High-rate quantum key distribution over 100 km using ultra-low-noise, 2-GHz sinusoidally gated InGaAs/InP avalanche photodiodes

N. Namekata, H. Takesue, T. Honjo, Y. Tokura, and S. Inoue

1Institute of Quantum Science, Nihon University, 1-8-14 Kanda-Surugadai, Chiyoda-ku, Tokyo, 101-8308, Japan
2NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa, 243-0198 Japan

Abstract: We have demonstrated quantum key distribution (QKD) over 100 km using single-photon detectors based on InGaAs/InP avalanche photodiodes (APDs). We implemented the differential phase shift QKD (DPS-QKD) protocol with electrically cooled and 2-GHz sinusoidally gated APDs. The single-photon detector has a dark count probability of $2.8 \times 10^{-8}$ (55 counts per second) with a detection efficiency of 6%, which enabled us to achieve 24 kbit/s secure key rate over 100 km of optical fiber. The DPS-QKD system offers better performances in a practical way than those achieved using superconducting single-photon detectors. Moreover, the distance that secure keys against the general individual attacks can be distributed has been extended to 160 km.

© 2011 Optical Society of America

OCIS codes: (270.5568) Quantum cryptography; (270.5570) Quantum detectors.

References and links
1. C. H. Bennett and G. Brassard, “Quantum cryptography: public-key distribution and coin tossing,” Proc. of IEEE International Conference on Computers, Systems and Signal Processing 1984, 175–179 (1984).
2. K. Inoue, E. Waks, and Y. Yamamoto, “Differential-phase-shift quantum key distribution,” Phys. Rev. Lett. 89(3), 037902 (2002).
3. H. K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” Phys. Rev. Lett. 94(23), 230504 (2005).
4. N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, “Towards practical and fast quantum cryptography,” arXiv:quant-ph/0411022 (2004).
5. D. Gottesman, H. K. Lo, N. Lutkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices,” Quantum Inf. Comput. 5, 325–360 (2004).
6. E. Waks, H. Takesue, and Y. Yamamoto, “Security of differential-phase-shift quantum key distribution against individual attacks,” Phys. Rev. A 73(1), 012344 (2006).
7. C. H. Bennet, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography,” J. Cryptology 5(1), 3-28 (1992).
8. H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, “Quantum key distribution over a 40 dB channel loss using superconducting single-photon detectors,” Nat. Photonics 1(6), 343–348 (2007).
9. D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, “High-rate, long-distance quantum key distribution over 250 km of ultra low loss fibres,” N. J. Phys. 11(7), 075003 (2009).
10. C. Gobby, Z. L. Yuan, and A. J. Shields, “Quantum key distribution over 122 km of standard telecom fiber,” Appl. Phys. Lett. 84(19), 3762–3764 (2004).
11. D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, “Fast and simple one-way quantum key distribution,” Appl. Phys. Lett. 87(19), 194108 (2005).
12. N. Namekata, G. Fujii, T. Honjo, H. Takesue, and S. Inoue, “Differential phase shift quantum key distribution using single-photon detectors based on a sinusoidally gated InGaAs/InP avalanche photodiode,” Appl. Phys. Lett. 91, 011112 (2007).
13. Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, “Gigahertz quantum key distribution with InGaAs avalanche photodiodes,” Appl. Phys. Lett. 92(20), 201104 (2008).
14. A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, “Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate,” Opt. Express 16(23), 18790–18797 (2008).
15. A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, “Continuous operation of high bit rate quantum key distribution,” Appl. Phys. Lett. 96(16), 161102 (2010).
16. A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K. Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki, and A. Tomita, “Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization,” Opt. Express 16(15), 11354–11360 (2008).
17. M. Pree, C. Pacher, R. Allamae, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Frst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hbel, G. Humer, T. Luether, M. Legr, R. Lieger, J. Lodewyck, T. Lormer, N. Litenhaus, A. Marhold, T. Matyas, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Theel1, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tuille-Broui, F. Vanne, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, “The SECOQC quantum key distribution network in Vienna,” N. J. Phys. 11(7), 075001 (2009).
18. A. Mirza and F. Petruccione, “Realizing long-term quantum cryptography,” J. Opt. Soc. Am. B 27(6), A185–A188 (2010).
19. The Tokyo QKD network demonstration, http://www.uqcc2010.org/index.html.
20. Swissquantum; the longest running project for testing QKD in a field environment, http://swissquantum.idquantique.com/.
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), 2797–2799 (2004).
22. G. Ribordy, N. Gisin, O. Guinnard, D. Stucki, M. Wegmueller, and H. Zbinden, “Photon counting at telecom wavelengths with commercial In-GaAs/InP avalanche photodiodes: Current performance,” J. Mod. Opt. 51(9), 1381–1398 (2004).
23. M. A. Itzler, R. Ben-Michael, C.-F. Hsu, K. Slomkowski, A. Tosi, S. Cova, F. Zappa, and R. Isposou, “Single photon avalanche diodes (SPADs) for 1.5 μm photon counting applications,” J. Mod. Opt. 54(2), 283–304 (2007).
24. A. Tomita and K. Nakamura, “Balanced, gated-mode photon detector for quantum-bit discrimination at 1550 nm,” Opt. Lett. 27(20), 1827–1829 (2002).
25. A. Yoshizawa, S. Odate, and H. Tsuchida, “Discharge pulse counting for low-noise single-photon detection at 1550 nm using InGaAs avalanche photodiode cooled to 130 K,” Jpn. J. Appl. Phys. 46(1), 220–222 (2007).
26. 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(21), 10043–10049 (2006).
27. N. Namekata, S. Adachi, and S. Inoue, “Ultra-low-noise sinusoidally gated avalanche photodiode for high-speed single-photon detection at telecommunication wavelengths,” IEEE Photon. Technol. Lett. 22(8), 529–531 (2010).
28. J. Zhang, P. Eraerds, N. Walenta, C. Barreiro, R. Thew, and H. Zbinden, “2.23 GHz gating InGaAs/InP single-photon avalanche diode for quantum key distribution,” Proc. SPIE 7681, 76810Z (2010).
29. Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, “High speed single photon detection in the near infrared,” Appl. Phys. Lett. 91(4), 041114 (2007).
30. Z. L. Yuan, A. W. Sharpe, J. F. Dynes, A. R. Dixon, and A. J. Shields, “Multi-gigahertz operation of photon counting InGaAs avalanche photodiodes,” Appl. Phys. Lett. 96(7), 071101 (2010).
31. H. Kamada, M. Asobe, T. Honjo, H. Takesue, Y. Tokura, Y. Nishida, O. Tadanaga, and H. Miyazawa, “Efficient and low-noise single-photon detection in 1550 nm communication band by frequency upconversion in periodically poled LiNbO3 waveguides,” Opt. Lett. 33(7), 639–641 (2008).
32. A. Korneev, P. Kouninov, V. Matvienko, G. Chulkova, K. Smirnov, B. Voronov, G. N. Goltsman, M. Currie, W. Lo, K. Wilscher, J. Zhang, W. Slyszy, A. Pearlman, A. Verevkin, and Roman Sobolewski, “Sensitivity and gigahertz counting performance of NbN superconducting single-photon detectors,” Appl. Phys. Lett. 84(26), 5338–5340 (2004).
33. S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, and Z. Wang, “Multipath channel SNSPD system with high detection efficiency at telecommunication wavelength,” Opt. Lett. 35(13), 2133–2135 (2010).
34. N. Namekata, S. Adachi, and S. Inoue, “1.5 GHz single-photon detection at telecommunication wavelengths using sinusoidally gated InGaAs/InP avalanche photodiode,” Opt. Express 17(8), 6275–6282 (2009).
35. G. Brassard and L. Salvail, in Advances in Cryptology-EUROCRIPT ’93 edited by T. Helleseth, Lecture Notes in Computer Science 765 (Springer), 410–423 (1994).
36. M. Curty, L. L. Zhang, H. K. Lo, and N. Lutkenhaus, “Sequential attacks against differential-phase-shift quantum
1. Introduction

Quantum key distribution (QKD) offers the possibility of distributing secure keys over distant parties. Since the initial proposal in 1984 [1], the QKD has rapidly progressed through extensive researches, i.e. invention of protocols [1–4], security proofs for various protocols [5,6], and experimental demonstrations [7–15]. The strong interest has recently turned to the realization of a practical QKD over an installed optical fiber network [16–20]. To date, QKD systems, which are robust (intrinsically [21] or by means of active stabilization [15]) against decoherence mechanisms in the optical fiber, have been developed. Therefore, the major factors that limit the performance of the QKD are the characteristics of single-photon detectors (SPDs) at telecom-wavelengths. The telecom-band SPDs have been developed by various approaches, e.g. a gated InGaAs/InP avalanche photodiode (APD) [22–30], the frequency-upconversion assisted silicon APD [31] and the superconducting nanowire single-photon detector (SNSPD) [32,33]. The SNSPD offers ultra-low dark counts and a low time jitter. These characteristics enabled us to construct the long-distance QKD system that distributes secure keys over the distance longer than 200 km [8,9]. However, the SNSPD requires a cryogenic cooling system, which is obviously a drawback to the practical application. From the practical point of view, a semiconductor-based SPD, i.e. an electrically cooled and gated InGaAs/InP APD, is most likely to fit a practical QKD system. However, the dark count probability of the gated APD $(10^{-5} \sim 10^{-6}$ with 10 % detection efficiency) is typically 2 or 3 orders of magnitude higher than that of the SNSPD, which indicates that the gated APDs cannot be applied to the QKD over a distance longer than 100 km ($>20$ dB channel loss). Moreover, the afterpulsing prevents the gated APD from being operated at a high repetition frequency. The gated APD essentially offers an ultra-low dark count probability comparable to that of the SNSPD at low temperature [24,25]. On the other hand, the repetition frequency of the gated APD has been increased through the efforts to detect a weak avalanche signal by special gating schemes. Especially the sinusoidally gated (SG-) and self-differencing (SD-) APDs achieved a multi-gigahertz repetition frequency of gate [26–30], and thus the high-speed QKD experiments have been demonstrated [13–16]. Therefore, the major challenges are that such rapidly gated APDs have low dark counts comparable with the SNSPD, and achieve the long-distance QKD with a high key distribution rate.

In this work, we investigated whether the SG-APD [27] can have an ultra-low dark counts and simultaneously have an afterpulsing probability low enough to implement the long-distance QKD with gigahertz clock rate by reducing the operating temperature. We used an electrical cooling system, not a cryogenic cooling system. We here demonstrated that the SG-APD operating in the low temperature regime achieved ultra-low dark count probability and realized the high-rate and long-distance QKD, and moreover the part of QKD performances exceeded those achieved with the SNSPD. In the QKD experiment, we employed the differential phase shift QKD (DPS-QKD) protocol, which enabled stable, high-clock rate and long-distance implementation with a simple setup [2,8,21], and we considered the security of the DPS-QKD protocol against the individual attacks [6].
2. Ultra-low-noise Sinusoidally gated InGaAs/InP avalanche photodiodes

Figure 1 shows the diagram of the SPDs which we used in the experiment. The single-mode fiber pigtailed InGaAs/InP APDs (Princeton Lightwave, PGA-300L) were used as the single-photon detection devices and operated with the sinusoidal gating [27]. The APDs were driven

![Diagram of SPD setup](image)

Fig. 1. Ultra-low-noise single-photon detectors based on 2-GHz sinusoidally gated InGaAs/InP avalanche photodiodes. SMF, single-mode fiber; PC, Peltier cooler; GPQC, gated passive quenching circuit; BEF, band elimination filter; B-AMP, 3-GHz bandwidth low-noise amplifier; LPF, low pass filter; CMP, comparator circuit. Avalanche signals were distilled, amplified and discriminated at each filter circuit (FL-1 and FL-2). FL-2 is identical with FL-1.

| Detector type | Operating temperature (K) | Detection efficiency ηd (%) | Dark count probability Pd | Afterpulsing probability Pab (%) | Repetition frequency ωg (GHz) |
|---------------|---------------------------|-----------------------------|--------------------------|-------------------------------|-----------------------------|
| Present work  | 193                       | 6.0                         | 2.8 × 10^-8              | 2                             | 2                           |
| SG-APD        | 243                       | 11.8                        | 3.79 × 10^-6 (55 cps)    | 1.43                          | 2                           |
| SD-APD [30]   | ~ 4                       | 1.4                         | 50 cps (7.6 kcps)        | -                             | 10 (or non-gated)            |
| SNSPD [8]     | ~ 4                       | (0.7)                       | (10 cps)                 | -                             | (non-gated)                  |
| SNSPD [33]    | ~ 4                       | 15                          | 100 cps                  | -                             |                             |

Table 1. Comparison of Single-Photon Detectors, *10 ps Time Window (TW) was Applied to Improve the Signal-to-Noise Ratio

by a gated passive quenching circuit (GPQC) [27]. Then each APD was cooled to 193 K by a 4-stage Peltier cooler. The APDs, GPQCs and coolers are housed in a vacuum chamber to avoid condensation. A 2-GHz sinusoidal voltage with a signal power of 22 dBm was used as gate voltages for each APD. The gate voltages were accurately synchronized with the photon arrival time using the phase controller in Synthesizer 2 and the coaxial-line stretcher (CLS)(See Fig. 2). The emerging signal from each GPQC passed through two band-elimination-filters (BEFs) centered at 2 GHz to reject the transferred gate voltage, where the total elimination ratio of the BEFs was 100 dB. The signal was amplified by 40 dB and passed a low-pass-filter (LPF) with a cut-off frequency f_{3dB} of 3 GHz to reject noises at higher frequencies. Finally the avalanche (detection) signal was discriminated by the comparator circuit (CMP) which accepts 500-ps pulse. The dark count probability per gate of SG-APD 1 was 2.8 × 10^-8 (55 counts per second, cps) with the detection efficiency of 6.0 %, while that of SG-APD 2 was 8.3 × 10^-8 (165 cps) with the same detection efficiency. The low dark counts was achieved by not only the low temperature operation but also the extremely short gate width (expected to be < 100 ps [34]). On the other
hand, as reduced the temperature, the lifetime of trapped carriers is made longer, which causes an increase in the afterpulsing probability. Fortunately, the lifetime extension due to reducing the operating temperature was not large. As a result, the afterpulsing probabilities were limited to 2% with the 50 ns dead time. The value of the afterpulsing probability is low enough to apply the SG-APDs to QKDs. Table 1 shows the comparisons of the SG-APDs to the other SPDs at telecommunication wavelength. The dark count probability of the SG-APD was achieved to be 2 orders of magnitude lower than that of the other APD-based SPDs with keeping the high detection efficiency and the 2-GHz repetition frequency. Furthermore, the performances of the SG-APD considerably approach those of SNSPDs.

3. Setup for QKD experiment

A QKD experiment was carried out using the ultra-low-noise and high-speed SG-APDs. Our QKD system implemented the DPS-QKD protocol [2,8,21]. The Experimental setup is schematically depicted in Fig. 2. The clock rate of the DPS-QKD system was 2 GHz, and electrical equipments in Alice and Bob stations were synchronized using a 10-MHz standard clock signal given by the synthesizer 1. In Alice station, a continuous-wave (cw) laser light at 1550 nm was modulated into coherent pulses using an electro-absorption modulator (EAM) operated by 10 GHz sinusoidal voltage. The duration of optical pulse was as short as 20 ps, thanks to the highly nonlinear response of the EAM. The pulse width is short enough to realize an efficient single-photon detection by the 2-GHz SG-APDs (the performances can be found in Sec. 2). After the optical pulse was amplified by an erbium-doped fiber amplifier (EDFA), its repetition frequency (originally 10 GHz) was reduced to 2 GHz using a LiNbO3 intensity modulator (LN-IM) operated with a rectangular pulse generated by a pulse pattern generator (PPG).

A phase modulator (PM) gave a phase shift $\Delta \phi$ to each coherent pulse. $\Delta \phi$ was randomly chosen from the two values, 0 or $\pi$, where we used a pseudo-random bit sequence given by a data timing generator (DTG). The phase shifted pulses were attenuated to the single-photon level by a variable attenuator (VATT). Taking the security of the DPS-QKD (discussed in Sec. 4) and our experimental conditions into account, the average photon number per pulse $\mu$ was set to 0.2 as the optimal value which enabled us to perform an efficient secure key distribution over a long distance. The quantum channel we used was a dispersion-shifted fiber (DSF). If we use the standard single-mode fiber as the quantum channel, the width of transmitted optical pulse would be broadened by the chromatic dispersion of the fiber. This causes deterioration of the detection efficiency of the gated APD and an increase on the inter-symbol interference.
However, the contributions from the dispersive broadening can be well suppressed by the pre-compensation technique [13].

In Bob station, the transmitted pulses were injected into a Mach-Zehnder interferometer based on a planar lightwave circuit (MZI-PLC). Since the clock rate was 2 GHz, we could use a MZI-PLC with a optical path difference of 0.5 ns. However, as a matter of experimental convenience, we actually used MZI-PLC designed with an 1-ns optical path difference. This change of the path difference requires only a modification of the key-sifting process, and it does not impact on the security proof of the original DPS-QKD protocol. The insertion loss and extinction ratio of the MZI-PLC we used were 2.1 dB and 20 dB, respectively. Two outputs of the MZI-PLC were led to SG-APD 1 and 2, where SG-APD 1 (SG-APD 2) clicked for 0 (π) phase difference between pulses 1-ns-distant from each other. Time instances of detector clicks were finally registered by the time interval analyzer (TIA).

We measured the timing jitter of the SPDs including the CMPs and the TIA when the APDs were illuminated by the optical pulse. Figures 3(a) and 3(b) show time histograms of the photon detection at SG-APD 1 and 2, respectively. Here, photons are detected after transmission through 100 km of optical fiber, while setting phase shift at a fixed value. The timing jitter of the single-photon detection systems was approximately 200 ps which was narrower than the 500 ps gate cycle, and any prominent tailing feature did not exist. However, the time jitter actually caused the inter-symbol interferences. In order to reduce them, we introduced a 400 ps time window to the time-instance data. The detection efficiency, the dark count probability and afterpulsing probability were reduced by 8 %.

![Histograms of the detected signal. Statistics of time-instances when photons were detected at (a) SG-APD 1 and (b) SG-APD 2 for a fixed phase modulation pattern.](image-url)
4. QKD performances

Before showing the experimental results, the theoretical analysis of the DPS-QKD performances are described. The sifted key generation rate was simply evaluated from the number of the photon detection. Then the secure key generation rate was evaluated taking the security against the general individual attack [6] into account in this work. The sifted key generation rate in the DPS-QKD system is given by

$$R_{sifted} = \nu(\mu T + 2P_d) \exp\left(-\frac{\nu \mu T \eta_d}{2}\right)$$

where $\nu$ is the system clock frequency, $\mu$ is the average number of photons per pulse, $P_d$ is the dark count probability per gate, and $T_d$ is the dead time of the TIA. $T$ is the overall efficiency that is expressed as $T = \eta_d \eta_t \eta_{tw}$, where $\eta_d$, $\eta_t$, and $\eta_{tw}$ are the detection efficiency of the SG-APDs, the transfer efficiency from Alice station to the SG-APDs in Bob station and the event reduction rate by the time window, respectively. The bit error rate is given by

$$e \sim \frac{(e_b + \eta_{tw} P_{ab}/2) \eta_{tw} P_d}{\eta_{tw} P_d}$$

where $P_{ab}$ and $P_{click}$ are the overall afterpulsing probability taking into account a dead time of 50 ns, and the total probability of the event counts, respectively, $e_b$ is the baseline error rate that is due to imperfections in the state preparation and the MZI-PLC. Finally, the secure key generation rate after an error correction and a privacy amplification is given by the expression [6].

$$R_{secure} = R_{sifted} \left[ -\{1 - 2\mu\} \log_2 \left(1 - e^2 - \frac{(1 - 6e)^2}{2}\right) + f(e) h(e) \right]$$
\[ h(e) = e \log_2 e + (1 - e) \log_2 (1 - e) \] 

The function depends on the error correction algorithm, and the bi-directional algorithm [35] was used for the error correction.

The key generation rates are plotted as a function of the communication distance in Fig. 4. Open and closed circles show the experimental results of the sifted key rates and the secure key rates, respectively. The theoretical curves, taking the detector performances and a baseline system error rate into account, are simultaneously shown in the same figure. At 100 km, secure keys were successfully generated with a rate of 24 kbit/s, which is higher than the previous record established with the SNSPD [8]. At 160 km, the secure key can be also generated with a rate of 0.49 kbit/s. In 165 km and 170 km fiber transmission experiments, we were not able to obtain the secure keys anymore, since bit error rates exceeded 4.1 % which was the threshold value for the secure key generation against the general individual attacks (Eq. (3) with \( \mu = 0.2 \)).

The maximum channel loss for secure key generation was found to be 33.6 dB which is the best result for QKD experiments using SPDs based on InGaAs/InP APDs. The present system implemented not only the long distance but also an ultra-high-speed QKD, i.e. in a short distance (10 km), a 1.1 Mbit/s secure key rate was achieved, which is comparable to the highest secure key rate reported in [14,15].

The keys generated in our experiment are secure against the general individual attacks. However, there are several other attacks that can be more efficient than the general individual attacks, especially when the transmission loss is large [36,37]. In addition, the unconditional security of the DPS-QKD protocol with a coherent light source has not been proven yet. Thus, a thorough security analysis on the DPS-QKD protocol is an important future consideration. We would like to note that the unconditional security of the DPS-QKD with a single photon source was proved by our colleague recently [38]. Also, a modified protocol that is more robust against sequential attacks [36,37] has been proposed [39]. We hope that we will eventually develop an unconditionally secure DPS-QKD system based on these theoretical efforts, together with the improvement of the devices and system technologies.

To achieve the unconditional security, we have to note the sifted key length as well [40]. In the implementation of the discrete-variable QKD protocols, we can distill the secret keys only when more than \( 10^5 \) bits of the sifted keys are exchanged and processed [40]. Although the lower bound \((10^5)\) of the sifted key length is not for the DPS-QKD protocol, we employed it as a minimum requirement of the sifted key length in this work. Therefore, to obtain each experimental result plotted in Fig. 4, \( 10^5 \)-bit sifted keys were exchanged. To obtain larger-size of sifted keys, the continuous operation such as Ref. [15] will be needed.

5. Conclusions

In conclusion, we performed a 2 GHz clocked DPS-QKD experiment using SPDs based on the SG-APD. A secure key rate of 24 kbit/s was achieved over 100 km of optical fiber, which indicates that the performances of the SG-APD exceeded those of the SNSPD [8]. Moreover, we have successfully distributed secure keys against the general individual attacks over 160 km of optical fiber. These results will accelerate the realization of a practical QKD over an installed optical fiber network.

Acknowledgments

H. Takesue, T. Honjo, and Y. Tokura. are supported by National Institute of Information and Communication Technology (NICT). N. Namekata and S. Inoue are supported by Strategic Information and Communications R & D Promotion Program (SCOPE) in Japan’s Ministry of Internal Affairs and Communications.