Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors

HIROKI TAKESUE[1]*, SAE WOO NAM[2], QIANG ZHANG[3], ROBERT H. HADFIELD[2†], TOSHIMORI HONJO[1], KIYOSHI TAMAKI[1] AND YOSHIHISA YAMAMOTO[3,4]

[1]NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 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]National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan
[†]Present address: Department of Physics, Heriot-Watt University, Edinburgh, EH14 4AS, United Kingdom
*e-mail: htakesue@will.brl.ntt.co.jp

Published online: 1 June 2007; doi:10.1038/nphoton.2007.75

We report the first quantum key distribution (QKD) experiment to enable the creation of secure keys over 42 dB channel loss and 200 km of optical fibre. We used the differential phase shift QKD (DPS-QKD) protocol, implemented with a 10-GHz clock frequency and superconducting single-photon detectors (SSPD) based on NbN nanowires. The SSPD offers a very low dark count rate (a few Hz) and small timing jitter (60 ps, full width at half maximum, FWHM). These characteristics allowed us to achieve a 12.1 bit s^{-1} secure key rate over 200 km of fibre, which is the longest terrestrial QKD over a fibre link yet demonstrated. Moreover, this is the first 10-GHz clock QKD system to enable secure key generation. The keys generated in our experiment are secure against both general collective attacks on individual photons and a specific collective attack on multiphotons, known as a sequential unambiguous state discrimination (USD) attack.

Quantum key distribution, or quantum cryptography, offers an ultimately secure means of distributing secret keys between two separate parties based on the laws of quantum mechanics[1]. We can realize unconditionally secure communication based on a one-time pad cryptosystem[2] using QKD. Since the first QKD experiment using a 32-cm free-space transmission line was reported in 1992 (ref. 3), the key distribution distance in QKD experiments has continued to increase. Most of those earlier experiments used the Bennett and Brassard 1984 (BB84) protocol[4] with attenuated laser light as the photon source, but did not generate secure keys because of their vulnerability to a photon number splitting (PNS) attack[5,6]. In a PNS attack, an eavesdropper (Eve) performs a quantum non-demolition (QND) measurement on each weak coherent pulse. If Eve finds more than one photon in one pulse, she keeps one photon in her quantum memory and sends the others to Bob through her lossless transmission line. After knowing the measurement basis from the public communication between Alice and Bob, Eve can perform a projective measurement for a stored photon, and thus obtain full information about the pulse without causing any bit errors. This attack seriously limits the performance of BB84-QKD systems implemented with coherent light sources. The most obvious but technologically difficult way to prevent a PNS attack is to use a deterministic single-photon source. Motivated by this reasoning, intensive research on single-photon sources is being undertaken worldwide[7–9]. In fact, several BB84-QKD experiments with deterministic single-photon sources have been carried out[10,11], but the improvement in the secure key rate has been limited due to the residual two-photon probability $P(2) \leq (1/2)\, g^{(2)}(0)$ of the single-photon source[12], where $g^{(2)}(0)$ denotes the second-order autocorrelation function of the source. An alternative approach is to find new protocols that are robust against a PNS attack[13–21]. With the decoy-state BB84 protocol[13–16], decoy pulses are randomly inserted that have an average photon number different from that of the signal pulses. Recently, a PNS-secure key distribution over a 107-km optical fibre with a bit rate of about 0.1 bit s^{-1} has been reported using superconducting transition edge sensors[22]. Several other PNS-tolerant protocols have also been studied, including the Bnnett 1992 protocol with a strong reference pulse[17,18], the Scarani–Acín–Ribordy–Gisin protocol[19] and the coherent one-way protocol[20].

We have been developing a QKD system based on the DPS-QKD protocol[21], which is another PNS-tolerant protocol[23]. We have already reported 100-km key distribution, which we achieved by implementing this protocol with a 1-GHz clock system and a high-speed, single-photon detector based on the frequency up-conversion technique[24,25]. Here we report a QKD experiment over 200 km of optical fibre with a 42.1-dB channel loss. In addition, we achieved a secure key rate of 17 kbit s^{-1} at 105 km, which is two orders of magnitude larger than the previous record[25]. These results were achieved as a result of two major technological advances: the use of SSPD (refs 26 and 27) and the implementation of a 10-GHz clock system. The very low dark count rate (a few Hz) and small timing jitter

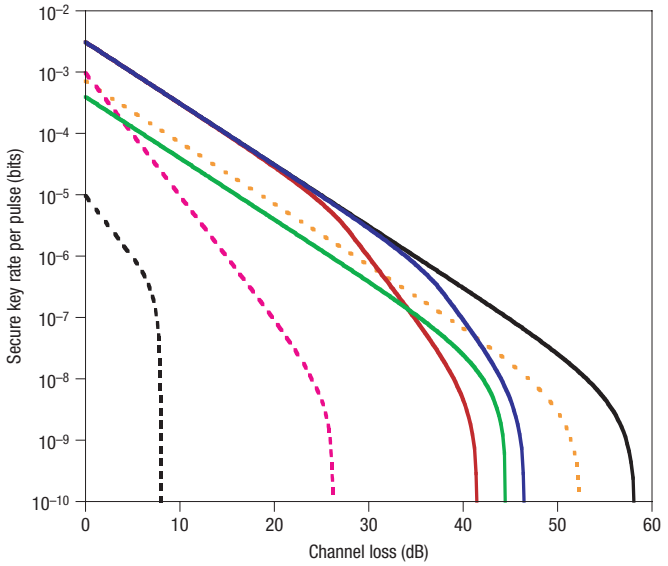

Figure 1 Secure key rate as a function of channel loss. Black solid line: BB84 with an ideal single-photon source; blue line: BB84 with a single-photon source with $g^{(2)}(0) = 10^{-6}$; red line: BB84 with a single-photon source with $g^{(2)}(0) = 10^{-5}$; yellow dotted line: decoy state protocol (vacuum + weak decoy state); green line: DPS-QKD; pink dashed line: BB84 with a single-photon source with $g^{(2)}(0) = 10^{-2}$; black dashed line: BB84 with an attenuated laser source.

(60-ps FWHM) of the SSPD, combined with the high repetition rate, narrow temporal-width coherent pulse train of the 10-GHz clock system, resulted in both a record transmission distance and secure bit rate in this experiment. With our experimental result, we can distil secret keys that are secure against both general collective attacks on individual photons[23] (including a PNS attack) and a sequential USD attack[28]. Note that the present paper reports the longest terrestrial QKD over an optical-fibre link yet demonstrated, which almost doubles the previous record, namely a PNS-secure key distribution distance of 107 km (ref. 22), and the first 10-GHz clock QKD experiment to enable secure key generation.

RESULTS

DPS-QKD PROTOCOL

With the DPS protocol[21], the information-carrying quantum state is defined over many pulses from a coherent laser source. The sender, conventionally called Alice in the field of cryptography, randomly modulates the phase of each pulse emitted from the source by $\{0,\pi\}$. The intensity of the pulse train is adjusted so that the average photon number per pulse becomes much less than one. Bob, the receiver, is equipped with a 1-bit delayed Mach–Zehnder interferometer, whose two output ports are followed by two single-photon detectors. When the phase difference between two adjacent pulses is 0 (π), detector 0 (1) clicks. Because the average photon number per pulse is much less than one, Bob's detectors click only occasionally. Bob discloses the time instances in which he observed the clicks to Alice via public communication, while withholding 'which-detector' information. With the time-instance information and original modulation data, Alice knows which detector clicked in those time instances at Bob's site. Therefore, Alice and Bob can share an identical bit string that can be used as a key for one-time pad cryptography.

Because a QND measurement on two consecutive pulses breaks the coherence of the multiple-pulse quantum state, a standard PNS attack based on a QND measurement introduces bit errors. Eve can reduce the error probability by increasing the number of pulses simultaneously monitored by a QND measurement, but the probability of Eve obtaining the key information also decreases, because the detector click, that is, a collapse of the wavefunction, occurs randomly and non-deterministically for Bob's and Eve's wavepackets. Even if Eve has the technology to undertake such a PNS attack on an arbitrary number of time slots, the fraction of information that Eve can obtain using a PNS attack is given by 2μ, where μ denotes the average photon number per pulse[23]. In the presence of system errors, Eve can also launch an optimal quantum measurement attack on a fraction of the photons transmitted to Bob, where the collision probability p_{c0} for each bit is bounded as

$$P_{c0} \leq 1 - e^2 - \frac{(1-6e)^2}{2} \tag{1}$$

and e denotes the system's innocent bit error rate. Then, considering a twofold attack composed of a PNS attack and an optimal quantum measurement attack, an upper bound for the collision probability of the n-bit sifted key, which we shall denote as p_c, is given by[23]

$$p_c = p_{c0}^{n(1-2\mu)} = \left(1 - e^2 - \frac{(1-6e)^2}{2}\right)^{n(1-2\mu)} . \tag{2}$$

Thus, the compression factor τ in the privacy amplification process is calculated as[29]

$$\tau = -\frac{\log_2 p_c}{n} = -(1-2\mu)\log_2\left[1 - e^2 - \frac{(1-6e)^2}{2}\right]. \tag{3}$$

The secure key rate R_{secure} is reduced from the sifted key rate R_{sifted} according to[5]

$$R_{\text{secure}} = R_{\text{sifted}}\{\tau + f(e)h(e)\} \tag{4}$$

where $h(e) = -e\log_2 e - (1-e)\log_2(1-e)$ is a binary entropy function, and $f(e)$ characterizes the performance of the error correction algorithm.

Figure 1 plots the theoretical secure key rates per pulse versus channel loss for DPS-QKD using a standard coherent laser source, the decoy state protocol, and BB84 using single-photon sources with varying $g^{(2)}(0)$ (ref. 12). We calculated the secure key rate of a decoy state system based on ref. 16, assuming the use of vacuum plus the weak decoy method. Here, we assumed the same detector condition as in the 10-GHz clock experiment described below (a quantum efficiency of 1.4%, a combined dark count rate of 50 Hz, a time window width of 50 ps and a 36% reduction in effective quantum efficiency caused by the time window). For the BB84 and decoy state system, we assumed an ideal implementation, namely active demodulation with no additional loss, so Bob uses only two single-photon detectors. The maximum channel loss of the DPS-QKD system is larger than that of the BB84 system using a single photon source with $g^{(2)}(0) = 10^{-5}$ and an efficiency, which is far beyond the current experimental reach: the best $g^{(2)}(0)$ for an experimental deterministic single-photon source is limited to 0.01 (refs 7–9)

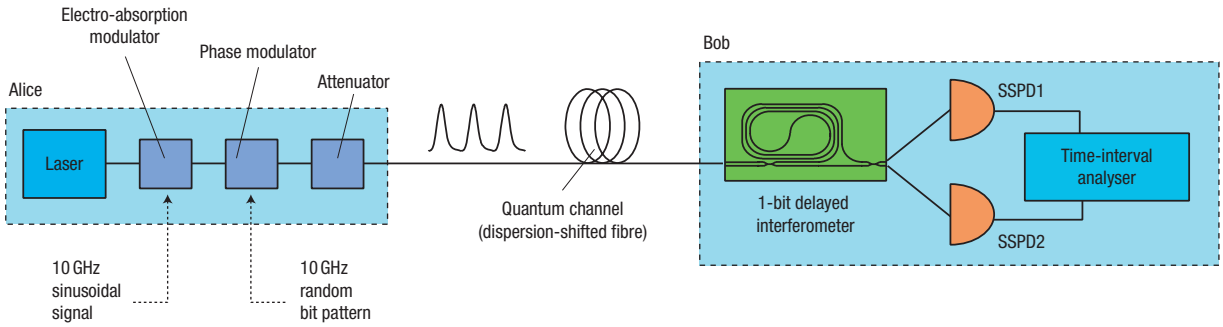

Figure 2 Experimental set-up for 10-GHz clock DPS-QKD

at present. The curve for the decay state protocol is similar to that of DPS-QKD but has a better secure key rate per pulse and maximum channel loss. Note that in an actual implementation, the key rate of a DPS-QKD system is usually larger than that of a decoy state system, because a DPS-QKD system uses the time domain more efficiently than a decoy state system. Heralded single-photon sources based on spontaneous parametric down-conversion have also been studied[30] and successfully implemented as photon sources for QKD systems[31,32]. With those sources, $g^{(2)}(0)$ improves as the average number of photon pairs generated through spontaneous parametric down-conversion decreases. Consequently, the maximum key distribution distance with this type of source can be similar to that with an ideal single-photon source, but the secure key generation rate decreases rapidly as the channel loss increases.

SYSTEM CONFIGURATION

Figure 2 shows the configuration of the 10-GHz clock DPS-QKD system. A continuous-wave output from a 1,557.40-nm wavelength laser is transformed into a 10-GHz clock pulse train by an InGaAsP electro-absorption modulator. We generated pulses with a FWHM of 15 ps. The phase of each pulse was modulated by a phase modulator driven by a 10-GHz pseudo-random bit pattern from a high-speed pulse pattern generator. The average photon number per pulse was adjusted to 0.2 by an optical attenuator. The quantum channel was a dispersion-shifted fibre or a single attenuator. Bob was equipped with a 1-bit delayed interferometer fabricated using planar lightwave circuit technology. The excess loss of the interferometer was 2.5 dB. Each output port of the interferometer was connected to an SSPD. The photon detection time instances and which-detector information were recorded using a time-interval analyser. In our experiment, sifted keys were actually generated between Alice and Bob, and the error rate was measured by directly comparing Alice's key with Bob's key. For each data point described below, we undertook five runs of QKD sessions, and the error rates and sifted key rates are the averages of the five runs. The secure key rates were calculated by putting the experimentally obtained error rates and sifted key rates in equation (4).

SSPD

Figure 3a shows a close-up image of an SSPD, which consists of a 100-nm-wide, 4-nm-thick NbN superconducting wire. The SSPD was coupled to a 9-μm core single-mode fibre as shown in Fig. 3b. The packaged detector was housed in a closed-cycle cryogen-free refrigerator with an operating temperature of 3 K for convenient use in quantum information experiments[33]. The detector operated in the following way. The superconducting wire was current-biased slightly below its critical current. When a photon hits the wire, a resistive hot spot is formed. Then the current distribution around the spot is perturbed and the current density exceeds the critical value. As a result, a non-superconducting barrier is formed across the entire width of the wire, and a voltage pulse is formed. By discriminating the leading edge of the voltage pulses, we can measure the photon arrival time with a high timing resolution. The quantum efficiency and dark count rate of the SSPD vary when the bias current is changed. The single-photon counting mechanism of an avalanche photodiode (APD) (consisting of absorption, diffusion and avalanche) results in excess dark counts and non-gaussian timing jitter characteristics. On the other hand, photon detectors based on superconducting devices show low dark counts because of the low-noise, cryogenic operation environment. Moreover, because the energy relaxation time constants of excited carriers in the chosen superconducting material (NbN) are very short[34] (tens of picoseconds), the SSPD has extremely good timing resolution. We measured the timing jitter of the SSPD by launching 10-ps pulses. Figure 3c compares the obtained histogram of the photon arrival time with that of a single-photon detector based on a frequency up-converter followed by a Si APD, which was used in our earlier DPS-QKD experiments[25]. Here, the blue squares and the line denote the histogram for the SSPD, and the red line is that for the up-conversion detector. Although the FWHM of the jitter was approximately 60 ps, which is larger than that of the up-conversion single-photon detectors, the histogram fits very well with the gaussian, and does not have a long tail, as observed in similar measurements for the up-conversion detectors[25]. Therefore, we can significantly reduce the error probability caused by intersymbol interference by using an SSPD. In addition, the measured dark count rate of the SSPD was <10 Hz (typically a few Hz) when the quantum efficiency was set at 0.7%, which is much smaller than that of the up-conversion detector operated with a similar quantum efficiency (350 Hz at 0.4% quantum efficiency[25]).

EXPERIMENT

We applied a narrow time window to the obtained time-instance data to further reduce the contributions of the dark counts and the intersymbol interference caused by neighbouring signals. To demonstrate the effectiveness of this technique, we obtained a histogram of the photon arrival time detected by one of two SSPDs. Here, the quantum efficiency and dark count rate of the SSPD were set at 0.7% and <10 Hz, respectively, and the channel loss was 31.7 dB. Figure 4a shows the histogram obtained when no time window was used. We observed a signal pulse overlap

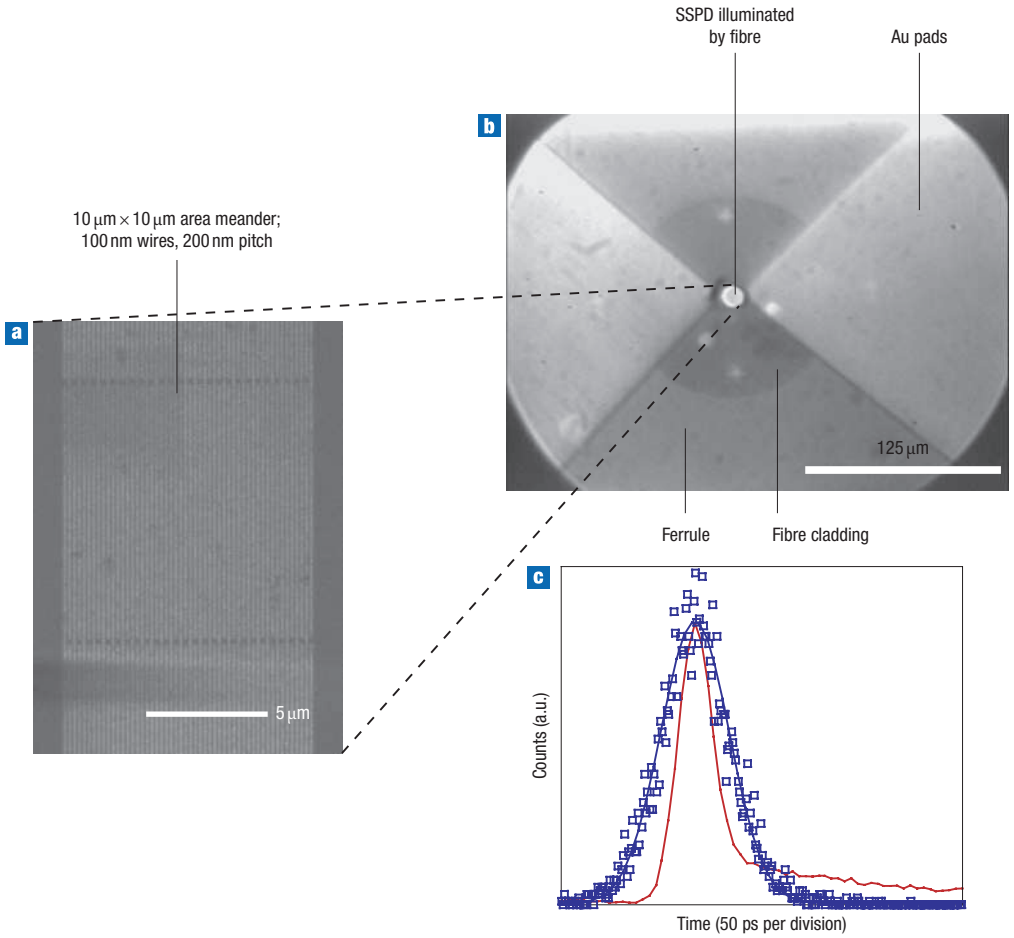

Figure 3 An SSPD. a, SSPD close-up image observed with scanning electron microscope. **b**, Fibre alignment under optical microscope. **c**, Plot of photon arrival time of SSPD (squares and blue line) and up-conversion detector (red line) for a 10-ps pulse input.

caused by detector timing jitter. However, the peaks were well separated when we used a 10-ps time window (Fig. 4b). The time window technique becomes more effective as the time resolution of the whole system improves. We demonstrated this in our experiment by using shorter optical pulses and photon detectors and electronics with less jitter.

In the QKD experiment, we set the quantum efficiency, combined dark count rate and time window width at 1.4%, 50 Hz and 50 ps, respectively. The obtained secure key rates are shown by the squares in Fig. 5a, where the filled and open symbols show fibre transmission points and points simulated with an optical attenuator, respectively. The solid line shows the theoretical curve calculated assuming a quantum efficiency, combined dark count rate and baseline system error of 1.4%, 50 Hz and 2.3%, respectively. The quantum bit error rates for each fibre length and attenuation are shown in Fig. 5b. The error rate for a 200-km fibre transmission was 4.0%. We also undertook a DPS-QKD experiment with a 1-GHz clock, and the results are shown by the triangles in Fig. 5a and b. The present result constitutes a significant improvement over previous QKD experiments, both in secure key generation rate and distribution distance. At 105 km, we successfully achieved a secure key rate of 17 kbit s^{-1}, which is two orders of magnitude greater than the previous record (166 bit s^{-1} at 100 km)[25]. In a 200-km fibre transmission experiment, we were able to generate secure keys with a bit rate of 12 bit s^{-1}. The maximum channel loss for secure key generation was 42.1 dB, which almost doubled the maximum PNS-secure key distribution distance of previous terrestrial QKD experiments over optical fibre[22].

DISCUSSION

Thus far, we have discussed security based on general collective attacks on individual photons. Now, we consider security against a sequential USD attack, which was proposed in ref. 28. The idea behind this type of attack is summarized here. First, we consider the most pessimistic scenario by assuming that Eve has a local oscillator that is phase-locked to the coherent light source owned by Alice. Thanks to this local oscillator, with probability $1-\exp(-2\mu)$, Eve can unambiguously determine whether each pulse is phase-modulated by 0 or π. When Eve obtains m ($>M$) successful sequential measurement outcomes, she constructs a train of m coherent pulses with phase modulations that depend on these measurement outcomes, and re-sends them to Bob. Here, M denotes a block length selected by Eve. If Eve obtains m ($=M$) successful sequential measurement outcomes, with probability P she re-sends a train of m coherent pulses with the corresponding phase modulations, and with a probability of $1-P$ she re-sends a vacuum. Finally, if Eve obtains m ($<M$) successful sequential measurement outcomes, she re-sends a vacuum. In this attack, no error occurs inside the pulse train, but the boundary between the pulse and

the vacuum causes a random error. Note that a high channel loss gives Eve an advantage, because the number of consecutive successful USD attacks is not necessarily large. Thus, this sequential USD attack can pose a potential threat when the channel loss is large.

To investigate the security against a sequential USD attack, we also calculated the error threshold for this attack. The error threshold for a 200-km transmission using SSPDs with 1.4% quantum efficiency (with 36% reduction of effective quantum efficiency by the time window) was 4.74%. With $\mu = 0.2$, the error threshold for generating keys that are secure against general collective attacks for individual photons is approximately 4.1%. This means that for our DPS-QKD experiments with SSPDs, general collective attacks on individual photons[23] give a tighter security bound than a sequential USD attack[28]. Therefore, the experimental data shown by the squares in Fig. 5 were all secure against both general collective attacks on individual photons and a sequential USD attack.

As mentioned above, we used a pseudo-random bit pattern for phase modulation at Alice's site. Note that in a real system, a true random bit pattern needs to be implemented to achieve security. Therefore, the realization of a true random bit pattern generator with a 10-GHz bit rate is an important subject for future research. Proof of the unconditional security of DPS-QKD is another important consideration for the future. Although we have already assumed a very tight security model based on general collective attacks on individual photons (which include a PNS attack) and a sequential USD attack, it is an interesting open question as to whether this protocol is secure against the most general attack. Also, proving the security of the DPS-QKD protocol, in which an information-carrying quantum state is not defined in a pulse but over many pulses, is now considered a major challenge in the field of quantum information science.

Our result is important not only for terrestrial QKD systems using optical-fibre networks but also for global-scale QKD systems using communication satellites[35–37]. According to ref. 35, we need >33-dB loss tolerance to undertake a key exchange to a near-Earth orbit (500–1,000 km range). Although a recent QKD test experiment, in which a key was not actually created, showed the possibility of key generation over >50-dB channel loss[38], the maximum channel loss of key distribution experiments has thus far been limited to around 35 dB (refs 36, 37 and 39). The present result is the first QKD experiment to enable PNS-secure key generation over >40-dB channel loss, so we believe that our DPS-QKD system with SSPDs is a promising candidate not only for intercity terrestrial QKD over optical fibre, but also for global QKD systems using communication satellites.

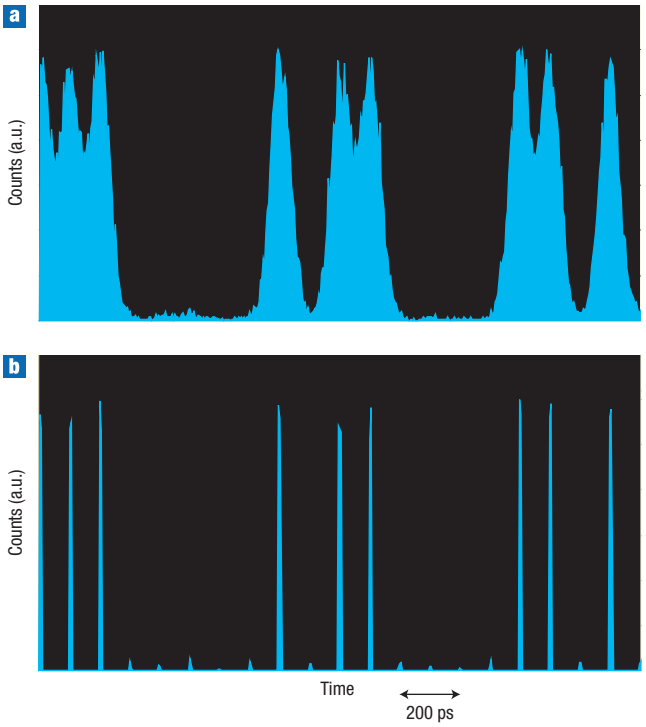

Figure 4 Histogram of received 10-GHz clock signal. a, Clock signal without time window and, **b**, with 10-ps time window.

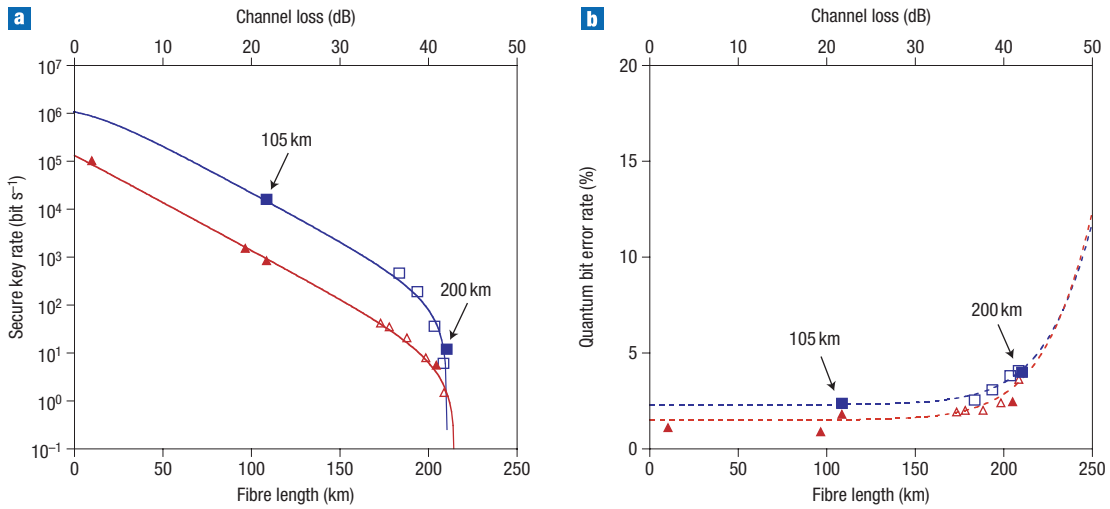

Figure 5 DPS-QKD experimental results. a, Secure key rate, and, **b**, quantum bit error rate, both as a function of fibre length with 0.2-dB km^{-1} loss and channel loss. The squares and triangles show measured secure key rates generated respectively by 10-GHz and 1-GHz clock systems with SSPDs. The filled and open symbols denote fibre transmissions and optical attenuation, respectively. The channel loss does not include the loss of the planar-lightwave-circuit interferometer.

METHODS

APPLICATION OF TIME WINDOW

The dark counts of a continuous-mode single-photon detector such as an SSPD are uniformly distributed in the time domain, and the signal count is observed at around the centre of each time slot. Therefore, we can improve the signal-to-noise ratio by appropriately time-gating the detected counts, which we realized using software. The time-interval analyser records the arrival times of the photons detected by the SSPDs. We know the centre positions of time slots by the clock signal from the high-speed pulse pattern generator for phase modulation. We check the obtained data to see if the arrival times are within a certain time range, which is the half-width of the time window, from the centre positions of the time slots. If the data are outside the window, we discard them.

CONDITIONS OF 10- AND 1-GHZ CLOCK QKD EXPERIMENTS

The quantum efficiency and dark count rate of the SSPD are changed by adjusting the bias current. In the experiment using the 10-GHz clock, the results of which are shown by the squares in Fig. 5, the quantum efficiency and dark count rate were set at 1.4% and 50 Hz, respectively. We also applied a 50-ps time window to the obtained data. The use of the time window reduced the effective quantum efficiency by 36%. The losses of the 105- and 200-km dispersion-shifted fibres including splice and connection losses were 21.7 and 42.1 dB, respectively. The horizontal axis of Fig. 5 denotes the length of fibre with a loss coefficient of 0.2 dB km^{-1}, so the positions of the filled squares deviate from the real fibre lengths.

In the experiment using the 1-GHz clock (triangles in Fig. 5), the quantum efficiency, dark count rate and time window width were 0.6%, 6 Hz and 100 ps, respectively. The reduction in effective quantum efficiency caused by the time window was 45%.

Received 15 January 2007; accepted 17 April 2007; published 1 June 2007.

References

1. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74,** 145–195 (2002).
2. Vernam, G. S. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Inst. Elec. Eng.* **45,** 109–115 (1926).
3. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. Experimental quantum cryptography. *J. Cryptology* **5,** 3–28 (1992).
4. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference of Computer Systems and Signal Processing*, Bangalore, India, 175–179 (IEEE, New York, 1984).
5. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61,** 052304 (2000).
6. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **85,** 1330–1333 (2000).
7. Santori, C., Fattal, D., Vučković, J., Solomon, G. S. & Yamamoto, Y. Indistinguishable photons from a single-photon device. *Nature* **419,** 594–597 (2002).
8. Kuhn, A., Hennrich, M. & Rempe, G. Deterministic single-photon source for a distributed quantum networking. *Phys. Rev. Lett.* **89,** 067201 (2002).
9. McKeever, J. *et al.* Deterministic generation of single photons from one atom trapped cavity. *Science* **303,** 1992–1994 (2004).
10. Waks, E. *et al.* Quantum cryptography with a photon turnstile. *Nature* **420,** 762 (2002).
11. Beveratos, A. *et al.* Single photon quantum cryptography. *Phys. Rev. Lett.* **89,** 187901 (2002).
12. Waks, E., Santori, C. & Yamamoto, Y. Security aspects of quantum key distribution with sub-Poisson light. *Phys. Rev. A* **66,** 042315 (2002).
13. Hwang, W. Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91,** 057901 (2003).
14. Lo, H. K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
15. Wang, X. B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94,** 230503 (2005).
16. Ma, X., Qi, B., Zhao, Y. & Lo, H. K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72,** 012326 (2005).
17. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68,** 3121–3124 (1992).
18. Koashi, M. Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse. *Phys. Rev. Lett.* **93,** 120501 (2004).
19. Scarani, V., Acin, A., Ribordy, G. & Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementation. *Phys. Rev. Lett.* **92,** 057901 (2004).
20. Stucki, D., Brunner, N., Gisin, N., Scarani, V. & Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **87,** 194108 (2005).
21. Inoue, K., Waks, E. & Yamamoto, Y. Differential-phase-shift quantum key distribution. *Phys. Rev. Lett.* **89,** 037902 (2002).
22. Rosenberg, D. *et al.* Long distance decoy state quantum key distribution in optical fiber. *Phys. Rev. Lett.* **98,** 010503 (2007).
23. Waks, E., Takesue, H. & Yamamoto, Y. Security of differential-phase-shift quantum key distribution against individual attacks. *Phys. Rev. A* **73,** 012344 (2006).
24. Takesue, H. *et al.* Differential phase shift quantum key distribution over 105 km fibre. *New J. Phys.* **7,** 232 (2005).
25. Diamanti, E., Takesue, H., Langrock, C., Fejer, M. M. & Yamamoto, Y. 100 km secure differential phase shift quantum key distribution with low jitter up-conversion detectors. *Opt. Express* **14,** 13073–13082 (2006).
26. Gol'tsman, G. N. *et al.* Picosecond superconducting single-photon optical detector. *Appl. Phys. Lett.* **79,** 705–707 (2001).
27. Verevkin, A. *et al.* Detection efficiency of large-active area NbN single-photon superconducting detectors in the ultraviolet to near-infrared range. *Appl. Phys. Lett.* **80,** 4687–4689 (2002).
28. Curty, M., Zhang, L.-L., Lo, H.-K. & Lütkenhaus, N. Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states. Preprint at <http://arxiv.org/abs/quant-ph/0609094> (2006).
29. Bennett, C. H., Brassard, G., Crépeau & Maurer, U. M. Generalized privacy amplification. *IEEE Trans. Inf. Theory* **41,** 1915–1923 (1995).
30. Fasel, S. *et al.* High-quality asynchronous heralded single-photon source at telecom wavelength. *New J. Phys.* **6,** 163 (2004).
31. Trifonov, A. & Zavriyev, A. Secure communication with a heralded single-photon source. *J. Opt. B* **7,** S772–S777 (2005).
32. Soujaeff, A. *et al.* Quantum key distribution at 1550 nm using a pulse heralded single photon source. *Opt. Express* **15,** 726–734 (2007).
33. Hadfield, R. H. *et al.* Single photon source characterization with a superconducting single photon detector. *Opt. Express* **13,** 10846–10853 (2005).
34. Il'in, K. S. *et al.* Picosecond hot-electron energy relaxation in NbN superconducting photodetectors. *Appl. Phys. Lett.* **76,** 2752–2754 (2000).
35. Kurtsiefer, C. *et al.* A step towards global key distribution. *Nature* **419,** 450 (2002).
36. Ursin, R. *et al.* Free-space distribution of entanglement and single photons over 144 km. Preprint at <http://arxiv.org/abs/quant-ph/0607182> (2006).
37. Schmitt-Manderback, T. *et al.* Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.* **98,** 010504 (2007).
38. Collins, R. J., Hadfield, R. H., Fernandez, V., Nam, S. W. & Buller, G. S. Low timing jitter detector for gigahertz quantum key distribution. *Electron. Lett.* **43,** 180–182 (2007).
39. Hiskett, P. A. *et al.* Long-distance quantum key distribution in optical fibre. *New J. Phys.* **8,** 193 (2006).

Acknowledgements

The authors thank E. Diamanti, M. M. Fejer, G. N. Gol'tsman, E. Ip, J. M. Kahn, G. Kalogerakis, L. G. Kazovsky, N. Y. Kim, C. Langrock, R. V. Roussev and Y. Tokura for their support during this research. Financial support was provided by the CREST and SORST programs of the Japan Science and Technology Agency (JST), the National Institute of Information and Communications Technology (NICT) of Japan, the MURI Center for Photonic Quantum Information Systems (ARO/ARDA DAAD19-03-1-0199), DTO, DARPA and the NIST Quantum Information Science Initiative.
Correspondence and requests for materials should be addressed to H.T.

Author contributions

H. Takesue designed and performed the experiments, analysed the data and wrote the paper, S. W. Nam performed the experiments and analysed the data, Q. Zhang performed the experiments, R. H. Hadfield performed the experiments, T. Honjo analysed the data, K. Tamaki analysed the data, and Y. Yamamoto planned the experiments.

Competing financial interests

The authors declare no competing financial interests.