

HOKKAIDO UNIVERSITY

Title	Efficient and low-noise single-photon avalanche photodiode for 1.244-GHz clocked quantum key distribution
Author(s)	Nambu, Y.; Takahashi, S.; Yoshino, K. et al.
Citation	Optics Express, 19(21), 20531-20541 https://doi.org/10.1364/OE.19.020531
Issue Date	2011-10-10
Doc URL	https://hdl.handle.net/2115/47433
Rights	©2011 Optical Society of America
Type	journal article
File Information	OE19-21_20531-20541.pdf



Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

Efficient and low-noise single-photon avalanche photodiode for 1.244-GHz clocked quantum key distribution

Y. Nambu,[1,*] S. Takahashi,[2] K. Yoshino,[1] A. Tanaka,[2] M. Fujiwara,[3] M. Sasaki,[2] A. Tajima,[2] S. Yorozu,[1] and A. Tomita[4]

[1]*Green Innovations Research Laboratories, NEC Corporation, 34 Miyukigaoka, Tsukuba, Ibaraki 305-8501, Japan*
[2]*System Platforms Research Laboratories, NEC Corporation, 1753 Shimonumabe, Nakahara, Kawasaki, Kanagawa 211-8666, Japan*
[3]*Quantum ICT Laboratory, National Institute of Information and Communications Technology, 4-2-1 Nukui-kitamachi, Koganei, Tokyo 184-8795, Japan*
[4]*Graduate School of Information Science and Technology, Hokkaido University, Kita 14 Nishi 9, Kita-ku, Sapporo, Hokkaido 060-0814, Japan*
[*]*y-nambu@ah.jp.nec.com*

Abstract: An efficient and low-noise 1.244-GHz gating InGaAs single-photon avalanche photodiode (SAPD) was developed for a high-speed quantum key distribution (QKD) system. An afterpulsing probability of 0.61% and a dark count probability per gate of 0.71×10^{-6} were obtained at a detection efficiency of 10.9% for 1.55-μm photons. Furthermore, our SAPD successfully coped with high detection efficiency (≤ 25%) and quite low afterpulsing noise (≤ 3% for ≤ 25% efficiency) at the same time. Its potential was verified using the actual QKD setups installed over a metropolitan area network.

©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," Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, 175–179, December (1984).
2. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**(3), 1301–1350 (2009).
3. I. D. Quantique, http://www.idquantique.com/
4. Q. Magi Technologies, Inc., http://www.magiqtech.com/MagiQ/Home.html
5. QuintessenceLabs Pty Ltd, http://www.quintessencelabs.com/
6. C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA Quantum Network," in Quantum Information and Computation III, E. J. Donkor, A. R. Pirich, and H. E. Brandt, eds., Proc. SPIE 5815, 138–149 (2005); arXiv:quant-ph/0503058v2.
7. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J. B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network," Opt. Express **19**(11), 10387–10409 (2011).
8. 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).
9. 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).
10. 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).
11. N. Namekata, H. Takesue, T. Honjo, Y. Tokura, and S. Inoue, "High-rate quantum key distribution over 100 km using ultra-low-noise, 2-GHz sinusoidally gated InGaAs/InP avalanche photodiodes," Opt. Express **19**(11), 10632–10639 (2011).
12. 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).

#151783 - $15.00 USD Received 26 Jul 2011; revised 6 Sep 2011; accepted 6 Sep 2011; published 3 Oct 2011
(C) 2011 OSA

13. 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).
14. J. Zhang, R. Thew, C. Barreiro, and H. Zbinden, "Practical fast gate rate InGaAs/InP single-photon avalanche photodiodes," Appl. Phys. Lett. **95**(9), 091103 (2009).
15. 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).
16. J. Zhang, P. Eraerdsa, N. Walentaa, C. Barreiroa, R. Thewa, and H. Zbinden, "2.23GHz gating InGaAs/InP single-photon avalanche diode for quantum key distribution," in Proc. SPIE 7681 (SPIE press, U.S.A.,2010) 76810Z.
17. N. Namekata and S. Inoue, "Ultra-low-noise high-speed single-photon detection using a sinusoidally gated InGaAs/InP avalanche photodiode," in Proc. SPIE **7945** (SPIE press,U.S.A., 2011) 79452K.
18. A. Korneev, P. Kouminov, V. Matvienko, G. Chulkova, K. Smirnov, B. Voronov, G. N. Goltsman, M. Currie, W. Lo, K. Wilsher, J. Zhang, W. Slysz, A. Pearlman, A. Verevkin, and R. Sobolewski, "Sensitivity and gigahertz counting performance of NbN superconducting single-photon detectors," Appl. Phys. Lett. **84**(26), 5338–5340 (2004).
19. S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, and Z. Wang, "Multichannel SNSPD system with high detection efficiency at telecommunication wavelength," Opt. Lett. **35**(13), 2133–2135 (2010).
20. A. Tanaka, M. Fujiwara, K. Yoshino, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, A Scalable Full Quantum Key Distribution System based on Colourless Interferometric Technique and Hardware Key Distillation," Proc. ECOC 2011, paper Mo.1.B.3 (2011).
21. S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, "Avalanche photodiodes and quenching circuits for single-photon detection," Appl. Opt. **35**(12), 1956–1976 (1996).
22. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**(23), 230503 (2005).
23. H. K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**(23), 230504 (2005).
24. Y. Nambu, K. Yoshino, and A. Tomita, "Quantum encoder and decoder for practical quantum key distribution using a planar lightwave circuit," J. Mod. Opt. **55**(12), 1953–1970 (2008).

1. Introduction

Quantum key distribution (QKD) is expected to make it possible for two distant parties to share secret keys via telecommunication [1]. As long as the quantum mechanics is correct and physical assumptions imposed on the local apparatuses of the legitimate users are justified, the secrecy of the shared keys can be proven to be information-theoretically secure [2]. Today, QKD is not merely an intellectual or technological challenge but has become a realistic application. Commercial products are now available [3–5], and the main stage of demonstration is changing from the laboratory to the field. Several QKD test benches in field networks have been established [6,7], and QKD field trials are being carried out day by day.

For QKD to be accepted by a broad spectrum of users, efficient QKD of long keys must be realized. For this solution, a GHz-clocked QKD system is being developed [8–11]. In these developments, an efficient and low-noise single photon detector (SPD) for the telecommunication window is necessary to ensure the performance of high-speed QKD. Currently, there are two main choices for SPDs for a GHz-clocked QKD system: a single-photon InGaAs avalanche photo diode (SAPD) [9, 12–17] or a superconducting nanowire SPD (SSPD) [18,19]. Although current SSPDs have sufficiently low noise, their efficiency has been limited. However, recent efforts have resolved this issue [19]. Indeed, SSPDs have been used to demonstrate high-speed QKD on the Tokyo QKD network [7]. Although SAPDs have inherent advantages, i.e., they are compact, energy-saving, and polarization-independent, developing an efficient and low-noise SAPD is necessary if they are to be really useful in a high-speed QKD network.

Dark count (DC) and afterpulsing (AP) are known to be major noise sources in the InGaAs SAPD. In particular, AP is quite troublesome for high-speed QKD because the necessary high rate of detection of photons induces severe AP noise. To suppress the noise, the SAPD is usually operated in the gated mode, and the overbias voltage is kept very low, although this inevitably reduces detection efficiency. To avoid this unwanted reduction in efficiency, it is crucial to detect weak avalanche signals hidden in the huge capacitive responses of the SAPD due to gated-mode operation [12,13]. However, this is not an easy task for rapid gating SAPDs with repetition rates over 1 GHz because the avalanche signal becomes weaker at higher repetition frequencies. Currently, the most promising solution involves application of a filtering technique. This is quite desirable for SAPDs using a gating

#151783 - $15.00 USD Received 26 Jul 2011; revised 6 Sep 2011; accepted 6 Sep 2011; published 3 Oct 2011
(C) 2011 OSA

voltage with a half duty cycle since it greatly simplifies the design and fabrication of the required filters. Sine wave gating (SG) and filtering [13], and square wave gating and self-differencing [12] have been applied for rapid gating SAPDs, and promising results have been reported [9, 12–17].

In this work, we report a high performance SAPD for a GHz-clocked QKD system. It is based on an SG and filtering technique. We achieved high detection efficiency (≤ 25%) and quite low AP noise (≤ 3% for ≤ 25% efficiency) simultaneously for 1.55-μm photon detection. In particular, an AP probability of 0.61% was obtained at a detection efficiency of 10.9%. Our efficient and low-noise SAPD is promising for high-speed QKD, and it successfully contributed to improving the performance of our GHz-clocked QKD system [7, 20].

2. Experimental setup

A diagram of our SG-SAPD system is shown in Fig. 1. The single-mode fiber pigtailed InGaAs APD (Princeton Lightwave, PGA-300) was embedded in the gated circuit [21]. A pair of SAPDs were installed in the stainless steel housing and cooled to ~−50°C by a two-stage Peltier cooler with air-cooling fan. Sinusoidal voltage of ~1.244-GHz from a master oscillator was amplified and purified by the band-pass-filter (BPF) centered at ~1.244-GHz. The sinusoidal voltage of about 16 V in amplitude was combined with a constant bias voltage of about 62 V to drive the SAPD. The signal from the SAPD was fed into the three-stage band elimination filters (BEFs): one for rejecting the second harmonics component and the others for rejecting the fundamental of the ~1.244-GHz sinusoidal voltage. In these filters, the capacitive responses of the SAPD were efficiently suppressed to less than −70 dB. The output of the last filter is amplified by a 1-GHz-bandwidth preamplifier (PRE AMP: ORTEC 9306).

We evaluated the detection efficiency, DC probability per gate, and AP probability of the SAPD. Evaluation of these parameters requires time-resolved measurement of photon detection timing, which was achieved by using a time interval analyzer (TIA: YOKOGAWA TA-520). To convert a signal into a logic signal acceptable for the TIA, we developed a novel synchronous discriminator (SD). It is synchronized with the gating signal by providing a referential sinusoidal wave from the master oscillator. By tuning the phase of the referential signal, we were able to efficiently discriminate a quite weak but synchronous avalanche signal from the random noise component.

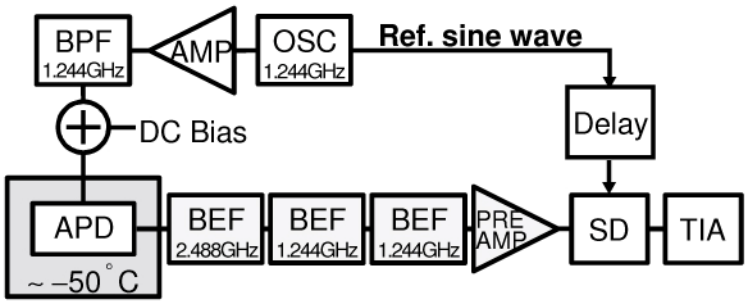


Fig. 1. Sinusoidally gated InGaAs SAPD. OSC: master oscillator; AMP: RF amplifier; SD: synchronous discriminator; PRE AMP: preamplifier.

3. Performance evaluation through time-resolved measurement

The detection efficiency η, DC probability per gate P_d, and AP probability P_a of the SAPD were evaluated as a function of applied bias voltages with the time-resolved measurement as shown in Ref [12,13]. We used 50-ps-wide and 10-MHz-repetition periodic weak laser pulses at 1.55 μm whose average photon number per pulse was set to 0.1. We first evaluated the temporal histogram of the count rate for the quasi-periodic photon detection events associated with a 10-MHz sequence of the laser emission. To maximize the photon count rate, we

#151783 - $15.00 USD Received 26 Jul 2011; revised 6 Sep 2011; accepted 6 Sep 2011; published 3 Oct 2011
(C) 2011 OSA

precisely tuned the relative delay between the sinusoidal voltage and the light pulses by using the digital phase shifter incorporated in the system. Figure 2 shows the temporal histogram around the illuminated gate (photon arrival time of 0 ns). When the light was blocked, the uppper histogram was obtained, which comes from the dark count events that happen only during optically active periods. When the light was irradiated, the histogram changed to the lower one. We found that the count rate in the illuminated gates increased by almost four orders of magnitude, which is associated with the real photon detection. For non-illuminated gates, we see a small increase in the background noise counts, which comes from the AP.

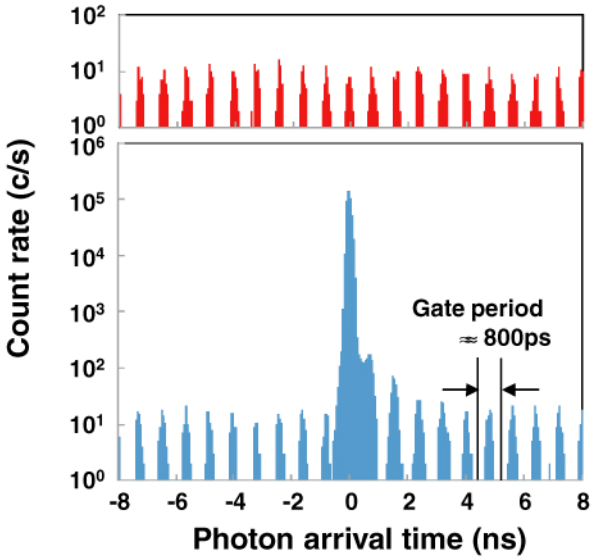


Fig. 2. Temporal histogram (logarithmic scale) of the photon count rate. The upper and lower traces show when the laser was blocked and illuminated, respectively.

Figure 2 suggests that the duration of the active time window was much smaller than the gate period. This is quite important for the operation of our QKD system. In our system, meaningless satellite pulses also arrive at the output ports of Bob's AMZI optics accompanied with the meaningful pulses for key generation, since our optical interferometers involve only passive devices. The system was designed so that those satellite pulses arriving between the gates are discarded by the gating operation which is expected to make the SAPD insensitive to them. This is confirmed by measuring photon count rates by scanning the laser pulse delay as shown in Fig. 3. We set η at ~10% and evaluated the count rates with two instruments: the TIA and the analog-to-digital converter (ADC) incorporated in our QKD setups. The two count rates are different because the count rate only in the illuminated gate was evaluated in the TIA (see below) while the total count rate was evaluated in the ADC. In both cases, the count rate fell almost to the dark count level at a $\approx \pm 400$ ps delay, which confirmed the expected action for our SAPD.

#151783 - $15.00 USD Received 26 Jul 2011; revised 6 Sep 2011; accepted 6 Sep 2011; published 3 Oct 2011
(C) 2011 OSA

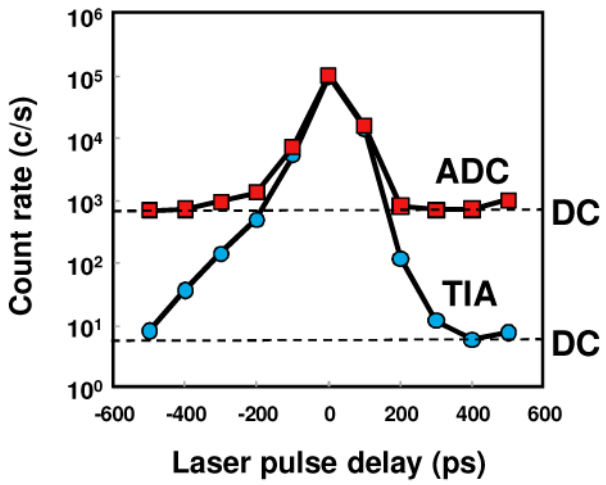


Fig. 3. Count rates as a function of laser pulse delay for measurements using TIA and ADC. The detector dark count levels for two measurements are indicated by the two dashed lines.

To evaluate P_d, P_a, and η, we counted the number of events per second in each gate period ≈800 ps in Fig. 2. Then we obtained the count rates per gate at the illuminated and non-illuminated gates, C_I and C_{NI}, as well as the dark count rate per gate C_D when the light was blocked. We evaluated the AP probability P_a according to Refs [12]. and [13], i.e.,

$$P_a = \frac{C_{NI} - C_D}{C_I - C_{NI}} R, \tag{1}$$

where R is the number of gates during one period of the laser pulse, which was $2^7 = 128$ in the present case. We investigated more than 50 devices. Figure 4 shows a map of measured (P_d, P_a) for devices operating at η ~10%. The data are scattered in the ranges from 0.1×10^{-6} to 50×10^{-6} for P_d and from 0.6 to 9% for P_a. For comparison, Table 1 lists the performance of GHz-gated InGaAs SAPDs. Note that almost all the data are located within the same ranges. This result indicates that the quality of the current SAPD is not well controlled. Figure 5 shows the P_d and P_a as functions of η for two devices that have the smallest and second smallest P_a at η ~10%. A P_d value in the order of 10^{-7} - 10^{-5} was obtained for η of 2– 25%. In particular, P_a ~0.61% (and P_d ~0.71×10^{-6}) was obtained for η ~10.9% for a 1.55-um photons. It should be noted that in comparison with the previously reported SAPDs, the AP noise of our SAPDs is notably reduced even for η much larger than 10%. For example, P_a was about 7% for η ~25% in Ref [15], while it was about 3% in our SAPDs. In the other reports, P_a values were much higher than 3% for a similar value of η. Therefore, our SAPD achieves low noise and high efficiency simultaneously, which has been difficult to achieve previously.

It should be noted that the definition of P_a in Eq. (1) is based on the tacit presupposition that the detection rate of AP noise, i.e., C_{NI}–C_D, should be proportionate to the detection rate of real photon, i.e., $C_I - C_{NI}$. This is because the former is generated by reemission of the trapped carriers in defects generated by the latter. To confirm this presupposition, we evaluated $C_I - C_{NI}$ and P_a for devices operating at η ~10% as a function of the average number μ of photons in the incident pulses. Figure 6 plots the results showing that P_a was almost independent of μ while $C_I - C_{NI}$ was almost proportional to μ. This indicates that C_{NI}–C_D was almost proportional to $C_I - C_{NI}$, which confirms the above presupposition.

We believe that the present data update the best performance report of the GHz-gated SAPD. However, unfortunately, we cannot attribute the origin of this improvement specifically. Both improvements in the APD and the experimental apparatuses such as filters and the detection electronics may have contributed to this improvement. In the following, we

#151783 - $15.00 USD Received 26 Jul 2011; revised 6 Sep 2011; accepted 6 Sep 2011; published 3 Oct 2011
(C) 2011 OSA

comment on the factors to improve the performance of GHz-clocked SAPDs. First of all, we believe that quality of APD is of primarily importance. Although the experimental apparatuses certainly affect the observed performance of the SAPDs, we never observed that the choice of the apparatuses changed bad device into good one. Moreover, if we carefully tune the apparatuses, almost the same results were reproduced with a statistically reasonability. Fine tuning of the apparatuses is of next importance. Especially, we could not achieve the current results without developing our SD which can discriminate fast and weak avalanche signal from the SAPDs exhaustively. The choice of the front-end preamplifier also affects the results significantly. We believe that the current results were obtained by the best choice of the APDs and best choice of the experimental apparatuses currently on hand.

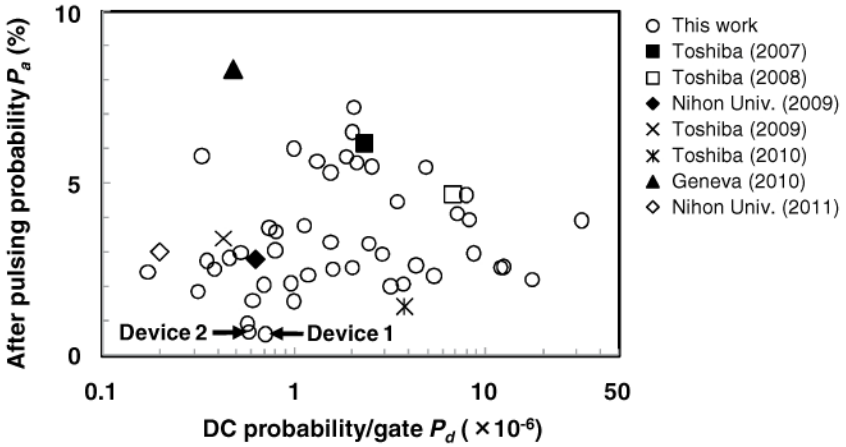


Fig. 4. Map showing (P_d, P_a) for devices operating at η ~10%. The previous data in Table 1 are also plotted for the reader's reference.

Table 1. Comparison of SAPD performance at 1.55-μm wavelength; ω_g: gating frequency.

		η (%)	P_d (gate-1)	P_a (%)	ω_g (GHz)
Present work	Device 1	10.9	0.71×10^{-6}	0.61	1.244
	Device 2	11.6	0.58×10^{-6}	0.69	
TREL(2007) [12]		10.9	2.34×10^{-6}	6.16	1.25
TREL(2008) [9]		10	6.8×10^{-6}	4.7	1.036
Nihon Univ. (2009) [13]		10.8	0.63×10^{-6}	2.8	1.5
TREL(2009) [14]		9.3	0.48×10^{-6}	3.4	0.92
TREL(2010) [15]		11.8	3.79×10^{-6}	1.42	2
		23.5	13.2×10^{-6}	4.84	
Geneva(2010) [16]		10	0.48×10^{-6}	8.3	2.23
Nihon Univ. (2011) [17]		9.6	0.2×10^{-6}	3	1
Nihon Univ. (2011) [11]		6.0	0.028×10^{-6}	2	2

#151783 - $15.00 USD Received 26 Jul 2011; revised 6 Sep 2011; accepted 6 Sep 2011; published 3 Oct 2011
(C) 2011 OSA

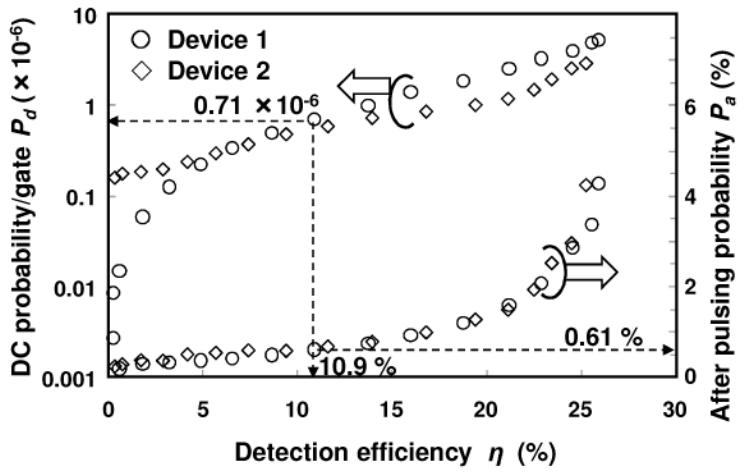


Fig. 5. DC probability per gate P_d and AP probability P_a as a function of detection efficiency η for two devices, device 1 and 2, that have the smallest and second smallest P_a at η ~10%. Error bars for P_a are smaller than symbols and not shown in the figure.

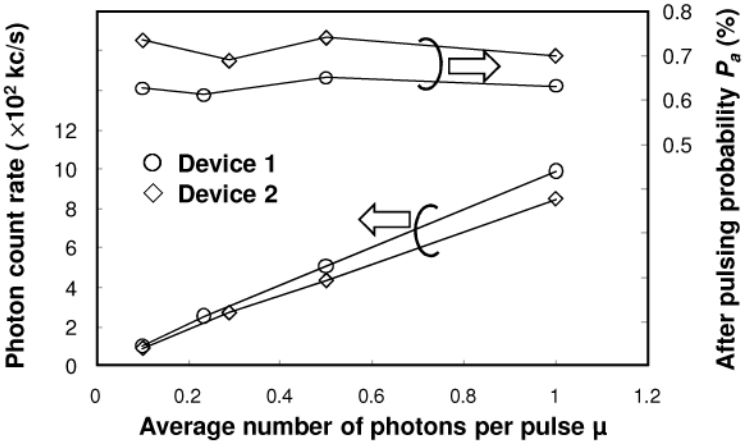


Fig. 6. Photon count rate in the illuminated gate and P_a for two devices operating at η ~10% as a function of the average number μ of photons in the incident pulses.

4. Screening the SAPDs

Since the quality of the current SAPD is not well controlled, the question arises as to how we can screen useful devices based on the time-resolved measurement results. Here, we seek guidelines for screening the SAPD. To consider this issue, we propose a simple model relating the quantum bit error rate (QBER), DC probability, and AP probability. We focus here on the QBER due only to the detector noise. The actual QBER also involves other sources of noise, such as those due to the limited visibility of the interferometers and spurious light originating from the clock signal and satellite pulses. However, they clearly do not influence the selection process.

First, we propose a model. The QBER due to the detector noise comes from the fact that the detection event is sometimes registered even if Bob does not receive a photon, which we call a null detection event. Of course, the detection event is sometimes registered if Bob receives more than one photon, which we call a true detection event. Let us imagine the measurement record of the QKD experiment. There is a random temporal sequence of null and true detection events in this record, for which we can estimate the rates C_{null} and C_{true}. After sifting the keys, half of the null detection events are erroneous and contribute to the

#151783 - $15.00 USD Received 26 Jul 2011; revised 6 Sep 2011; accepted 6 Sep 2011; published 3 Oct 2011
(C) 2011 OSA

QBER, while ideally none of the true events contribute to the QBER. Thus, we may estimate the lower bound (LB) of QBER by

$$QBER_{LB} = \frac{\frac{1}{2}C_{null}}{C_{true} + \frac{1}{2}C_{null}}. \quad (2)$$

Let us imagine the hypothetical record of the time-resolved measurement. There would be a temporal sequence of null and true detection events although true events are distributed quasi-periodically in the record that reflects a 10-MHz sequence of the laser emission. Here, we assume that different sequences of null and true events in these two records have little effect on the noise generation in the SAPD. Then we simply identify C_{null} with the count rate at all of the non-illuminated gates; $C_{null} \rightarrow RC_{NI}$ and C_{true} with the photon count rate at the illuminated gate; $C_{true} \rightarrow C_I - C_D$ evaluated in chapter 3. Thus, we identify

$$QBER_{LB} = \frac{\frac{1}{2}RC_{NI}}{C_I - C_{NI} + \frac{1}{2}RC_{NI}}. \quad (3)$$

Here, we simplify our discussion to explain the consequence of our model. First, from Eq. (1) and $P_a \ll R$, it follows that

$$C_{NI} = \left(1 + \frac{P_a}{R}\right)^{-1}\left(\frac{P_a}{R}C_I + C_D\right) \approx \frac{P_a}{R}C_I + C_D. \quad (4)$$

Next, we take into account the order estimation of the three rates C_I, C_{NI}, and C_D. Table 2 lists the typical values obtained in the measurement. From this table, we find $C_I - C_D \gg RC_{NI}$ and obtain

$$QBER_{LB} \approx \frac{1}{2}\frac{RC_{NI}}{C_I - C_{NI}} = \frac{1}{2}P_a\frac{C_{NI}}{C_{NI} - C_D} \approx \frac{1}{2}\left(P_a + \frac{RC_D}{C_I}\right) = \frac{1}{2}\left(P_a + \frac{\omega_g P_d}{C_I}\right), \quad (5)$$

where ω_g is the gate frequency.

Table 2. Order estimation of three rates C_I, C_{NI}, and C_D, where R = 128.

C_I [kc/s]	RC_{NI} [kc/s]	RC_D [kc/s]
100	1.5	0.85
250	2.4	0.85
500	4.2	0.85

In the rightmost expression of Eq. (5), the first term shows the contribution from the AP, and the second term that from the DC. Note that the second term depends on the photon count rate, while P_a does not, as shown in Fig. 6. When the photon count rate is low enough that $P_a \ll \omega_g P_d/C_I$ is satisfied, the contribution from the DC is predominant. On the contrary, when the photon count rate is high enough that $P_a \gg \omega_g P_d/C_I$ is satisfied, AP noise is predominant and $QBER_{LB}$ approaches $P_a/2$.

We are now ready to discuss the issue of screening the useful SAPD. The upper and lower traces in Fig. 7 show the plots of Eq. (5) for $QBER_{LB}$ = 2 and 1%, respectively, together with the measurement results of (P_d, P_a) for our devices. Here, broken, dash-dotted, and dash-two-dotted lines indicate those plots when the photon count rate at the illuminated gate was assumed to be $C_I - C_D \approx C_I$ = 15, 150 kc/s, and 1 Mc/s, respectively. Note that, for our actual QKD setups (see later), the corresponding sifted key rates are 30, 300 kbps, and 2 Mbps,

#151783 - $15.00 USD Received 26 Jul 2011; revised 6 Sep 2011; accepted 6 Sep 2011; published 3 Oct 2011
(C) 2011 OSA

respectively. These plots give the criteria in screening the SAPDs that should satisfy an arbitrary requirement on the system QBER. For example, suppose that we require $QBER_{LB} \leq 2\%$ for $C_I - C_D \approx C_I = 150$ kc/s when our device is used in a QKD system. Then, the devices with the measured (P_d, P_a) ranging in the lower left-hand area of the associated plot, i.e., the dash-dotted curve in the upper trace, should satisfy this requirement.

In Fig. 7, it is evident that the plots shift towards the left hand side as the photon count rate decreases. Therefore, when the photon count rate is low, selecting an SAPD with lower P_d has a significant impact on improving the QBER. On the contrary, when the photon count rate is high, we can select SAPDs having similar P_a values but not a very small P_d without increasing the system QBER significantly. We should note that because the photon count rate depends on the parameters of the optical link in the installation conditions, such as length and loss in the fiber, the screening process also depends on those parameters. Therefore, it is important to find out those parameters before the installation in order to screen the useful SAPDs.

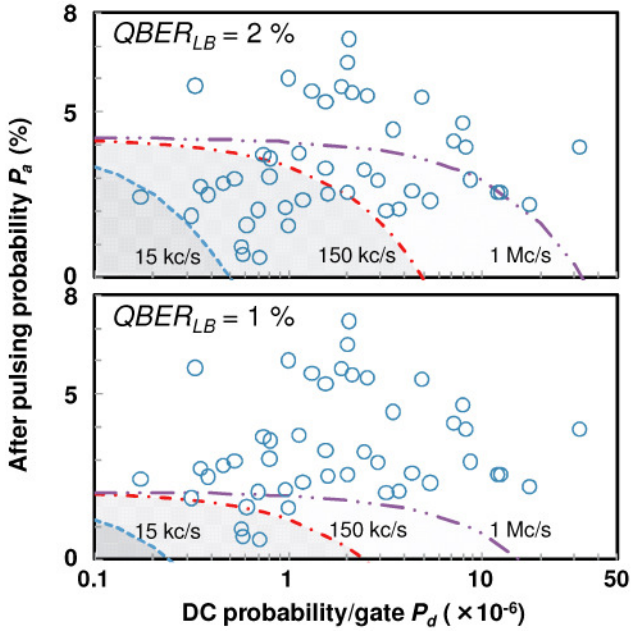


Fig. 7. Criteria in screening the SAPDs that satisfy $QBER_{LB} \leq 2\%$ (upper trace) and $QBER_{LB} \leq 1\%$ (lower trace) for three photon count rates $C_I - C_D \approx C_I = 15$ (broken line), 150 kc/s (dash-dotted line), and 1 Mc/s (dash-two-dotted line).

5. Performance evaluation using actual QKD setup

It should be careful enough to conclude that the QKD system should enjoy the potential of our SAPDs. This is because different electronics are used to detect avalanche signals in the QKD system and in the time-resolved measurement to evaluate the SAPDs. It is not surprising that these electronics have different sensitivity to noise. Therefore, it is important to confirm the potential of the present SAPDs using the actual QKD setups.

To this end, we conducted experiment using the actual QKD setups. In this experiment, the 8-bit high-speed ADC was used to register the avalanche signal instead of SD and TIA. Its sampling rate was twice the system repetition, i.e., 2.488 GS/s. The details of the QKD setup are described elsewhere [20]. It is based on the decoy state BB84 QKD system [22,23]. A two-input, four-output asymmetric Mach-Zehnder interferometer (2×4 AMZI) is embedded in the receiver (Bob) [24]. The four output ports of Bob's AMZI are assigned to the four measurement states by Bob. We focused our attention on the QBER of photons arriving at one detector, device 1 in Fig. 5, which was connected to one of the output ports of Bob's optics.

#151783 - $15.00 USD Received 26 Jul 2011; revised 6 Sep 2011; accepted 6 Sep 2011; published 3 Oct 2011
(C) 2011 OSA

We evaluated the QBER of randomly coded photons with an initial photon number of ~0.5 photons/pulse and after being transmitted through the 45-km-long installed optical fiber. To determine how the AP affected the QBER, we utilized the hold-off function incorporated in our QKD system. It reduces the contribution of AP noise in the stored key data by discarding a set number of data recorded during a short period of time (hold-off period) after true photon detection. Accordingly, the measured QBER should depend on the hold-off period. We evaluated QBER as a function of η by changing the hold-off period for 12.8–300 ns. Figure 8 shows the QBER and sifted key rate as a function of detection efficiency η for photons arriving at device 1. As expected, the observed QBER strongly depended on the hold-off time. QBER of ~4% was obtained for η ~25% and for the hold-off period larger than 200 ns. This indicates that our SAPD successfully coped with high detection efficiency and quite low AP noise at the same time.

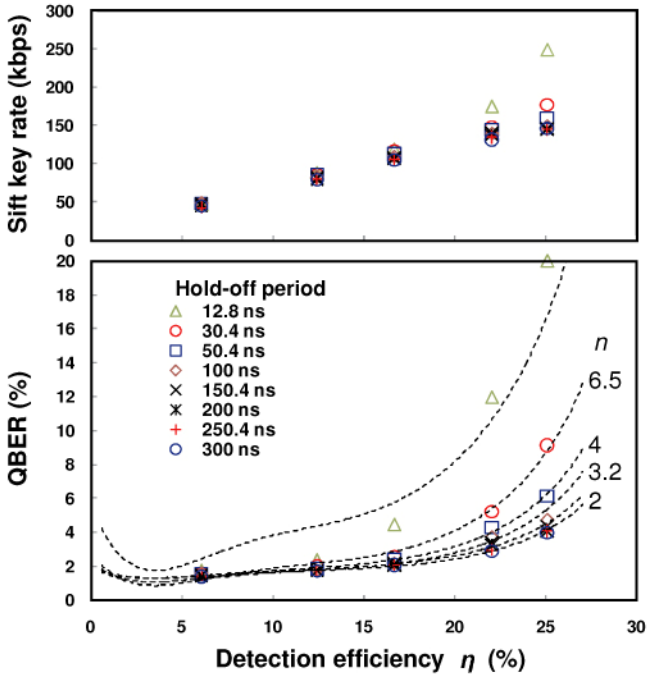


Fig. 8. QBER and sifted key rate as a function of detection efficiency η for photons arriving at device 1.

The present result suggests that substantial AP noise contributes to QBER, which is analyzed by model fitting based on our model. We defined the sensitivity n of the system to the AP noise as $n = P_a^{ADC} / P_a$, where P_a^{ADC} is the AP probability experienced by the ADC in our QKD setups and P_a is the AP probability measured by the time-resolved measurement. We calculated $QBER_{LB}$ expected for a given detection efficiency η by using Eq. (5) and replacing $P_a \rightarrow P_a^{ADC} = nP_a$, where P_a and P_d are the values expected for η from the time-resolved measurement (Fig. 5), C_l is the value associated with η observed during the QKD experiment, and n is a free adjustable parameter depending on the hold-off period. We introduced another free adjustable parameter to incorporate a constant additional contribution to the QBER due to noise sources other than the detector noise. We obtained the fitted curve of QBER shown by the broken lines in Fig. 8. We found that our model explains the experimental results well. The correlation between the AP noise (Fig. 5) and the system QBER (Fig. 8) suggests that AP noise dominates the other sources of noise in determining the QBER when the detection efficiency is high. The results show that our efficient and low-noise SAPD is promising for reducing QBER for high-rate detection and for achieving high-speed

#151783 - $15.00 USD Received 26 Jul 2011; revised 6 Sep 2011; accepted 6 Sep 2011; published 3 Oct 2011
(C) 2011 OSA

QKD. The sensitivity n is shown as a function of the hold-off period in Fig. 9. Unexpectedly, n approached not 1 but about 2 for hold-off periods larger than 200 ns in our QKD system. This indicates that our ADC has higher sensitivity to AP noise than the SD and the TIA have, i.e., there is room for further improvement for the former. Here, it should be noted that our method for screening the SAPD is valid for a QKD system with $n \neq 1$. In this case, the predicted curves of $QBER_{LB}$ do not change, but the measured (P_d, P_a) should be replaced with (P_d, nP_a) in Fig. 7 in order to screen the useful SAPDs.

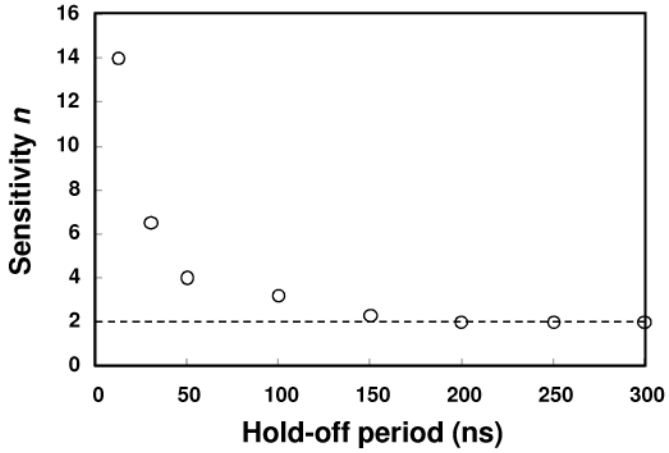


Fig. 9. Sensitivity n of ADC to AP noise as a function of the hold-off period.

Finally, the potential of our SAPDs was further confirmed by a full QKD demonstration on a 45-km-long wavelength-division-multiplex optical link in the Tokyo QKD network [20]. A secure key generation rate of ~90 kbps was achieved with the decoy method [22,23], which was slightly larger than those obtained with SSPDs. At the same time, the QBER was kept at ~3%, which is comparable to those obtained with SSPDs. The details will be reported elsewhere

6. Conclusion

We have successfully developed an efficient and low-noise 1.244-GHz gating InGaAs SAPD. We achieved an afterpulsing probability of ~0.61% for a detection efficiency of ~10.9% for a 1.55-μm photons. Our SAPD successfully coped with high detection efficiency (≤ 25%) and quite low afterpulsing noise (≤ 3% for ≤ 25% efficiency) at the same time. The potential of our APDs was confirmed in a test using the actual GHz-clocked QKD setups installed over the metropolitan area network. The current results were obtained through our continuing efforts to find out the best APD and the best experimental setup to detect the fast and weak avalanche signal from it. We hope that our results accelerate the research, development and diffusion of quantum cryptography.

Acknowledgements

The authors thank H. Satoh at NEC for his technical support in machining the SAPD housing. This work was supported by the project on “Research and development for practical realization of quantum cryptography” of NICT under the Ministry of Internal Affairs and Communications of Japan.

#151783 - $15.00 USD Received 26 Jul 2011; revised 6 Sep 2011; accepted 6 Sep 2011; published 3 Oct 2011
(C) 2011 OSA