Decoy state quantum key distribution with a photon number resolved heralded single photon source

Tomoyuki Horikiri and Takayoshi Kobayashi
Core Research for Evolutional Science and Technology (CREST), Japan Science and Technology Corporation (JST), Tokyo, Japan and Department of Physics, Graduate School of Science, University of Tokyo, 7-3-1 Hongo, Bunkyo, Tokyo, 113-0033, Japan

(Received 28 November 2005; revised manuscript received 14 February 2006; published 23 March 2006)

Recently a long distance and high key rate quantum key distribution (QKD) has become possible by the idea of the decoy state method. We show that a longer distance QKD is possible by utilizing a heralded single photon source (utilizing spontaneous parametric down-conversion) as a source instead of a weak coherent pulse (WCP) as proposed in the original decoy state method. Moreover, the key rate is improved by utilizing a presently available photon number resolving detector as a trigger detector of the heralded single photon source and it is shown to approach the key rate of the WCP.

DOI: 10.1103/PhysRevA.73.032331 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum key distribution has drawn considerable attention as a method of achieving a shared absolutely secure private key [1]. However, there are imperfections in the real world which can make it difficult to guarantee security: for instance, loss by absorption in the quantum communication channel, imperfections in the light source, or inefficiencies of detectors in the detection system. Whether security under such conditions is possible is a major problem, and recently security in the situation where both sources and detectors have imperfections has been proven [2] and a lower bound to the key rate has been given. The problem is that this key rate is very small and the possible transmission distance is short.

However, we see a great improvement in the key generation rate and the distance with the proposed decoy state method by Hwang [3]. The method has been advanced by several researches [4–6,15]. Now we can consider experimental setups that were thought insecure, but can indeed be shown to be secure. Put simply, to generate keys over long distances experimentalists choose high intensity light. On the other hand, before the decoy state method, security could not be guaranteed when high intensity light is used over long distances.

In the decoy state method any attacks of an eavesdropper (Eve) influence the detection rate or the error rate for an n-photon signal. By this method we can achieve a great improvement, and we use even a conventional laser as the source. In this paper we show that if we use a different source called a heralded single photon source (HSPS) and a presently available photon number resolving detector as a trigger detector of the HSPS, longer distance secure communication can be attained. This improvement is possible because we can utilize the coincidence property of spontaneous parametric down-conversion to reduce the dark count probability. Suppression of multiphoton probability due to the photon number resolving detector contributes to the increase of the key rate.

The paper is organized as follows. In Sec. II we overview the decoy state method. Then we consider the use of a heralded single photon source as a source in Sec. III. In Sec. IV it is shown that it is possible to increase the key rate if an available photon number resolving detector is used for the trigger of the heralded single photon source. We speculate about practical aspects in Sec. V, and the realizability of our proposal is considered.

II. DECOY STATE METHOD

In the decoy state method decoy pulses are designed to sneak between signal pulses at random, and the loss of the signal and error rate are estimated by checking the loss of the decoy pulses (it is postulated by quantum mechanics that Eve cannot distinguish signal from decoy) and legal users can check tapping. Any attacks by an eavesdropper affect the signal and/or error rate. Thus whatever the eavesdropper's attacks are, they can be detected. The main advantage of the decoy state method is that the estimated probability from a single photon signal can be larger than that given in Ref. [2] (we call this GLLP) in which the part in the sifted key originating from a single photon cannot be estimated well. In GLLP, all multiphoton signals that leave Alice's source are assumed to be detected by Bob, and the detection probability of a single photon was estimated as $Q_\mu - p_{\text{multi}}$ where Q_μ is the total detection probability, given that a pulse of mean photon number μ is emitted by Alice, and p_{multi} is the probability Alice emits more than one photon. However, in the decoy state method the actual signal probability originating from a single photon can be calculated from the detection data of Bob. This probability is important when we calculate the secure key rate as in Eqs. (5) and (6). The difference is large in the case where the distance becomes long.

In the original decoy state based schemes a weak coherent pulse (WCP) is assumed as a light source. Gain (overall detection probability) Q_μ and key bit error rate E_μ, which are necessary to calculate the key rate, are given as follows:

$$Q_\mu = Y_0 e^{-\mu} + Y_1 e^{-\mu}\mu + Y_2 e^{-\mu}(\mu^2/2) + \cdots + Y_n e^{-\mu}(\mu^n/n!) + \cdots , \tag{1}$$

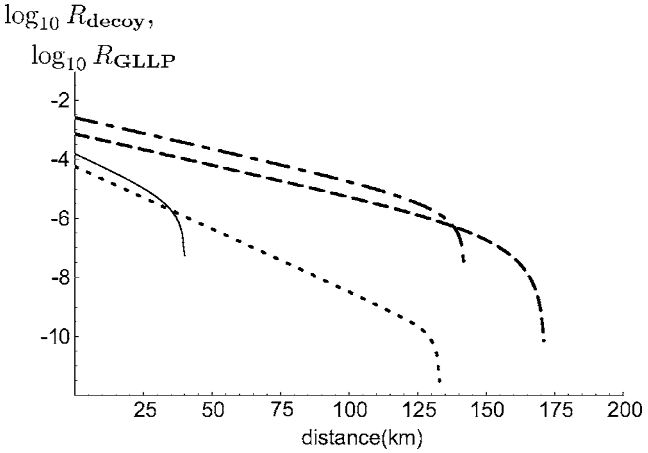

FIG. 1. Key rate. Solid curve: R_{GLLP} for the WCP. Dotted curve: R_{GLLP} for the HSPS. Dotted-dashed curve: R_{decoy} for the WCP. Dashed curve: R_{decoy} for the HSPS.

$$Q_\mu E_\mu = Y_0 e^{-\mu} e_0 + Y_1 e^{-\mu} \mu e_1 + Y_2 e^{-\mu} (\mu^2/2) e_2 + \cdots + Y_n e^{-\mu} (\mu^n/n!) e_n + \cdots, \quad (2)$$

where Y_n is Bob's detection probability conditioned that an n-photon pulse is sent by Alice. e_n is a key error probability when an n-photon pulse is launched. Therefore total gain Q_μ (total error rate E_μ) is the total detection (error) probability given that a pulse of mean photon number μ is emitted by Alice and can be directly observed by Bob. From Eqs. (1) and (2), Q_μ (E_μ) is a linear function of Y_n (e_n); thus, they can detect attacks that change Y_n or e_n if they prepare several values of μ [15]. Y_n and e_n are given as follows:

$$Y_n = \eta_n + Y_0 - \eta_n Y_0 \approx \eta_n + Y_0, \quad (3)$$

$$e_n = \left(e_{detector} \eta_n + \frac{1}{2} Y_0 \right) \Big/ Y_n, \quad (4)$$

where $\eta_n = 1-(1-\eta)^n$ is the probability that at least one photon out of n photons is detected (η is a product of transmittance of the quantum channel and detection probability of Bob), Y_0 is the contribution of the dark count and stray light, and e_{det} is the probability that a photon hits an erroneous detector due to a misalignment of the system or other imperfections in the optical setups. Because these values can be calculated beforehand (properties of the channel, source, and detection system are assumed to be well known by users), we can compare the known channel values to see if there is an attack.

The key rates in GLLP and the decoy state method are given as follows [2,5]:

$$R_{\text{decoy}} = q\{- Q_\mu f(E_\mu) H_2(E_\mu) + Q_1 [1 - H_2(e_1)]\}, \quad (5)$$

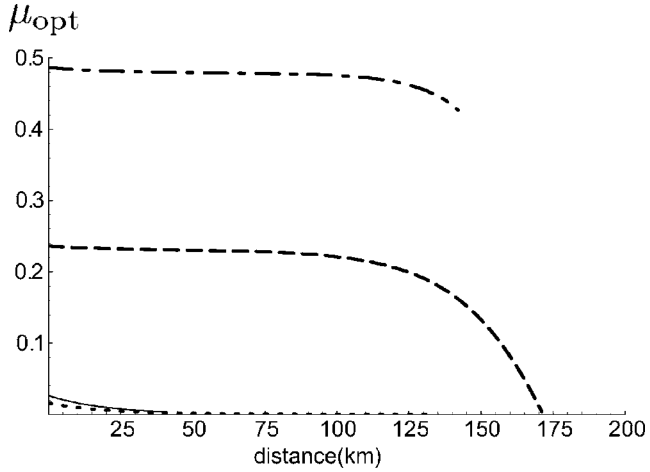

FIG. 2. Optimal mean photon number. Solid curve: R_{GLLP} for the WCP. Dotted curve: R_{GLLP} for the HSPS. Dotted-dashed curve: R_{decoy} for the WCP. Dashed curve: R_{decoy} for the HSPS.

$$R_{\text{GLLP}} = q\left\{ - Q_\mu f(E_\mu) H_2(E_\mu) + (Q_\mu - p_{\text{multi}}) \times \left[1 - H_2\left(\frac{E_\mu}{\Omega} \right) \right] \right\}. \quad (6)$$

Q_1 is the gain of single photon states, $q=\frac{1}{2}$ in the ordinary Bennett-Brassard 1984 (BB84) protocol, $H_2(e)$ is a binary entropy function, and $f(e)$ is the bidirection error correction efficiency.

This formula is a function of overall transmittance because it includes $Y(n)$'s. Thus we can calculate the distance dependence of the key rate. When the key rate is positive, we can do secure key generation between two parties. Positive areas of the two are greatly different [5]. When the transmittance η is large, the advantage of the decoy state method is small because there are no big differences in the probability of two or more photons leaving the source and that after the transmission. The advantage grows when the transmittance becomes small which happens when the distance gets larger. The smaller the transmittance we can tolerate, the longer the distances we can attain. A distance extension of about 100 km became possible by the decoy state method [4,5].

III. HERALDED SINGLE PHOTON SOURCE

A heralded single photon source [7–11] that uses one mode of a spontaneous parametric down-conversion (SPDC) as a trigger has the possibility of allowing longer distance transmission than the WCP as mentioned in Ref. [12]. The photon number distribution of a single mode SPDC is thermal (here we consider just one mode after separation by a polarizing beam splitter or a dichroic mirror and photon numbers of separated two modes are the same),

$$P(n) = \frac{\mu^n}{(1+\mu)^{n+1}}. \quad (7)$$

(Sub-Poissonian light can be generated if a shutter is used at the exit of the source. We consider this later.) Therefore,

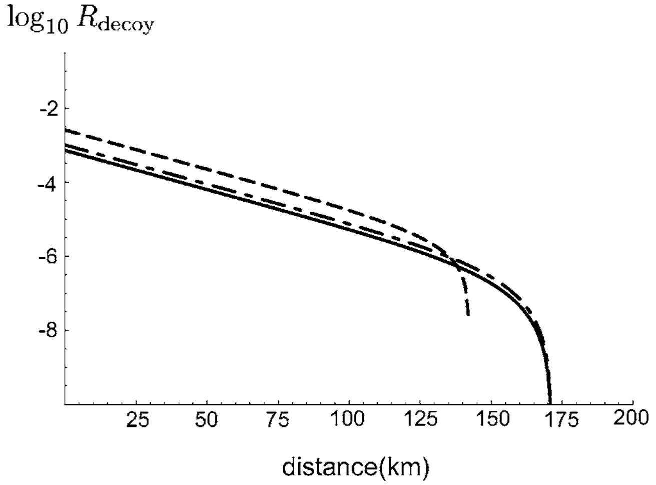

FIG. 3. Key rate: (a) Dashed curve: WCP. (b) Dotted-dashed curve: HSPS with TMD (η_A=0.6). (c) Solid curve: HSPS without TMD(η_A=0.6).

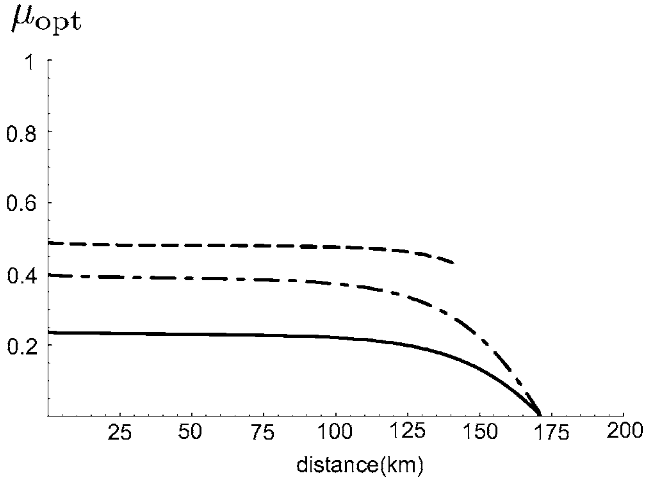

FIG. 4. Optimal mean photon number. (a) Dashed curve: WCP. (b) Dotted-dashed curve: HSPS with TMD (η_A=0.6). (c) Solid curve: HSPS without TMD(η_A=0.6).

when we consider the probability that it gives more than one photon among nonempty signals $P(n \geqslant 2 | n \geqslant 1) = \frac{1-P(0)-P(1)}{1-P(0)}$; that of the thermal distribution $P^{\rm thermal}(n \geqslant 2 | n \geqslant 1) = \frac{\mu}{1+\mu}$ is larger than the Poisson distribution $P^{\rm Poisson}(n \geqslant 2 | n \geqslant 1) = \frac{1-e^{-\mu}(1+\mu)}{1-e^{-\mu}}$. The higher the probability $P(n \geqslant 2 | n \geqslant 1)$ is, the lower the secure key rate is. Therefore, the secure key generation rate by using SPDC with a thermal distribution becomes smaller than the WCP. On the other hand, the dark count probability becomes low because it only has to make the detector of the key generation signal open by triggering.

Here we examine whether the distance is improved when the decoy state method is used. For this light source, Q_μ and E_μ are given as follows due to the thermal property of the photon number distribution and the imperfect detection efficiency of the threshold (just capable of distinguishing zero photon from nonzero) trigger detector:

$$Q_\mu = \sum_{i=1} Y_i [1 - (1 - \eta_A)^i] \frac{\mu^i}{(1+\mu)^{i+1}} + Y_0 d_A \frac{1}{1+\mu},$$

$$E_\mu Q_\mu = \sum_{i=1} e_i Y_i [1 - (1 - \eta_A)^i] \frac{\mu^i}{(1+\mu)^{i+1}} + \frac{1}{2} Y_0 d_A \frac{1}{1+\mu},$$

$$Q_1 = Y_1 \eta_A \frac{\mu}{(1+\mu)^2},$$

where η_A is a trigger detection efficiency and d_A is a dark count probability of the trigger detector. The second terms of Q_μ and E_μ are contributions by dark count and stray light (Q_0, e_0). Because photon number is not resolved, all signals including at least one photon $1-(1-\eta_A)^n$ are used as a key.

The key rates are calculated by substituting parameters into the formulas (5) and (6). Results are given in Figs. 1 and 2.

Parameters are taken from [16] as in Ref. [5]. The dark count probability of the trigger detector is 5×10^{-8}. The key rate is greatly improved compared with the HSPS in the case of no decoy states. This obviously shows the usefulness of the decoy state method even in the case of the HSPS. The cutoff distance is extended about 30 (40) km in the HSPS-decoy state compared with the WCP-decoy (HSPS no decoy) state as shown in Fig. 1. For clarification, we show the case of WCP no decoy in the figure. The maximum value is smaller than WCP (we assume η_A=0.6) because of the thermal distribution and inefficiencies of the detectors. The mean photon number of $\mu \approx O(1)$ can be used in the decoy state method, and it means that photons are included in almost all pulses. Because the click occurs almost every pulse, it might seem to be thought that the advantage of triggering is lost. However, we can understand from Fig. 2 that the optimal mean photon number is almost flat until the cutoff distance and suddenly cutoff occurs for WCP. The optimal mean photon number begins to fall gently in the HSPS and the cutoff has been extended to the place where it becomes too low. The cutoff becomes gradual because the dark count probability is lower than the WCP and then a distance extension can be achieved. It is understood that the HSPS can correspond to some degree by lowering the mean photon number while the cutoff occurs suddenly in the WCP because of a rapid increase of the error probability.

IV. HSPS WITH A TIME-MULTIPLEXED DETECTOR

Next, we consider the case in which a photon number resolving detector is used as the trigger detector of a heralded single photon source. Here a time-multiplexed detector (TMD) is considered [13,14]. This consists of an optical fiber loop, 50-50 couplers, and single photon detectors that do not have the ability to resolve. An incident pulse is divided into two paths by a 50-50 coupler. The differences in path length are larger than the dead time of the detector. The two pulses are recombined at a second 50-50 coupler which splits the pulses equally into two paths and directs them into one of two single photon detectors. Thus N=4 spatiotemporal modes are generated. Two or more photons in the incidence

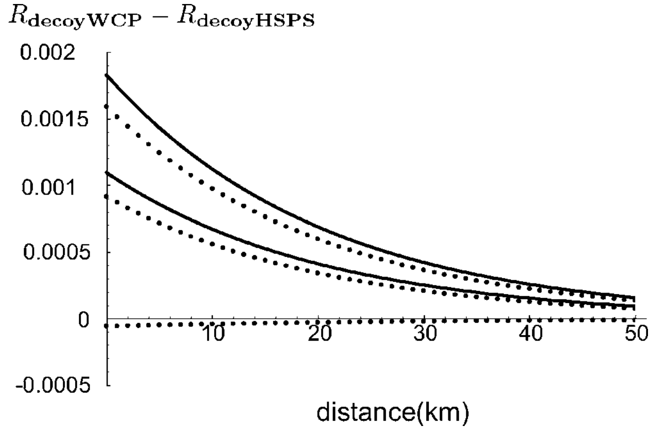

FIG. 5. $R_{\text{decoy WCP}}-R_{\text{decoy HSPS}}$. (a) Solid curve: $R_{\text{decoy WCP}}-R_{\text{decoy HSPS}}$ (η_A=0.6 and 1 from above). (b) Dotted curve: $R_{\text{decoy WCP}}-R_{\text{decoy HSPS-TMD}}$ (η_A=0.6, 0.8, and 1 from above).

pulse are separated with a high probability, and in each mode, only the zero- or one photon probabilities are large. Therefore, the photon number is found by counting the detection number in single photon detectors. The probability $P(l|m)$ of l counts for m incident photons is given by [13]

$$P(l|m) = \binom{N}{l}\sum_{j=0}^{l}(-1)^j\binom{l}{j}\left[(1-\eta_A)+\frac{(l-j)\eta_A}{N}\right]^m. \quad (8)$$

Here, $N=2^x$ and x is the number of fiber couplers; thus, N is the number of modes generated by the 50-50 couplers (we take $x=2$ so $N=4$ here) and η_A is the quantum efficiency of the single photon detectors. The gain and error rates are as follows:

$$Q_\mu = \sum_{i=0} Y_i P(1|i)\frac{\mu^i}{(1+\mu)^{i+1}}, \quad (9)$$

$$Q_0 = Y_0 N d_A \frac{1}{1+\mu}, \quad (10)$$

$$E_\mu Q_\mu = \sum_{i=0} e_i Y_i P(1|i)\frac{\mu^i}{(1+\mu)^{i+1}}, \quad (11)$$

$$Q_1 = Y_1 P(1|1)\frac{\mu}{(1+\mu)^2}. \quad (12)$$

In this case, Q_1 is the same as the HSPS without a TMD, because no matter which time mode is selected by the fiber loop as for one photon, the detection probability is just the detection probability of a single photon detector. Since multimode fiber can be used, it is possible to take a value close to 1 though strictly the value is smaller than 1 by the coupling probability and transmittance of the fiber, but we ignore this because the situation is the same as a threshold detector and the loss at the fiber is absorbed into the overall detection efficiencies. Results are given in Figs. 3 and 4. Parameters are taken from [16] as in Ref. [5]. The larger key rate than the case originally without a TMD for the trigger detector is obtained but it is still close to the one for no TMD. In Fig. 5 we show the difference between the WCP and HSPS. The key rate of the HSPS without a TMD never exceeds that of the WCP, and even the trigger detection efficiency is unity. However, that of the HSPS with a TMD can exceed the case for $\eta_A=1$. Though it cannot exceed the WCP in the case for relatively low efficiencies (for example, $\eta_A=0.8$), it can exceed the case for the HSPS without a TMD ($\eta_A=1$). The separation probability of two or more photons rises by increasing mode number (four-mode TMD is assumed here). However, the increase of the key rate is very small, so we do not show it.

V. IMPLEMENTATION

We can use the mean photon number of order 1 in the decoy state method that uses the SPDC photon source as seen. Roughly speaking, one down-conversion should occur by one pump pulse. Even with weak pump light, 8.5×10^5 coincidences (s mW) has been reported recently in quasi-phase-matched KTP waveguides [8]. As a method of generating decoy pulses it is in principle possible to utilize fundamental light from which pump light for SPDC is made by second harmonic generation, because the center wave length is the same as degenerate SPDC light. However, there are actually differences in the spectrum in fundamental light and the generated SPDC light. In experiments an interference filter is widely used to improve interference by narrowing the spectrum width. It can be used to match the spectrum of the decoy and that of the signal. However, it is easy to use an intensity modulator at random, generating signal and decoy from the same source. The upper bound of the bit rate in this method is not a repetition rate of the pulse. One down-conversion per pulse on average is possible as described above. The upper bound is determined by the speed of the trigger detector. The detector in the visible range where the quantum efficiency is high and the dark count probability is small has a dead time of about 50 ns. As a result, the upper bound of the frequency of the trigger becomes about 20 MHz. In the TMD (four-mode here) there are two temporal modes as for an incident one pulse. Thus it becomes half (about 10 MHz).

If we use a cw pump and a mechanical shutter at the exit of the source, then we can get sub-Poisson photon statistics. Thus the key rate can be increased compared with the thermal source. In this case the upper limit of the bit rate is determined by the repetition rate of the pulse generated by the shutter. However, it is possible to use an eletro-optical modulator instead of a mechanical shutter. By the use of a modulator we can get a good extinction rate, enough to obtain a sub-Poissonian statistic.

We have shown that the distance of a secure key distribution can be extended by using a heralded single photon source that uses SPDC light as a source and the key rate is increased by the use of the decoy state method. Moreover, it has been shown that it is possible to increase the key generation rate by using a time-multiplexed detector as a trigger detector.

ACKNOWLEDGMENT

We thank D. Markham for his help.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[2] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **5**, 325 (2004).

[3] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

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

[5] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[6] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt, e-print quant-ph/0503002.

[7] C. K. Hong and L. Mandel, Phys. Rev. Lett. **56**, 58 (1986).

[8] A. B. U'Ren, C. Silberhorn, K. Banaszek, and I. A. Walmsley, Phys. Rev. Lett. **93**, 093601 (2004).

[9] S. Takeuchi, R. Okamoto, and K. Sasaki, Appl. Opt. **43**, 5708 (2004).

[10] T. B. Pittman, B. C. Jacobs, and J. D. Franson, Opt. Commun. **246**, 545 (2005).

[11] S. Mori, J. Söderholm, N. Namekata, and S. Inoue, e-print quant-ph/0509186.

[12] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

[13] M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, Phys. Rev. A **68**, 043814 (2003).

[14] D. Achilles, C. Silberhorn, C. Sliwa, K. Banazek, and I. A. Walmsley, Opt. Lett. **28**, 2387 (2003).

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

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