughter pulses: the (strong) reflected pulse $T_i$ of intensity $I_i$ and the transmitted pulse $\Omega_i$. The intensity of pulse $T_i$ is detected in detector $D$. Given the intensity of the pulse $T_i$ and the reflection-transmission ratio $\mathcal{R}$ of the beam splitter, the intensity of the pulse $\Omega_i$ can be calculated. The attenuator $A$ is controlled instantaneously according to the single-shot detection outcome (the electrical current) of $D$. If Alice wants to produce a constant intensity $w$ for the outcome pulse $\omega_i$, the instantaneous attenuation should be set to be $\mathcal{R}w/I_i$ exactly. If the measurement and the feedforward instantaneous attenuation are done accurately, the intensity of the outcome pulse $\omega_i$ is a constant. However, there could be *random* errors in the measurement outcome (the electrical current of $D$) and in the instantaneous attenuation, and these errors cause random fluctuations of the intensity of the light pulse $\omega_i$. (The intensity of the outcome pulse $\omega_i$ should be controlled to be larger than $2\mu'$ in the scheme.)

There are many ways to do the instantaneous attenuation. For example, one can make use of photon polarization. Set the polarization of pulse $F_i$ to be horizontal. If the polarization of pulse $\Omega_i$ is rotated by a certain angle, the intensity of the pulse after passing through a horizontal polarizer will be decreased accordingly. Alternatively, one can also attenuate a light pulse with a phase shift. The light is first split into two beams and then a phase shift is taken on one beam. After combining these two beams in a beam splitter, one output beam will be attenuated accordingly. Here we require feedforward control of the attenuation, i.e., the polarization rotation or the phase shift at each time, to be determined by the measurement outcome (electrical current) of detector $D$. This type of feedforward technique has been demonstrated in a recent experiment with electronic optical modulators (EOMs) in another application [22]. There, the overall delay time for a complete feedforward polarization rotation is about 150 ns, which requires an optical fiber of 30 m long to delay the light. The switching time of an EOM is about 65 ns [22]. This allows an overall repetition rate of more than 15 MHz, which exceeds the repetition rates of the existing decoy-state experiments already. The EOM switching time can be further shortened [23]. Pulse $\omega_i$ from Fig. 1 is used as the input light pulse in our protocol as shown in Fig. 2.

Given these random errors, whenever Alice wants to use $\mu$ or $\mu'$, she actually uses

$$\mu_i = (1+\delta_i)\bar{\mu}, \quad \mu_i' = (1+\delta_i')\bar{\mu}'. \tag{8}$$

Alice does not know the value of the instantaneous fluctuation $\delta_i$ or $\delta_i'$. Here $\bar{\mu}, \bar{\mu}'$ are the averaged intensities of the decoy and signal pulses

$$\bar{\mu} = \frac{1}{N}\sum_{1}^{N} \mu_i, \quad \bar{\mu}' = \frac{1}{N'}\sum_{1}^{N'} \mu_i', \tag{9}$$

and $N, N'$ are number pulses in classes $Y, Y'$, respectively. As shown in Sec. IV, the values of $\bar{\mu}, \bar{\mu}'$ can be determined in very narrow ranges as

$$\bar{\mu} \in [\mu_-, \mu_+], \quad \bar{\mu}' \in [\mu_-', \mu_+'] \tag{10}$$

using the circuit shown in Fig. 2. We shall make use of the following important fact:

$$\sum_{0}^{N} \delta_i = \sum_{0}^{N'} \delta_i' = 0 \tag{11}$$

in the calculation. Since the intensity error of each individual pulse is random and independent, the state of each class can be represented by a single-pulse state. The true state of a pulse in class $Y$ (decoy pulse) can be written into the following convex form:

$$\rho_\mu = \frac{1}{N}\sum_{i,n=0}^{N} \hat{\rho}_{\mu_i} = a_0|0\rangle\langle 0| + a_1|1\rangle\langle 1| + a_c\rho_c, \tag{12}$$

with $a_0 = \Sigma_i e^{-\mu_i}/N$, $a_1 = \Sigma_i \mu_i e^{-\mu_i}/N$, $a_c = 1 - a_0 - a_1$; $\hat{\rho}_{\mu_i}$ is the density operator of the coherent state of intensity $\mu_i$ as defined in Eq. (2) with $x = \mu_i$, and $\rho_c$ is the density operator of all multiphoton pulses in class $Y$. Explicitly,

$$a_c\rho_c = \frac{1}{N}\sum_{i=1}^{N}\sum_{n=2}^{\infty} \frac{\mu_i^n e^{-\mu_i}}{n!}|n\rangle\langle n|. \tag{13}$$

The state of a signal pulse is

$$\rho_{\mu'} = \frac{1}{N'}\sum_{i=1}^{N'}\sum_{n=0}^{\infty} \hat{\rho}_{\mu_i'}. \tag{14}$$

Here $\hat{\rho}_{\mu_i'}$ is a coherent state of intensity $\mu_i'$, as defined by Eq. (2) with $x = \mu_i'$. If $\bar{\mu}'$ is sufficiently larger than $\bar{\mu}$ and the intensity error is not too large, we can also write $\rho_{\mu'}$ in a convex form including $\rho_c$:

$$\rho_{\mu'} = a_0'|0\rangle\langle 0| + a_1'|1\rangle\langle 1| + a_c'\rho_c + a_d'\rho_d \tag{15}$$

with $a_0' = \Sigma_i e^{-\mu_i'}/N'$, $a_1' = \Sigma_i \mu_i' e^{-\mu_i'}/N'$, $a_c' = (\Sigma \mu_i'^2 e^{-\mu_i'}/N')/(\Sigma \mu_i^2 e^{-\mu_i}/N) a_c$, $a_d' \geqslant 0$, and $\rho_d$ a density operator. Given these convex forms of the decoy and the signal states, we have the following equations:

$$S_\mu = a_0 S_0 + a_1 s_1 + a_c s_c,$$

$$S_{\mu'} = a_0' S_0 + a_1' s_1 + a_c' s_c + a_d' s_d. \tag{16}$$

Here $S_0, S_\mu, S_{\mu'}$ are the observed counting rates of pulses in classes $Y_0, Y, Y'$, respectively. Therefore we regard them as known parameters in the protocol. $s_1$ and $s_c$ are unknown variables of the counting rates of single-photon pulses and pulses of state $\rho_c$; $s_d$ is the counting rate of state $\rho_d$ which is regarded as an unknown parameter. The values of parameters $\{a_x | x = 0, 1, c\}, \{a_x' | x = 0, 1, c, d\}$ are not determined yet. In practice, the number of pulses is always finite; therefore statistical fluctuation for the counting rate of a certain state is unavoidable. In general, we can assume $s_x' = (1 - r_x)s_x$, $x = 1, c$, and $\{s_1', s_c'\}$, $(\{s_1, s_c\})$ are the counting rates of single-photon pulses and $\rho_c$ pulses from class $Y'$ $(Y)$ respectively. The ranges of $\{r_x | x = 1, c\}$ can be determined by classical sampling theory. The vacuum counts from classes $Y, Y'$ can also be a bit different from that of class $Y_0$. We use the notations $s_0, s_0'$ for the counting rates of vacuum pulses in classes $Y, Y'$; their possible ranges can also be determined by classical sampling theory. If we define $b_c' = (1 - r_c)a_c'$, Eq. (16) is changed to the following form for the nonasymptotic case:

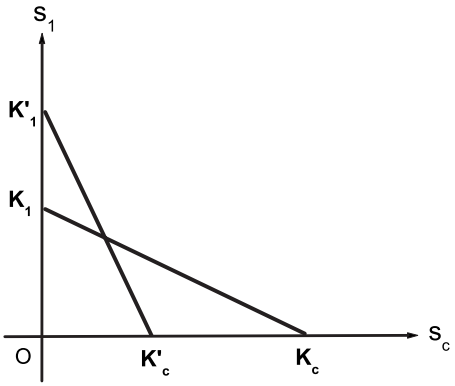


FIG. 3. Graphics of Eq. (17) in $s_1$-$s_c$ plane. Obviously, the $s_1$ value will be raised if $K_1$ or $K_c$ is raised, or if $K_1'$ or $K_c'$ is decreased. This leads to our theorem.

$$\mathcal{S} = a_1 s_1 + a_c s_c,$$

$$\mathcal{S}' = a_1' s_1 + b_c' s_c, \tag{17}$$

and $\mathcal{S} = S_\mu - a_0 s_0$, $\mathcal{S}' = S_{\mu'} - a_0' s_0' + f_1 - a_d' s_d$, and $f_1 = r_1 a_1' s_1$. Therefore, it will be secure if we find the smallest value $s_1$ satisfying the equation above among all possible values for the parameters $\mathcal{S}, \mathcal{S}', a_1, a_c, a_1', b_c'$. In general, this can be done numerically. But there are too many undetermined parameters here; therefore the complexity of numerical solution can be huge. In what follows we first make an analytical study of how to obtain the worst-case solution for $s_1$ given the ranges of all parameters, and then we show how to determine the range of each parameter.

Define $K_1 = \mathcal{S}/a_1$, $K_c = \mathcal{S}/a_c$, $K_1' = \mathcal{S}'/a_1'$, $K_c' = \mathcal{S}'/b_c'$. We can always find a meaningful solution for $s_1, s_c$ if

$$K_1' > K_1 > 0, \quad K_c > K_c' > 0, \tag{18}$$

as shown in Fig. 3. The solution of $s_1, s_c$ is the crossing point of the two lines in the $s_c$-$s_1$ plane. In this plane, it is easy to see that the $s_1$ value rises if $K_1'$ or $K_c'$ decreases, or if $K_1$ or $K_c$ rises. Therefore, the largest possible values of $K_1', K_c'$ and the smallest possible values of $K_1, K_c$ will produce the lower bound of $s_1$. Therefore we have the following theorem.

*Theorem*. Given Eq. (17), if Eq. (18) holds, the maximum values of the parameters in set $U = \{a_0 s_0, a_1, a_c, f_1\}$ and the minimum values of the parameters in set $V$

$=\{a_0 s_0', a_1', b_c', a_d', s_d\}$ will give the smallest non-negative value of $s_1$ that satisfies Eq. (17).

Given this theorem, the remaining task is to determine the upper bounds of parameters in set $U$ and the lower bounds of parameters in set $V$. We have the following bound values for those parameters involved in Eq. (17):

$$e^{-\mu_+} \leqslant a_0 \leqslant e^{-\mu_-}(1+\bar{\mu}^2\delta^2/2),$$

$$(1-\mu_-\delta^2)\mu_- e^{-\mu_-} \leqslant a_1 \leqslant \mu_+ e^{-\mu_+},$$

$$a_c \leqslant 1 - e^{-\mu_+} - \mu_+ e^{-\mu_+} + \mu_+\delta^2/2, \tag{19}$$

$$a_0' = \frac{1}{N}\sum e^{-\mu_i'} \geqslant e^{-\bar{\mu}_+'},$$

$$a_1' \geqslant (1-\mu_-'\delta'^2)\mu_-' e^{-\mu_-'},$$

$$b_c' \geqslant (1-r_c)\frac{\mu_-'^2(1-e^{-\mu_-}-\mu_- e^{-\mu_-})}{(1+\delta^2)\mu_+^2 e^{\mu_-'-\mu_+}},$$

$$a_d' s_d \geqslant 0, \tag{20}$$

with $\delta=\mathrm{Max}\{\delta_i\}$, $\delta'=\mathrm{Max}\{\delta_i'\}$, and $\mu_\pm$ and $\mu_\pm'$ are bound values of the averaged intensity of the decoy pulses or the signal pulses, respectively, as defined in Eq. (10). The derivations of the inequalities above are shown in the Appendix. The task remaining is to determine the values of $\mu_\pm$ and $\mu_\pm'$. These can be done by simple tomography at Alice's side.

## IV. DETERMINE THE AVERAGED INTENSITIES BY SIMPLE TOMOGRAPHY

Alice can, as shown in Fig. 2, every time first produce a pulse of intensity $2\mu_i$ or $2\mu_i'$ through attenuating the pulse $\omega_i$. The pulse is then split by a 50:50 beam splitter. The transmitted mode is sent to Bob, while the reflected mode goes to a low-efficiency photon detector, e.g., with a detection efficiency of $\xi \leqslant 10\%$. Suppose she has observed the clicking rate of $h+d_0$ and $h'+d_0$ for those $N$ reflected pulses of intensity $\{\mu_i\}$ and $N'$ reflected pulses of intensity $\{\mu_i'\}$, respectively. Here $d_0$ is the dark count rate of her detector. Mathematically,

$$\sum_0^N (1-e^{-\xi\mu_i})/N = h, \tag{21}$$

which is equivalent to

$$\xi\bar{\mu} - \frac{\sum(1+\delta_i^2)\xi^2\bar{\mu}^2}{2N} + \cdots = h. \tag{22}$$

This leads to the following facts:

$$\bar{\mu} \geqslant h/\xi, \tag{23}$$

$$\xi\bar{\mu} - \frac{\sum(1+\delta_i^2)\xi^2\bar{\mu}^2}{2N} \leqslant h. \tag{24}$$

The following inequality is obtained after solving Eq. (24):

$$\bar{\mu} \leqslant \mu_+ = \frac{1-\sqrt{1-2h(1+\zeta)}}{\xi(1+\zeta)} \approx h/\xi + h^2(1+\zeta)/(2\xi) \tag{25}$$

and $\zeta=\Sigma\delta_i^2/N \leqslant \delta^2$, $\delta=\mathrm{Max}\{|\delta_i|\}$. Using the Taylor expansion of Eq. (21) we obtain a tightened lower bound formula based on Eqs. (23) and (25),

$$\bar{\mu} \geqslant \mu_- = h/\xi + h^2/(2\xi) - \xi^2\mu_+^3/3! \tag{26}$$

Replacing $h$ with $h'$ in Eqs. (25) and (26) we can also bound $\bar{\mu}'$:

$$\bar{\mu}' \geqslant \mu_-' = h'/\xi + h'^2/(2\xi) - \xi^2\mu_+'^3/3! \tag{27}$$

and

$$\bar{\mu}' \leqslant \mu_+' = \frac{1-\sqrt{1-2h'(1+\zeta')}}{\xi(1+\zeta')} \approx h'/\xi + h'^2(1+\zeta')/(2\xi) \tag{28}$$

with $\zeta'=\Sigma\delta_i'^2/N' \leqslant \delta'^2$, $\delta'=\mathrm{Max}\{\delta_i'\}$. Alice can now know the bounds of all parameters in Eqs. (19) and (20) with the observed values $h,h'$ and the above formulas for $\bar{\mu},\bar{\mu}'$.

## V. EFFICIENCY EVALUATION

We shall compare the efficiency of two protocols, the ideal protocol where the intensity of light pulses from each class is controlled exactly (0, $\mu$, or $\mu'$) and our protocol where the intensity of each light pulses is inexactly controlled. In a real experiment using our protocol, Alice simply reads $h,h'$ values and then calculates the lower bound of $s_1$. Here we assume the model that Alice has observed

$$h = 1-e^{\xi\mu} \approx \xi\mu - \xi^2\mu^2/2, \quad h' = 1-e^{\xi\mu'} \approx \xi\mu' - \xi^2\mu'^2/2 \tag{29}$$

in carrying out our protocol. Here $\mu$ and $\mu'$ are the intensity values Alice wants to use for decoy and signal pulses. In carrying out our protocol, Alice tries her best to produce intensities $\mu,\mu'$ as accurately as possible. [*Remark*. Equation (29) is only an assumed model to forecast what $h,h'$ would be observed if one did the experiment using our method. In a real experiment, one simply uses the observed values of $h,h'$ instead of Eq. (29).] Given these, we can calculate bounds for $\bar{\mu}$ and $\bar{\mu}'$ by our earlier equations. We take the following assumptions: $\mu=0.2$, $\mu'=0.6$, $\xi=5\%$ for Alice's detection efficiency, a linear channel with transmittance $\eta=10^{-4}$, $S_0=s_0=s_0'=0$, $N=10^9$, and $\delta=\delta'$. In both protocols we use $f_1 \leqslant 10a_1\sqrt{s_1/N\mu e^{-\mu}}$ and $r_c \geqslant 10\sqrt{1/s_c(1-a_0-a_1)N}$. As shown in Ref. [5], the probability that the actual value of the statistical fluctuation goes beyond any of the assumed ranges above is exponentially small. To compare the efficiencies of our protocol and the ideal protocol, we only need to compare the solutions of Eq. (17) for the two protocols. We now denote $s_1,\tilde{s}_1$ to be the lower bounds of single-photon transmittance verified from our protocol and from the ideal protocol, respectively. The lower bound of the fraction of single-photon counts from class $Y'$ is given by

TABLE I. Efficiency comparison of our protocol and an ideal protocol.

| | $\delta$ | | | | | | |
|---|---|---|---|---|---|---|---|
| | 5% | 10% | 15% | 20% | 25% | 30% | 35% |
| $T$ | 99.8% | 99.6% | 99.2% | 98.7% | 98.0% | 97.2% | 96.3% |
| $R$ | 99.7% | 99.0% | 97.9% | 96.3% | 94.4% | 91.9% | 89.2% |

$$\Delta_1' = s_1\mu' e^{-\mu'}(1-\mu'\delta^2)/(1-e^{-\eta\mu'}),$$

$$\tilde{\Delta}_1' = \tilde{s}_1\mu' e^{-\mu'}/(1-e^{-\eta\mu'}). \quad (30)$$

$\Delta_1'$ is for our protocol, $\tilde{\Delta}_1'$ is for the ideal protocol. We shall calculate $T=s_1/\tilde{s}_1$, $R=\Delta_1'/\tilde{\Delta}_1'$. We find very good results given various $\delta$ values, as shown in Table I. Moreover, the results of our protocol can even be improved because there are obviously better ways to bound $\zeta,\zeta'$ more tightly. For example, suppose we know that the fluctuation of more than 90% of the pulses is less than 10%, even though the largest fluctuation is 50%; we have $\zeta \leqslant 3.4\%$ and we can verify $R \geqslant 96\%$ with $\delta^2$ being replaced by $\zeta$ in all equations. For another example, Alice can use two detectors of efficiencies $\xi_1,\xi_2$ to tightly verify the upper bound of $\zeta$. Every time she first produces a pulse of intensity $3x$. She equally divides the pulse into three modes, mode $b$ is sent to Bob, and modes 1 and 2 are sent to detectors 1 and 2 at her side, respectively. Using the number of counts of each detector at her side, she can verify an upper bound of the $\zeta$ value almost equal to the true value.

Our theorem is based on the conditions of Eq. (18). These conditions are related to the statistical fluctuations, which are dependent on the value of $s_1,s_c$. But we can verify these conditions before knowing the exact values of $s_1,s_c$. Denote $\eta=S_\mu/\mu$. There are only two possibilities for the value of $s_c$, i.e., $s_c \geqslant 2\eta$ or $s_c < 2\eta$. If $s_c \geqslant 2\eta$, we have the bound values of

$$f_1 \leqslant 10a_1\sqrt{\frac{\eta}{a_1 N}}, \quad 1-r_c \geqslant 1-\sqrt{\frac{1}{2\eta a_c N}}. \quad (31)$$

Given these, we can easily verify Eq. (18) and then obtain the lower bound value of $s_1$ through our theorem. If $s_c < \eta$, using the first equality of Eq. (17) we find that $s_1 > \eta$, which is a very good result because in the normal case of a linear lossy channel, the true value of $s_1$ is just $\eta$. Therefore, given whatever value of $s_c$, it is secure if we use $\mathrm{Min}\{\eta,\mathbf{s}_1\}$ as the verified lower bound of the single-photon counting rate ($\mathbf{s}_1$ is the calculated result with the assumption $s_c \geqslant 2\eta$.) Normally, one should find that $\mathbf{s}_1 \leqslant \eta$. In such a case, the $\mathbf{s}_1$ value is used to distill the final key. If $\mathbf{s}_1 > \eta$, one must use $\eta$ as the fraction of untagged bits for the final key distillation.

In the above discussions, we have assumed that the vacuum pulses in class $Y_0$ are exactly produced. But there could also be errors in producing the vacuum pulses of class $Y_0$. This can be easily resolved as shown below. In general, $S_0 \neq 0$. We can safely set $s_0'=0$ according to our theorem and we need to consider only the upper bound of $s_0$. Asymptotically, we can simply replace $s_0$ by $S_0$ even though pulses in $Y_0$ are not strictly vacuum. Assume that the actual state in $Y_0$ is $\rho_0=(1-\epsilon_0)|0\rangle\langle 0|+\epsilon_1|1\rangle\langle 1|+\epsilon_m\rho_m$. Here $\rho_m$ is a state of multiphoton pulses, $\epsilon_m=O(\epsilon_1^2)$, $\epsilon_1 \ll 1$, and $\epsilon_0=\epsilon_1+\epsilon_m$. Therefore, we have

$$S_0 = (1-\epsilon_0)s_0 + \epsilon_1 s_1 + \epsilon_m s_m. \quad (32)$$

This leads to a preliminary upper bound of $s_0 \leqslant S_0/(1-\epsilon_0)$. We then replace $s_0$ in Eq. (17) and solve the equation for lower bound of $s_1$. We assume $s_1 \geqslant 1.5S_0$ at this stage; otherwise the protocol should be discarded. A new bound of $s_0 \leqslant S_0/(1-\epsilon_0)-\epsilon_1 s_1 \leqslant S_0$ is obtained if Eq. (32) is used again. According to our theorem, the result is secure if the $s_0$ value is overestimated. Therefore one can simply use $S_0$ even though the vacuum pulses in class $Y_0$ are not exactly vacuum.

## VI. DISCUSSION

We have assumed that the intensity error of each pulse is independent and random in our protocol above. However, if the feedforward control is not used, the intensity error may not be perfectly random and the results here do not directly apply. If the intensities of each pulse are correlated, then neither the state of the decoy pulses nor the state of the signal pulses can be represented by a single-pulse state. Also, the counting rate of single-photon pulses from different classes can be different even if there are infinite pulses of each class. Consider an extreme example. The intensity of each individual pulse is 10% larger than the assumed values ($\mu$ or $\mu'$) for the first half of the decoy and signal pulses and 10% smaller than the assumed values for the second half. Eve's channel transmittance is $4\eta$ for the first half of the pulses and $\eta$ for the second half of the pulses. (Eve can change the channel transmittance according to the averaged pulse intensities of a certain time interval. She can detect the intensity change through measuring the pulses in a very short period, given that the system repetition rate larger than 1 MHz.) The counting rate of the single-photon pulses in class $Y$ is

$$s_1 = \frac{1.1\mu e^{-1.1\mu}\times 4\eta + 0.9\mu e^{-0.9\mu}\times\eta}{1.1\mu e^{-1.1\mu}+0.9\mu e^{-0.9\mu}}. \quad (33)$$

The counting rate of single-photon pulses in class $Y$ is

$$s_1' = \frac{1.1\mu' e^{-1.1\mu'}\times 4\eta + 0.9\mu' e^{-0.9\mu'}\times\eta}{1.1\mu' e^{-1.1\mu'}+0.9\mu' e^{-0.9\mu'}}. \quad (34)$$

Given $\mu=0.2$, $\mu'=0.6$, we find that

$$s_1/s_1' = 1.023\,35 > 1. \quad (35)$$

Therefore, the single-shot feedforward scheme in our protocol or any other scheme to guarantee the randomness of intensity error is necessary. Of course we can also use the protocol in Ref. [24] where randomness is not required, but the protocol requires producing the decoy and signal pulses from the same father pulse and using a stable two-value attenuator. Another alternative is presented in Ref. [25] where the only condition for a secure final key is to know the larg-

est possible intensity error, given any error pattern, but the final key rate decreases drastically with small intensity errors.

## VII. CONCLUDING REMARKS

In summary, we have shown that the decoy-state method can work efficiently even if there are large errors in the light intensity, if the intensity errors of each pulse are random. The lower bound of the fraction of untagged bits can be verified efficiently since the effect of linear terms of the fluctuation disappears, and we only need to consider the quadratic terms in the protocol. It should be interesting to implement the protocol here in the future.

## ACKNOWLEDGMENTS

We thank Z.-L. Yuan and Y.-K. Jiang for discussions. This work was supported in part by the National Basic Research Program of China through Grant Nos. 2007CB807900, 2007CB807901.

## APPENDIX

In this appendix we derive the inequalities of (19) and (20). First, $a_0=(1/N)\Sigma e^{-\mu_i}=(1/N)e^{-\bar{\mu}}\Sigma e^{-\bar{\mu}\delta_i}$. After the Taylor expansion, we have

$$\sum e^{-\bar{\mu}\delta_i}=\sum\left(1-\bar{\mu}\delta_i+\frac{\bar{\mu}^2\delta_i^2}{2}-\cdots\right). \tag{A1}$$

Using the facts that $\Sigma\delta_i=0$ and $\delta=\mathrm{Max}\{|\delta_i|\}$, we obtain

$$e^{-\bar{\mu}}\leqslant a_0\leqslant e^{-\bar{\mu}}(1+\bar{\mu}^2\delta^2/2). \tag{A2}$$

Further, the fact that $\mu_-\leqslant\bar{\mu}\leqslant\mu_+$ leads to

$$e^{-\bar{\mu}_+}\leqslant a_0\leqslant e^{-\bar{\mu}_-}(1+\bar{\mu}^2\delta^2/2). \tag{A3}$$

This is the first inequality in Eq. (19). We have the following equivalent form for $a_1=(1/N)\Sigma\mu_i e^{-\mu_i}$:

$$a_1=\frac{1}{N}\bar{\mu}e^{-\bar{\mu}}\sum(1+\delta_i)\left(1-\bar{\mu}\delta_i+\frac{1}{2}\bar{\mu}^2\delta_i^2-\cdots\right). \tag{A4}$$

This means

$$\bar{\mu}e^{-\bar{\mu}}(1-\bar{\mu}\delta^2)\leqslant a_1\leqslant\bar{\mu}e^{-\bar{\mu}}, \tag{A5}$$

which gives rise to

$$\mu_-e^{-\mu_-}(1-\mu_-\delta^2)\leqslant a_1\leqslant\mu_+e^{-\mu_+}, \tag{A6}$$

the second inequality of Eq. (19). Next we consider $a_c=1-a_0-a_1=1-(1/N)\Sigma(e^{-\mu_i}+\mu_i e^{-\mu_i})$. As a result of Taylor expansion

$$a_c=1-e^{-\bar{\mu}}\left(1+\bar{\mu}-\frac{\delta^2\bar{\mu}^2}{2}+\cdots\right), \tag{A7}$$

which leads to

$$1-e^{-\bar{\mu}}-\bar{\mu}e^{-\bar{\mu}}\leqslant a_c\leqslant 1-e^{-\bar{\mu}}-\bar{\mu}e^{-\bar{\mu}}+e^{-\bar{\mu}}\bar{\mu}^2\delta^2/2. \tag{A8}$$

Given the bounds of of $\bar{\mu}$, we have

$$1-e^{-\bar{\mu}_-}-\bar{\mu}_-e^{-\bar{\mu}_-}\leqslant a_c\leqslant 1-e^{-\bar{\mu}_+}-\bar{\mu}_+e^{-\bar{\mu}_+}+e^{-\bar{\mu}_+}\bar{\mu}_+^2\delta^2/2. \tag{A9}$$

The derivations of the first two inequalities in Eq. (20) are same as far Eq. (19). We only show the third one here. To obtain the lower bound, we have

$$\frac{\sum\mu_i'^2e^{-\mu_i'}/N'}{\sum\mu_i^2e^{-\mu_i}/N}\geqslant\frac{\bar{\mu}'^2e^{-\bar{\mu}'}}{(1+\delta^2)\bar{\mu}^2e^{-\bar{\mu}}}. \tag{A10}$$

Therefore we have

$$a_c'\geqslant\frac{\bar{\mu}'^2e^{\bar{\mu}-\bar{\mu}'}a_c}{\bar{\mu}^2(1+\delta^2)}\geqslant\frac{\mu_-'^2(1-e^{-\bar{\mu}_-}-\bar{\mu}_-e^{-\bar{\mu}_-})}{(1+\delta^2)\mu_+^2e^{\mu_-'-\mu_+}}. \tag{A11}$$

Given that $b_c'=(1-r_c)a_c'$, we arrive at the third inequality of Eq. (20).

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] M. Dusek, N. Lütkenhaus, M. Hendrych, in *Progress in Optics*, edited by E. Wolf (Elsevier, Amsterdam, 2006), Vol. 35; N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).
[4] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[5] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[6] X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).
[7] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[8] J. W. Harrington *et al.*, e-print arXiv:quant-ph/0503002.
[9] R. Ursin *et al.*, e-print arXiv:quant-ph/0607182.
[10] 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).
[11] M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004); K. Tamaki, N. Lükenhaus, M. Loashi, and J. Batuwantudawe, e-print arXiv:quant-ph/0607082.
[12] M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg, Opt. Express **4**, 383 (1999); D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, New J. Phys. **4**, 41 (2002); H. Kosaka *et al.*, Electron. Lett. **39**, 1199 (2003); C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004); X.-F. Mo *et al.*, Opt. Lett. **30**, 2632 (2005); G. Wu, J. Chen, Y. Li, L.-L. Xu, and H.-P. Zeng, Phys. Rev. A **74**, 062323 (2006).
[13] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995); H. P. Yuen, Quantum Semiclassic. Opt. **8**, 939

(1996).
[14] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[15] H. Inamori, N. Lütkenhaus, and D. Mayers, e-print quant-ph/0107017; D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[16] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006); Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, in Proceedings of ISIT, Harbin 2006 (unpublished), p. 2094.
[17] Cheng-Zhi Peng, Jun Zhang, Dong Yang, Wei-Bo Gao, Huai-Xin Ma, Hao Yin, He-Ping Zeng, Tao Yang, Xiang-Bin Wang, and Jian-Wei Pan, Phys. Rev. Lett. **98**, 010505 (2007).
[18] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, J. E. Nordholt, A. E. Lita, and S. W. Nam, Phys. Rev. Lett. **98**, 010503 (2007).
[19] T. Schmitt-Manderbach *et al.*, Phys. Rev. Lett. **98**, 010504 (2007).
[20] Z.-L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **90**, 011118 (2007).
[21] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, New J. Phys. **8**, 193 (2006).
[22] R. Prevedel *et al.*, Nature (London) **445**, 65 (2007).
[23] Y. Soudagar *et al.*, e-print arXiv:quant-ph/0605111.
[24] X.-B. Wang, C.-Z Peng, and J.-W. Pan, Appl. Phys. Lett. **90**, 031110 (2007).
[25] X.-B. Wang, C.-Z. Peng, J. Zhang, and J.-W. Pan, e-print arXiv:quant-ph/0612121.
[26] H.-K. Lo, Quantum Inf. Comput. **5**, 413 (2005).
[27] M. Koashi, e-print arXiv:quant-ph/0505018; e-print arXiv:quant-ph/0609180.