Quantum cryptography using pulsed homodyne detection

T. Hirano,* H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki
Department of Physics, Gakushuin University, Toshima-ku, Tokyo, 171-8588, Japan
(Received 5 July 2000; revised manuscript received 2 June 2003; published 29 October 2003)

We report an experimental quantum key distribution that utilizes pulsed homodyne detection, instead of photon counting, to detect weak pulses of coherent light. Although our scheme inherently has a finite error rate, homodyne detection allows high-efficiency detection and quantum state measurement of the transmitted light using only conventional devices at room temperature. Our prototype system works at 1.55 μm wavelength and the quantum channel is a 1-km standard optical fiber. The probability distribution of the measured electric-field amplitude has a Gaussian shape. The effect of experimental imperfections such as optical loss and detector noise can be parametrized by the variance and the mean value of the Gaussian distribution.

DOI: 10.1103/PhysRevA.68.042331 PACS number(s): 03.67.Dd, 42.50.Lc

I. INTRODUCTION

The standard quantum key distribution (QKD) scheme uses photon counting as a means to detect weak light pulses [1]. The security of practical implementations of the photon counting scheme is limited by imperfections in the experiments, such as multiphoton part of the signal, channel losses, low detection efficiency, and dark counts of the detector. Brassard *et al.* provided a necessary condition for secure QKD taking into account these imperfections [2]. Recently Inamori *et al.* presented a proof of unconditional security of the practical QKD protocol against a cheater with unlimited computational power [3].

There are two currently available methods for detecting weak light. One is the photon counting method, and the other is homodyne detection. One technical limitation of the photon counting method is that at present there exists no efficient photon counter for infrared light, especially for 1.55 μm where optical loss in an optical fiber is minimum. State-of-the-art experiments used a specially designed photon-counting system made up of cooled avalanche photodiode operated in a gated Geiger mode [4]. In this operation mode, it is impossible to resolve the photon number and there is a trade-off between the detection efficiency and the dark-count probability. For example, a quantum efficiency of 11% for 1.55 μm with a dark-count probability of 7×10^{-7} per pulse is reported [5].

In this paper, we propose using pulsed homodyne detection for implementing the Bennett-Brassard 1984 (BB84) protocol with phase coding [6]. As we will explain, the above limitations associated with photon counting can be resolved by using homodyne detection. In order to demonstrate the experimental feasibility of our scheme, we have performed QKD by sending light pulses at 1.55 μm wavelength through an optical fiber of 1 km length.

The paper is organized as follows. In Sec. II, we first review the essential features of homodyne detection. We then explain our implementation of QKD. In Sec. III, we discuss the security aspects of the protocol. In Sec. IV, we present the experimental setup. In Sec. V, experimental results are presented.

II. HOMODYNE DETECTION AND PROTOCOL

Homodyne detection (sometimes called quadrature phase homodyne measurement) is a well-established quantitative method for measuring the quadrature-amplitude operator of the radiation field [7,8]. It has been developed as a means of detecting reduced quadrature-amplitude fluctuations (squeezed states of light) [9]. In this method, a weak signal field interferes with a strong local oscillator (LO) on a beam splitter, and the difference of the intensities of the two outputs of the beam splitter is measured. When the LO is much stronger than the signal, the output of the homodyne detector is proportional to the quadrature-amplitude operator of the signal field [8]. This is a very efficient method for measuring the quadrature amplitude of the signal, although no information on the conjugate quadrature is obtained.

In 1993, Smithey *et al.* demonstrated the determination of the Wigner distribution and the density matrix of a light field by measuring not only the variances but also the distributions of the quadrature amplitude of the field [10]. They used pulsed homodyne detection and the so-called optical homodyne tomography (OHT) method in which the inverse Radon transform of the distributions was calculated. Pulsed homodyne detection differs from the usually used method of using radio frequency spectral analysis of the current to study noise at high frequencies: in the pulsed homodyne detection, photoelectrons generated by each pulse are separately amplified by a low-noise charge-sensitive amplifier, so a single measurement on the quadrature amplitude of the signal pulse is performed for each pulse. A measurement of the density matrix provides all knowable information allowed by quantum mechanics. Of course, it is impossible to measure the density matrix of a *single* quantum system; we need the ensembles of the same quantum state. Such ensembles can be prepared by randomly switching the QKD and OHT procedures at the cost of a lowered QKD transmission rate. However, even without the OHT, distributions of the quadrature amplitude for some phases are obtained in the QKD procedure, thus limiting the range of allowable eavesdropping strategies.

Note that if a QKD protocol uses a phase coding relative

*Electronic address: takuya.hirano@gakushuin.ac.jp

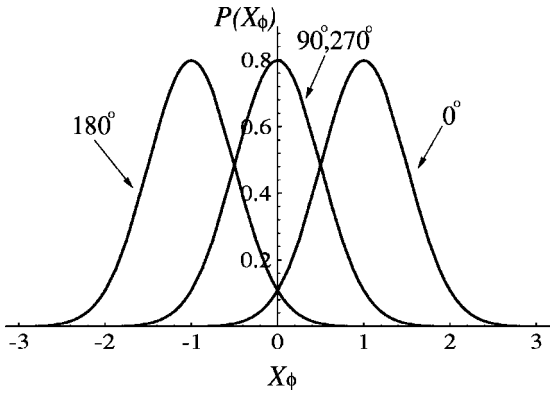

FIG. 1. Theoretical probability distributions of the quadrature amplitude for total phase shifts are 0°, 90°, 180°, and 270°. The signal photon number is 1 photon/pulse.

to bright light as proposed in Refs. [11,12], Eve as well as Bob can perform homodyne detection, although such possibilities have seldom been discussed so far. Also from this viewpoint, it is important to investigate QKD using homodyne detection. Recently, several authors have presented quantum cryptography using homodyne detection. These proposals use Einstein-Podolsky-Rosen–type correlation or squeezed states [13], or coherent states whose phase and amplitude are modulated with Gaussian random number [14]. Our scheme uses only coherent states with four kinds of phase modulation so that experimental realization is easier.

We will now explain our implementation of QKD in more detail. The protocol is basically an interferometric QKD using four nonorthogonal states (4+2 protocol) [12] except for the detection method. Laser pulses are split by an unsymmetrical beam splitter into two arms of a Mach-Zehnder interferometer. Pulses in one arm, which we will call the LO, contain many photons (typically, 10^6 photon/pulse), and pulses in the other arm, which we will call the signal, contain photons at quantum level (less than 1 photon/pulse). Alice applies a random $\phi_A=0°$, 90°, 180°, and 270° phase shift to the signal; Bob, a random $\phi_B=0°$, 90° phase shift to the LO. Bob then performs balanced homodyne detection. To put it concretely, Bob combines the signal field with the LO field by a 50-50 beam splitter. Two photodiodes (PDs) are used to monitor the intensities from two output ports. Finally, the two PD outputs are subtracted, and the difference of photoelectrons N_ϕ is measured. We denote the total phase shift between the signal and the LO by $\phi=\phi_A-\phi_B$.

The normalized quadrature amplitude of the signal is obtained by $X_\phi=N_\phi/2\sqrt{n_{LO}}$, where the quadrature amplitude is defined by $\hat{X}=(\hat{a}_{sig}+\hat{a}_{sig}^\dagger)/2$, and $\hat{a}_{sig}$ is the annihilation operator of the signal. For each pulse, X_ϕ takes a random value due to quantum fluctuations. Theoretically, the probability distribution $P(X_\phi)$ is given by integrating the Wigner distribution over the conjugate variable $X_{\phi+90°}$ [15]. When the signal is in a coherent state, $P(X_\phi)$ is given by a Gaussian function with a standard deviation of 1/2. Figure 1 shows $P(X_\phi)$ for $\phi=0°$, 90°, 180°, and 270° when the average signal photon number is 1. The probability distribution for $\phi=90°$, $P(X_{90})$, and that for $\phi=270°$, $P(X_{270})$, are the same, so it is impossible to differentiate them; in this case, Bob selected the wrong basis. It is, however, possible to differentiate $\phi=0°$ from $\phi=180°$. To do this, Bob sets up two threshold values X_+ and X_- where $X_-\leqslant X_+$. In the following, we set $X_-=-X_+$. If the measured quadrature amplitude X_ϕ is larger than X_+ (in this case, we say that Bob's result is plus side), Bob judges that $\phi=0°$. If X_ϕ is smaller than X_- (Bob's result is minus side), Bob judges that $\phi=180°$. Finally, if X_ϕ is between X_- and X_+ (Bob gets an inconclusive result), Bob abandons the judgment. Note that because $P(X_0)$ overlaps $P(X_{180})$, Bob's judgment is not always true and there exists intrinsic error probability. This intrinsic bit error rate e_{int} is the probability that ϕ is actually 180° even when Bob's result is plus side, or $\phi=0°$ for Bob's minus-side result. The larger the X_+, the smaller the e_{int}, but at the same time the probability p_{inc} that Bob gets inconclusive results becomes larger. We define postselection efficiency p_d as the probability that Bob gets plus- or minus-side results ($p_d=1-p_{inc}$). A remarkable feature of our implementation of QKD is that both e_{int} and p_d are functions of the n_{sig} and X_+. The values of e_{int} and p_d can be easily calculated by using the error function. For example, when $n_{sig}=1$ and $X_+=X_-=0$, $e_{int}=0.023$ and $p_d=1$. If we choose $X_+=-X_-=0.5$, e_{int} is greatly reduced to 0.0016, while $p_d=0.84$ changes a little. When $n_{sig}=0.1$ and $X_+=-X_-=1$, $e_{int}=0.047$ and $p_d=0.090$. In order to compare the performance of our scheme to that of the photon-counting scheme, we may define ''effective'' quantum efficiency $\eta_d=p_d/n_{sig}$. In the last case, therefore, $\eta_d=0.90$. These values demonstrate the excellent performance of homodyne detection.

After an appropriate number of pulses have been transferred, Bob tells Alice which phase shift he applied for each pulse. Alice, then, tells Bob which phase shifts were correct. The correctly measured data are interpreted as a binary sequence according to the coding scheme ($\phi_A=0°$ or 90°)=1 and ($\phi_A=180°$ or 270°)=0 for Alice, and (plus-side result)=1 and (minus-side result)=0 for Bob. Finally, Alice and Bob perform error correction and privacy amplification procedures.

III. SAFETY

In this paper we mainly address the difference of our system from the photon-counting system in terms of security analysis. Because Alice announces the basis of all pulses after the quantum transmission, Bob can graph two probability distributions: one is for pulses for which he selected the correct basis ($\phi=0°$ or 180°), the other is for pulses for which he selected the wrong basis ($\phi=90°$ or 270°). We may classify Eve's strategies into two categories; strategies in the first category *do* change these probability distributions, and strategies in the second category *do not*.

The intercept-resend eavesdropping strategy, in which Eve intercepts selected light pulses, measures them, and then resends an appropriate state to Bob, belongs to the first category. For Eve's intercept-resend eavesdropping not to change the distributions, Eve must determine Alice's phase shift with high accuracy. This is because if Eve's resend state

is different from Alice's original state, Bob's probability distribution for the correct and/or wrong basis varies in general. For example, if Eve resends the vacuum state (sends nothing) to Bob, Bob's probability distribution for the correct basis becomes a mixture of Gaussians not only centered at $\pm\sqrt{n_{sig}}$ but also centered at 0. It is clear, however, that if n_{sig} is sufficiently small, the nonorthogonality between the four states becomes significant, thus, Eve cannot differentiate the four states with high accuracy. The change in the probability distributions for some of Eve's strategies is explicitly calculated in Ref. [16]. Nonlinear optical processes, such as amplification or parametric processes, generally change the quantum state of light, sophisticated eavesdropping strategies should also fall into the first category. The resolution of measuring the quadrature-amplitude distribution becomes higher as the number of pulses increases. Thus, eavesdropping strategies belonging to the first category are in principle detectable without announcing the bit values of test pulses.

The beam splitting attack is the most obvious strategy that belongs to the second category. If there is an optical loss in the communication channel (this is always true for long-distance transmission), Eve can, in principle, replace the original channel with a more transparent one, and then put a beam splitter on the channel. This beam-splitting attack does not change the state of the transmitted light, so Bob cannot detect the presence of Eve. Moreover, because Eve can stay closer to Alice than Bob, the signal intensity at Eve's port may be higher than the one at Bob's port. The question is whether it is possible to generate secure keys when the signal-to-noise ratio of a cheater is better than the legitimate receiver. To answer this question, we have calculated the collision probability and the secure key creation rate when Eve performs balanced homodyne detection [16]. For example, when there are 6-dB losses in the system (Eve's signal-to-noise ratio is three times better than the receiver), the creation rate is 5×10^{-3} for $n_{sig}=1$ where optimal threshold value is $X_+=1.0$. Thus the answer to the above question is affirmative. The reason for this is as follows: First, due to quantum fluctuations entering from the dark port of the beam splitter, Eve's measurement result is uncorrelated with Bob's. The situation is analogous to the Yuen-Kim protocol where the existence of independent noise for Eve and Bob is assumed [17]. In our protocol the uncertainty relation of quantum mechanics assures the existence independent noise. Second, the bit error rate of the legitimate receiver can be decreased to an arbitrary small value by raising the threshold (the postselection efficiency p_d also decreases). That is, Bob can choose pulses for which he occasionally obtained large quadrature values. Because of the independence of the noise, Eve's error rate for pulses that Bob chooses remains unchanged. Only the legitimate receiver can choose his useful pulses. This asymmetry between the legitimate receiver and a cheater gives the legitimate receiver a great advantage. Recently, Silberhorn *et al.* also show that secure QKD is possible even when Eve's signal-to-noise ratio is better than Bob if an appropriate postselection mechanism is employed [18]. Detailed security analysis in general situations is the subject of future investigation.

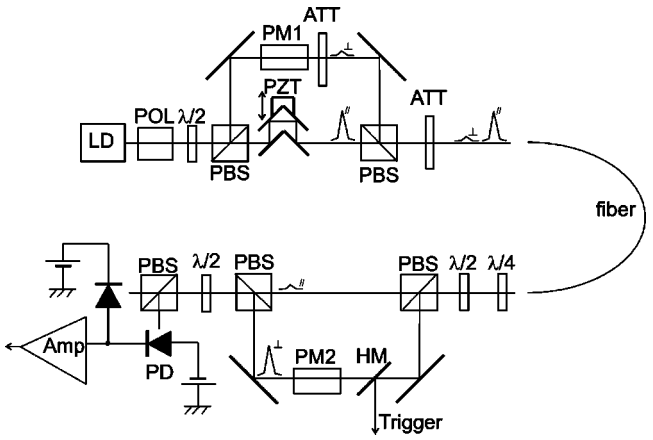

FIG. 2. Experimental setup. We used a four-state protocol in which keys are encoded in the phase difference between two pulses: $(0°,180°)$ or $(90°,270°)$. In the transmission fiber (1 km length), two pulses have mutually orthogonal polarization and are delayed by 500 psec. The light source is a 1.55-μm-wavelength semiconductor diode laser.

IV. EXPERIMENTAL APPARATUS AND METHOD

In order to demonstrate the feasibility of our scheme, we have performed a prototype QKD experiment. The experimental setup is shown in Fig. 2. In this prototype experiment, we do not use fiber-optical components except for the fiber and the fiber couplers.

The light source is a 1.55-μm-wavelength pulsed diode laser (PicoQuant PDL-800) that generates $\sim$0.4-nsec-duration pulses when the output pulse energy is 10 pJ (pulse duration is $\sim$0.1-ns for the output pulse energy of 2 pJ). The measured coherence length of the laser pulse after traversing 1-km optical fiber was 0.07 mm. The laser pulses can be triggered through an external trigger input or an internal clock whose repetition rate is 80 MHz. In the QKD experiment a digital output of a PC is connected to the external trigger input. In the typical setup, the average output pulse energy in the external trigger mode is measured to be 1.33 times larger than that in the internal trigger mode. Using this ratio (external-to-internal ratio), we can easily determine the pulse energy in the external mode from a measurement of the average power in the internal mode.

After traversing a glan laser linear polarizer, the laser output is split by a half-wave plate $\lambda/2$ and a polarizing beam splitter (PBS) into the signal and LO pulse. An electro-optical phase modulator (PM1, NewFocus model 4004) is used to modulate the phase of the signal pulse (Alice's modulator). Then the signal pulse is attenuated to a single-photon level by using two variable attenuators. A piezoelectric transducer is used to adjust the offset of the interferometer. We use time and polarization division to separate the signal and the LO in a transmission fiber [19]. The length of the fiber was 1 km, and two pulses were delayed by 0.5 nsec. A quarter-wave plate $\lambda/4$ and a half-wave plate are used to control the polarization of the signal and the LO after they traverse the fiber. A portion of the LO pulse is split by a partial mirror (HM) and used to trigger Bob's analog-to-digital (A/D) converter. PM2 is a homemade electro-optical

modulator whose aperture size is 3×3 mm^2 (Bob's modulator). The signal and the LO overlap each other in time on the second PBS. A careful alignment is needed to spatially overlap these beams. The fringe visibility $V=0.93$ was realized in the experiment. Their polarizations are then rotated by 45° so they interfere on the third PBS. Typical phase drift of our interferometer was about $\lambda/25$ in 200 sec.

The homodyne detector consists of two In-Ga-As PDs (Kyoto semiconductor KPDE020-56), a charge-sensitive amplifier (Amptek A250 using 2SK152), and shape amplifiers (Amptek A275). These electronics are installed inside a copper box and battery powered in order to reduce electric noise. The external feedback resistor and external feedback capacitor of A250 are 11 MΩ and 1 pF, respectively. The detector output is recorded by the A/D board installed in a PC.

The quantum efficiencies of the PDs were measured to be 0.80 ± 0.02 and 0.84 ± 0.02 using a power meter (Newport 818-IR) and a picoammeter (Keithley 485). The gain of the amplifier (A250+A275) was calibrated by injecting the external-mode laser pulse and measuring the output voltage using the A/D board. The number of photoelectrons generated by the laser pulse was determined by measuring the average power of the laser in the internal mode and using the external-to-internal ratio and the quantum efficiency. Note that, in this procedure, the calibration of photoelectron number relies on the picoammeter. The measured gain was 29.5 ± 0.2 V/pC.

In this prototype experiment, the key distribution was performed using a software running on a standard PC. In the software Alice's phase shifts were determined by pseudorandom numbers, then the corresponding voltage values were stored in an array variable for a certain number of pulses. Bob's bases were also determined by pseudorandom numbers and the corresponding voltage values were stored in another array variable. For each pulse, Alice and Bob's phase modulation were set through D/A ports, a laser pulse was triggered through the digital output, and then the output of the homodyne detector was recorded through A/D port. The repetition rate of the laser was 1.4×10^4 pulses/sec. The maximum repetition rate was mainly limited by the response time of the D/A board. The phase offset of the interferometer was adjusted by the following procedure. First, Alice sent 2×10^3 pulses and announced all her phase modulations. Bob measured the quadrature distributions, and calculated the mean values of the quadrature amplitudes for four kinds of phase shifts. If the phase offset was correct, Alice sent 20×10^3 or 30×10^3 pulses for the key distribution. After this, Alice again sent 2×10^3 pulses in order to check the phase offset.

In order to adjust the photon number of the signal at the input end of the fiber (n_{sig}^{in}), we first calculated the desired photon number just after the output fiber coupler using the loss of the optical fiber ($10^{-0.03}=0.93$) and the transmittance of the fiber-coupling lens (0.97, Newport F-L40B), and then we calculated the desired average power of the signal in the internal mode using the external-to-internal ratio. Next, by using the transmittance of the attenuators, we calculated the desired average power when the attenuators were adjusted for maximum transmission. Finally, the average power of the internal-mode signal was measured with the power meter.

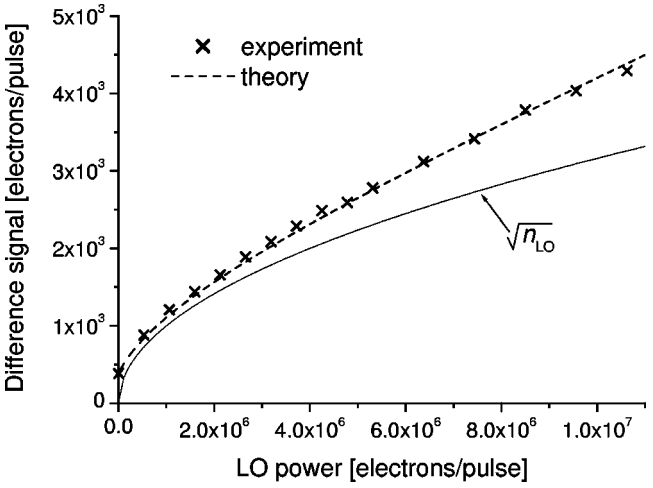

FIG. 3. The standard deviation of the difference signal as a function of the LO power. The dashed line is a fit by $\sqrt{(\Delta n_{amp})^2+n_{LO}+\beta n_{LO}^2}$ with $\beta=7.5\times10^{-8}$.

V. EXPERIMENTAL RESULTS AND DISCUSSION

The noise performance of the homodyne detector is shown in Fig. 3. In this figure the standard deviation of the difference signal (Δn) is shown as a function of the LO power n_{LO}. The input signal was in the vacuum state (no input) and the two photodiode's currents were balanced. The vertical axis was calibrated by using the gain of the amplifier. The overall electronic detection noise Δn_{amp} was 390 electrons rms. As the LO power increases, the difference noise deviates from the ideal square-root behavior (solid line) due to classical noises. The experimental data fit well with the equation, $\Delta n=\sqrt{(\Delta n_{amp})^2+n_{LO}+\beta n_{LO}^2}$, where $\beta=7.5\times10^{-8}$. Excess noise ratio $\Delta n/\sqrt{n_{LO}}$ takes the minimum of 1.1 for $n_{LO}=1.5\times10^6$.

Figure 4 shows the measured quadrature-amplitude distribution for $\phi=0°$, 90°, 180°, and 270°. There was a total of 1.5×10^6 pulses. The horizontal axis represents the normalized quadrature amplitude and the bin width is 2.6×10^{-2}. The average photon number of the signal at the input end of the fiber (n_{sig}^{in}) was set to be 1.0 photon/pulse. The number of photoelectrons was adjusted to be 1.5×10^6 electrons/pulse ($n_{LO}=1.5\times10^6$). The total of 1.5×10^6 data consists of 30 sets of 20×10^3 data and thirty sets of 30×10^3 data.

The most significant result from Fig. 4 is that the distributions are well fitted with Gaussian functions. This means that even if there exists some imperfections in the experiment, the probability distribution of the quadrature amplitude observed by Bob is Gaussian in the absence of the eavesdropper. The effect of imperfections such as channel losses and detector noise appears in two points. One is the decrease of the mean value of the distribution for $\phi=0°$ and 180°, and the other is the increase of the standard deviations of the distributions.

The mean values and the standard deviations of the dis-

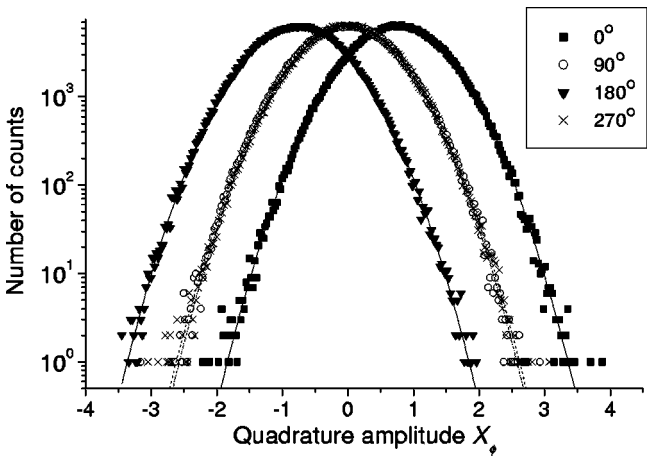

FIG. 4. The measured quadrature amplitude distributions for different total phase shifts between the signal and the LO pulse (0°, 90°, 180°, and 270°). The total number of pulses is 1.5×10^6 and the bin width is 2.6×10^{-2}. The signal power was 1.0 photons/pulse, and the LO power was 1.5×10^6 electrons/pulse. The solid lines and dotted lines are fits with Gaussian functions.

tributions are shown in Table I. The measured values of the mean are consistent with theoretical values of $\pm\sqrt{n_{sig}^{in}T\eta_{PD}}V=\pm\ 0.75$, where $T(=0.79\pm0.02)$ represents the optical loss including the fiber loss, coupler loss and losses in Bob's interferometer, and η_{PD} is the mean quantum efficiency of PDs. The standard deviations are slightly larger than that expected from the excess noise ratio of $0.5\times1.1=0.55$ probably due to the excess noise of the signal and the phase error.

Sifted keys can be obtained using the procedure explained in Sec. II. The first ten pulses out of 1.5×10^6 pulses are shown in Table II as an example where the threshold value X_+ is set to be 0.500.

In this table Bob selected correct basis for eight pulses, and the absolute values of normalized quadrature amplitude (QA) are greater than the threshold for four of them. There is no error between Alice's bit and Bob's bit. For all datasets, the number of correct-basis pulses was 750 417 out of 1.5×10^6 pulses, and the postselection efficiency p_d is $513\,280/750\,417=0.68$. Quantum bit error rate (BER) is $15\,923/332\,419=3.1\times10^{-2}$. The postselection efficiency is 1.2 times smaller and the bit error rate is 19 times larger than that calculated in the ideal situation (see Sec. II). This is because the decrease of the mean value due to experimental imperfections gives rise to the decrease of p_d and the increase of BER, and the increase of the standard deviation gives rise to the increase of p_d and the increase of BER for a fixed threshold value.

TABLE I. Mean and standard deviations of measured $P(X_\phi)$.

ϕ	Mean	Standard deviation
0°	0.759	0.621
90°	−0.001	0.626
180°	−0.758	0.623
270°	0.003	0.615

TABLE II. The first ten pulses ($X_+=0.500$).

Alice's bit	ϕ_A	ϕ_B	Basis	QA	Bob's bit	Success
1	90	0	×	−0.448		
0	180	0	○	−1.206	0	○
1	90	90	○	0.912	1	○
0	270	90	○	−1.311	0	○
1	0	0	○	1.514	1	○
1	90	90	○	0.310		
0	270	90	○	−0.474		
1	0	90	×	0.284		
0	180	0	○	−0.134		
1	0	0	○	−0.161		

Figure 5 shows the measured p_d and BER as a function of the threshold value X_+ for $n_{sig}^{in}=1.0$. For example, when $X_+=0$, $p_d=1$, and BER was 0.11, and when $X_+=0.857$, $p_d=0.443$, and BER was 1.02×10^{-2}. The error bars represent the statistical error. Solid lines show theoretical curves calculated using the values shown in Table I. The excellent agreement between the experimental data and the theory manifests the fact that the quadrature-amplitude distribution obeys Gaussian distribution. Figure 6 shows the measured p_d and BER for various signal powers. The total number of pulses sent by Alice for each signal power was 10^5 except for $n_{sig}^{in}=1.0$. Solid lines are theoretical curves assuming Gauss-

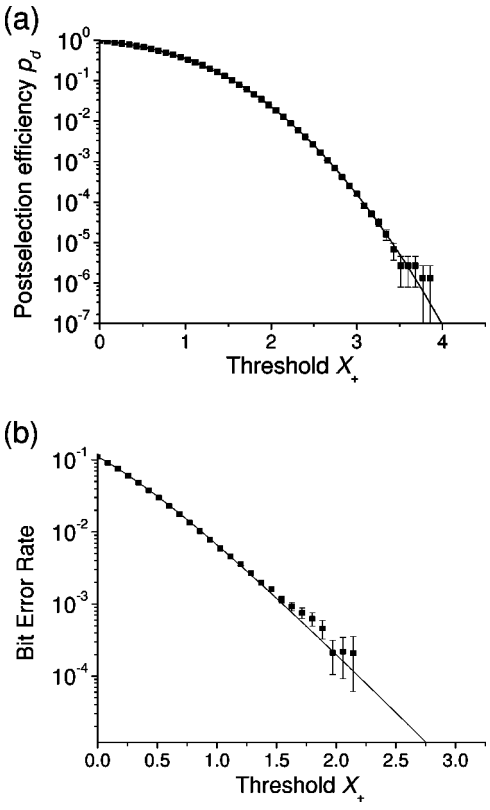

FIG. 5. (a) Postselection efficiency and (b) bit error rate as a function of a threshold value when the signal power was 1.0 photons/pulse.

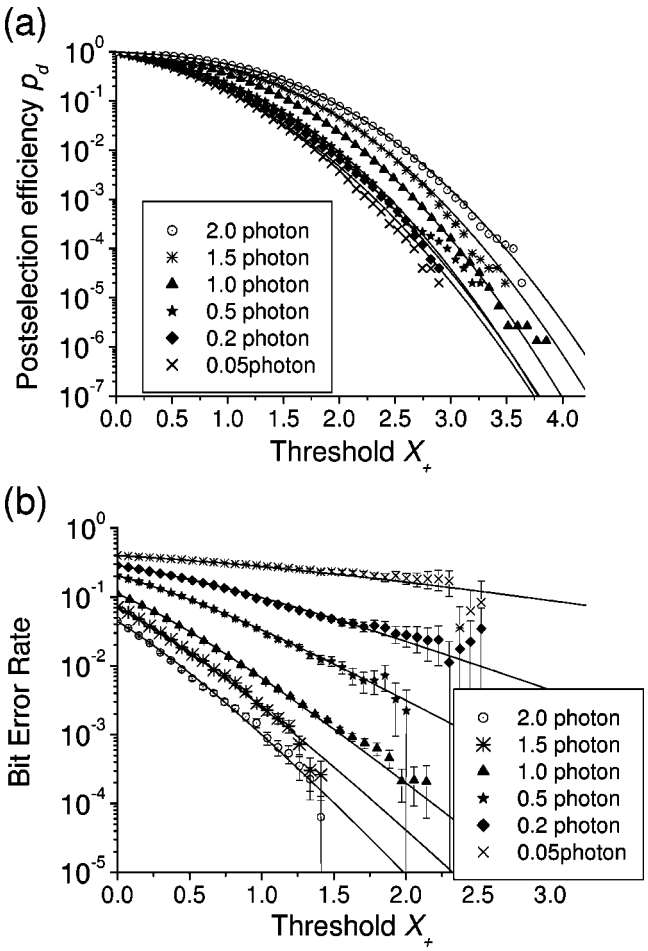

FIG. 6. Postselection efficiency and bit error rate as a function of threshold for various signal powers.

ian distributions. These are in good agreement with experimental data also for weak signal power.

With respect to the security of our system in a practical situation, the experimental result that the measured quadrature amplitude distributions are well fitted with Gaussian functions has important consequences. First, Eve's eavesdropping strategy will be limited to the one that preserves Gaussian distribution even in the presence of experimental imperfections, because, otherwise, the attempt by Eve will be detected in principle. Second, the error rate can be reduced to an arbitrarily small value by raising the threshold value (It is worth remembering that p_d also decreases). This is in contrast with the photon-counting scheme where the error rate is bounded by the dark count of the detector.

VI. CONCLUSION

In conclusion, we have presented a scheme for QKD that utilizes pulsed homodyne detection in the phase-encoding BB84 protocol. The scheme has an inherently finite error rate, but previous schemes also have finite error rates in practice. The advantage of our scheme is that the error rate can be decreased to an arbitrary small value by raising the threshold value. However, it should be noted that the postselection efficiency also decreases in this case. Another advantage is that measuring the distributions of quadrature amplitudes limits the allowable eavesdropping strategies. In addition, if Alice randomly adds auxiliary phase shift, the density matrix of the signal could be measured by optical homodyne tomography. We have performed a prototype QKD experiment at 1.55 μm wavelength. The measured quadrature-amplitude distributions were well fitted with Gaussian functions. The effects of experimental imperfections can be parametrized by the variance and the mean value of the Gaussian distribution.

ACKNOWLEDGMENTS

We thank M. Koashi, A. Shimizu, T. Kuga, Y. Torii, and T. Kuwamoto for helpful discussions, and K. Kotani, T. Mihirogi, J. Fujii, K. Komori, and M. Yanagihara for work during the early stage of the experiment. T.H. acknowledges the financial support from the Research Foundation for Opto-Science and Technology. This work was supported by the CREST, JST, and ''R&D support scheme for funding selected IT proposals'' of MPHPT, Japan.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[3] H. Inamori, N. Lütkenhaus, and D. Mayers, e-print quant-ph/0107017.
[4] P.D. Townsend, Opt. Fiber Technol. **4**, 345 (1998); M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg, Opt. Express **4**, 383 (1999); D. Bethune and W. Risk, IEEE J. Quantum Electron. **36**, 340 (2000); R.J. Hughes, G.L. Morgan, and C.G. Peterson, J. Mod. Opt. **47**, 533 (2000); D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, e-print quant-ph/0203118.
[5] A. Tomita and K. Nakamura, Opt. Lett. **27**, 1827 (2002); e-print quant-ph/0206150.
[6] The idea was first presented at the Sectional Meeting of the Physical Society of Japan, 1998 [T. Hirano, Meet. Abstr. Phys. Soc. Jpn. **53**, 341 (1998)]; e-print quant-ph/0008037.
[7] H.P. Yuen and V.W.S. Chan, Opt. Lett. **8**, 177 (1983).
[8] U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge, University Press, Cambridge, 1997).
[9] See, e.g., R.E. Slusher, L.W. Hollberg, B. Yurke, J.C. Mertz, and J.F. Valley, Phys. Rev. Lett. **55**, 2409 (1985); E.S. Polzik, J. Carri, and H.J. Kimble, *ibid.* **68**, 3020 (1992); T. Hirano and M. Matsuoka, Opt. Lett. **15**, 1153 (1990).
[10] D.T. Smithey, M. Beck, M.G. Raymer, and A. Faridani, Phys. Rev. Lett. **70**, 1244 (1993).
[11] C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[12] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[13] M. Hillery, Phys. Rev. A **61**, 022309 (2000); T.C. Ralph, *ibid.* **61**, 010303 (1999); M.D. Reid, *ibid.* **62**, 062308 (2000); Y.

Nambu, A. Tomita, Y. Chiba-Kohno, and K. Nakamura, *ibid.* **62**, 012312 (2000); N.J. Cerf, M. Levy, and G. Van Assche, *ibid.* **63**, 052311 (2001); D. Gottesman and J. Preskill, *ibid.* **63**, 022309 (2002).

[14] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002); F. Grosshans, G.V. Assche, J. Wenger, R. Brouri, N.J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[15] K. Vogel and H. Risken, Phys. Rev. A **40**, 2847 (1989).

[16] R. Namiki and T. Hirano, Phys. Rev. A **67**, 022308 (2003).

[17] H.P. Yuen and A.M. Kim, Phys. Lett. A **241**, 135 (1998); A. Tomita and H. Hirota, J. Opt. B: Quantum Semiclassical Opt. **2**, 705 (2000).

[18] Ch. Silberhorn, T.C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).

[19] C. Marand and P.D. Townsend, Opt. Lett. **20**, 1695 (1995).