Long-distance entanglement-based quantum key distribution over optical fiber

T. Honjo[1,8], S. W. Nam[2], H. Takesue[1,8], Q. Zhang[3,7], H. Kamada[1], Y. Nishida[4], O.Tadanaga[4], M. Asobe[4], B. Baek[2], R. Hadfield[2], S. Miki[5], M. Fujiwara[5], M. Sasaki[5], Z.Wang[5], K. Inoue[1,6,8] and Y. Yamamoto[3,7]

[1]NTT Basic Research Laboratories, NTT Corporation, Atsugi-shi 243-0198, Japan
[2]National Institute of Standards and Technology, 325 Broadway, Boulder, Colorado 80305, USA
[3]E. L. Ginzton Laboratory, Stanford University, 450 Via Palou, Stanford, California 94305-4088, USA
[4]NTT Photonics Laboratories, NTT Corporation, Atsugi-shi 243-0198, Japan
[5]National Institute of Information and Communication Technology, 4-2-1 Nukui-kitamachi, Koganei, Tokyo 184-8795, Japan
[6]Osaka University, Suita, Osaka, 565-0871 Japan
[7]National Institute of Information, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan
[8]CREST, Japan Science and Technology Agency, 5 Sanbancho, Chiyoda-ku, Tokyo, 102-0075, Japan
[*]Corresponding author: honjo@will.brl.ntt.co.jp

Abstract: We report the first entanglement-based quantum key distribution (QKD) experiment over a 100-km optical fiber. We used superconducting single photon detectors based on NbN nanowires that provide high-speed single photon detection for the 1.5-μm telecom band, an efficient entangled photon pair source that consists of a fiber coupled periodically poled lithium niobate waveguide and ultra low loss filters, and planar lightwave circuit Mach-Zehnder interferometers (MZIs) with ultra stable operation. These characteristics enabled us to perform an entanglement-based QKD experiment over a 100-km optical fiber. In the experiment, which lasted approximately 8 hours, we successfully generated a 16 kbit sifted key with a quantum bit error rate of 6.9 % at a rate of 0.59 bits per second, from which we were able to distill a 3.9 kbit secure key.

OCIS codes: (190.4370) Nonlinear optics,fibers; (270.0270)Quantum optics

References and links

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145 (2002).
2. H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over 40 dB channel loss using superconducting single-photon detectors," Nat. Photonics **1**, 343 (2007).
3. A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661-663 (1991).
4. C. H. Bennett, G. Brassard and N. D. Mermin, "Quantum cryptography without Bell's theorem," Phys. Rev. Lett. **68**, 557-559 (1992).
5. T. Jennewein, C Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," Phys. Rev. Lett. **84**, 4729-4732 (2000).
6. D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, "Entangled state quantum cryptography: eavesdropping on the Ekert protocol," Phys. Rev. Lett. **84**, 4733-4736 (2000).
7. W. Tittel, J. Brendel, H. Zbinden and N. Gisin, "Quantum Cryptography using entangled photons in energy-time Bell states," Phys. Rev. Lett. **84**, 4737-4740, (2000).
8. S. Fasel, N. Gisin, G. Ribordy, and H. Zbinden, "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**, 2013148 (2004).
9. A. Poppe A. Fedrizzi, R. Ursin, H. Bohm, T. Lorunser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, A. Zeilinger, "Practical quantum key distribution with polarization entangled photons," Opt. Express, **12**, 3865-3871 (2004).
10. T. Honjo, H. Takesue and K. Inoue, "Differential-phase quantum key distribution experiment using a series of quantum entangled photon pairs," Opt. Lett. **32**, 1165 (2007).
11. A. Yoshizawa, R. Kaji and H. Tsuchida, "Gated-mode single-photon detection at 1550 nm by discharge pulse counting," Appl. Phys. Lett. **84**, 3606 (2004).

#101807 - $15.00 USD Received 22 Sep 2008; revised 28 Oct 2008; accepted 28 Oct 2008; published 4 Nov 2008

12. M. A. Albota and F. N. C. Wong, , "Efficient single-photon counting at 1.55 μm by means of frequency upconversion," Opt. Lett. **29**, 1449-1451 (2004).
13. C. Langrock, E. Diamanti, R. V. Roussev, Y. Yamamoto, M. M. Fejer, and H. Takesue, "Highly efficient single-photon detection at communication wavelengths by use of upconversion in reverse-proton-exchanged periodically poled LiNbO3 waveguides," Opt. Lett. **30**, 1725-1727 (2005).
14. N. Namekata, S. Sasamori, and S. Inoue, "800 MHz single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating," Opt. Express **14**, 10043-10049 (2006).
15. G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams and R. Sobolewski, "Picosecond superconducting single-photon optical detector," Appl. Phys. Lett. **79**, 705 (2001).
16. S. Tanzilli, W. Tittel, H. De Riedmatten, H. Zbinden, P. Baldi, M. De Micheli, D. B. Ostrowsky, and N. Gisin, "PPLN waveguide for quantum communication," Euro Phys. J. **18**, 155-160 (2002).
17. A. Yoshizawa, R. Kaji, and H. Tsuchida, "Generation of polarization-entangled. photon pairs at 1550 nm using two PPLN waveguides," Electron. Lett. **39**, 621-622 (2003).
18. X. Li, P. L. Voss, J. E. Sharping and P. Kumar, "Optical-fiber source of polarization-entangled photons in the 1550 nm telecom band," Phys. Rev. Lett. **94**, 053601 (2005).
19. H. Takesue and K. Inoue, "Generation of polarization entangled photon pairs and violation of Bell's inequality using spontaneous four-wave mixing in a fiber loop," Phys. Rev. A **70**, 031802(R) (2004).
20. H. Takesue, Y. Tokura, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, and S. Itabashi, "Entanglement generation using silicon wire waveguide," Appl. Phys. Lett. **91**, 201108 (2007).
21. T. Honjo, K. Inoue and H. Takahashi, "Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer," Opt. Lett. **29**, 23, 2797, (2004).
22. J. Brendel, W. Tittel, H. Zbinden and N. Gisin, "Pulsed energy-time entangled twin-photon source for quantum Communication," Phys. Rev. Lett. **82**, 2594 (1999).
23. I. Marcikic, H. de Riedmatten, W. Tittel, V. Scarani, H. Zbinden, and N. Gisin, "Time-bin entangled qubits for quantum communication created by femtosecond pulses," Phys. Rev. A **66**, 062308 (2002).
24. H. Takesue and K. Inoue, "Generation of 1.5-um band time-bin entanglement using spontaneous fiber four-wave mixing and planar lightwave circuit interferometers," Phys. Rev. A **72**, 041804(R) (2005).
25. T. Honjo, H. Takesue, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe and K. Inoue, "Long-distance distribution of time-bin entangled photon pairs over 100 km using frequency up-conversion detectors," Opt. Express, **15**, 13957-13964 (2007).
26. M. Asobe, H. Miyazawa, O. Tadanaga, Y. Nishida, and H. Suzuki, "Wavelength conversion using quasi-phase matched $LiNbO_3$ waveguides," The Optical Electronics and Communications Conference, Yokohama, Japan, July 8-12 2002, paper PD2-8.
27. R. H. Hadfield, M. J. Stevens, S. S. Gruber, A. J. Miller, R. E. Schwall, R. P. Mirin, and S. W. Nam, "Single photon source characterization with a superconducting single photon detector," Opt. Express **13**, 10846-10853 (2005).
28. S. Miki, M. Fujiwara, M. Sasaki, A. J. Miller, R. H. Hadfield, S. W. Nam and Z. Wang, "Large sensitive-area NbN nanowire superconducting single-photon detectors fabricated on single-crystal MgO substrates," Appl. Phys. Lett. **92**, 061116 (2008).
29. P. R. Tapster and J. G. Rarity, "Photon statistics of pulsed parametric light," J. Mod. Optics **45**, 595-604 (1998).
30. H. Takesue, "Long-distance distribution of time-bin entanglement generated in a cooled fiber," Opt. Express **14**, 3453 (2006).
31. E. Waks, A. Zeevi, and Y. Yamamoto, "Security of quantum key distribution with entangled photons against individual attacks," Phys. Rev. A **65**, 052310 (2002).

1. Introduction

Quantum key distribution (QKD) is being studied as a way of providing unconditionally secure communications [1]. Although many QKD experiments have been successfully demonstrated, extending the transmission distance remains a challenging problem. Optical fiber is the most interesting long-distance transmission medium, and so many QKD experiments with 1.5-μm photons have been performed over optical fiber. In particular, QKD using weak coherent laser light has been intensively investigated, and 200-km secure key distribution has been successfully demonstrated [2]. However, further extension by simply improving the experimental equipment is thought to be difficult. A QKD scheme using entangled photon pairs is a promising candidate for achieving a longer transmission distance. In this scheme, we can place an entangled photon pair source between two parties so that this scheme has the potential to extend the total key distribution distance. Furthermore, key bit information is retrieved from a correlation embedded solely in a photon pair so that no information is leaked to an eavesdropper as a result of signal source imperfections, thus enabling us to realize long-distance secure key distribution.

#101807 - $15.00 USD Received 22 Sep 2008; revised 28 Oct 2008; accepted 28 Oct 2008; published 4 Nov 2008

The first entanglement based QKD protocol (E91) in which Bell's inequality was used to detect eavesdropping, was proposed by Ekert in 1991 [3]. The following year, Bennett, Brassard and Mermin proposed another entanglement-based QKD protocol, which is now referred to as the BBM92 protocol [4]. The BBM92 protocol is an entanglement variant of the BB84 protocol. After these proposals, several pioneering experimental demonstrations were performed [5-10]. Although the entanglement based QKD has the potential to surpass the current QKD records, the maximum fiber transmission distance is limited to a few tens of kilometers for the following reasons [8-10].

Photons in the 1.5-μm band are preferred for long distance fiber transmission because conventional silica fiber has its minimum loss in this band. However, no high-speed single photon detector or efficient entangled photon pair source were available for this band at that time. In long distance entanglement based QKD experiments, detection events where both photons in a pair are detected simultaneously at each site (coincidence events) are very rare due to the losses in the long fiber. This means it takes a very long time to generate sufficient key bits to evaluate the system. A high-speed single photon detector and an efficient entangled photon pair source are indispensable if we are to improve this situation. Furthermore, coincidence events are rare in long-distance QKD experiments thus making a stable experimental setup indispensable.

As regards a single photon detector in the 1.5-μm band, an InGaAs/InP avalanched photo diode based single photon detector has been widely used. However, its operating speed is slow and it is limited to less than ~10 MHz in terms of suppressing erroneous counts [1,11]. Recently, several high-speed single photon detectors operating in this band have been proposed and developed. These include a frequency up-conversion single photon detector [12,13], a sinusoidal gating InGaAs/InP single photon detector [14] and a superconducting single photon detector (SSPD) [15]. The high-speed operation minimizes the probability of missing the chance to detect photons so we can increase the probability of coincidence event detection. In particular, an SSPD provides low noise (low dark count rate) and small timing jitter (60 ps, full width at half maximum) in addition to high-speed operation.

As regards an entangled photon pair source in the 1.5-μm band, several types have been proposed and developed in recent years. There are two major approaches. One is to use a spontaneous parametric down conversion process in a periodically poled lithium niobate (PPLN) waveguide [16,17]. The other is to use a spontaneous four-wave mixing process in dispersion shifted fiber or silicon wire waveguides [18-20].

In this paper, we report an entanglement-based BBM92 quantum key distribution (QKD) experiment over a 100-km optical fiber. Three key components ensured the success of the long-distance entanglement-based QKD experiment. SSPDs based on NbN nanowires provided high-speed operation. An entangled photon pair source, which consisted of a fiber coupled periodically poled lithium niobate (PPLN) waveguide and ultra low loss filters provided efficient distribution of entangled photon pairs. A planar lightwave circuit Mach-Zehnder interferometer (PLC-MZI) provided very stable operation [21]. In particular, the use of the PLC-MZI made our experimental setup very stable. We performed a quantum key distribution experiment continuously for ~ 8 hours and successfully generated a 16 kbit sifted key with a quantum bit error rate of 6.9 %, from which we can distill a 3.9 kbit secure key after error correction and privacy amplification.

2. BBM92 QKD with time-bin entangled photon pairs

First, we briefly explain the BBM92 QKD protocol with time-bin entangled photon pairs [7]. Time-bin entanglement has an attractive feature in terms of fiber transmission, since it utilizes the differential phase of two sequential pulses and thus is robust against polarization fluctuations in the fiber.

#101807 - $15.00 USD Received 22 Sep 2008; revised 28 Oct 2008; accepted 28 Oct 2008; published 4 Nov 2008

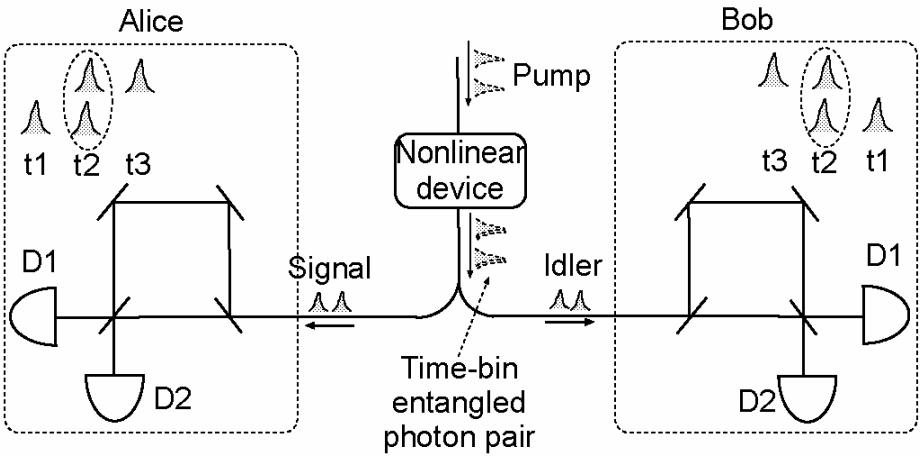

Fig. 1. Schematic diagram of BBM92QKD with time-bin entangled photon pairs.

Figure 1 shows a schematic diagram of BBM92 QKD with time-bin entangled photon pairs. Time-bin entanglement involves the superposition of two photon-pair states in two different time instances. A time-bin entangled photon pair is usually generated by pumping a non-linear optical medium with coherent double pulses. Two photons are simultaneously generated by a spontaneous parametric process, such as a parametric down conversion process or a four wave mixing process [22-24]. When we set the pump power at a relatively small value where the probability of both pulses generating photon pairs is very low, we can generate a time-bin entangled photon pair. Its quantum state is described by

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|1\rangle_s|1\rangle_i + |2\rangle_s|2\rangle_i), \tag{1}$$

where, $|k\rangle_x$ represents a state in which there is a photon in the k th time slot in mode x, signal (s) or idler (i). The signal and idler photons are separated by an optical filter, and then transmitted to Alice and Bob, respectively. At each site, each photon is passed through a 1-bit delay MZI, which splits the photon into three time slots, t1, t2 and t3. In the 2nd time slot, a state in which the photon passed through the long path of the MZI and another state in which the photon passed through the short path of the MZI interfere with each other. The final state is described by

$$\begin{aligned}|\psi\rangle_f = \frac{1}{4}[2i|t1\rangle_a|t1\rangle_b \ldots + (e^{i(\theta_a+\theta_b)}+1)(|D1,t2\rangle_a|D1,t2\rangle_b - |D2,t2\rangle_a|D2,t2\rangle_b) \\ -i(e^{i(\theta_a+\theta_b)}-1)(|D2,t2\rangle_a|D1,t2\rangle_b + |D2,t2\rangle_a|D1,t2\rangle_b) \ldots - 2e^{i(\theta_a+\theta_b)}|t3\rangle_a|t3\rangle_b],\end{aligned} \tag{2}$$

where $|tn\rangle_x$ represents a state in which a photon is detected at time slot tn on side x, $|Dn, tn\rangle_x$ represents a state in which a photon is detected at time slot tn and detector d on side x, and θ_x represents the phase difference of the MZI on side x, Alice (a) or Bob (b). In Eq. (2), the states in which Alice and Bob detect photons at different time slots are omitted. A pair consisting of the 1st and 3rd time slots is called time-basis and the 2nd time slot is called energy-basis. To obtain a perfect correlation, we set the sum of the phase differences, $\theta_a+\theta_b$, of these MZIs at 0. When we post-select a case where both Alice and Bob detect photons in the t2 time slot (energy-basis), the final state is described by Eq. (3).

#101807 - $15.00 USD Received 22 Sep 2008; revised 28 Oct 2008; accepted 28 Oct 2008; published 4 Nov 2008

$$\left|\psi_f\right\rangle_{energy-base} = \frac{1}{\sqrt{2}}(\left|D1\right\rangle_a\left|D1\right\rangle_b - \left|D2\right\rangle_a\left|D2\right\rangle_b) \quad (3)$$

Here, $|d>_x$ represents a state in which a photon is detected at detector d on side x, Alice (a) or Bob (b). In this case, a correlation appears between detectors. On the other hand, when we post-select the case where both Alice and Bob detect a photon in time slot t1 or t3 (time-basis), the final state is described by Eq. (4).

$$\left|\psi_f\right\rangle_{time-base} = \frac{1}{\sqrt{2}}(i\left|t1\right\rangle_a\left|t1\right\rangle_b - \left|t3\right\rangle_a\left|t3\right\rangle_b) \quad (4)$$

Here, $|t>_x$ represents a state in which a photon is detected at time slot t on side x, Alice (a) or Bob (b). In this case, a correlation appears between the detection times. Selection on the above basis is made spontaneously with no active selection procedure.
When Alice and Bob detect photons, they record the detection time and which detector clicked. After the detection, they disclose their measurement basis through the classical channel. If they detect photons in the same basis, they can generate a key bit from the above correlations. Otherwise, they simply discard the event. By repeating this sequence, Alice and Bob can generate a sifted key bit string.

3. Experimental setup

Figure 2 shows the setup we used for our QKD experiments [25]. A continuous lightwave emitted from an external-cavity semiconductor laser at a wavelength of 1551 nm was converted into a pulse stream by a $LiNbO_3$ intensity modulator. The pulse width and repetition frequency were 100 ps and 1 GHz, respectively. A series of double pulses was generated by extinguishing one of three sequential pulses with another intensity modulator. The coherence time of the laser output was ~10 μs, which is far longer than the temporal interval between the double pulses. The pulses were amplified with an erbium-doped fiber amplifier (EDFA) and filtered through a fiber Bragg grating filter that suppresses the amplified spontaneous emission noise from the EDFA. After passing through a polarization controller, the pulses were launched into PPLN (1), where a series of 775.5-nm double pulses was generated by the second harmonic generation process. The output light from PPLN (1) was input into filters that transmitted the 775.5-nm pulses while eliminating the remaining 1551-nm light. The series of 775.5-nm double pulses was polarization-controlled and then input into PPLN (2). A series of time-bin entangled photon pairs was generated in PPLN (2) by the parametric down conversion process [26]. The pump, signal and idler frequencies are denoted by $f_{p,}$,f_s and f_i, respectively. These three frequencies have a relationship of $f_{p,} = f_s + f_i$,.

The total loss that included the excess loss in PPLN (2) and the fiber-coupling loss was estimated to be 4.45 dB for the signal and 3.95 dB for the idler. The output from PPLN (2) was input into a filter that transmitted the 1551-nm light while eliminating the remaining 775.5-nm light. The loss of this filter was 0.05 dB for 1.5-μm photons. The photons were input into a dielectric band-pass filter that separated the 1547-nm signal light and the 1555-nm idler light. The spectral width of this filter was 100 GHz, and its loss was 0.35 dB for 1547 nm and 0.53 dB for 1555 nm. After this separation, the signal and idler were transmitted over a 50-km dispersion shifted fiber (DSF) with a loss of 0.21 dB/km, respectively. They were then launched into 1-bit delayed PLC-MZIs whose path length difference was 20 cm [21]. The loss of the interferometer was about 2.0 dB. The phase difference between the two paths was precisely and stably adjusted by controlling the interferometer temperature. Four SSPDs were installed at the output port of the MZI [27,28]. The quantum efficiency of one of the SSPDs was 2.0 %, and those of the others were all 0.7%. The dark count rate was around 250 cps for each detector, which was negligible in our experiment. The slight large dark count rate was due to the electrical noise in our laboratory. The full width at half maximum of the jitter was approximately 60 ps, which was small enough to discriminate 1-ns interval pulses. The output

#101807 - $15.00 USD Received 22 Sep 2008; revised 28 Oct 2008; accepted 28 Oct 2008; published 4 Nov 2008

signals of the photon detectors were input into a time interval analyzer to record the detection events.

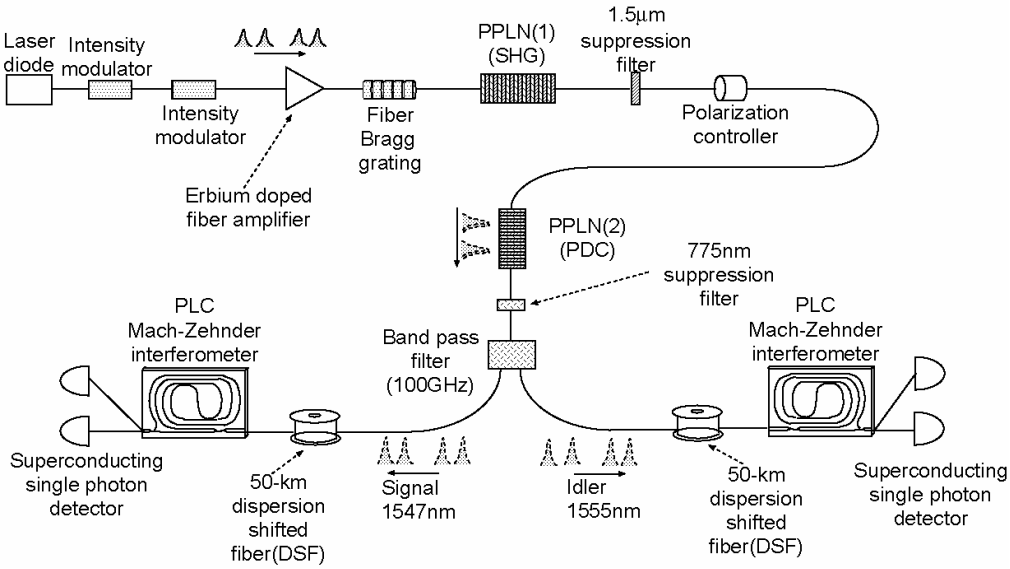

Fig. 2. Experimental setup.

4. Experimental results

First, we performed experiments without installing a 50-km optical fiber. Before conducting the BBM92 QKD experiment, we performed two-photon interference experiments. Since these experiments only concerned interference time slots (energy-basis), we used a 1-GHz pulse train containing entangled photon pairs instead of a series of time-bin entanglements (i.e., pairs of two pulses). One of the two photon detectors at each site was used for the measurement. The coincidence was recorded with the temperature of the PLC MZI fixed for the signal and changed for the idler. We can tune the phase difference of the interferometer by changing the temperature. The average number of photon pair per pulses was adjusted to 0.016, which corresponded to an average number of photon pairs of 0.032 per time-bin entanglement slot (i.e., sequential double pulses). Figure 3 shows the results. Throughout the measurement, the count rates of the signal and idler detectors were ~36 and ~11 kcps, respectively. Although the count rates remained unchanged, we observed a deep modulation in the coincidence rate as the interferometer temperature changed. A visibility of 93.8 % was obtained in the coincidence fringe without subtracting background noise such as accidental coincidence and the dark count. To check the above experimental results, we estimated the visibility of the coincidence fringe theoretically. In our experiment, the pump pulse duration was longer than the coherence time of the down-converted photons so that the probability of n pairs in a given pulse had a Poisson distribution [29]. Taking this characteristic of the photon pair source into account, we can express the count probability of each photon detector per time slot, denoted by c_s and c_i , respectively, as [30].

$$c_s = \frac{\mu_c}{2}\alpha_s + d_s, \tag{5}$$

$$c_i = \frac{\mu_c}{2}\alpha_i + d_i, \tag{6}$$

#101807 - $15.00 USD Received 22 Sep 2008; revised 28 Oct 2008; accepted 28 Oct 2008; published 4 Nov 2008

where μ_c, α_x and d_x are the average number of correlated photon pairs per pulse, the transmittance for channel x, and the dark count rate for channel x, with x=s (signal) or i (idler).

By using these equations, we can express the coincidence rate and accidental coincidence, denoted by R_{cc} and R_{acc}, respectively, as follows.

$$R_{cc} = \frac{1}{4}\mu_c \alpha_s \alpha_i, \tag{7}$$

$$R_{acc} = \left(\frac{\mu_c}{2}\alpha_s + d_s\right)\left(\frac{\mu_c}{2}\alpha_i + d_i\right) \tag{8}$$

The visibility of the two photon interference fringe, V, is then given by

$$V = \frac{(R_{cc} + R_{acc}) - R_{acc}}{(R_{cc} + R_{acc}) + R_{acc}} = \frac{R_{cc}}{R_{cc} + 2R_{acc}} \quad . \tag{9}$$

Substituting the estimated average number of photon pairs per pulse of 0.016 and the loss of each arm, which includes the quantum efficiency of the detector and the intrinsic loss of the MZI, we theoretically estimated the visibility to be 96.8%. The slight degradation in the experimental results must result from imperfect interference in the PLC MZIs.

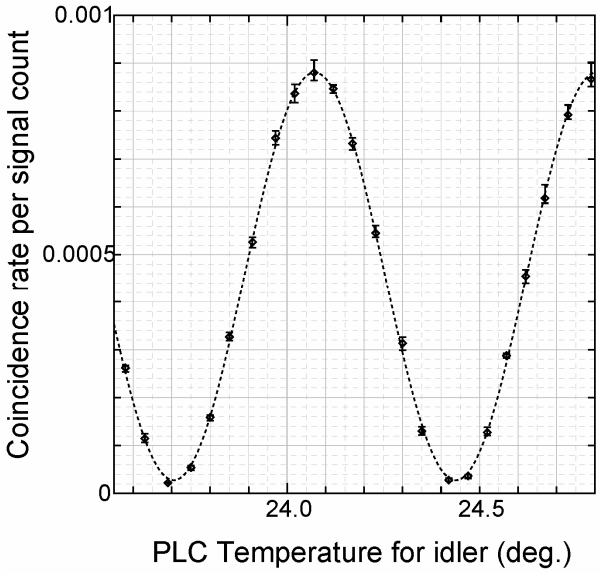

Fig. 3. Two-photon interference fringe with no transmission fiber.

We then performed a BBM92 QKD experiment using four SSPDs. We adjusted the temperature of the PLC-MZI at which perfect correlations were observed. The average number of photon pairs per time-bin entanglement slot was adjusted to 0.04. We continuously recorded detection events for ~1.5 hours. We then generated a sifted key from the recorded events according to the BBM92 QKD protocol. We successfully generated a 125,556-bit sifted key with a quantum bit error (QBER) of 2.35%. The sifted key generation rate was

#101807 - $15.00 USD Received 22 Sep 2008; revised 28 Oct 2008; accepted 28 Oct 2008; published 4 Nov 2008

estimated to be 29.4k bps. As for the time-basis, a 63,080-bit sifted key was created with a QBER of 1.6%. For the energy-basis, a 62,476-bit sifted key was obtained with a QBER of 3.1%. The QBER in the energy-basis is ~1% larger than that in the time-basis because of the imperfect interference in the PLC-MZIs. We also theoretically estimated the sifted key generation rate and QBER. The sifted key generation rate, R_{sift}, is expressed as follows.

$$R_{sift} = f(R_{cc} + R_{acc}) \cong \frac{f}{2}\mu_t \alpha_s \alpha_i \tag{10}$$

where μ_t is the average number of photon pairs per time-bin entanglement slot, and f is the repetition frequency of the distribution of the time-bin entanglement slots, and the other parameters are the same as in Eqs. (5) and (6). Half of the accidental coincidences contribute to the error and so QBER is expressed as follows.

$$QBER = \frac{2R_{acc}}{R_{cc} + 4R_{acc}} \cong \frac{\mu_t}{2(1+\mu_t)} \tag{11}$$

Note that the average number of photon pairs per pulse, μ_c is μ_t / 2 in this evaluation. Substituting the estimated average number of photon pairs per time-bin entanglement slot of 0.04 and the other experimental conditions, we theoretically estimated the sifted key generation rate to be 30.0 bps and the QBER to be 1.9 %, which shows that our experimental results are reasonable. In addition, we estimated the secure key generation rate from the above experimental results. The secure key distribution rate against any individual attack for the BBM92 QKD protocol is given by the following expression [31]:

$$R_{\sec ure} = R_{sift}[-\log_2(\frac{1}{2} + 2e - 2e^2) + f(e)(e\log_2 e + (1-e)\log_2(1-e))] \tag{12}$$

where e and $f(e)$ represent the bit error rate in a sifted key and the performance of the error correction algorithm, respectively. With the above equation, an 86,248-bit secure key will be distilled from our sifted keys with a key generation rate of 20.2 bps.

Next, we inserted a 50-km DSF spool between the entanglement source and the interferometer for both the signal and idler. The total loss of the 50-km DSF spool, including connector and splicing losses, was ~10.5 dB. Therefore, the total loss between PPLN (2) and the photon detector was ~17.4 dB for the signal and ~17.0 dB for the idler. In the same way as with no fiber transmission, we performed a two-photon interference experiment first. Figure 4 shows the results. The average number of photon pairs per pulse was 0.07, which corresponds to an average number of photon pairs of 0.14 per time-bin entanglement slot. Throughout the measurement, the count rates at the signal and idler detectors were ~12.0 and ~3.1 kcps, respectively. Although the count rates remained unchanged, we observed a deep modulation in the coincidence rate as the interferometer temperature changed. A visibility of 85.0 % was obtained in the coincidence fringe without subtracting background noise such as accidental coincidence and the dark count.

The theoretically estimated visibility was 87.7%. The slight degradation in the experiment must result from imperfect interference in the PLC MZIs and statistical fluctuation in the experiment at a small coincidence rate.

#101807 - $15.00 USD Received 22 Sep 2008; revised 28 Oct 2008; accepted 28 Oct 2008; published 4 Nov 2008

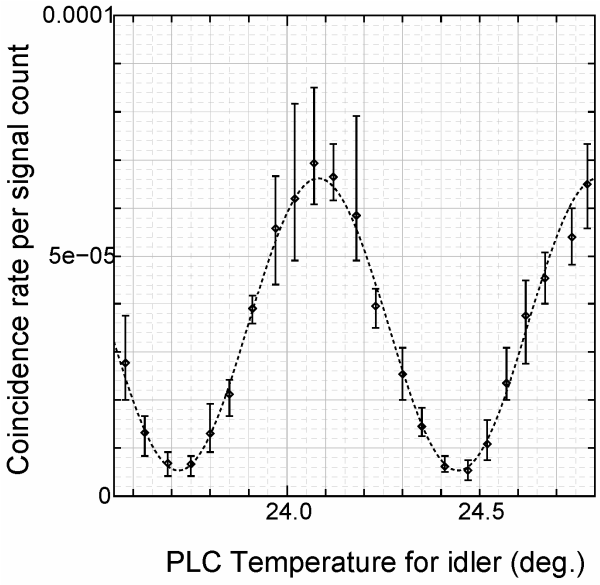

Fig. 4. Two-photon interference fringe after transmission over 100-km dispersion shifted fiber.

Finally, we performed a 100-km BBM92 QKD experiment. After adjusting the temperature of the PLC-MZIs to that at which perfect correlations were obtained, we recorded detection events continuously for ~8 hours. Then, we generated a sifted key from the recorded events according to the BBM92 QKD protocol. We successfully generated a 16,217-bit sifted key with a QBER of 6.91%. The sifted key generation rate was estimated to be 0.57 bps. As regards the time-basis, an 8,083-bit sifted key was created with a QBER of 6.22%. On the other hand, with the energy-basis an 8,134-bit sifted key was created with a QBER of 7.59%. The theoretically estimated sifted key generation rate and QBER were 0.83 bps and 6.14%, respectively. Based on Eq. (12) and the above results, our experiment provided a 3,904-bit secure key at a rate of 0.14 bps. Thus, we successfully demonstrated the probability of secure key distribution over a 100-km optical fiber with the entanglement based BBM92 QKD protocol. In this experiment, the transmission distance was limited to ~100 km. The origin of this limitation was the small coincidence rate, which meant that the long measurement time limited the transmission distance. If high quantum efficiency single photon detectors with high-speed operation are available, we can extend the transmission distance by simply replacing the detectors.

5. Summary

In summary, we reported an entanglement-based quantum key distribution (QKD) experiment over a 100-km optical fiber. Using superconducting single photon detectors (SSPDs), a PPLN based entanglement photon pair source, and PLC Mach Zehnder interferometers, we successfully generated a 16-kbit sifted key with a quantum bit error rate of 6.9 % at a rate of 0.59 bits per second, from which we can distill a 3.9-kbit secure key based on the individual attack security model. This is the first entanglement-based QKD experiment over a 100-km optical fiber.

#101807 - $15.00 USD Received 22 Sep 2008; revised 28 Oct 2008; accepted 28 Oct 2008; published 4 Nov 2008