10-GHz clock differential phase shift quantum key distribution experiment

Hiroki Takesue[1,2], Eleni Diamanti[3], Carsten Langrock[3], M. M. Fejer[3] and Yoshihisa Yamamoto[3]

[1]*NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, 243-0198, Japan.*

[2]*CREST, Japan Science and Technology Agency, 4-1-8 Honcho, Kawaguchi, Saitama, 332-0012, Japan*

[3]*Edward L. Ginzton Laboratory, Stanford University, Stanford, California 94305-4085*

htakesue@will.brl.ntt.co.jp

Abstract: This paper reports the first quantum key distribution experiment implemented with a 10-GHz clock frequency. We used a 10-GHz actively mode-locked fiber laser as a source of short coherent pulses and single photon detectors based on frequency up-conversion in periodically poled lithium niobate waveguides. The use of short pulses and low-jitter up-conversion detectors significantly reduced the bit errors caused by detector dark counts even after long-distance transmission of a weak coherent state pulse. We employed the differential phase shift quantum key distribution protocol, and generated sifted keys at a rate of 3.7 kbit/s over a 105 km fiber with a bit error rate of 9.7%.

OCIS codes: (270.0270) Quantum optics; (060.0060) Fiber optics and optical communications

References and links

1. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145-195 (2002).
2. P. D. Townsend, "Secure key distribution system based on quantum cryptography" Electron. Lett. **30** 809 (1994).
3. G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard and H. Zbinden, "Automated 'plug & play' quantum key distribution," Electron. Lett. **34** 2116 (1998).
4. M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren and E. Sundberg, "Experiments on long wavelength (1550 nm) "plug and play" quantum cryptography systems," Opt. Express **4** 383 (1999).
5. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, "Quantum key distribution over 67 km with a plug & play system," New J. Phys. **4** 41 (2002).
6. A. Yoshizawa, R. Kaji and H. Tsuchida,"10.5 km fiber-optic quantum key distribution at 1550 nm with a key rate of 45 kHz," Jpn. J. Appl. Phys. **43** (2004) L735.
7. 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**, 2797 (2004).
8. H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue and Y. Yamamoto, "Differential phase shift quantum key distribution experiment over 105 km fibre," New J. Phys. **7**, 232 (2005).
9. C. Gobby, Z. L. Yuan and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," Appl. Phys. Lett. **84** 3762-3764 (2004).
10. R. T. Thew, S. Tanzilli, L. Krainer, S. C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden and N. Gisin, "Low-jitter up-conversion detectors for telecom wavelength QKD," New J. Phys. **8** 32 (2006).
11. K. Inoue, E. Waks and Y. Yamamoto, "Differential phase shift quantum key distribution," Phys. Rev. Lett. **89**, 037902 (2002).

#73420 - $15.00 USD Received 26 July 2006; revised 12 September 2006; accepted 13 September 2006

12. K. Inoue, E. Waks and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," Phys. Rev. A **68**, 022317 (2003).
13. K. Inoue and T. Honjo, "Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack," Phys. Rev. A **71**, 042305 (2005).
14. E. Diamanti, H. Takesue, T. Honjo, K. Inoue, and Y. Yamamoto, "Performance of various quantum-key-distribution systems using 1.55-μm up-conversion single-photon detectors," Phys. Rev. A **72**, 052311 (2005).
15. E. Waks, H. Takesue and Y. Yamamoto, "Security of differential-phase-shift quantum key distribution against individual attacks," Phys. Rev. A **73**, 012344 (2006).
16. 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 $LiNbO_3$ waveguides," Opt. Lett., **30**, 1725 (2005).

1. Introduction

Fiber-based quantum key distribution (QKD) systems have been studied very intensively in recent years [1]. Since the first QKD experiment over an optical fiber spool [2], many QKD systems have been demonstrated [3, 4, 5, 6]. Currently, intensive efforts are being made to increase the key generation rate and distribution distance. Fiber-based QKD experiments with a 1-GHz clock [7, 8] and long-distance QKD over $>$100 km of fiber [8, 9] have already been reported.

The main factor that limited the key distribution distance in previous experiments was bit errors caused by detector dark counts. The most straightforward way to increase the secure key distribution distance is to reduce the dark counts. Another effective approach is to increase the timing resolution of the whole system, which means that we use shorter pulses for photon transmission and photon detectors with shorter timing jitters. In such a system, the dark counts are randomly distributed in the time domain, but the detected signal counts are concentrated in small time segments. As a result, we can effectively increase the signal to noise ratio, which results in fewer bit errors.

A simple and effective way to increase the key generation rate is to increase the clock rate of the system. Since a 10-Gbit/s system is already in practical use in current (classical) optical communication, many components designed for such high-speed optical communication systems can be used to realize a 10-GHz clock QKD system. The biggest problem for such a system is the timing jitter of the single photon detectors. For example, the detectors based on frequency up-conversion in a periodically poled lithium niobate (PPLN) waveguide used in [8] had a timing jitter of $\sim$500 ps, which is too large for a 10-GHz clock system. Recently, a single photon interference experiment using up-conversion detectors with improved jitter has been reported [10].

In this paper, we report the first DPS-QKD system with a 10-GHz clock frequency. We used a 10-GHz actively mode-locked laser as a coherent pulse source. As regards the detectors, we used up-conversion detectors with improved jitter characteristics. The short pulses from the mode-locked laser and the low jitter characteristic of the detector improved the time resolution of the system, which resulted in a significant reduction of the dark count contribution to the bit errors. As a result, we successfully generated 3.7-kbit/s sifted keys over 105 km of fiber with 9.7% error rate.

2. Differential phase shift quantum key distribution protocol

Figure 1 shows a schematic diagram of DPS-QKD [11, 12]. Alice modulates the phase of each pulse emitted from a coherent pulse source by $\{0, \pi\}$ using a phase modulator. The pulse train is then attenuated so that the average photon number per pulse is smaller than one (typically 0.2), and transmitted over an optical fiber. The output pulses from the fiber are received by

#73420 - $15.00 USD Received 26 July 2006; revised 12 September 2006; accepted 13 September 2006

Bob. Bob is equipped with a 1-bit delayed Mach-Zehnder interferometer whose two output ports are connected to single photon detectors 1 and 2. When the phase difference between two adjacent pulses is 0 (π), Bob observes a click at detector 1 (2). Since the average photon number per pulse is much less than 1, Bob observes clicks only occasionally. Bob records time instances in which he observed clicks, and which detector clicked. After detecting the photons, Bob discloses the time instances in which he observed clicks, while holding the which-detector information secret. Alice knows the phase differences at the particular time instances from her original modulation data, which are completely correlated to the which-detector information that Bob obtained in his measurement. As a result, Alice and Bob can construct an identical random bit string by allocating phase difference 0 as bit 0 and π as bit 1, which can be used later as a key for one-time pad cryptography.

In terms of a quantum mechanical description, DPS-QKD protocol is described as follows. If we assume the coherence time of the laser source as being infinite, the state that Alice prepares is expressed as

$$|\Psi\rangle = \left(\frac{1}{\sqrt{N}}\sum_{k=1}^{N} e^{i\phi_k}|k\rangle_1\right) \otimes \left(\frac{1}{\sqrt{N}}\sum_{k=1}^{N} e^{i\phi_k}|k\rangle_2\right) \otimes \cdots \otimes \left(\frac{1}{\sqrt{N}}\sum_{k=1}^{N} e^{i\phi_k}|k\rangle_M\right), \qquad (1)$$

where N, ϕ_k and M are the total number of time slots, the classical phase modulation at time slot k ($=\{0,\pi\}$), and the number of photons in N time slots, respectively. The phase difference between adjacent time slots $\phi_{k+1}-\phi_k$ corresponds to bit "0" or "1". Since the average number of photons per pulse is set at much smaller than 1, the number of photons M is much smaller than the number of phase differences, $N-1$. This means that it is impossible to reconstruct the whole wavefunction including $N-1$ phase differences with $M(<N-1)$ measurements. Thus, the security of DPS-QKD is based on the non-orthogonality of a wavefunction spanned by many time slots.

A merit of DPS-QKD is its robustness against photon number splitting attack, even though it uses a coherent light source [8, 13, 14]. Security of DPS-QKD is proven against general individual attack [15], which makes DPS-QKD an attractive solution for constructing long-distance QKD systems with currently available technologies.

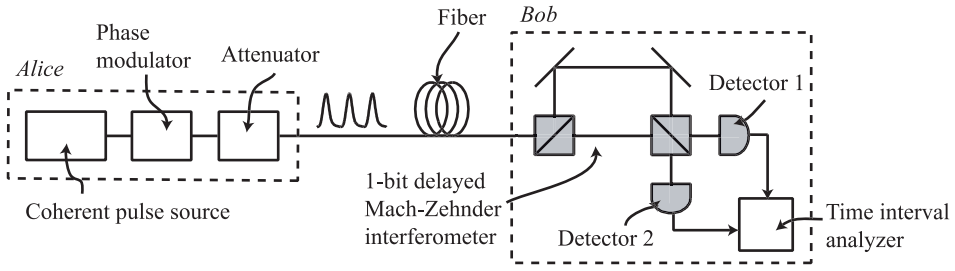

Fig. 1. Schematic diagram of differential phase shift quantum key distribution.

3. Experiments

3.1. Generation of coherent pulse train at 10-GHz clock frequency

We used an actively mode-locked fiber laser operated at 10.0 GHz (Calmar Optocom PSL-10) as a coherent pulse source. The full width at half maximum (FWHM) of the pulses was 10 ps. A typical pulse train observed using a sampling oscilloscope with a 53 GHz bandwidth is shown in Fig. 2. The side peak observed in each pulse is probably due to the non-ideal response of the

#73420 - $15.00 USD Received 26 July 2006; revised 12 September 2006; accepted 13 September 2006

photodetector. To confirm that the phase coherence was preserved between adjacent pulses, we input the pulse train into a 1-bit delayed Mach-Zehnder interferometer with 100 ps delay time whose output ports were connected to two optical power meters. When the phase difference induced by the interferometer was adjusted to obtain a dark fringe at one of the ports, the ratio of the two output powers was ∼20 dB, which is probably limited by the crosstalk of the interferometer. We then applied a phase modulation with an alternating pattern ($0\pi0\pi0\pi$..), by which we switched the port where the majority of light was output. Here too, the ratio of the two output powers was ∼20 dB. This implies that the error caused by imperfect interferometry in a QKD experiment is suppressed to ∼1%. This value is similar to that observed in our previous QKD experiments with a 1-GHz clock frequency using coherent pulses generated by modulating CW semiconductor laser light with an external intensity modulator [7, 8].

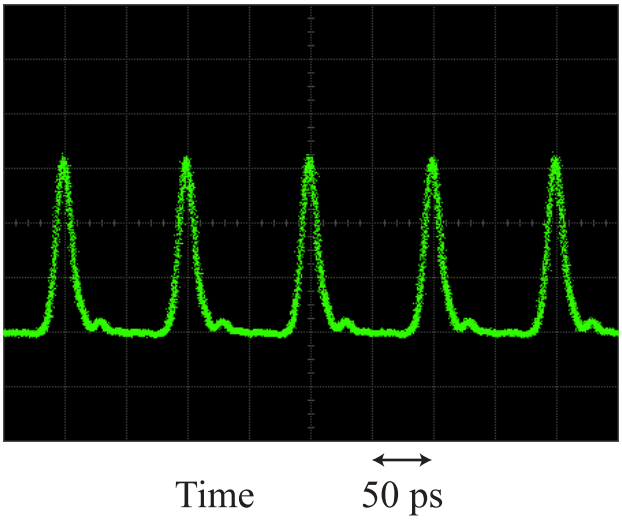

Fig. 2. 10-GHz pulse train from a fiber mode-locked laser monitored by a sampling oscilloscope with a 53 GHz bandwidth.

3.2. *Up-conversion detectors*

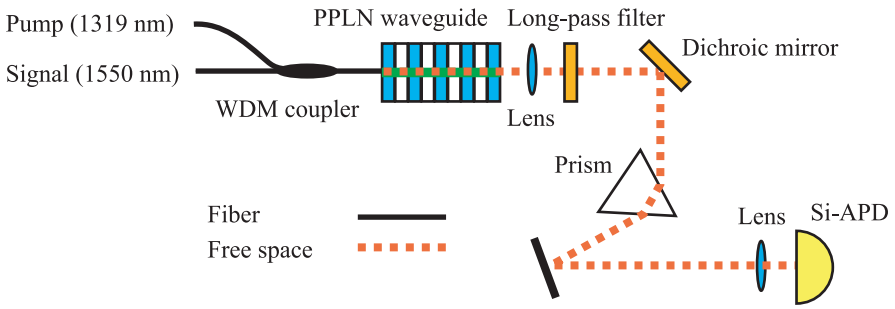

Fig. 3. Configuration of up-conversion detector.

A schematic diagram of the up-conversion detector is shown in Fig. 3 [16]. A 1550-nm signal photon was combined with 1319-nm CW pump light from a Nd-YAG laser via a wavelength

#73420 - $15.00 USD Received 26 July 2006; revised 12 September 2006; accepted 13 September 2006

division multiplexing (WDM) fiber coupler, and input into a PPLN waveguide. The wavelength of the signal photon was converted to 713 nm through the sum frequency generation process in the PPLN waveguide. The output light from the PPLN waveguide was input into a wavelength filter to suppress the second harmonic signal of the pump (0.66 μm), and then reflected by a dichroic mirror to separate long-wavelength photons (1.3 and 1.5 μm). The reflected light is then input into a prism to further suppress the pump and SHG components, and finally focused onto a low-jitter Si-APD (MPD photon counting detector module). When we input a $\sim$100-mW pump light, we obtained a peak quantum efficiency of $\sim$8 %. However, as reported in [16], dark counts caused by the spurious nonlinear effect increased quadratically as the pump power increased. Therefore, in the following QKD experiments, we set the quantum efficiencies of the up-conversion detectors at relatively small values, to enable us to obtain a better signal to noise ratio.

We measured the timing jitter of the up-conversion detectors. We input pulses with a 3-ps FWHM and a 1-GHz repetition frequency, and obtained a histogram of the detected signal. A typical histogram is shown in Fig. 4(a), where the count rate was at around 300,000 cps. The FWHM was $\sim$30 ps, which is sufficiently smaller than the 100 ps time interval of the 10-GHz clock system. However, a long tail was observed, which constituted a major source of bit errors in the QKD experiments. To evaluate the tail, we measured both the FWHM and the full width at tenth maximum (FWTM) as a function of count rate. The result is shown in Fig. 4(b). Both FWHM and FWTM increased as the count rate increased. In particular, the FWTM increased significantly when the count rate approached 1 MHz. This means that the error increases significantly when the transmission loss is small or the quantum efficiencies of the detectors are high.

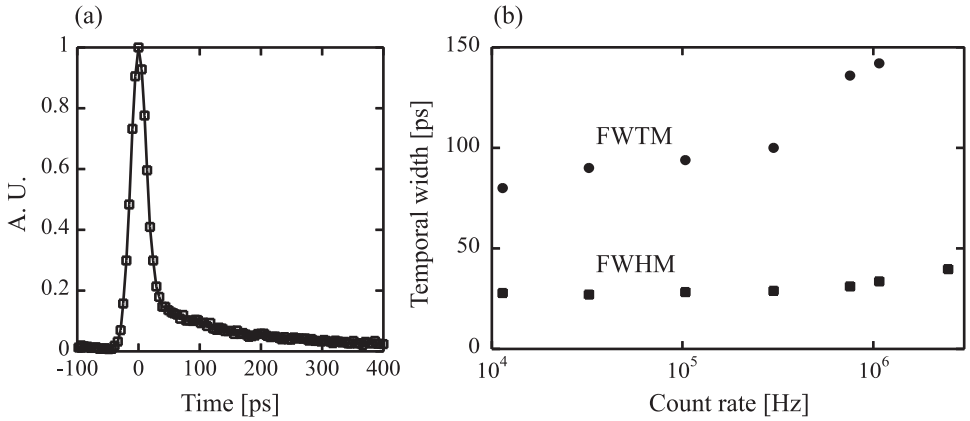

Fig. 4. (a) Typical histogram of detection signals from the up-conversion detector at a count rate of 300,000. (b) Full widths at half maximum and tenth maximum as a function of count rate.

3.3. QKD experiments

We undertook QKD experiments using the setup shown in Fig. 1. Alice and Bob were located in the same room, and fiber transmission was undertaken using spools of dispersion shifted fiber with a zero dispersion wavelength of 1550 nm. The phase modulator was driven at a bit rate of 10 Gbit/s by a pseudo-random bit sequence signal from a high-speed pulse pattern generator (Anritsu MP1765A). We used a Mach-Zehnder interferometer fabricated using planar lightwave circuit (PLC) technology, which was developed for 10-Gbit/s differential phase shift keying

#73420 - $15.00 USD Received 26 July 2006; revised 12 September 2006; accepted 13 September 2006

(DPSK) optical communication systems. The insertion loss of the PLC interferometer was 2.5 dB. We set the quantum efficiencies of two up-conversion detectors at 0.26 and 0.28%, thus allowing us to obtain the best signal to noise ratio for a long-distance transmission. The sum of the dark count rates of the two detectors was 650 cps. The photon detection time instances and which-detector information were recorded using a time interval analyzer (TIA) (Ortec 9308). To further reduce the effect of the dark counts and timing jitter, we applied a time window to the recorded data. Note that a sifted key was actually generated in our experiments and the error rates were measured by comparing Alice's key with Bob's key directly. For each data point described below, we ran five key distribution sessions. The error rates and sifted key rates are the average values of the five runs.

First, in order to determine the optimum time window width, we measured the sifted key rate for a 105 km transmission and plotted it as a function of time window width. The result is shown in Fig. 5(a). Using this experimental result, the dark count induced error rate, e_d, is calculated with the following equation.

$$e_d = \frac{f_c d \Delta t}{2R_{sifted}(\Delta t)} \tag{2}$$

Here, f_c, d, Δt, and R_{sifted} denote the clock frequency, the dark count rate per second, the time window width and the sifted key rate, respectively. e_d is calculated by plugging the experimentally obtained sifted key rate shown in Fig. 5(a) in Eq. (2), whose result is shown in Fig. 5(b). This result shows that e_d improves as Δt is reduced, but the improvement begins to saturate when Δt is smaller than 20 ps. When Δt is below 10 ps, the improvement could no longer be seen. This saturation of the error rate improvement results from the timing jitter of the up-conversion detectors discussed above. Therefore, we used a 10-ps time window in the following key generation experiments.

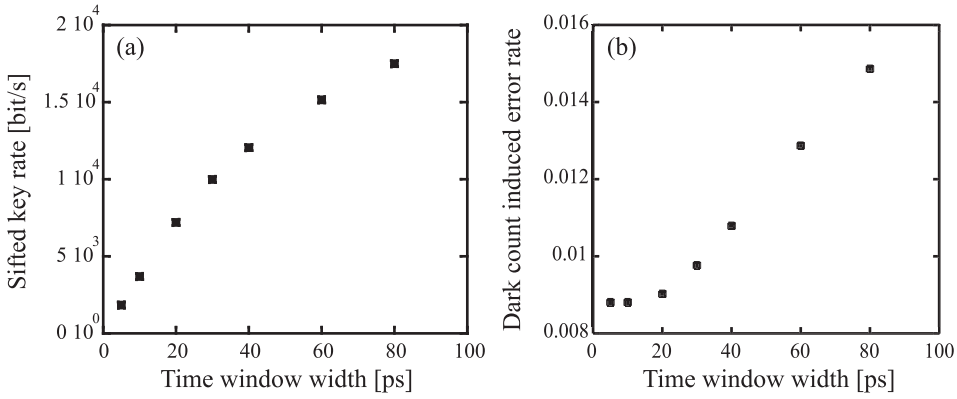

Fig. 5. (a) Sifted key rate and (b) estimated error rate caused by dark counts as a function of time window width at 105 km key distribution.

We inserted 10, 30, 75 and 105 km of fiber between Alice and Bob, and generated a sifted key. The results of our fiber transmission experiments are summarized in Table I. The squares in Fig. 6 show the error rates as a function of transmission fiber length. We have generated 3.7-kbit/s sifted keys over 105 km of fiber with a 9.7% error rate. Interestingly, we did not observe significant variation in the error rates when we used fibers with different lengths. Although the error rate usually increases as the transmission length increases, we observed even larger error rates at 10 and 30 km than at 75 and 105 km. This is because, as we saw in Fig. 4(b), the timing jitter increased when the count rate was increased due to the small transmission loss. The

#73420 - $15.00 USD Received 26 July 2006; revised 12 September 2006; accepted 13 September 2006

estimated error rate caused by the dark count is shown by the circles in Fig. 6. Here, the dark count induced error rate was so small that it was negligible when the transmission distance was shorter than 75 km. The slight increase in the total error rate at 105 km was probably caused by the increased dark count contribution. Nevertheless, the error rate caused by the dark count at 105 km was still less then 1%. Thus, the presented result clearly demonstrates the effectiveness of using short pulses and low-jitter detectors to improve the dark count induced error rate.

In this experiment, the long tails of the detection signals from the up-conversion detectors resulted in a relatively large error rate of $\sim$10%. At the 105 km transmission, 0.9% is from the dark counts, 1% is due to the imperfect extinction ratio of the interferometer, and the rest is induced the intersymbol interference caused by the long tail. Therefore, we should be able to significantly reduce the error rate by improving the timing jitter characteristics of the detector.

Unfortunately, the present experiments did not generate a secure key based on a security model against general individual attacks [15], because of the large intersymbol interference. We need an error rate as small as $\sim$4% to distill secure keys from sifted keys. If we can eliminate errors caused by the tail completely, we will be able to generate secure keys over 105 km of fiber even with the other components unchanged, and probably extend the secure key distribution distance even further. A possible way to improve the jitter characteristics is to use photo-multiplier tubes (PMT) instead of Si-APD for the up-conversion detectors, since PMTs generally exhibit better tail characteristics than Si-APDs.

Table I. Summary of fiber transmission experiment

Distance [km]	10	30	75	105
Fiber loss [dB]	2.4	6.5	16.1	22.1
Sifted key generation rate [kbit/s]	267$\pm$14	93.8$\pm$12.5	15.5$\pm$0.5	3.69$\pm$0.21
Error rate [%]	10.9$\pm$1.5	10.1$\pm$0.6	9.2$\pm$0.9	9.7$\pm$0.7
Dark count induced error rate [%]	0.012	0.035	0.19	0.88

#73420 - $15.00 USD Received 26 July 2006; revised 12 September 2006; accepted 13 September 2006

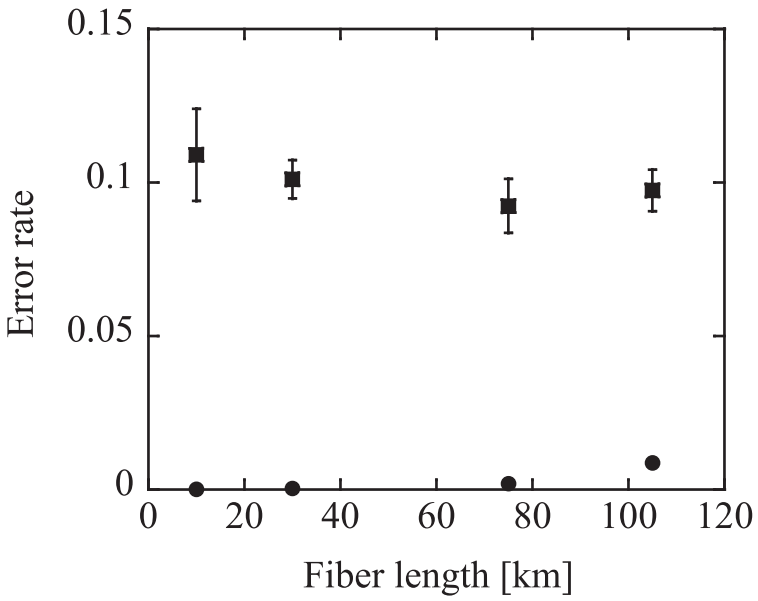

Fig. 6. Error rates (squares) and estimated error rates caused by dark counts (circles) as a function of transmission fiber length.

#73420 - $15.00 USD Received 26 July 2006; revised 12 September 2006; accepted 13 September 2006

4. Summary

We have reported the first QKD experiment with a 10-GHz clock frequency. We employed the DPS-QKD protocol implemented with a 10-GHz fiber mode-locked laser as a coherent pulse source and low-jitter up-conversion detectors, and successfully generated 3.7-kbit/s sifted keys over a 105-km fiber with a error rate of 9.7%. We showed that we can significantly reduce the dark count contribution to bit errors by using short pulses from a mode-locked laser, and up-conversion detectors with improved timing jitter characteristics. The remaining problem is the long tail of the detection signal, which limited the performance of this QKD system. If we will improve the jitter characteristic of the up-conversion detectors, we should be able to generate secure keys over the distance considerably longer than 100 km using the 10-GHz clock DPS-QKD system.

Acknowledgments

The authors thank G. Kalogerakis for providing fiber spools and electronic components. H. Takesue thanks T. Honjo and Y. Tokura for helpful discussions and support during his stay at Stanford University. This work was supported by SORST program of Japan Science and Technology Agency (JST), National Institute of Information and Communications Technology (NICT) of Japan, and MURI Center for Photonic Quantum Information Systems (ARO/ARDA DAAD19-03-1-0199).

#73420 - $15.00 USD Received 26 July 2006; revised 12 September 2006; accepted 13 September 2006