New Journal of Physics
The open-access journal for physics

Differential phase shift quantum key distribution experiment over 105 km fibre

H Takesue[1,3], E Diamanti[2,3], T Honjo[1], C Langrock[2], M M Fejer[2], K Inoue[1] and Y Yamamoto[1,2]

[1] NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato
Wakamiya, Atsugi, Kanagawa, Japan
[2] E.L. Ginzton Laboratory, Stanford University, 450 Via Palou, Stanford,
CA 94305-4088, USA
E-mail: htakesue@will.brl.ntt.co.jp

New Journal of Physics **7** (2005) 232
Received 12 August 2005
Published 18 November 2005
Online at http://www.njp.org/
doi:10.1088/1367-2630/7/1/232

Abstract. We report a quantum key distribution experiment based on the differential phase shift keying (DPSK) protocol with a Poissonian photon source, in which secure keys were generated over >100 km fibre for the first time. We analysed the security of the DPSK protocol and showed that it is robust against strong attacks by Eve, including a photon number splitting attack. To implement this protocol, we developed a new detector for the 1.5 μm band based on frequency up-conversion in a periodically poled lithium niobate waveguide followed by an Si avalanche photodiode. The use of detectors increased the sifted key generation rate up to >1 Mbit s^{-1} over 30 km fibre, which is two orders of magnitude larger than the previous record.

Contents

[3] These authors contributed equally to this work.

1. Introduction

The publication of several theoretical papers in 2000 [1, 2] has made the quantum key distribution (QKD) community well aware that a photon number splitting (PNS) attack by Eve severely limits the secure key distribution distance in BB84 [3] QKD systems with Poissonian photon sources. Although there have already been many fibre-based BB84 QKD experiments that have used Poissonian photon sources [4]–[11], only a few have been able to produce keys that are secure against Eve's PNS attack. The secure key generation rate of such systems scales with the square of the system transmittance, which means that long-distance secure key distribution is very difficult when using the BB84 protocol with Poissonian sources. Recently, Gobby *et al* reported a secure BB84 QKD experiment over 50 km that used InGaAs avalanche photodiodes (APDs) with a very small dark count rate [11], but with an extremely small secure key generation rate of about 0.1 bit s^{-1}. Recent studies have shown that the secure key distribution distance of the BB84 protocol with Poissonian sources can be significantly extended by implementing decoy states [12]–[16]. Although this scheme seems promising, experimental realization is still at an early stage with a reported distance of 15 km [16]. The use of a single photon source can significantly increase the secure key generation rate and distribution distance [17, 18]; however, such a light source is not yet available for the 1.5 μm band. Entanglement-based QKD [19]–[23] systems are more robust against a PNS attack than BB84, but the maximum key distribution distance has not exceeded 30 km so far [23], mainly due to the difficulty involved in the generation and coincidence detection of an entangled photon pair in the 1.5 μm band. The use of quantum repeaters based on nested entanglement purification and swapping [24] constitutes another candidate for long-distance quantum communication. However, to realize such a system, we need to overcome a number of technological challenges. These challenges include capturing entangled photon pairs in quantum memories either by the cavity QED technique [25] or the electromagnetically induced transparency technique [26, 27], and by storing qubits of information in quantum memories with a long coherence time of typically 1–10 s.

In this paper, we report a very simple QKD system, in which secure keys were generated over >100 km fibre for the first time. We used an alternative protocol of differential phase shift keying (DPSK) [28] but with a Poissonian source. We analysed the security of the DPSK protocol and showed that it is robust against hybrid attacks including a collective PNS attack over consecutive pulses, an intercept-and-resend (I-R) attack and a beamsplitting (BS) attack, because of the non-deterministic collapse of a wavefunction in a quantum measurement. To implement this protocol, we developed a new detector for the 1.5 mm band based on frequency up-conversion in a periodically poled lithium niobate (PPLN) waveguide followed by a Si APD [29]. The use of the detectors increased the sifted key generation rate up to >1 Mbit s^{-1} over 30 km fibre, which is two orders of magnitude larger than the previous record [9].

2. DPSK-QKD

The DPSK protocol provides an effective solution for overcoming a PNS attack with a simple system architecture and currently available technologies. Figure 1 shows a diagram of a QKD system based on the DPSK protocol. Alice randomly modulates the phase of a weak coherent pulse train by $\{0, \pi\}$ for each pulse, and sends it to Bob with an average photon number of less than 1 per pulse. Bob measures the phase difference of each consecutive pulse with a 1-bit delay

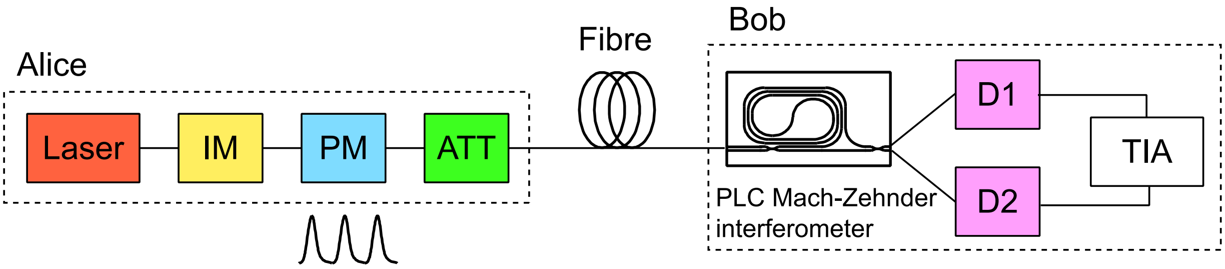

Figure 1. Schematic diagram of DPSK-QKD. IM, intensity modulator; PM, phase modulator; ATT, optical attenuator.

interferometer followed by two detectors placed at the interferometer output ports. Detector 1 (D1) clicks when the phase difference is 0 and D2 clicks when the phase difference is π. Because the average photon number per pulse is less than 1, Bob observes clicks only occasionally and at a random time instance. Bob informs Alice of the time instances at which he observes clicks. From her modulation data, Alice knows which detector clicked in Bob's site. By designating D1 and D2 clicks as 0 and 1, respectively, they can share an identical bit string.

We now describe the security of the DPSK protocol. In BB84 QKD systems with Poissonian photon sources, Eve can obtain qubit information by undertaking a quantum nondemolition (QND) measurement of the photon number on each pulse and extracting one photon from a pulse containing multiphotons (PNS attack). She can also launch an I-R attack on some of the single-photon pulses and block the remaining single photon pulses. As the fibre loss increases, she can suppress more single-photon pulses. In order to overcome this hybrid attack by Eve, the average photon number per pulse must be reduced along with the fibre loss. As a result, the secure key generation rate scales with the square of the system transmittance. In contrast, in the case of the DPSK protocol, a PNS attack on each pulse is obviously useless because information is encoded in the phase correlation between two consecutive pulses. An effective attack against the DPSK protocol is a PNS attack on two consecutive pulses, in which Eve undertakes a QND measurement of the total photon number in two consecutive pulses and extracts one photon when she observed two or more photons in two particular pulses. However, such an attack breaks the phase coherence between adjacent pulses and must induce bit errors with a probability of $1/4$. Thus, a PNS attack on two consecutive pulses cannot be launched on the DPSK protocol without inducing bit errors, and so the number of bits that can be obtained by this attack is always limited by the system's error rate. Eve can reduce the error probability by increasing the number of pulses for the PNS attack, but the probability that Eve obtains the same information as Bob decreases. Therefore, this collective PNS attack is not effective against the DPSK protocol, even though a PNS attack against the BB84 protocol with a Poissonian source is very powerful.

Instead, Eve can obtain coherent copies of the quantum states of pulses by inserting a beam splitter in the transmission line. This coherent BS attack does not introduce any errors and cannot be distinguished from innocent fibre loss. Along with the BS attack, Eve can also undertake an I-R attack as long as the bit errors induced by the I-R attack are kept smaller than the innocent bit errors of the system. In the following, we discuss the security of the DPSK protocol against Eve's hybrid BS and I-R attack. Although we do not know whether this hybrid attack is the optimum attack against the DPSK protocol, this attack is more effective than the collective PNS attack on consecutive pulses that we mentioned above.

Eve replaces a lossy fibre with transmittance α and imperfect detectors with a quantum efficiency η with her lossless fibre and perfect detectors[4], and splits Alice's transmitter output into two paths with a BS. One beam with an average photon number of $\mu N\alpha\eta$ is sent to Bob through her lossless fibre so that Bob does not notice her eavesdropping from a change in the count rate. Here, μ is the average photon number per pulse and N is the number of pulses in the coherence time of a source. The other beam with an average photon number of $\mu N(1-\alpha\eta)$ is stored in her quantum memory. After Bob announces the time instances at which he obtained clicks, Eve puts her photons into her interferometer. However, each photon in her N-slot wavefunction is detected completely randomly at one of N different time instances. The probability that she obtains the phase modulation data at a desired time instance is $2\mu(1-\alpha\eta)$. An increase in the probability by a factor of two stems from the fact that she can use an interferometer equipped with an optical switch at the input side instead of a 50 : 50 BS: she turns it on only at the time instances at which she wants interferometry. Thus, for the total sifted keys of n_{sif} bits, Eve has full information on $2\mu n_{sif}(1-\alpha\eta)$ bits. Note that the mutual information between Eve and Bob is independent of the system transmittance (including detector quantum efficiency) $\alpha\eta$ if $\alpha\eta \ll 1$. Therefore, the mutual information between Eve and Bob can be made small simply by choosing a small μ that is independent of $\alpha\eta$ if $\alpha\eta \ll 11$. Eve can also launch an I-R attack by taking advantage of the system's innocent bit errors. Eve further splits some photons from the transmitted $\mu N\alpha\eta$ photons, and measures the phase differences with her interferometer, which is identical to Bob's. She then sends a signal only at time instances at which she detects photons. For each intercepted photon, she resends a single photon, which is split into two time slots through an interferometer identical to Bob's, in which the relative phase between the two time slots is modulated by 0 or π according to the measurement results. When this fake photon arrives at Bob's site, he counts the photon possibly at three time instances. The ratio of the probabilities of detecting a photon at these time instances is 1 : 2 : 1, where the correct phase difference is obtained only for the second time instance. Consequently, a fake photon induces an error in the first and third time instances with a probability of 1/4. This means that Eve can attack $4en_{sif}$ photons, where e represents the innocent bit error rate of the system. With these intercepted photons, Eve can obtain full information on $2en_{sif}$ bits (when Bob observes a click for the resent photons at the second time instance), but no information on the remaining bits. To summarize the above argument, the collision probability between bits owned by Bob and Eve is expressed as follows [1]:

$$p_c = \left(\frac{1}{2}\right)^{n_{sif}\left[1-2\mu(1-\alpha\eta)-2e\right]}. \tag{1}$$

Using the above equation, the compression factor of the privacy amplification τ_1 is calculated using the following equation (1).

$$\tau_1 = 1 + \frac{1}{n_{sif}} \log_2 p_c. \tag{2}$$

[4] The assumption that Eve can replace Bob's imperfect detectors with perfect ones may seem unrealistic. However, as pointed out in [2], there are certain ways in which Eve can improve the characteristics of Bob's detectors. For example, Eve can change the wavelength of the photons to a region of higher detection efficiency. A similar argument can be applied to the dark count rate. In order to account for this, our security analysis is based on the very conservative assumption that Eve has control of the quantum efficiency and dark count rate of Bob's detectors.

Then, the secure key generation rate R_s after error correction and privacy amplification is calculated to be [1]

$$\begin{aligned} R_s &= R_{ng}\{1 - \tau_1 + f(e)[e\log_2 e + (1-e)\log_2(1-e)]\} \\ &= R_{ng}\{1 - 2\mu(1-\alpha\eta) - 2e + f(e)[e\log_2 e + (1-e)\log_2(1-e)]\}, \end{aligned} \tag{3}$$

where $f(e)$ characterizes the performance of the error correction algorithm. R_{ng} is the sifted key generation rate per second given by

$$R_{ng} = \mu\alpha\eta f_c \exp(-\mu\alpha\eta f_c t_d/2). \tag{4}$$

Here, f_c and t_d represent the clock frequency and the detector dead time. The factor 1/2 in the exponent arises from the fact that the average number of photons per second that reach each detector is $\mu\alpha f_c/2$. In the following theoretical calculations, we assumed a bi-directional error-correction protocol. When we assume that the bit error rate $e = 0$ and the transmittance α is small, equation (3) is reduced to

$$R_s \approx \mu\alpha\eta f_c(1 - 2\mu). \tag{5}$$

Equation (5) shows that the secure key generation rate scales linearly with the system transmittance α. This characteristic is identical to those of the single-photon-based BB84 protocol [17, 18], the coherent-state-based B92 protocol with a strong reference pulse [30], the BB84 protocol with decoy state [13] and a recently proposed protocol similar to DPSK [31].

Recently, Lo and Preskill reported that the security of a BB84 system with a weak coherent source without phase randomization is seriously compromised if Eve obtains phase reference information of the source [32]. Although a more thorough analysis is obviously needed, we believe that such an attack is possibly inefficient against the DPSK protocol for the following two reasons.

1. With plug-and-play systems [5, 6, 8], the phase reference can be easily obtained by measuring the phase of a strong pulse. However, the retrieval of the phase reference for homodyne detection is hard for the DPSK protocol, which employs a weak binary PSK signal, because of the intrinsic quantum noise of a local oscillator.
2. Even if such a reference local oscillator wave is reconstructed, adaptive homodyne detection has a lower bound of bit error rate due to the intrinsic overlap of two coherent states with an average photon number of 0.2 or less.

The security model presented in this section is based on specific attacks such as PNS, I-R and BS attacks, and there may be an attack that is more effective than these. Therefore, it is important to undertake a more general security analysis of the DPSK protocol that is not based on specific attacks, and this is currently under way.

3. Up-conversion detector

Next, we explain the up-conversion detector, which is shown schematically in figure 2(a) [29]. A 1560 nm photon is combined with a strong pump light whose wavelength is 1319 nm, and injected into a PPLN waveguide. In the waveguide, a 715 nm photon is generated via the sum

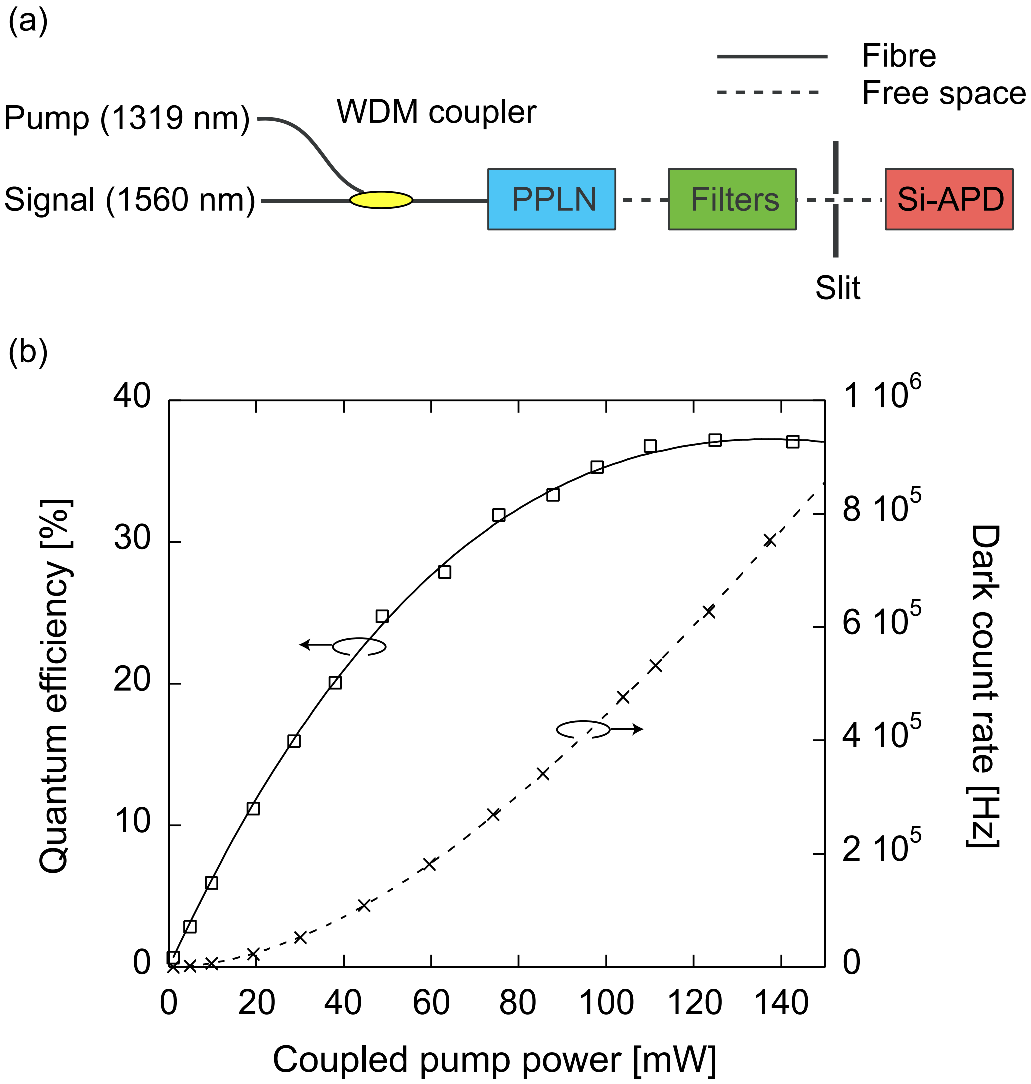

Figure 2. (a) Schematic diagram of the up-conversion detector. (b) Quantum efficiency and dark count rate as functions of pump power.

frequency generation (SFG) process. The internal conversion efficiency from a 1560 nm photon to a 715 nm photon exceeds 99%. The overall conversion efficiency, including input coupling loss, waveguide loss and output coupling loss, is estimated to be approximately 65%. The following filters suppress the noise photons such as the residual pump and second harmonic generation (SHG) of the pump light.[5] The SFG photon is detected with a single photon counting module (SPCM) based on a Si APD (PerkinElmer SPCM-AQR-14), which has a high quantum efficiency (about 70%) and a low dark count rate (about 50 Hz). The overall quantum efficiency, including reflection and coupling losses, and the dark count of the up-conversion detector used in our QKD experiments are plotted in figure 2(b) as a function of pump power. While the peak quantum

[5] More specifically, a dichroic mirror was used to suppress the residual pump and signal light, and a long-pass filter as well as a prism was used to suppress the SHG of the pump light. For more details on the configuration of up-conversion detectors, see [29].

efficiency was as high as about 37% with a coupled pump power of around 120 mW, the dark counts increased quadratically as we increased the pump power, which was mainly due to noise photons generated by the spontaneous Raman scattering process inside the waveguide and the input fibre pigtail.

The up-conversion detector for a QKD system can be operated in a non-gated mode, thanks to the low afterpulse probability of the SPCM. When we use non-gated mode detectors with a dead time t_d, the sifted key generation rate R_{ng} of a DPSK-QKD system with equal probabilities of '0' and 'π' modulation can be calculated as equation (4). With a small dead time and a large loss, as in our experiment, the exponential part of equation (4) is close to unity. Therefore, R_{ng} increases with clock frequency f_c, which is as large as 1 GHz in our experiment. This non-gated mode operation of the up-conversion detector resulted in a significant increase in the key rate in our experiment, as reported below.

4. Experiment

We now describe experiments that we undertook using the set-up shown in figure 1. At Alice's site, a continuous light from an external cavity semiconductor laser was modulated into a pulse train with a 1 GHz clock frequency using a $\mathrm{LiNbO_3}$ intensity modulator. The pulse width was 100 ps. The phase of each pulse was then modulated by $\{0, \pi\}$ with a $\mathrm{LiNbO_3}$ phase modulator. We used a 1 Gbit s^{-1} pseudo-random bit sequence with a length of $2^7 - 1$ generated by a data generator (Tektronix DG2040) as the phase modulation signal. After appropriate attenuation, the pulse train was sent to Bob's site through a fibre, where a 1-bit delay interferometer based on planar lightwave circuit (PLC) technology [33] was installed. The insertion loss of the interferometer was 2.5 dB, and the extinction ratio was >20 dB. The up-conversion detectors were connected to the two output ports of the interferometer. The dead time of the SPCMs was 50 ns. Each click at the photon counters was recorded using a time interval analyser (TIA) (Ortec 9308). To avoid bit errors due to large dark counts introduced by the up-converter, we kept the pump power at a relatively low level. The average photon number per pulse μ was set at its optimum value for each transmittance α, which was calculated using equation (3), to maximize the secure key generation rate. The optimum μ was around 0.16–0.18, depending on α, η and the dark count rate. We measured the sifted key generation rate and bit error rate five times for each transmittance, and took the average value. The sifted keys were actually generated between Alice and Bob, and the error rate was measured by directly comparing the yielded sifted keys of Alice and Bob, not by estimating them with the histogram data described below. We calculated the secure key generation rates of the experiments with equation (3) using the sifted key generation rates and bit error rates obtained in the experiments, i.e., error correction and privacy amplification were not actually implemented. Fibre transmission experiments were undertaken using fibre spools, with Alice and Bob located in the same room.

Figures 3(a) and (b) show histograms of detected photons counted by D1 and D2, respectively for a fixed modulation pattern after a 20 km fibre transmission. These data were taken with only one detector connected to TIA. μ and η of both detectors were set at 0.1 and 8.8%. The tailing distribution observed in this figure was mostly due to detector timing jitter. To reduce the contribution of erroneous clicks caused by this broadening of the received signal, we applied time gating to the recorded data, which also reduces the effective dark counts per time gate. Figure 4 shows the secure key generation rate as a function of fibre length, where the

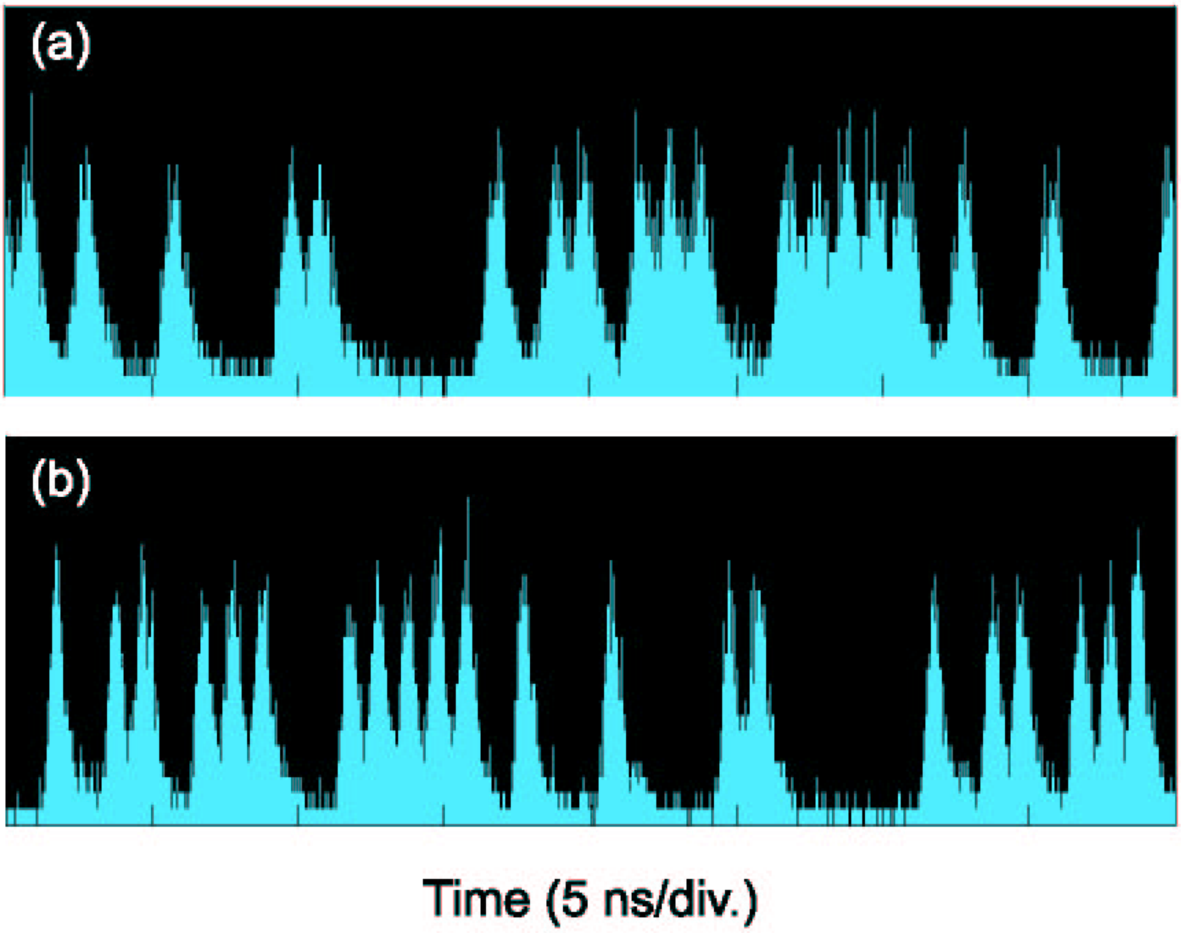

Figure 3. Histograms of the received signal at (a) D1 and (b) D2 for a fixed modulation pattern.

squares represent the secure key generation rate of the fibre transmission and × symbols show the experimental results simulating a fibre loss with an optical attenuator when we set the overall detector quantum efficiency and the time window at 8.8% (at pump powers of approximately 15 mW) and 0.6 ns, respectively. Note that the use of a 0.6 ns time window reduced the effective detection efficiency by 33%. Under these operating conditions, the total dark count rate of the two detectors was 26 kHz. We used dispersion-shifted fibre for the fibre spools in order to avoid chromatic dispersion-induced pulse broadening. As a result, the pulse broadening caused by chromatic dispersion was negligible compared with that caused by the timing jitter of the detectors. The green line shows a theoretical prediction of the secure key generation rate at those quantum efficiency and dark count values, where μ is optimized to maximize the secure key generation rate at each fibre loss. This theoretical curve fits very well with the experimental results. The sifted key generation rates at corresponding fibre lengths are indicated by diamonds in figure 4. At fibre lengths of 30 km or less, we achieved a sifted key generation rate of more than 1 Mbit s^{-1}, which is two orders of magnitude larger than the previous record [9]. The secure key generation rate was 0.455 Mbit s^{-1} over 20 km of optical fibre. Thus, even with the moderate 8.8% quantum efficiencies, the key rate increased significantly, thanks to the non-gated mode operation

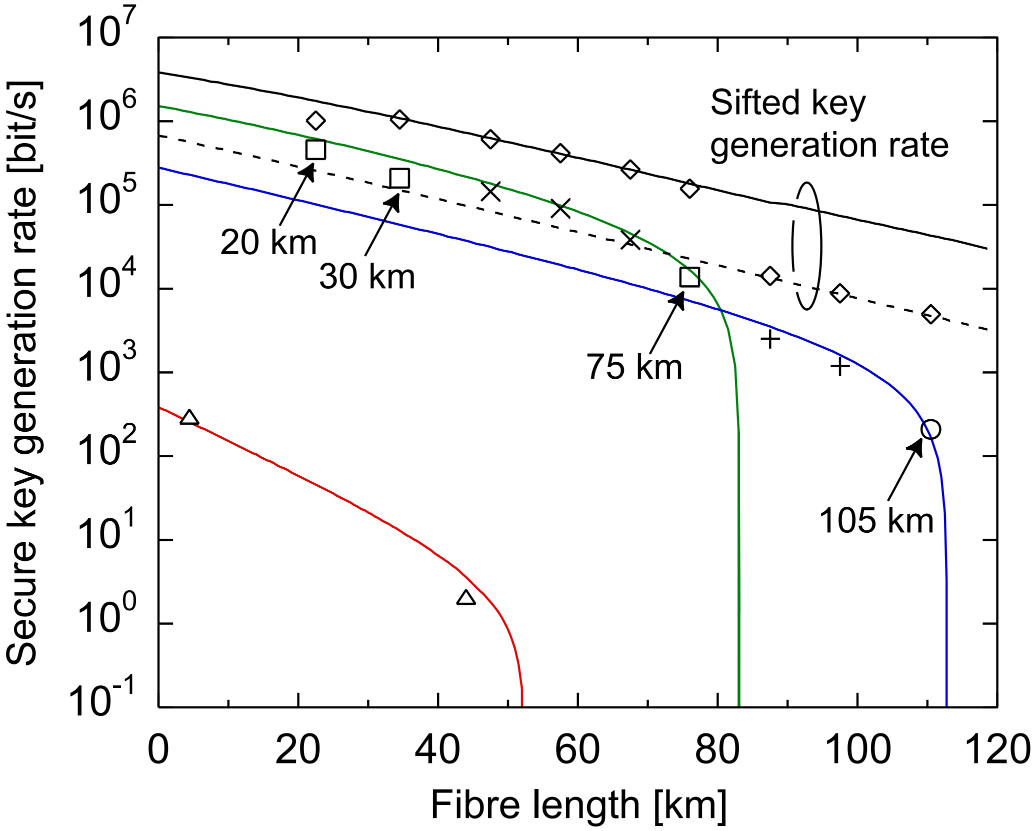

Figure 4. Secure key generation rate as a function of length of fibre with 0.2 dB km^{-1} loss. □, fibre transmission (experiment, $\eta = 8.8\%$); ×, simulated points with attenuator (experiment, $\eta = 8.8\%$); ○), fibre transmission (experiment, $\eta = 2.0\%$); +, simulated points with attenuator (experiment, $\eta = 2.0\%$); △, fibre transmission with BB84 and InGaAs APD (experiment described in [11]). Green line, DPSK and up-conversion detector operated at $\eta = 8.8\%$ (theory). Blue line, DPSK and up-conversion detector operated at $\eta = 2.0\%$ (theory). Red line, BB84 and InGaAs APD (theory). A system error of 3% is assumed. The characteristic of the InGaAs APD is based on [11]. The diamonds show the experimental data for sifted key generation rates at corresponding fibre lengths. The solid and dotted black lines show the theoretically predicted sifted key generation rates for $\eta = 8.8$ and 2%, respectively.

of our up-conversion detectors. We then set the pump powers, quantum efficiency, dark count and time window width at approximately 3 mW, 2.0%, 2.7 kHz and 0.2 ns, respectively, to further reduce the errors caused by the dark counts. Here, the use of the 0.2 ns time window reduced the effective detection efficiency by 55%. The experimental results are shown by a circle (105 km fibre transmission) and + symbols (attenuator), while the blue line is the theoretical calculation. By using the above detection set-up, the secure key yielded a rate of 209 bit s^{-1}. The bit error rate at 105 km was 7.95%. The sources of the errors were estimated as follows: 1% is accounted for by the 20 dB extinction ratio of the PLC interferometer, 5.5% is from the detector dark counts and the rest is due to timing jitter. The triangles and red line show the experimental and theoretical secure key generation rates when we assumed a BB84 protocol with a Poissonian photon source and recently developed InGaAs photon counters [11]. It is clear that our result significantly outperforms a QKD system based on the BB84 protocol, as regards both secure key generation rate and distance. We also calculated the secure key distribution distance of a BB84 QKD system with a Poissonian source combined with our up-conversion detectors operated under the same conditions as in our 105 km transmission experiment (i.e. 2.0% quantum efficiency, 1.35 kHz dark count rate per detector and 0.2 ns time window), using the theory described in [2]. As a result, the secure key distribution distance is at most 64 km over fibre with a 0.2 dB km^{-1} loss even when we can eliminate all the optical loss except that of the fibre. This clearly shows that the use of the DPSK protocol was essential in terms of increasing the secure key distribution distance to 105 km.

In our experiment, the secure key distribution distance was limited by two impairments of the up-conversion detectors: a large dark count rate resulting from noise photons generated in the waveguide, and the large timing jitter of the SPCM.[6] If we can eliminate the noise photons and achieve a negligible timing jitter compared with pulse width, the secure key distribution distance will reach 300 km. For example, noise photons due to spontaneous Raman scattering are expected to be suppressed by setting the pump wavelength longer than the signal wavelength. Therefore, the development of entanglement-based quantum repeater systems will be meaningful only when the system length can exceed 300 km.

5. Conclusion

We described a DPSK-QKD experiment, in which secure keys were generated over >100 km fibre for the first time. We analysed the security of the DPSK protocol and showed that it is robust against hybrid attacks including a collective PNS attack over consecutive pulses, an I-R attack and BS attack. In addition, the use of the detectors based on frequency up-conversion in PPLN waveguides increased the sifted key generation rate up to >1 Mbit s^{-1} over 30 km fibre, which is two orders of magnitude larger than the previous record.

Acknowledgments

The authors thank N Lutkenhaus, M Koashi and E Waks for discussions of security issues. They also thank M Morita and Y Tokura for encouragement throughout this research. This work was supported in part by the National Institute of Information and Communications Technology (NICT) of Japan. Financial support provided by the MURI Center for Photonic Quantum Information Systems (ARO/ARDA DAAD19-03-1-0199) is also acknowledged.

[6] For a fibre length of 20 km, we used $\mu = 0.1$ instead of using the optimum value of $\mu = 0.17$. This is because the timing jitter of the SPCM used in the experiment surged when the count rate increased, and thus we could not enlarge μ at this relatively low loss point. As a result, the maximum sifted key generation rate did not greatly exceed 1 Mbit s^{-1}. The large timing jitter also led to a larger bit error rate, which resulted in a reduction of the secure key distribution distance.

References

[1] Lutkenhaus N 2000 Security against individual attacks for realistic quantum key distribution *Phys. Rev.* A **61** 052304

[2] Brassard G, Lutkenhaus N, Mor T and Sanders B C 2000 Limitations on practical quantum cryptography *Phys. Rev. Lett.* **85** 1330

[3] Bennett C H and Brassard G 1984 *Proc. Int. Conf. of Computer Systems and Signal Processing (Bangalore, 1984)* vol 85 (New York: IEEE) p 175

[4] Townsend P D, Rarity J G and Tapster P R 1993 Single photon interference in 10 km long optical fibre interferometer *Electron. Lett.* **29** 634

[5] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H and Gisin N 1997 'Plug and play' systems for quantum cryptography *Appl. Phys. Lett.* **70** 793

[6] Bourennane M, Gibson F, Karlsson A, Hening A, Jonsson P, Tsegaye T, Ljunggren D and Sundberg E 1999 Experiments on long wavelength (1550 nm) 'plug and play' quantum cryptography systems *Opt. Exp.* **4** 383

[7] Hughes R J, Morgan G L and Peterson C G 2000 Quantum key distribution over a 48 km optical fibre network *J. Mod. Opt.* **47** 533

[8] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 Quantum key distribution over 67 km with a plug&play system *New J. Phys.* **4** 41

[9] Yoshizawa A, Kaji R and Tsuchida H 2004 10.5 km fiber-optic quantum key distribution at 1550 nm with a key rate of 45 kHz *Japan. J. Appl. Phys.* **43** L735

[10] 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

[11] Gobby C, Yuan Z L and Shields A J 2005 Unconditionally secure quantum key distribution over 50 km of standard telecom fibre *Electron. Lett.* **40** 25

[12] Hwang W Y 2003 Quantum key distribution with high loss: toward global secure communication *Phys. Rev. Lett.* **91** 057901

[13] Lo H K, Ma X and Chen K 2005 Decoy state quantum key distribution *Phys. Rev. Lett.* **94** 230504

[14] Wang X B 2005 Beating the photon-number-splitting attack in practical quantum cryptography *Phys. Rev. Lett.* **94** 230503

[15] Ma X, Qi B, Zhao Y and Lo H K 2005 Practical decoy state for quantum key distribution *Preprint* quant-ph/0503005

[16] Zhao Y, Qi B, Ma X, Lo H K and Qian L 2005 Experimental quantum key distribution with decoy states *Preprint* quant-ph/0503192

[17] Waks E, Inoue K, Santori C, Fattal D, Vuckovic J, Solomon G and Yamamoto Y 2002 Quantum cryptography with a photon turnstile *Nature* **420** 762

[18] Beveratos A, Brouri R, Gacoin T, Villing A, Poizat J P and Grangier P 2002 Single photon quantum cryptography *Phys. Rev. Lett.* **89** 187901

[19] Jennewein T, Simon C, Weihs G, Weinfurter H and Zeilinger A 2000 Quantum cryptography with entangled photons *Phys. Rev. Lett.* **84** 4729

[20] 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

[21] Ribordy G, Brendel J, Gautier J D, Gisin N and Zbinden H 2001 Long-distance entanglement-based quantum key distribution *Phys. Rev.* A **63** 012309

[22] Aspelmeyer M *et al* 2003 Long-distance free-space distribution of quantum entanglement *Science* **301** 621

[23] Fasel S, Gisin N, Ribordy G and Zbinden H 2004 Quantum key distribution over 30 km standard fiber using energy-time entangled photon pairs *Eur. Phys. J.* D **30** 143

[24] Briegel H J, Dur W, Cirac J I and Zoller P 1998 Quantum repeaters: the role of imperfect local operation in quantum communication *Phys. Rev. Lett.* **81** 5932

[25] Cirac J I, Zoller P, Kimble H J and Mabuchi H 1997 Quantum state transfer and entanglement distribution among distant nodes in a quantum network *Phys. Rev. Lett.* **78** 3221

[26] Lukin M D, Fleischhauer M, Zibrov A S, Robinson H G, Velichansky V L, Hollberg L and Scully M O 1997 Spectroscopy in dense coherent media: line narrowing and interference effects *Phys. Rev. Lett.* **79** 2959

[27] Hau L V, Harris S E, Dutton Z and Behroozi C H 1999 Light speed reduction to 17 metres per second in an ultracold atomic gas *Nature* **397** 594

[28] Inoue K, Waks E and Yamamoto Y 2002 Differential-phase-shift quantum key distribution *Phys. Rev. Lett.* **89** 037902

[29] 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$_3$ waveguides *Opt. Lett.* **30** 1725

[30] Koashi M 2004 Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse *Phys. Rev. Lett.* **93** 120501

[31] Gisin N, Ribordy G, Zbinden H, Stucki D, Brunner N and Scarani V 2004 Towards practical and fast quantum cryptography *Preprint* quant-ph/0411022

[32] Lo H-K and Preskill J 2005 Phase randomization improves the security of quantum key distribution *Preprint* quant-ph/0504209

[33] Himeno A, Kato K and Miya T 1998 Silica-based planar lightwave circuits *IEEE J. Sel. Top. Quantum Electron.* **4** 913