Simple and Efficient Quantum Key Distribution with Parametric Down-Conversion

Yoritoshi Adachi,[1,2,*] Takashi Yamamoto,[1,2] Masato Koashi,[1,2] and Nobuyuki Imoto[1,2]

[1]*Division of Materials Physics, Department of Materials Engineering Science, Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*

[2]*CREST Research Team for Photonic Quantum Information, 4-1-8 Honmachi, Kawaguchi, Saitama 331-0012, Japan*

(Received 15 October 2006; published 2 November 2007)

We propose an efficient quantum key distribution protocol based on the photon-pair generation from parametric down-conversion (PDC). It uses the same experimental setup as the conventional protocol, but a refined data analysis enables detection of photon-number splitting attacks by utilizing information from a built-in decoy state. Assuming the use of practical detectors, we analyze the unconditional security of the new scheme and show that it improves the secure key generation rate by several orders of magnitude at long distances, using a high intensity PDC source.

DOI: 10.1103/PhysRevLett.99.180503 PACS numbers: 03.67.Dd, 42.65.Lm

Quantum key distribution (QKD) is a promising application of quantum information, with which two distant legitimate users (the sender Alice and the receiver Bob) can share a common random bit string, known as a secret key, with negligible leak to an eavesdropper Eve. The first QKD protocol has been proposed by Bennett and Brassard in 1984, which is called BB84 [1]. The original BB84 protocol proposes the use of an ideal single-photon source, and secure key distribution should be possible up to the distance at which Bob's photon detection rate and his dark counting rate are comparable. Since such an ideal single-photon source is not available today, weak coherent pulses (WCPs) from attenuated lasers are commonly used as a photon source [2–7]. The WCP has two imperfections: the multiphoton part and the vacuum part. The multiphoton part is vulnerable against photon-number splitting (PNS) attacks [8], and one must reduce the energy of the WCP in order to reduce the fraction of the multiphoton part. This leads to a very low key rate. The existence of the vacuum part simply leads to a reduction of Bob's photon detection rate, resulting in a shorter distance limit. Recent analyses [9,10] show that the former problem can be avoided by randomly mixing pulses with different energies (decoy states) [11]. But about half of the pulses are still in the vacuum state, and hence the distance limit falls short of the one with the ideal single-photon source.

Another candidate of photon sources within reach of current technology is conditional generation of single photons based on parametric down-conversion (PDC) [12]. The state of the photons generated in two modes A and S by PDC can be written as [13]

$$|\Psi\rangle_{AS} = \sum_{n=0}^{\infty} \sqrt{p_n}\,|n\rangle_A|n\rangle_S, \tag{1}$$

$$p_n \equiv \mu^n(1+\mu)^{-(n+1)}, \tag{2}$$

where $|n\rangle$ represents the state of n photons and μ is the average photon-pair rate. If Alice measures the mode A by an ideal photon-number-resolving detector with unit efficiency and selects the cases where just one photon has been detected, she would conditionally obtain an ideal single photon in mode S. But in practice, she must use a threshold (on-off) detector with nonunit efficiency, which cannot distinguish one from two or more photons. In this case, she selects the cases where the detection has occurred (triggered events). The good news is that the dark count rate of current detectors is very low, and we can still neglect the vacuum part of mode S for triggered events (see Fig. 1). Hence this source achieves the same distance limit as the ideal source. On the other hand, the mode S contains multiphotons, which is the same drawback as the WCP. One must decrease μ and thereby reduce the rate of triggering to avoid PNS attacks, leading to a severely low key rate. The remedies for this problem proposed so far are accompanied by introduction of additional complexity to the experimental setup, such as the random amplitude modulation for the use of decoy states and/or replacing Alice's detector by detector arrays in space or in time domain to improve the photon-number-resolving ability [14,15].

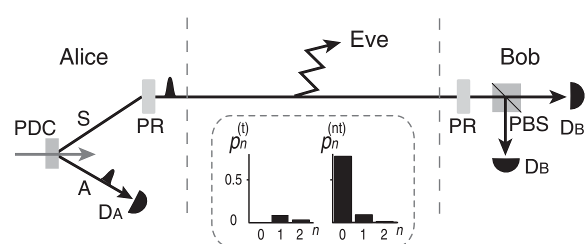

FIG. 1. The experimental setup of QKD system with PDC. Alice and Bob choose the bases by polarization rotators (PR's). Bob detects the photons by two threshold detectors (D_B's) after a polarizing beam splitter (PBS). The inset shows the photon-number distributions of the triggered events $p_n^{(t)}$ and the nontriggered events $p_n^{(\mathrm{nt})}$, when $\mu = 0.3$, $\eta_A = 0.5$, and $d_A = 10^{-6}$.

In this Letter, we propose a very simple solution. Nothing is added to the experimental setup of the PDC with a triggering detector. The crux of our new protocol is to run the BB84 protocol regardless of whether Alice's detector is triggered or not. By comparing the detection rates for the triggered events and the nontriggered events, we can detect the presence of PNS attacks. We assume that threshold detectors are used by Alice and Bob and derive a formula for the unconditionally secure key rate. Borrowing the parameters in a recent experiment, our calculation shows that the key rate is improved by several orders of magnitude compared to the conventional security analysis.

We first look at the property of Alice's source composed of PDC with Eq. (1) and a threshold detector D_A with efficiency η_A and dark count rate d_A. Let γ_n be the probability of detection (triggering) at D_A when n photons are emitted in mode S. Since n photons are emitted also in mode A, we have

$$\gamma_n = 1 - (1 - d_A)(1 - \eta_A)^n. \tag{3}$$

Then n-photon emission events (at rate p_n) are divided into the events with triggering (at $p_n^{(t)}$) and the events without triggering (at $p_n^{(\mathrm{nt})}$), where $p_n^{(t)} = p_n\gamma_n$ and $p_n^{(\mathrm{nt})} = p_n(1 - \gamma_n)$, whose distributions typically look like Fig. 1.

Alice changes the polarization of the pulse in mode S according to the BB84 protocol and sends it to Bob. Bob measures this signal by a polarization rotator and a polarizing beam splitter followed by two threshold detectors, as in Fig. 1. We say the signal is "detected" by Bob if at least one of the detectors clicks. When both detectors click, Bob assumes his outcome to be a random bit value. Let Q_n be the rate of events where Alice emits n photons in mode S and Bob detects the signal. These events are also divided into two groups: the events accompanied by Alice's triggering (at rate $Q_n^{(t)}$) and the rest (at $Q_n^{(\mathrm{nt})}$), where $Q_n^{(t)} = Q_n\gamma_n$ and $Q_n^{(\mathrm{nt})} = Q_n(1 - \gamma_n)$. Behind these relations lies the fact that the state of PDC in Eq. (1) becomes a direct product once we condition on the photon number n in mode S. Hence there should be no correlations between the triggering at D_A and any event occurring in mode S. This fact also ensures that the quantum bit error rate (QBER) e_n when Alice emits n photons in mode S should be the same whether or not the triggering occurs at D_A. Therefore, the overall detection rate $Q^{(t)}$ and the QBER $E^{(t)}$ with triggering, and the overall detection rate $Q^{(\mathrm{nt})}$ and the QBER $E^{(\mathrm{nt})}$ without triggering are expressed by

$$Q^{(t)} = \sum_{n=0}^{\infty} Q_n^{(t)}, \qquad Q^{(\mathrm{nt})} = \sum_{n=0}^{\infty} Q_n^{(\mathrm{nt})}, \tag{4}$$

$$E^{(t)} = \sum_{n=0}^{\infty} \frac{Q_n^{(t)} e_n}{Q^{(t)}}, \qquad E^{(\mathrm{nt})} = \sum_{n=0}^{\infty} \frac{Q_n^{(\mathrm{nt})} e_n}{Q^{(\mathrm{nt})}}. \tag{5}$$

These four quantities are observed in the actual protocol, while there is no way to measure directly the contributions from each photon number, except for e_0, which is always $1/2$.

We discuss the security of our protocol by Gottesman-Lo-Lütkenhaus-Preskill formula [16,17], which is written as follows for the key rate $R^{(t)}$ with triggering:

$$R^{(t)} = q\{-Q^{(t)} f(E^{(t)}) H_2(E^{(t)}) + Q_0^{(t)} + Q_1^{(t)}[1 - H_2(e_1)]\}. \tag{6}$$

The formula has recently been proved [18] to be valid even if Bob's detection is made by threshold detectors as in Fig. 1, as long as the two detectors have the same efficiency. Here $q(= 1/2)$ is the protocol efficiency, $f(E)$ is the error correction efficiency, and $H_2(E)$ is the binary entropy function. Since $Q_0^{(t)}$, $Q_1^{(t)}$, and e_1 are not exactly determined in the actual protocol, we must adopt the worst value of $R^{(t)}$ in the possible range of these parameters.

In the conventional protocol, we only observe $Q^{(t)}$ and $E^{(t)}$. In this case, we rely on the obvious inequality $Q_n^{(t)} \le p_n^{(t)}$ to obtain an upper bound on the multiphoton contribution $Q_{\mathrm{multi}}^{(t)} \equiv \sum_{n=2}^{\infty} Q_n^{(t)}$. This bound is meaningful only when $Q^{(t)} > p_{\mathrm{multi}}^{(t)} \equiv \sum_{n=2}^{\infty} p_n^{(t)}$. Since the scaling to μ and the channel transmission η_c is $Q^{(t)} \sim O(\eta_c\mu)$ and $p_{\mathrm{multi}}^{(t)} \sim O(\mu^2)$, we have to choose $\mu \sim O(\eta_c)$ and hence $R^{(t)} \sim O(\eta_c^2)$ at best, which means a rapid decrease of the key rate against the distance [see Fig. 2(f) below].

Now we will show that observation of nontriggered events, $Q^{(\mathrm{nt})}$ and $E^{(\mathrm{nt})}$, leads to a significant improvement of the key rate. The crucial relation is

$$Q_n^{(t)} = r_n Q_n^{(\mathrm{nt})}, \tag{7}$$

where $r_n \equiv \gamma_n/(1 - \gamma_n) = p_n^{(t)}/p_n^{(\mathrm{nt})}$. Eve cannot alter r_n since it is determined by Alice's parameters η_A and d_A. From Eq. (3), we see

$$0 \le r_0 < r_1 < r_2 < r_3 \cdots. \tag{8}$$

By comparing $r \equiv Q^{(t)}/Q^{(\mathrm{nt})}$ with r_n's, we have a clue about the distribution $Q_n^{(t)}$ over the photon number. The mechanism can be explained in two different ways. If we assume Alice's measurement by D_A occurs earlier, then it looks as if she randomly switches between two distributions, $\{p_n^{(t)}\}$ and $\{p_n^{(\mathrm{nt})}\}$. This is rather similar to the idea of one-decoy-state QKD [9]. Comparing r and $r_n = p_n^{(t)}/p_n^{(\mathrm{nt})}$ gives a clue about the PNS attacks, namely, r should be close to r_1 in the normal operation, but it will approach r_2 if Eve exploits the multiphoton events. If we assume Alice's measurement occurs after Bob's detection, we notice that the photon-number distribution at mode A conditioned on Bob's detection is proportional to Q_n. Hence Alice physically possesses the distribution about which she wants to learn, and she makes a measurement by D_A. The averaged rate $Q^{(t)}/(Q^{(\mathrm{nt})} + Q^{(t)})$ should then be compared with γ_n, which is equivalent to the comparison between r and $r_n = \gamma_n/(1-\gamma_n)$.

The remaining question is whether such a clue is enough to improve the key rate significantly. In the decoy state methods, we can tailor the number and the amplitudes of decoy states at will, but here we have no such freedom except for the strength μ of PDC. This is answered by conducting a quantitative analysis as follows. From Eqs. (7) and (8), we have $r_2 Q_n^{(\mathrm{nt})} \le Q_n^{(t)}$ for $n \ge 2$. Applying Eq. (4) leads to $r_2(Q^{(\mathrm{nt})} - Q_0^{(\mathrm{nt})} - Q_1^{(\mathrm{nt})}) \le Q^{(t)} - Q_0^{(t)} - Q_1^{(t)} = rQ^{(\mathrm{nt})} - r_0 Q_0^{(\mathrm{nt})} - r_1 Q_1^{(\mathrm{nt})}$. We thus obtain the minimum value of $Q_1^{(\mathrm{nt})}$ as a function of the only remaining unknown parameter $x \equiv Q_0^{(\mathrm{nt})}/Q^{(\mathrm{nt})}$:

$$\frac{Q_1^{(\mathrm{nt})}}{Q^{(\mathrm{nt})}} \ge \frac{r_2 - r - (r_2 - r_0)x}{r_2 - r_1} \equiv \xi(x). \tag{9}$$

From Eqs. (5) and (7) with $e_0 = 1/2$, an upper bound on e_1 is given by

$$e_1 \le [Q^{(t)}E^{(t)} - Q_0^{(t)}e_0]/Q_1^{(t)} \le \frac{2rE^{(t)} - r_0 x}{2r_1\xi(x)} \equiv \epsilon_t(x). \tag{10}$$

In a similar way, we have another bound

$$e_1 \le \frac{2E^{(\mathrm{nt})} - x}{2\xi(x)} \equiv \epsilon_{\mathrm{nt}}(x). \tag{11}$$

Combining the two bounds, we have

$$e_1 \le \epsilon(x) \equiv \min\{\epsilon_t(x), \epsilon_{\mathrm{nt}}(x)\}. \tag{12}$$

Consequently, in the limit of large block size with which the estimation errors are negligible, the key rate from the triggered events is given by

$$R^{(t)}/q = -Q^{(t)}f(E^{(t)})H_2(E^{(t)}) + Q^{(\mathrm{nt})}\min_x\{r_0 x + r_1\xi(x) \times [1 - H_2(\epsilon(x))]\}, \tag{13}$$

where the minimum is taken over the range $0 \le x \le \min\{2E^{(t)}(r/r_0), 2E^{(\mathrm{nt})}\}$. This minimization should be numerically calculated in general, and we give examples later. Before that, we here discuss the scaling of the key rate $R^{(t)}$ against the channel transmission η_c. Up to the distance at which the influence of the dark countings of Bob's detectors becomes substantial, the error rates $E^{(t)}$ and $E^{(\mathrm{nt})}$ are almost independent of η_c. The detection rates $Q^{(t)}$ and $Q^{(\mathrm{nt})}$ are both proportional to η_c, and their ratio r is also independent of η_c. Then, the functions $\xi(x)$, $\epsilon_t(x)$, and $\epsilon_{\mathrm{nt}}(x)$ are independent of η_c, and hence the key rate in Eq. (13) scales as $R^{(t)} \sim O(\eta_c)$. The PDC strength μ only affects the constant factor here, and its optimum value is independent of η_c. This is a significant improvement over the rate of the conventional protocol, $R^{(t)} \sim O(\eta_c^2)$.

When the distance is not so large, we may produce a secret key also from the nontriggered events. In this case, it is more efficient when the error reconciliation is separately applied to the triggered events and to the nontriggered events, but the privacy amplification is applied together, namely, after the two reconciled keys are concatenated. The key rate $R^{(\mathrm{both})}$ in this strategy is given by

$$R^{(\mathrm{both})}/q = -Q^{(t)}f(E^{(t)})H_2(E^{(t)}) - Q^{(\mathrm{nt})}f(E^{(\mathrm{nt})})H_2(E^{(\mathrm{nt})}) + Q^{(\mathrm{nt})}\min_x\{(1+r_0)x + (1+r_1)\xi(x)[1 - H_2(\epsilon(x))]\}. \tag{14}$$

The final key rate is thus given by $R = \max\{R^{(\mathrm{both})}, R^{(t)}\}$.

Next, we assume a channel model and show numerical examples of the key rate R as a function of the distance l. Let $\eta_c = 10^{-\alpha l/10}$ be the channel transmission, η_B be the quantum efficiency of Bob's detectors, and $\eta \equiv \eta_c\eta_B$. The background rate p_d of each detector is the combination of the rates of the dark count and the stray light, which are assumed to happen independently. For simplicity, we assume that both detectors have the same background rate. $Q_n^{(t)}$ is then given by

$$Q_n^{(t)}/p_n^{(t)} = 1 - (1-\eta)^n(1-p_d)^2, \tag{15}$$

and $Q^{(t)}$ is calculated by taking summation. Let e_d be the probability that a photon sent from Alice hits the erroneous detector, which is independent of the length of the quantum channel. Then we have, after some calculation,

$$2Q_n^{(t)}e_n/p_n^{(t)} = 1 - (1-\eta)^n(1-p_d)^2 - (1-p_d) \times [(1-\eta e_d)^n - (1-\eta+\eta e_d)^n], \tag{16}$$

and $E^{(t)}$ is calculated by taking summation. $Q^{(\mathrm{nt})}$ and $E^{(\mathrm{nt})}$ are calculated similarly.

The values of the parameters are chosen as follows. Alice may use a nondegenerate PDC and obtain visible and telecom-wavelength photons in mode A and S, respectively. Therefore, we assume a typical silicon avalanche photodiode for D_A, which has $d_A = 10^{-6}$ and (a) $\eta_A = 0.5$. We also show the case with (b) $\eta_A = 0.1$ to see the dependence on η_A. The remaining parameters are borrowed from the experiment by Gobby *et al.* [2], which are $\alpha = 0.21$ [dB/km], $p_d = 8.5 \times 10^{-7}$, $\eta_B = 0.045$, $e_d = 3.3[\%]$, and $f(E^{(t)}) = f(E^{(\mathrm{nt})}) = 1.22$. For each distance l, we have chosen the optimum value μ_{opt} for μ so that the key rate is highest, and the result is shown in Fig. 2 as curves (a) and (b). The step at ~130 km, more pronounced on curve (b), appears since the nontriggered events cease to contribute to the final key at this distance. Beyond this distance, the difference in η_A causes a slightly low key generation rate for (b). We have also shown [curve (f)] the key rate for the conventional analysis with $d_A = 0$ and $\eta_A = 1$. The remaining parameters are chosen to be the same. In comparison to this key rate with $O(\eta_c^2)$ dependence, the key rates in our new protocol scale as $O(\eta_c)$, and the improvement reaches several orders of

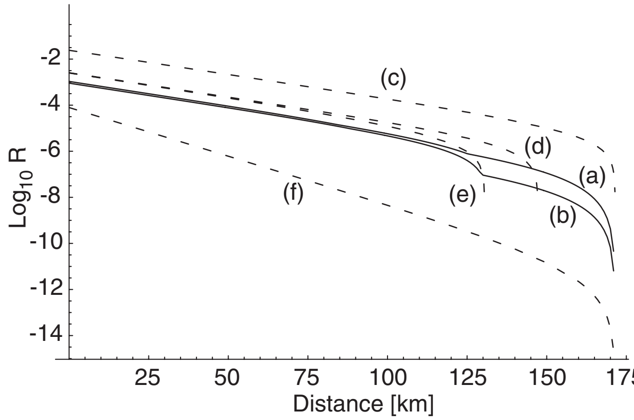

FIG. 2. Achievable key rates for different implementations of BB84. The calculations are done in the case of (a) the efficient PDC protocol with $\eta_A = 0.5$ and $d_A = 10^{-6}$, (b) the efficient PDC protocol with $\eta_A = 0.1$ and $d_A = 10^{-6}$, (c) ideal single-photon source, (d) WCP with infinite number of decoy states, (e) WCP with one decoy state, and (f) the conventional PDC protocol with $\eta_A = 1$ and $d_A = 0$.

magnitude as the distance gets larger. Let us emphasize again that the two protocols use exactly the same experimental setup.

For comparison, we included key rates for schemes using WCP with decoy states [curves (d) and (e)] [9]. At shorter distances, the difference comes from that of the optimal mean photon number. For example, μ_{opt} of (d) is 0.48 while that of (a) is 0.19. This may be caused by the higher multiphoton rate of PDC, whose photon-number distribution p_n is thermal. However, the present scheme has a positive key gain up to almost the same distances as with an ideal photon source [curve (c)]. The fact that no additional elements are needed in the PDC setup to beat PNS attacks makes it a viable candidate for the practical QKD. Recently Ma *et al.* [19] have shown that the achievable distance of WCP is further improved by two-way classical communication and post-processing. This interesting scheme also improves that of our scheme.

Finally, it is worth to discuss the feasibility of the present scheme. As shown in Ref. [20], high photon-pair generation from PDC ($\mu = 0.9$) using PPLN devices is possible in current technologies. The repetition rate of our scheme will be limited by that of D_A, but it can be improved by a high-repetition photon detection scheme [21]. Unlike WCP schemes, the achievable distances with the single-photon source and the PDC source depend on the coupling efficiency between the source and the single-mode fiber. In the case of PDC from PPLN waveguide, we can estimate the coupling efficiency of more than 80% in the current experiment [22], which still leads to a longer achievable distance than WCP schemes. The PDC source and the single-photon source also suffer from other losses in mode S such as ones at the polarization rotator, so further reduction of the losses is an important subject in the future experimental studies.

In conclusion, we have proposed an efficient QKD protocol with PDC, which utilizes the events discarded in the conventional PDC protocol to derive tighter bounds on the rate and the QBER of the single-photon part. The only difference between the present and the conventional protocol is the classical data processing. We found that the key rate is significantly improved in the new protocol.

We thank R. Namiki and F. Takenaga for helpful discussions. This work was supported by 21st Century COE Program by the Japan Society for the Promotion of Science and a MEXT Grant in Aid for Young Scientists (B) No. 17740265.

*adachi@qi.mp.es.osaka-u.ac.jp

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–197.
[2] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[3] D. Stucki *et al.*, New J. Phys. **4**, 41 (2002).
[4] T. Kimura *et al.*, Jpn. J. Appl. Phys. **43**, L1217 (2004).
[5] Y. Zhao, B. Qi, X. Ma, H.-K Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).
[6] C.-Z. Peng *et al.*, Phys. Rev. Lett. **98**, 010505 (2007).
[7] P. A. Hiskett *et al.*, New J. Phys. **8**, 193 (2006).
[8] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[9] H.-K. Lo, X.-F. 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).
[10] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[11] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[12] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[13] B. Yurke and M. Potasek, Phys. Rev. A **36**, 3464 (1987).
[14] T. Horikiri and T. Kobayashi, Phys. Rev. A **73**, 032331 (2006).
[15] W. Mauerer and C. Silberhorn, Phys. Rev. A **75**, 050305(R) (2007).
[16] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comput. **5**, 325 (2004).
[17] H.-K. Lo, Quant. Inf. Comput. **5**, 413 (2005).
[18] M. Koashi, arXiv:quant-ph/0609180.
[19] X. Ma *et al.*, Phys. Rev. A **74**, 032330 (2006).
[20] S. Mori, J. Söderholm, N. Namekata, and S. Inoue, Opt. Commun. **264**, 156 (2006).
[21] N. Namekata, S. Sasamori, and S. Inoue, Opt. Express **14**, 10 043 (2006).
[22] C. Langrock *et al.*, Opt. Lett. **30**, 1725 (2005).