

## Observation of 1.5 $\mu\text{m}$ band entanglement using single photon detectors based on sinusoidally gated InGaAs/InP avalanche photodiodes

Benjamin Miquel<sup>1,2</sup> and Hiroki Takesue<sup>1,3</sup>

<sup>1</sup> NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi 243-0198, Japan

<sup>2</sup> Ecole Normale Supérieure, 24 rue Lhomond, 75005 Paris, France

<sup>3</sup> CREST, JST, 4-1-8 Honcho, Kawaguchi-shi, Saitama, 332-0012, Japan

E-mail: [benjamin.miquel@ens.fr](mailto:benjamin.miquel@ens.fr) and [htakesue@will.brl.ntt.co.jp](mailto:htakesue@will.brl.ntt.co.jp)

*New Journal of Physics* **11** (2009) 045006 (15pp)

Received 29 November 2008

Published 30 April 2009

Online at <http://www.njp.org/>

doi:10.1088/1367-2630/11/4/045006

**Abstract.** We describe the application of single photon detectors based on InGaAs/InP avalanche photodiodes incorporating the sinusoidal gating technique into a 1.5  $\mu\text{m}$  band entanglement measurement. We constructed two detectors based on this technique with a 500 MHz gate frequency. Using these detectors, we successfully demonstrated the high-speed and high signal-to-noise ratio observation of 1.5  $\mu\text{m}$ -band time-bin entangled photon pairs.

**Contents**

<b>1. Introduction</b>	<b>2</b>
<b>2. Comparison of telecom-band single photon detectors for entanglement-based QKD</b>	<b>3</b>
<b>3. Single photon detectors based on sinusoidally gated InGaAs/InP APDs</b>	<b>6</b>
3.1. Principle of the sinusoidal gating technique	6
3.2. Detector set-up	7
3.3. Detector characterization	8
<b>4. Observation of time-bin entangled photon pairs</b>	<b>10</b>
4.1. Generation of 1.5 $\mu\text{m}$ band time-bin entangled photon pairs using a dispersion shifted fibre (DSF)	10
4.2. Coincidence-to-accidental ratio (CAR) measurement	11
4.3. Observation of two-photon interference	12
<b>5. Conclusion</b>	<b>13</b>
<b>Acknowledgments</b>	<b>13</b>
<b>References</b>	<b>13</b>

**1. Introduction**

Great progress has been made on quantum key distribution (QKD) systems over optical fibres in the last 10 years [1]. The key distribution distances of QKD systems using attenuated laser sources have already exceeded 100 km [2, 3]. However, QKD systems with attenuated laser sources often suffer from unconditional security problems. For example, QKD systems based on the Bennett Brassard 1984 protocol [4] implemented with attenuated laser sources are known to be vulnerable to an attack called photon number splitting (PNS) [5]. Although the use of ‘decoy states’ is effective in increasing the distance [6] and a successful QKD experiment over a 107 km fibre has been undertaken with this scheme [7], the implementation of decoy states complicates the signal processing significantly and thus results in a huge system cost overhead.

In contrast, entanglement-based QKD is promising with a view to achieving long-distance key distribution with relatively simple signal processing [8, 9]. Since the security of QKD can be analysed by quantifying the amount of entanglement shared between two parties [10], we expect to realize QKD with a high level of security simply by distributing entangled photons to two parties. In fact, Waks *et al* showed that we can realize entanglement-based QKD that is secure against individual attacks using practical components such as entanglement sources based on spontaneous parametric processes and threshold detectors, which are single photon detectors with no photon number discrimination ability [11]. Also, recent work by Tsurumaru and Tamaki [12], Beaudry *et al* [13] and Koashi *et al* [14] independently showed that we can achieve unconditionally secure QKD using entanglement sources that probabilistically emit multi-pairs and threshold detectors. Another merit of entanglement-based QKD is that we can eliminate the need for a random number generator, which has been an unresolved issue as regards a high-speed, attenuated laser-based QKD system with a GHz clock rate [3].

Although entanglement-based QKD has been intensively developed for free-space systems [15], there have only been a few experiments in the telecom wavelength bands [16]–[19]. As far as we know, only two experiments ([18] and [19], both by our group)

have been conducted using two  $1.5 \mu\text{m}$  band photons. This is mainly because of the slow and inefficient single photon detectors available for use in the  $1.5 \mu\text{m}$  band.

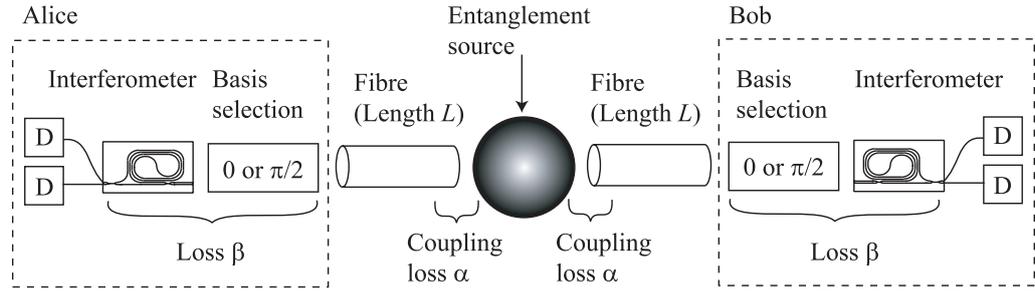
In the experiment reported in [18], we used single photon detectors based on InGaAs/InP avalanche photodiodes (APDs) operated in a conventional gated mode with a gate frequency of 5 MHz [20]. This slow gate frequency resulted in a very slow sifted key rate of  $0.3 \text{ bit s}^{-1}$  even without a transmission fibre. In our second experiment [19], we employed superconducting single photon detectors (SSPD) and time-bin entangled photons generated at a clock frequency of 333 MHz. Thanks to the very low dark count probability of the SSPDs, we successfully distributed keys over 100 km ( $50 \text{ km} \times 2$ ) fibres. However, mainly because of the relatively low quantum efficiency of the SSPDs ( $\sim 1\%$ ), the obtained secure key rate was as low as  $0.14 \text{ bit s}^{-1}$ . This small key rate has unfortunately made our entanglement-based QKD systems impractical.

Recently, groups from Nihon University [21] and Toshiba Cambridge [22] reported  $1.5 \mu\text{m}$  band single photon detection using InGaAs/InP APDs with improved gate frequencies. Namekata *et al* employed a sinusoidal signal as a gate, and inserted filters that reject the sinusoidal signal at the output, by which they can efficiently suppress the APD capacitive response to the gate signal at the output [21]. In the scheme demonstrated by Yuan *et al*, a self-differentiation circuit was inserted so that the APD capacitive response to the rectangular gate could be cancelled out [22]. With these techniques, we can detect smaller avalanche signals. As a result, we can reduce the gate voltage supplied to the APD, which results in a smaller afterpulse probability. Or if we accept an afterpulse probability that is similar to that of a conventional gated-mode InGaAs/InP APD, we can increase the gate frequency to a range typically between 500 MHz and 1.25 GHz. These techniques have already been used in several point-to-point QKD experiments [23, 24].

In this paper, we describe the observation of  $1.5 \mu\text{m}$  band entangled photons using high-speed InGaAs/InP APDs. In section 2, we show that these high-speed InGaAs/InP APD-based single photon detectors are attractive candidates for realizing practical entanglement-based QKD systems over optical fibres, based on numerical calculation. In section 3, we describe the two single photon detectors that we constructed using 500 MHz sinusoidally gated InGaAs/InP APDs. Section 4 reports the observation of time-bin entangled photons using high-speed single photon detectors and a significant increase in the speed of  $1.5 \mu\text{m}$  band entanglement measurement. Section 5 summarizes the paper.

## 2. Comparison of telecom-band single photon detectors for entanglement-based QKD

In this section, we compare the performance of entanglement-based QKD systems with various types of telecom-band single photon detectors using a numerical simulation. The simulation model is shown in figure 1. We assume the protocol proposed by Bennett *et al* in 1992, which we refer to as BBM92 [9], implemented with a sequential time-bin entanglement and an active basis selection scheme using differential phase modulation [25]. A  $1.5 \mu\text{m}$  band entangled photon pair source generates a pulsed entangled photon train through a spontaneous parametric process such as spontaneous parametric downconversion and spontaneous four-wave mixing (SFWM). We assume that the number distribution of the photon pairs per pulse is Poissonian with an average value of  $\mu$ . The signal and idler photons are input into transmission fibres with a collection efficiency of  $\alpha$ . Each fibre has a length  $L$  with a loss coefficient of  $0.2 \text{ dB km}^{-1}$ . Then, each photon is passed through a phase modulator for the basis selection and input into a 1-bit delayed Mach–Zehnder interferometer. The total transmittance of the phase modulator and the



**Figure 1.** Simulation model. D: single photon detector.

interferometer is denoted by  $\beta$ . The two output ports of the interferometer are connected to the single photon detectors. Alice and Bob apply phase modulations to the incoming pulses with a value that is randomly chosen from  $\{0, \pi/2\}$ . It is only when the phase difference between pulses given by their phase modulation coincided that the measurement results between Alice and Bob exhibit correlation [25].

In [26], we reported a detailed theory for calculating the two-photon interference visibility obtained by entangled pairs generated by spontaneous parametric sources. We can modify the theory for use in calculating the error rate of the QKD system shown in figure 1. By taking account of the fact that four detectors and active demodulation are used, the probability of obtaining a coincidence that can contribute to the key is well approximated with the following equation:

$$R_c = \frac{1}{4}\mu\alpha_t^2\eta^2 + 2\left(\frac{1}{2}\mu\alpha_t\eta + d\right)^2. \quad (1)$$

Here,  $\alpha_t$  denotes the total collection efficiency ( $=\alpha\beta 10^{-0.02L}$ ) and  $\alpha_t\eta$  is assumed to be much smaller than 1. In an intuitive picture, the first term in equation (1) corresponds to the probability of a coincidence caused by a correlated pair. On the other hand, the second term denotes the probability of an accidental coincidence caused by the uncorrelated pairs generated in a multi-pair emission event, which we denote by  $R_{acc}$ .

$$R_{acc} = 2\left(\frac{1}{2}\mu\alpha_t\eta + d\right)^2. \quad (2)$$

The sifted key rate is given by

$$R_{sifted} = f_c R_c, \quad (3)$$

where  $f_c$  denotes the clock frequency of the whole system or the gate frequency of the detectors. Since half of the accidental coincidences contribute to errors, the error rate  $e$  is obtained as

$$e = \frac{R_{acc}}{2R_c}. \quad (4)$$

The rate of the final key that is secure against general individual attacks is given by the following equation [11]:

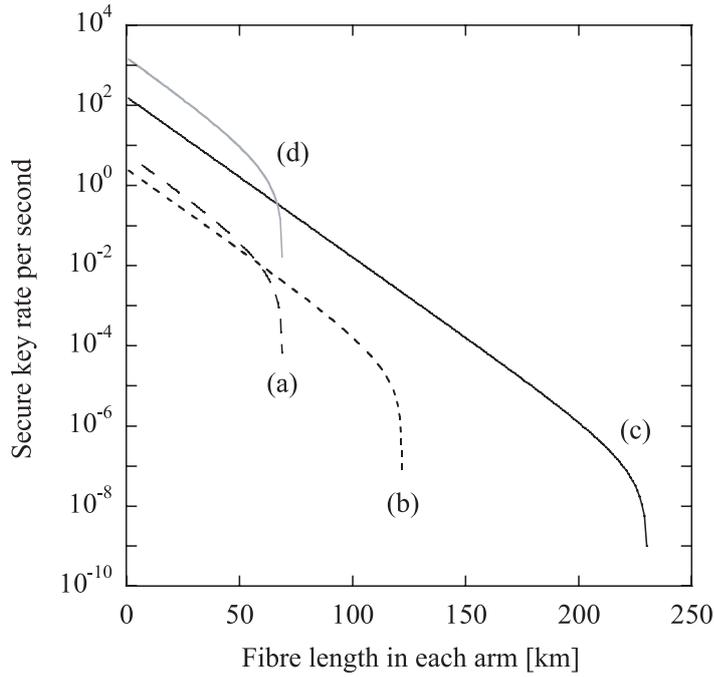
$$R_s = R_{sifted}\{\tau(e) - f(e)h(e)\}. \quad (5)$$

Here,  $\tau(e)$  denotes the privacy amplification factor of the BBM92 protocol that is given by [11]

$$\tau(e) = -\log_2\left(\frac{1}{2} + 2e - 2e^2\right) \quad (6)$$

**Table 1.** Typical parameters for various 1.5  $\mu\text{m}$  band single photon detectors.

	$\eta$	$P_d$	$f_{c \text{ max or } f_g}$
Conventional InGaAs/InP APD [20]	0.1	$1.0 \times 10^{-5}$	4 MHz
Up-conversion detector [28]	0.004	$3.5 \times 10^{-8}$	1 GHz
SSPD [3]	0.01	$6 \times 10^{-10}$	10 GHz
High-speed InGaAs/InP APD [21, 22]	0.1	$1.0 \times 10^{-5}$	1 GHz

**Figure 2.** Secure key rate as function of fibre length in each arm. (a) Conventional gated-mode InGaAs/InP APDs, (b) up-conversion detectors, (c) SSPDs and (d) high-speed InGaAs/InP APDs.

and  $h(e)$  is the binary entropy function that is expressed as

$$h(e) = -e \log_2 e - (1 - e) \log_2 (1 - e). \quad (7)$$

Also,  $f(e)$  characterizes the performance of the error correction algorithm.

We calculated the secure key rate as a function of the fibre length between the entanglement source and Alice/Bob for four types of single photon detector: conventional gated-mode InGaAs/InP APDs [20], up-conversion detectors [27, 28], SSPDs [3, 29] and high-speed InGaAs/InP APDs [21, 22]. The quantum efficiencies, dark count probabilities and the maximum clock frequency or gate frequency for each detector are listed in table 1. We used the  $f(e)$  value shown in [11], and assumed that there is no baseline system error and that the errors are caused only by the detector dark counts. The average photon pair number per pulse  $\mu$  was optimized to maximize the secure key rate for each fibre length. The result is shown in figure 2. It is clear that the SSPDs and the up-conversion detectors are more effective in increasing the secure key distribution distance than detectors based on InGaAs/InP APDs. The

maximum distribution distances are 460 (230 km  $\times$  2) for SSPDs and 244 km (122 km  $\times$  2) for up-conversion detectors. However, at approximately those maximum distribution distances, the secure key rates are very low. For example, the secure key rate for a fibre length of 400 km (200 km  $\times$  2) with SSPDs is  $\sim 1.2 \times 10^{-6}$  bit s $^{-1}$ , which means that we need  $\sim 230$  h to establish 1 key bit, and this is obviously useless in real communication. Therefore, the maximum distance over which meaningful QKD is possible is in fact limited by the secure key rate with those high signal-to-noise ratio detectors. If we assume that we require a minimum secure key rate of 1 bit s $^{-1}$ , then the maximum key distributions with the detectors listed in table 1 are 38 km (conventional gated-mode InGaAs/InP detectors), 20 km (up-conversion detectors), 110 km (SSPD), and 126 km (high-speed InGaAs/InP detectors). Thus, if we consider both the error rate and the secure key rate, high-speed InGaAs/InP detectors can perform better than other detectors depending on the bit rate requirement. In addition, InGaAs/InP APDs do not require cryogenic cooling as with the SSPD, or additional optics as with the up-conversion detectors. Therefore, we believe that the high-speed APDs constitute a promising candidate for realizing practical entanglement-based QKD systems.

Here, we briefly note that intensive research is being undertaken to improve the SSPDs' quantum efficiencies. For example, it is shown that the quantum efficiency of an SSPD chip (which presumably does not include the loss involved in the photon collection or the coupling between fibre and the device) can be as high as 57% with an integrated optical cavity and an anti-reflection coating [30]. Thus, those devices may be useful for realizing high-speed entanglement-based QKD if they are successfully incorporated into a practical photon detection system in the near future.

### 3. Single photon detectors based on sinusoidally gated InGaAs/InP APDs

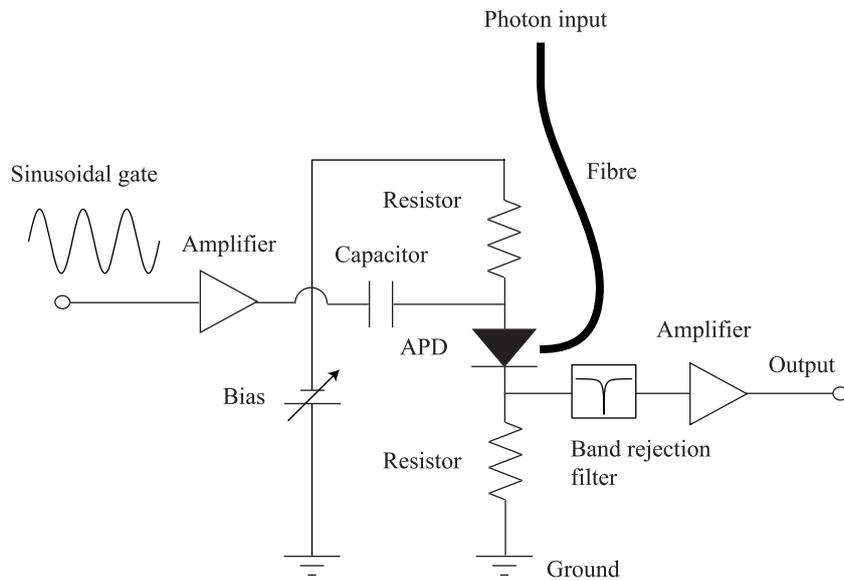
#### 3.1. Principle of the sinusoidal gating technique

Here, we briefly review the principle of single photon detection using a sinusoidally gated InGaAs/InP APD [21]. When the APD is biased over the breakdown voltage  $V_B$ , an incoming photon excites an electron-hole pair in an absorption region and it is amplified into a macroscopic current, which is called an avalanche. An unexpected avalanche, namely a dark count, can be triggered by either a thermal carrier or a trapped carrier from a previous avalanche. Geometrical and chemical impurities in the APD's active layer sometimes trap carriers and release them at a later time, and the carrier causes another avalanche without an incoming photon: this phenomenon is known as an afterpulse.

In single photon counting applications, we usually cool the APD with a Peltier cooler so that we can reduce the dark counts caused by the thermal carrier. However, if we cool the APD too much, the afterpulse probability increases, because the temporal period a carrier trapped in an impurity tends to become longer as the temperature is reduced. For the above reasons, the APD is typically operated in a temperature range of  $-70$  to  $-30^\circ$ .

Even when the APD is cooled, such a detector is too noisy to be run in the Geiger mode, so we generally use it in the gated mode: the APD is periodically biased over  $V_B$ , but is disabled most of the time by being biased below  $V_B$ . Usually, a dc signal  $V_{dc}$  is applied, in addition to a time-dependent signal.

We employed a rectangular pattern as a gate signal in the conventional gated mode. With this method, it is difficult to distinguish the avalanche signals from the APD capacitive response



**Figure 3.** Detector set-up.

to the gate signal [22]. As a result, we needed to use a relatively large gate signal (or large dc bias) so that we could obtain a larger avalanche signal that could be easily distinguished from the APD capacitive response. The larger avalanche (i.e. larger number of carriers) increases the probability of carrier trapping by impurities, and thus results in a larger afterpulse probability.

Sinusoidally gated APDs performed better than conventional gated-mode APDs [21]. In addition to the usual dc bias, we employ a sinusoidal signal as a gate. With this scheme, while the avalanche signals are close to the delta function in the time domain, the APD capacitive response (which is also a sinusoidal signal) is a delta function in the frequency domain. As a result, we can easily distinguish the avalanche from the APD capacitive response in the frequency domain, and thus we can reduce the afterpulse probability by reducing the gate voltage. Or if we accept a similar level of afterpulse probability to that of conventional gated mode detectors, we can significantly increase the gate frequency.

### 3.2. Detector set-up

Our detector set-up is shown in figure 3. The APD is surrounded by a gated passive quenching circuit (GPQC). We used a synthesizer to produce the gate signal at a frequency of  $f_g = 500$  MHz, which passes through a phase shifter and an amplifier, and is then input into the GPQC. The sinusoidal signal is converted into another sinusoidal signal at the same frequency as a result of capacitive response of the APD. When an avalanche occurs, a peak is added to the sinusoidal signal. At the output, band rejection filters are inserted to eliminate the 500 MHz component. Then, the output signal is amplified and input into a discriminator. In the following, the deadtime and the discrimination level set by the discriminator are expressed as  $\tau$  and  $V_{disc}$ , respectively. Although numerous parameters can be adjusted, we adopted the following process: first, we set  $V_g$  at 10 V (peak-to-peak), then we set  $V_{disc}$  at the smallest possible value without it being overwhelmed by noise and then we increased the dark count probability  $P_d$  by changing  $V_{dc}$ . Although this approach is simple, we obtained similar results to those obtained when  $P_d$  is

changed by varying other parameters (for instance,  $V_g$ ). Furthermore, in our set-up,  $V_{dc}$  was by far the easiest parameter to increase without inducing instability.

### 3.3. Detector characterization

A continuous light from an external-cavity diode laser with a wavelength of 1551 nm is modulated into pulses with an intensity modulator driven by a pulse generator. The pulse width and the repetition frequency are 100 ps and 100 MHz, respectively. Using calibrated optical attenuators, we set the average input photon number per second at  $N_{\text{input}} = 10^6$ . The synthesizers and the pulse generator are synchronized. Therefore, we can ensure that photons arrive when the detector is gated by tuning the phase shifter. We can insert a deadtime  $\tau$  ranging from 40 ns to 1.6  $\mu\text{s}$  using the discriminator. If we denote the count rate per second and the overall afterpulse probability as  $C_r$  and  $P_a$ , respectively, we can evaluate the quantum efficiency with the following formula:

$$\eta = \frac{1}{N_{\text{input}}} \left\{ \frac{C_r}{(1 - \tau C_r)(1 + P_a)} - P_d f_g \right\}. \quad (8)$$

The quantity  $P_d f_g$  can simply be read on the counter, in the absence of light. Therefore, if we measure  $P_a$ , we can determine  $\eta$  using equation (8).

We measured  $P_a$  by observing the autocorrelation of the dark counts [31]. The dark count signal from the discriminator is divided into two paths and input into a time interval analyser (TIA). One channel is directly input as a start signal and the other is delayed by  $\sim 100$  ns and used as a stop signal for the TIA. We define the correlation function,  $\pi(n)$ , which denotes the probability that an afterpulse event occurs at the  $n$ th gate from the start pulse. Then, the waveform we obtain with the TIA is given by  $N_s\{\pi(n) + d\}$ , where  $N_s$  and  $d$  are the number of start pulses and the dark count probability per gate, respectively. Then, the overall afterpulse probability  $P_a$  is obtained as

$$P_a(n_d) = \sum_{n=n_d}^{\infty} \pi(n), \quad (9)$$

where  $n_d (= \tau f_g)$  is the number of gates in the deadtime set by the discriminator and the TIA.

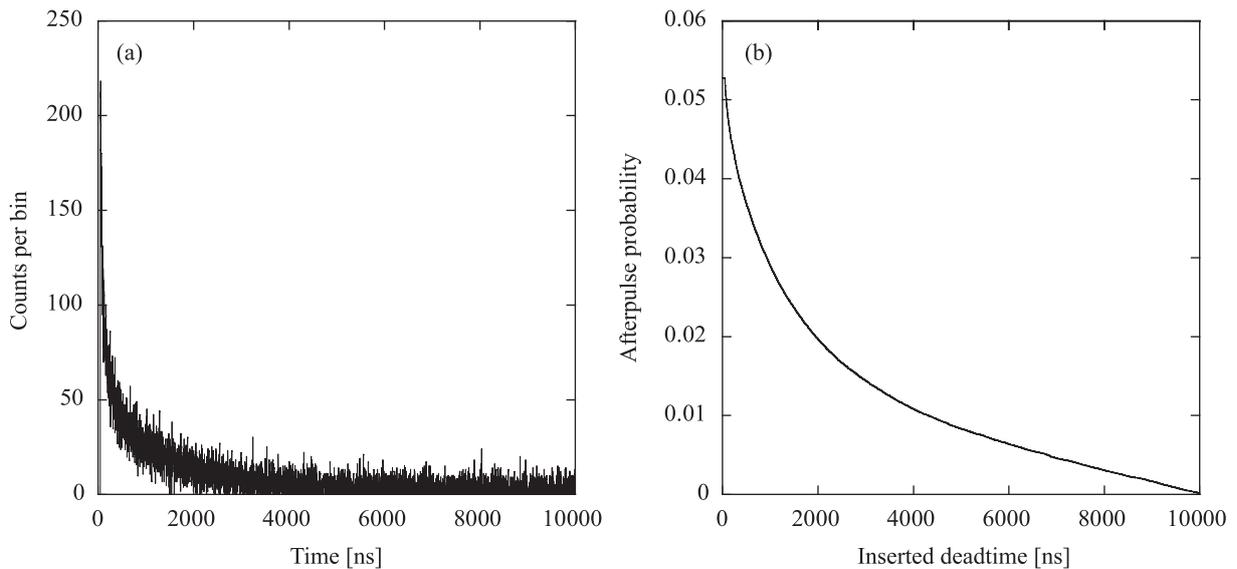
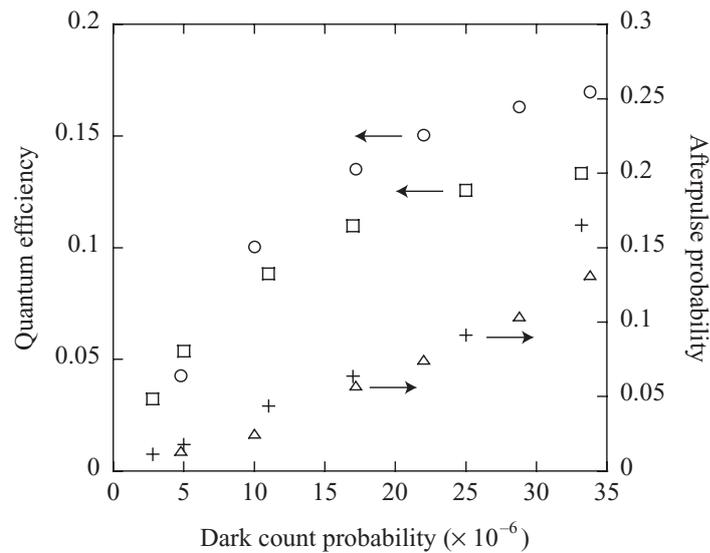
A typical histogram obtained with the TIA is shown in figure 4(a). Here, the dark count probability was set at  $d = 1.7 \times 10^{-5}$  by adjusting  $V_{dc}$ . Using equation (9), the overall afterpulse probability can be calculated as a function of the inserted deadtime, as shown in figure 4(b). This suggests that even without any deadtime (except for the 40 ns deadtime inserted by the TIA), the afterpulse probability has already been suppressed to  $\sim 5\%$ . In this way, we measured  $P_a$  for various  $d$  values. Then, using the measured  $P_a$  and  $C_r$  for each  $d$ , we finally obtained  $\eta$  as a function of  $d$  using equation (8).

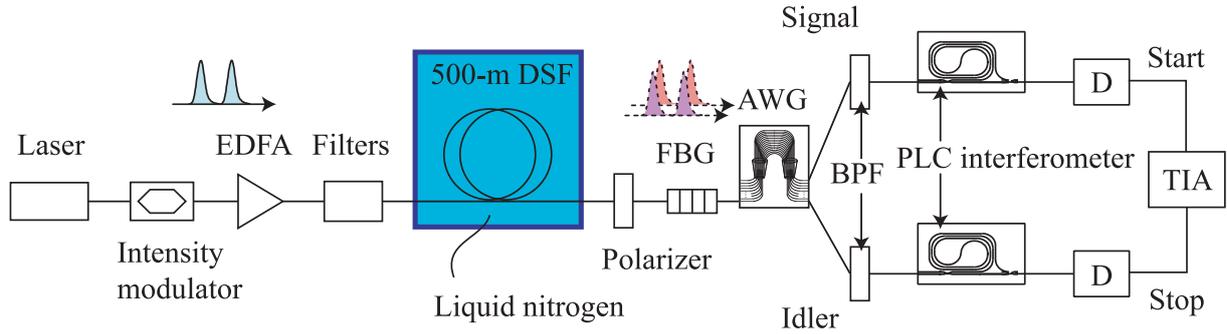
We constructed two channels of single photon detectors, which we denote as channels 1 and 2. The afterpulse probability of channel 1 was much larger than that of channel 2 (whose afterpulse characteristics are shown in figure 4). Therefore, we inserted a 400 ns deadtime into channel 1 so that the afterpulse probability was reduced to a similar level to that of channel 2. The quantum efficiency and the afterpulse probability as a function of the dark count probability for the two channels are shown in figure 5. Thus, we successfully constructed two channels of 500 MHz gated-mode single photon detectors using sinusoidally gated InGaAs/InP APDs.

In the entanglement measurement experiments that follow, we operated the two detectors under the conditions shown in table 2.

**Table 2.** Operating conditions of two single photon detectors during the observation of time-bin entangled photon pairs.

	$\eta$ (%)	$d$	$P_a$ (%)	Deadtime
Channel 1	11	$1.8 \times 10^{-5}$	4.0	400 ns
Channel 2	13	$1.6 \times 10^{-5}$	4.0	40 ns

**Figure 4.** (a) Autocorrelation function measurement result. (b) Overall afterpulse probability as a function of the inserted deadtime, deduced from (a).**Figure 5.** Quantum efficiency and afterpulse probability as a function of dark count, for both channels.



**Figure 6.** The time-bin entanglement observation set-up.

#### 4. Observation of time-bin entangled photon pairs

##### 4.1. Generation of 1.5 $\mu\text{m}$ band time-bin entangled photon pairs using a dispersion shifted fibre (DSF)

The set-up for generating and observing 1.5  $\mu\text{m}$  time-bin entangled photon pairs is shown in figure 6 [32, 33]. A continuous laser light from an external cavity diode laser with a wavelength of 1551.1 nm was modulated into a pulse train with a pulse width of 100 ps and a repetition frequency of 500 MHz by using an intensity modulator. The pulse train was amplified using an erbium-doped fibre amplifier (EDFA), and launched into a DSF after being passed through filters to eliminate the amplified spontaneous emission noise from the EDFA. In the DSF, a sequential time-bin entangled state was generated through SFWM. The quantum state of a generated photon pair is approximately given by

$$|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{k=1}^N |k\rangle_s |k\rangle_i. \quad (10)$$

Here,  $|k\rangle_z$  denotes a state in which there is a photon in a temporal position  $k$  and a mode  $z (= s, i)$ , and  $N$  is the number of pulses in which the phase coherence of the pump is preserved. The DSF was cooled with liquid nitrogen to suppress the noise photons caused by spontaneous Raman scattering [33]. The photons output from the DSF were passed through a polarizer to eliminate noise photons with a polarization state that was orthogonal to the photon pair polarization state. The photons were input into a fibre Bragg grating (FBG) to suppress the pump photons and then launched into an arrayed waveguide grating (AWG) to separate signal and idler photons. The wavelengths of the signal and the idler were 1547.9 and 1554.3 nm, respectively, both with a 0.2 nm (25 GHz) bandwidth. Each photon was passed through an optical bandpass filter to further suppress the noise photons, and then launched into a 1-bit delayed Mach–Zehnder interferometer fabricated using planar lightwave circuit (PLC) technology [32]. The photons output from the interferometers were detected by single photon detectors based on sinusoidally gated InGaAs/InP APDs. The signal and idler channels were connected to channels 1 and 2 of the detectors, respectively. The detection signals from the single photon detectors were input into a time interval analyzer (TIA) for coincidence measurements.

The state  $|k\rangle_z$  is transformed by the PLC interferometer as follows:

$$|k\rangle_z \rightarrow \frac{1}{2} (|k\rangle_z + e^{i\phi_z} |k+1\rangle_z). \quad (11)$$

With the above transformation, the state shown by equation (10) is transformed as follows:

$$|\Psi\rangle \rightarrow \frac{1}{4\sqrt{N}} \left[ |1\rangle_s |1\rangle_i + \sum_{k=2}^N \{ (e^{i(\phi_s+\phi_i)} + 1) |k\rangle_s |k\rangle_i \} + e^{i(\phi_s+\phi_i)} |N+1\rangle_s |N+1\rangle_i \right]. \quad (12)$$

Here, only those terms that contribute to the coincidence are shown. This equation implies that we can observe two-photon interference in any time slot except for the very first and last slots in the whole photon pulse train, and the probability of obtaining the coincidence is given by  $\frac{1}{4N}$  at the peak of the two-photon interference fringe.

When the number distribution of the photon pairs is given by a Poissonian with an average photon-pair number per pulse of  $\mu$ , the coincidence rate at the peak of the two-photon interference fringe  $R_p$  is approximately given by [26]

$$R_p = f_g \left\{ \frac{1}{4} \mu \alpha_s \alpha_i \eta_s \eta_i + \left( \frac{1}{2} \mu \alpha_s \eta_s + d_s \right) \left( \frac{1}{2} \mu \alpha_i \eta_i + d_i \right) \right\}, \quad (13)$$

where  $\alpha_z$ ,  $\eta_z$  and  $d_z$  denote the total collection efficiency the detector quantum efficiency, and the dark count probability per gate for the mode  $z$  ( $= s, i$ ), respectively. This equation is valid when  $\alpha_z \eta_z \ll 1$ . In our experiment,  $\alpha_s$  and  $\alpha_i$  were both  $\sim -8.5$  dB including the insertion loss of the PLC interferometer. Therefore, equation (13) gives a good approximation of the peak coincidence rate.

#### 4.2. Coincidence-to-accidental ratio (CAR) measurement

The CAR is often used to evaluate the strength of the temporal correlation between correlated photons. Prior to the entanglement observation, we measured the CAR of the photon pairs generated by the SFWM in the DSF using our detectors.  $CAR > 1$  implies the existence of a temporal correlation between the photons, and a larger CAR means a stronger correlation.

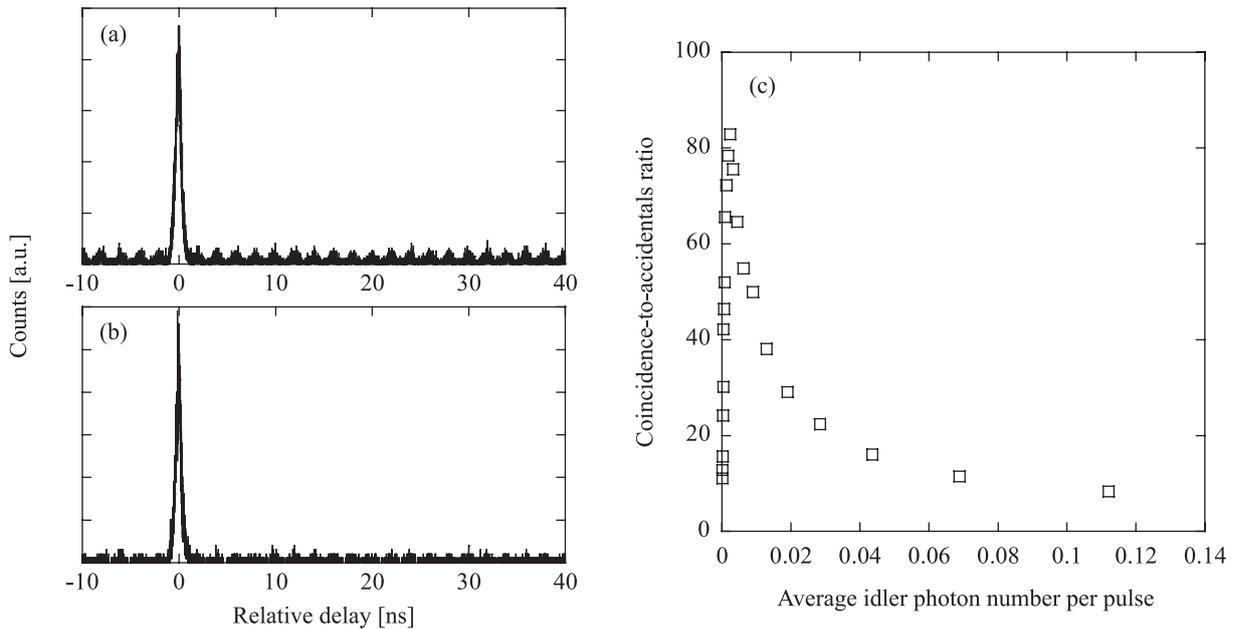
According to [26], the theoretical CAR  $C$  is obtained with the following equation.

$$C = 1 + \frac{\mu \alpha_s \alpha_i \eta_s \eta_i}{(\mu \alpha_s \eta_s + d_s)(\mu \alpha_i \eta_i + d_i)}. \quad (14)$$

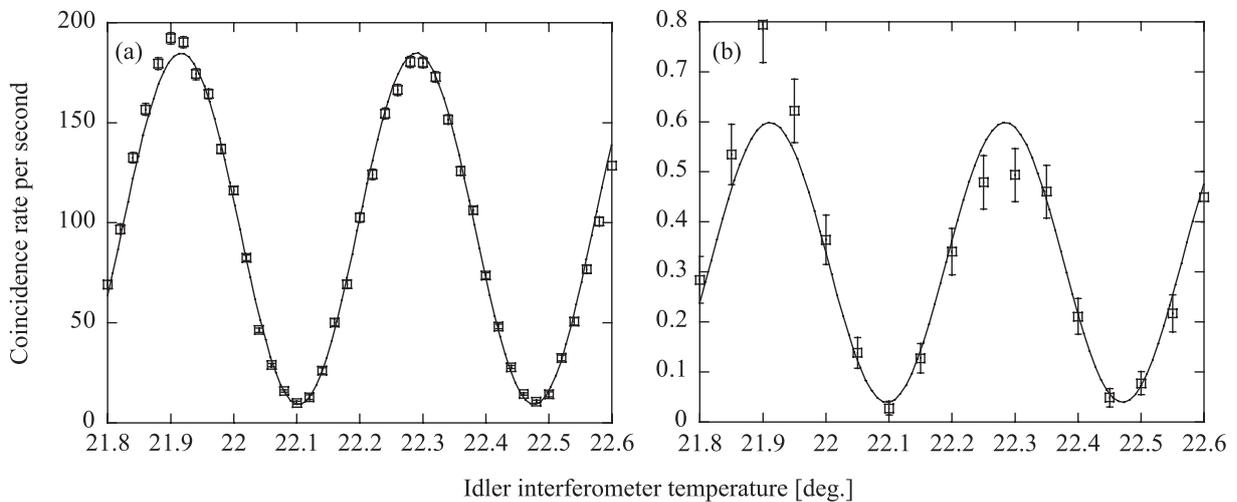
This equation implies that the CAR generally improves if we reduce  $\mu$ , but is eventually limited by the detector dark counts if  $\mu$  is set too small.

We removed the interferometers from the set-up shown in figure 6 and measured the coincidence counts using the TIA. Typical histograms obtained with the TIA measurements are shown in figure 7(a) (average idler photon number per pulse: 0.019) and figure 7(b) (0.002). The main peak, which is caused by the coincidences between photons generated with the same pump pulse, corresponds to the ‘coincidences’. On the other hand, the small side peaks (which are more apparent in figure 7(a) than in (b)) are caused by the coincidences between photons generated in different temporal positions, and these peaks provide an estimation of the number of accidental coincidences contained in the main peak. We obtain the CAR by dividing the counts in the main peak by the average counts in the side peaks.

The measured CAR as a function of the average idler photon number per pulse  $\mu_i$  is plotted in figure 7. The CAR reached its maximum value of 83 at  $\mu_i = 0.002$ . In [33], we reported a CAR obtained using the same set-up (and the same DSF) with conventional gate-mode detectors operated at a frequency of 4 MHz, in which the maximum CAR was 28. This clearly shows that our sinusoidally gated detectors have both a much higher gate frequency and a better signal-to-noise ratio than the conventional gated-mode detectors used in [33].



**Figure 7.** Histograms of coincidence counts obtained using TIA for idler average photon numbers per pulse of (a) 0.019 and (b) 0.002. The CARs for (a) and (b) were 29 and 83, respectively. (c) CAR as a function of average idler photon number per pulse.



**Figure 8.** Coincidence fringes (a) with sinusoidally gated detectors and (b) conventional gated-mode detectors.

#### 4.3. Observation of two-photon interference

We observed two-photon interference using the set-up shown in figure 6. We fixed the temperature of the interferometer for the signal, and swept that for the idler, while measuring the coincidence counts.  $\mu$  was set at  $\sim 0.01$ . The result is shown in figure 8(a). We obtained a clear two-photon interference fringe with a visibility of  $90.6 \pm 1.5\%$ . The peak coincidence rate

estimated from the fitted curve was  $184.8 \text{ counts s}^{-1}$ . The peak coincidence rate calculated with equation (13) was  $362 \text{ bits s}^{-1}$ . This relatively large discrepancy between theory and experiment is caused by the noise photons: a previous report [33] shows that even when the DSF was cooled with liquid nitrogen, a significant number of noise photons were generated through spontaneous Raman scattering, which reduced the actual number of correlated photons and thus resulted in the smaller coincidence rate.

For comparison, we undertook the same measurement using two conventional gated-mode APDs with a 4 MHz gate frequency. The quantum efficiencies and dark count probabilities of the detectors were  $\sim 8\%$  and  $\sim 5 \times 10^{-5}$ , respectively. All the other parameters, including the average photon-pair number per pulse, were set at the same values as those used for the experiment with the sinusoidally gated APDs. The obtained two-photon interference fringe is shown in figure 8(b). The visibility of the fitted curve was  $87.8 \pm 9.6\%$ . It is clear that a better signal-to-noise ratio and an increased measurement speed with the sinusoidally gated APDs resulted in a larger visibility with less uncertainty. The peak coincidence rate obtained from figure 8(b) was  $0.6 \text{ counts s}^{-1}$ , which means that the use of sinusoidally gated APDs led to an increase in the coincidence rate by a factor of  $\sim 300$ . Equation (13) suggests that the peak coincidence rate is approximately proportional to  $\eta_s \eta_i f_g$ . Using the parameter values of our experimental set-up, the calculated ratio of the peak coincidence rate obtained with the sinusoidally gated APDs to that for the conventional gated-mode APDs is 280, which agrees well with the experimental result. Thus, we successfully achieved a significant increase in the speed of the coincidence fringe measurement by using the sinusoidally gated APDs.

## 5. Conclusion

We reported the observation of  $1.5 \mu\text{m}$  band entangled photons using single photon detectors based on InGaAs/InP APDs with the sinusoidal gating technique. First, we showed that high-speed detectors based on InGaAs/InP APDs are potentially useful for practical QKD systems based on entangled photon pairs. Then, we constructed two detectors using the sinusoidal gating technique that operated at a gate frequency of 500 MHz. With those detectors, we achieved a significant reduction in the measurement time compared with that when using conventional gated-mode APDs. We consider these high-speed single photon detectors based on InGaAs/InP APDs to be useful for realizing practical quantum communication over optical fibre networks.

## Acknowledgments

We thank Professor Shuichiro Inoue and Dr Naoto Namekata of Nihon University for fruitful discussions on sinusoidally gated single photon detectors.

## References

- [1] Gisin N and Thew R 2007 Quantum communication *Nat. Photonics* **1** 165
- [2] Gobby C, Yuan Z L and Shields A J 2004 Quantum key distribution over 122 km of standard telecom fiber *Appl. Phys. Lett.* **84** 3762
- [3] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 Quantum key distribution over a 40 dB channel loss using superconducting single-photon detectors *Nat. Photonics* **1** 343

- [4] Bennett C H and Brassard G 1984 *Proc. Int. Conf. Computer Systems and Signal Processing (Bangalore, India)* p 175
- [5] Lutkenhaus N 2000 Security against individual attacks for realistic quantum key distribution *Phys. Rev. A* **61** 052304
- [6] Hwang W Y 2003 Quantum key distribution with high loss: toward global secure communication *Phys. Rev. Lett.* **91** 057901  
Lo H K, Ma X and Chen K 2005 Decoy state quantum key distribution *Phys. Rev. Lett.* **94** 230504  
Wang X B 2005 Beating the photon-number-splitting attack in practical quantum cryptography *Phys. Rev. Lett.* **94** 230503
- [7] Rosenberg D, Harrington J W, Rice P R, Hiskett P A, Peterson C G, Hughes R J, Lita A E, Nam S W and Nordholt J E 2007 Long distance decoy state quantum key distribution in optical fiber *Phys. Rev. Lett.* **98** 010503
- [8] Ekert A K 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661
- [9] Bennett C H, Brassard G and Mermin D 1992 Quantum cryptography without Bell's theorem *Phys. Rev. Lett.* **68** 557
- [10] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol *Phys. Rev. Lett.* **85** 441
- [11] Waks E, Zeevi A and Yamamoto Y 2002 Security of quantum key distribution with entangled photons against individual attacks *Phys. Rev. A* **65** 052310
- [12] Tsurumaru T and Tamaki T 2008 Security proof for quantum-key-distribution systems with threshold detectors *Phys. Rev. A* **78** 032302
- [13] Beaudry N J, Moroder T and Lutkenhaus N 2008 Squashing models for optical measurements in quantum communication *Phys. Rev. Lett.* **101** 093601
- [14] Koashi M, Adachi Y, Yamamoto T and Imoto N 2008 Security of entanglement-based quantum key distribution with practical detectors arXiv:0804.0891v1
- [15] Ursin R *et al* 2007 Entanglement-based quantum communication over 144 km *Nat. Phys.* **3** 481
- [16] Tittel W, Brendel J, Zbinden H and Gisin N 2000 Quantum cryptography using entangled photons in energy-time Bell states *Phys. Rev. Lett.* **84** 4737
- [17] Fasel S, Gisin N, Ribordy G and Zbinden H 2004 Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs: a comparison of two chromatic dispersion reduction methods *Eur. Phys. J. D* **30** 143
- [18] Honjo T, Takesue H and Inoue K 2007 Differential-phase quantum key distribution experiment using a series of quantum entangled photon pairs *Opt. Lett.* **32** 1165
- [19] Honjo T *et al* 2008 Long-distance entanglement-based quantum key distribution over optical fiber *Opt. Express* **16** 19118
- [20] Ribordy G, Gautier J D, Zbinden H and Gisin N 1998 Performance of InGaAs/InP avalanche photodiodes as gated-mode photon counters *Appl. Opt.* **37** 2272
- [21] Namekata N, Sasamori S and Inoue S 2006 800 MHz Single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating *Opt. Express* **14** 10043
- [22] Yuan Z L, Kardynal B E, Sharpe A W and Shields A J 2007 High speed single photon detection in the near infrared *Appl. Phys. Lett.* **91** 041114
- [23] Namekata N, Fujii G, Inoue S, Honjo T and Takesue H 2007 Differential phase shift quantum key distribution using single-photon detectors based on a sinusoidally gated InGaAs/InP avalanche photodiode *Appl. Phys. Lett.* **91** 011112
- [24] Yuan Z L, Dixon A R, Dynes J F, Sharpe A W and Shields A J 2008 Gigahertz quantum key distribution with InGaAs avalanche photodiodes *Appl. Phys. Lett.* **92** 201104
- [25] Inoue K 2005 Quantum key distribution using a series of quantum correlated photon pairs *Phys. Rev. A* **71** 032301

- [26] Takesue H and Shimizu K Effects of multiple pairs on visibility measurements of entangled photons generated by spontaneous parametric processes *J. Mod. Opt.* submitted
- [27] Langrock C, Diamanti E, Roussev R V, Yamamoto Y, Fejer M M and Takesue H 2005 Highly efficient single-photon detection at communication wavelengths by use of upconversion in reverse-proton-exchanged periodically poled LiNbO<sub>3</sub> waveguides *Opt. Lett.* **30** 1725
- [28] Diamanti E, Takesue H, Langrock C, Fejer M M and Yamamoto Y 2006 100 km differential phase shift quantum key distribution experiment with low-jitter up-conversion detectors *Opt. Express* **14** 13073
- [29] Golt'sman G N, Kunev O, Chulkova G, Lipatov A, Semenov A, Smirnov K, Williams C and Sobolewski R 2001 Picosecond superconducting single-photon optical detector *Appl. Phys. Lett.* **79** 705
- [30] Rosfjord K M, Yang J K W, Dauler E A, Kerman A J, Anant V, Voronow B M, Gol'tsman G N and Berggren K K 2006 Nanowire single-photon detector with and integrated optical cavity and anti-reflection coating *Opt. Express* **14** 527
- [31] Owens P C M, Rarity J G, Tapster P R, Knight D and Townsend P D 1994 Photon counting with passively quenched germanium avalanche *Appl. Opt.* **33** 6895
- [32] Takesue H and Inoue K 2005 Generation of 1.5  $\mu\text{m}$  band time-bin entanglement using spontaneous fiber four-wave mixing and planar light-wave circuit interferometers *Phys. Rev. A* **72** 041804
- [33] Takesue H and Inoue K 2005 1.5  $\mu\text{m}$  band quantum photon pair generation in dispersion-shifted fiber: suppression of noise photons by cooling fiber *Opt. Express* **13** 7832