PHOTONICS Research

High-speed and high-performance polarization-based quantum key distribution system without side channel effects caused by multiple lasers

HEASIN KO,[1,3] BYUNG-SEOK CHOI,[1] JOONG-SEON CHOE,[1] KAP-JOONG KIM,[1] JONG-HOI KIM,[1] AND CHUN JU YOUN[1,2,*]

[1]Photonic/Wireless Convergence Components Research Division, Electronics and Telecommunications Research Institute, Daejeon 34129, South Korea
[2]School of Advanced Device Technology, University of Science & Technology, Daejeon 34113, South Korea
[3]e-mail: seagod.ko@etri.re.kr
**Corresponding author: cjyoun@etri.re.kr*

Received 15 November 2017; revised 8 January 2018; accepted 17 January 2018; posted 19 January 2018 (Doc. ID 313600); published 28 February 2018

Side channel effects such as temporal disparity and intensity fluctuation of the photon pulses caused by random bit generation with multiple laser diodes in high-speed polarization-based BB84 quantum key distribution (QKD) systems can be eliminated by increasing the DC bias current condition. However, background photons caused by the spontaneous emission process under high DC bias current degrade the performance of QKD systems. In this study, we investigated the effects of spontaneously emitted photons on the system performance in a high-speed QKD system at a clock rate of 400 MHz. Also, we show further improvements in the system performance without side channel effects by utilizing the temporal filtering technique with real-time field-programmable gate array signal processing.

OCIS codes: (270.5565) Quantum communications; (270.5568) Quantum cryptography; (140.5960) Semiconductor lasers.

https://doi.org/10.1364/PRJ.6.000214

1. INTRODUCTION

A free-space quantum key distribution (QKD) system provides the availability of unconditionally secure key exchanges between two distant parties without a fiber network infrastructure. Polarization is normally adopted as a physical observable for free-space QKD systems, and it has been largely studied and demonstrated in diverse situations such as moving platform [1], aircraft [2], long distance [3], and daylight conditions [4]. Recently, successful distribution of entangled photon pairs over a distance of 1200 km using a quantum satellite [5] and satellite-to-ground QKD [6] was reported, which arouses expectations that unconditionally secure bit exchanges through a global network will be feasible in the near future. However, such unconditional quantum security is only guaranteed with implementations where all components, both in the sender and receiver, are properly operated without any device loopholes [7–11].

In most free-space QKD systems, multiple semiconductor lasers with passive optics are utilized to randomly generate four different polarization states [1–6]. One of the polarization states can be transmitted by turning on one of the laser diodes exclusively for each time slot. We recently reported on side channel effects in random bit generation with multiple laser diodes in a polarization-based QKD system [11]. In that paper, we clearly showed that the temporal position and intensity of the photon pulses from each laser diode can vary widely depending on the time interval between consecutive pulses from a single laser, which is called temporal disparity and intensity fluctuation. Although this issue is extremely critical in terms of the security of polarization-based QKD systems with multiple laser diodes, it has not been clearly investigated because these effects are not severe for speeds of operation of 100 MHz or lower, which are adopted in most representative free-space QKD demonstrations [1–4]. However, these side channel effects apparently do occur in high-speed QKD systems, especially under conditions of low DC bias current injected into laser diodes, due to the dynamics of the initial carrier density and photon density. Since unconditional security is threatened by these side channel effects, such effects must be eliminated in the physical implementation, which can be accomplished by increasing the DC bias current injected into the laser diodes. Unfortunately, as a result, the performance of the QKD system will be unavoidably degraded due to the background photon noise from the spontaneous emission process of four laser diodes, especially for high DC bias current conditions.

In this paper, we experimentally demonstrate, for the first time (to our knowledge), the unavoidable performance degradation of a high-speed polarization-based BB84 [12] QKD system with multiple laser diodes used to eliminate the side channel effects. In our work, we first demonstrated that it is possible to achieve superior performance with a QKD system under zero DC bias condition even for a clock speed of 400 MHz, which is several times faster than previous representative free-space BB84 QKD demonstrations [1–5]. Second, we investigated how the side channels of temporal disparity and intensity fluctuation under zero DC bias current threaten the security of the system. Third, we repeated the QKD experiments under high DC bias current, where the side channels were effectively closed. We quantitatively measured how the background photon noises caused by the spontaneous emission process under high DC bias current limited the performance of the quantum bit error rate (QBER) and secure key rate. Here we showed that the photon counts by spontaneous emission of the laser diodes can be a dominant factor that limits the performance of the high-speed system beyond the dark counts of single photon detectors (SPDs). In addition, we demonstrated that the system performance can be significantly improved by using the temporal filtering technique. Finally, we discussed some strategies toward obtaining superior performance for high-speed QKD systems without the aforementioned side channel effects.

The remaining part of this paper is structured as follows. In Section 2, the experimental setup for measuring the effects of the DC bias current on the performance of the QKD system is described. The experimental results of the QBER and key rates when side channel effects are neglected and eliminated are presented in Section 3. In addition, improvements in the system performance from using the temporal filtering technique, as well as some analyses, are presented. In Section 4, further discussion toward producing high-speed and high-performance polarization-based QKD systems is presented. Some concluding remarks are presented in Section 5.

2. EXPERIMENTAL SETUP

The experimental setup for measuring the effects of different DC bias currents of laser diodes on the performance of QKD systems is shown in Fig. 1. We implemented a polarization-based BB84 QKD system with four semiconductor laser diodes and passive optics such as beam splitters, polarization beam splitters, half-wave plates, and neutral density filters. We randomly injected electrical pulses into each laser diode, as shown in Fig. 1, which results in aperiodic current injection in terms of each laser diode. Single longitudinal mode vertical-cavity surface-emitting lasers (VCSELs) with a lasing wavelength of 787.5 nm were utilized for photon sources. We injected electrical current pulses of 200 ps full width at half-maximum (FWHM) to each laser diode to generate optical pulses of 65 ps FWHM. Note that the optical pulse width is smaller than that of the electrical pulse injection due to the dynamics of large signal modulation with the gain-switching method [13]. The amplitude of the current pulses was controlled differently for different values of I_{DC} so that we could generate similar optical pulses with a width of 65 ps, where I_{DC} is the DC bias current injected into the laser diodes, as shown in the current pulse diagram in Fig. 1. The photon pulses were generated at a clock rate of 400 MHz and attenuated to a mean photon number of 0.5. Note that clock speed can be increased to a higher speed than 400 MHz due to the fact that the width of the optical pulses is 65 ps. The clock signal for synchronization at a wavelength of 1550 nm was combined with the quantum signal using a dichroic mirror. A neutral density filter with 10 dB attenuation was added to emulate the channel loss.

The combined quantum signal and clock signal were split through another dichroic mirror in the receiver. The clock signal, which was recovered through a high-speed photodetector, was processed at the field-programmable gate array (FPGA) to

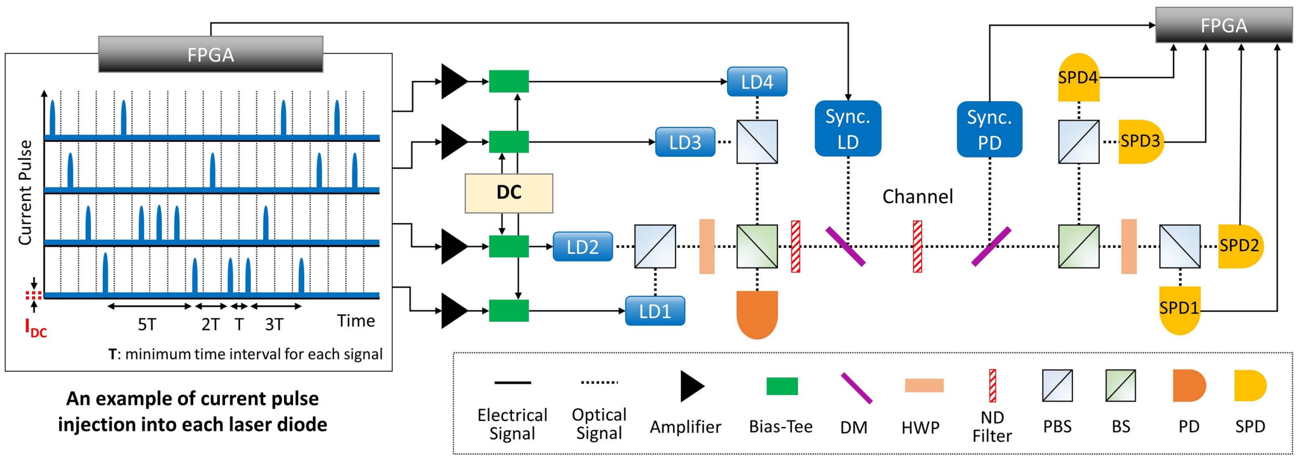

Fig. 1. Experimental setup for measuring performance degradation of a polarization-based BB84 QKD system under high DC bias current. An example of aperiodic current signals generated from a FPGA is depicted. FPGA, field-programmable gate array; LD, laser diode; Sync. LD, synchronization laser diode; Sync. PD, synchronization photodiode; DM, dichroic mirror; HWP, half-wave plate; ND filter, neutral density filter; PBS, polarization beam splitter; BS, beam splitter; PD, photodetector; SPD, single photon detector.

synchronize it with the quantum signal. Quantum signal detection was carried out with a four-channel Si avalanche photodiode based SPD (PerkinElmer SPCM-AQ4C) whose dark counts are lower than 500 counts/s per channel and detection efficiency is approximately 50% at the wavelength of our laser diodes. Bob's system loss, including optics loss, fiber coupling loss, sifting loss, and detection efficiency, was measured as 8 dB. The sifting process of raw keys and estimation of the QBER were conducted with an FPGA-based real-time signal processing system. The QKD operation was carried out in darkroom conditions to effectively eliminate other stray photons. Note that background noise photons caused by the spontaneous emission process of four laser diodes exist, which can differ according to the level of I_{DC}.

The detection probability distribution of the received signals is depicted in Fig. 2. Even though the transmitted optical pulse width was approximately 65 ps, photon detection events were temporally broadened to approximately 750 ps FWHM. Note that the detection probability distribution was unavoidably broader than the generated optical pulse width due to several factors, such as SPD response jitter, clock signal jitter, and differential digital data signal skews. In our system, most of the detection events were covered within the temporal region of 1.5 ns.

It is natural to set I_{DC} as zero, because any nonzero I_{DC} generates spontaneously emitted photons for all temporal regions. In other words, we should set I_{DC} as zero to turn on one of the four laser diodes exclusively for each time slot; otherwise, the four laser diodes always generate spontaneously emitted photons, which can definitely increase QBERs. Here, we measured the QBER and key rates at $I_{\mathrm{DC}} = 0$, which is the condition in which the output photons from spontaneous emission are negligible. We repeated the experiment with $I_{\mathrm{DC}} = 0.95 I_{\mathrm{th}}$ (I_{th} represents the lasing threshold level of the laser diodes), which is the minimum I_{DC} level of our VCSELs, to eliminate temporal disparity and intensity fluctuation at a clock rate of 400 MHz. For $I_{\mathrm{DC}} = 0.95 I_{\mathrm{th}}$, we investigated how the performance of the QKD system was degraded due to the detrimental effects of spontaneously emitted photons. We further used the temporal filtering technique to remove the unwanted photon detections from all detection events to improve the system performance of the QBER and secure key rate, which occurred at the stage of post-processing with the FPGA signal processing system. By adopting the temporal filtering technique, we ignored the photon signals detected in the unwanted temporal regions, which were mostly noises from the spontaneous emission process spread over all temporal regions. The valid signal window due to temporal filtering, centering on the peak detection probability, was decreased from 2.5 to 0.5 ns, with steps of 0.25 ns, to effectively filter out the background photon noises.

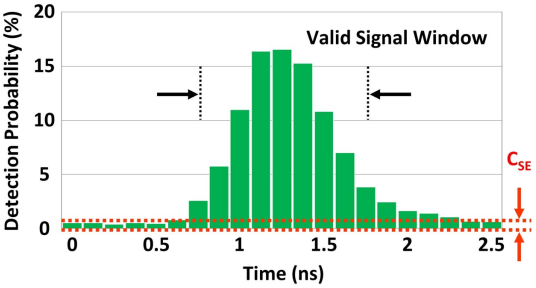

Fig. 2. Detection probability distribution of the received signals under $I_{\mathrm{DC}} = 0.95 I_{\mathrm{th}}$, which was estimated at the FPGA with a timing resolution of 125 ps. C_{SE} represents the photon counts created by the spontaneous emission process.

3. EXPERIMENTAL RESULTS

A. QKD Operation without Considering the Side Channel Effects

The side channel effects that occurred in our system at a clock rate of 400 MHz for the condition with $I_{\mathrm{DC}} = 0$ are shown in Fig. 3(a). The optical pulses shown in Fig. 3(a) represent the second pulses out of any two consecutive pulses for different time intervals from a single laser diode. The time positions of the second pulses are depicted with respect to the current pulse injection to investigate temporal disparity among the second pulses. Here, time t represents the expected time position of the output pulses. As described in Ref. [11], the pulses are temporally distinguishable based on the time intervals between two consecutive pulses, which can significantly endanger the system security if Eve utilizes previously known attack strategies accordingly [14,15]. In addition, intensity fluctuation results in the degradation of the security performance of a BB84 QKD even for decoy-state QKD systems [16–18]. Thus, such side channels effects must be eliminated to guarantee the security of the QKD system.

Any QKD system that does not consider such side channel effects may be wrongly interpreted as an unconditionally secure one with superior QBER and key rates, because the security loophole from such side channel effects is not reflected in the performance parameters such as QBER and sifted key rates. The performance of the QKD system for $I_{\mathrm{DC}} = 0$ is shown in Figs. 3(b) and 3(c). In this case, a QBER of 1.04% and key rate of 1.213 Mbps were achieved at a signal window of 2.5 ns, even without implementing the temporal filtering technique. We verified that the QBER can be decreased to approximately 0.56% by reducing the signal window to 0.5 ns, as shown in Fig. 3(b). Here, reducing the signal window alleviates the effects on the QBER caused by system jitter and clock drift. Also, detection events caused by dark counts of the SPD itself are eliminated as the signal window decreases. The impact of downsizing on the sifted key rates was imperceptible in a signal window range of 2–2.5 ns, as shown in Fig. 3(c), because most signal photons exist within the range of 2 ns, as shown in Fig. 2. Further downsizing yielded some reduction in the sifted key rate, which became significant when the size was smaller than 1 ns. The secure key rate was calculated with the assumption of the decoy method [19,20] using the following simple equation [21]:

$$R \approx q\{-\eta\mu f(e_{\mathrm{det}}) H_2(e_{\mathrm{det}}) + \eta\mu e^{-\mu}[1 - H_2(e_{\mathrm{det}})]\}, \quad \textbf{(1)}$$

where q is the sifting ratio, μ is the mean photon number, η is the transmittance, e_{det} is the QBER, $f(e_{\mathrm{det}})$ is the error correction coefficient for a given e_{det}, and $H_2(e_{\mathrm{det}})$ is the Shannon entropy, where $H_2(e_{\mathrm{det}}) = -e_{\mathrm{det}} \log_2(e_{\mathrm{det}}) - (1 - e_{\mathrm{det}}) \log_2(1 - e_{\mathrm{det}})$. Here, we used 1.22 for $f(e_{\mathrm{det}})$. The optimal window size in terms of the secure key rate was approximately 2.25 ns, as shown

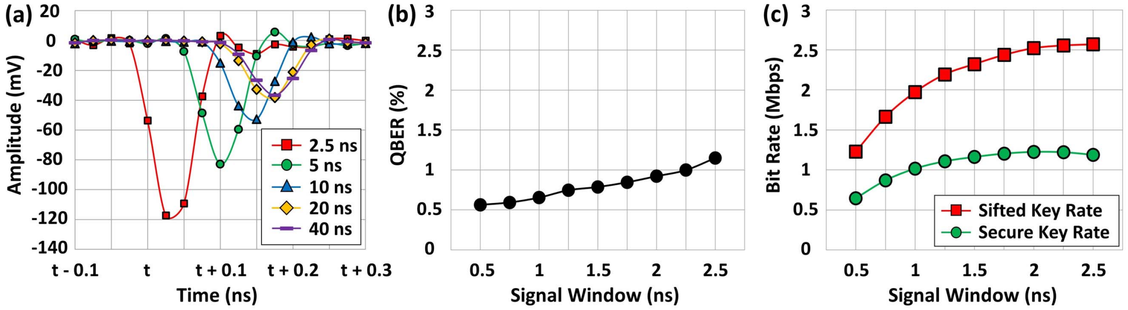

Fig. 3. Side channel effects and the performance of the QKD system under $I_{\mathrm{DC}} = 0$. (a) Side channel effects of temporal disparity and intensity fluctuation. Second pulses out of two consecutive pulses in a 1 s time block are measured for different time intervals from 2.5 to 40 ns. Details of the measurement methods are described in [11]. (b) QBER as a function of the signal window with temporal filtering. The signal window was resized from 2.5 to 0.5 ns, with a resolution of 0.25 ns. (c) Sifted key rate and secure key rate as functions of the signal window with temporal filtering.

in Fig. 3(c), where the secure key rate was recorded as 1.222 Mbps. However, even though the system achieved superior performance parameters of QBER and key rates, the security of the QKD under $I_{\mathrm{DC}} = 0$ can be threatened due to the aforementioned side channel effects of temporal disparity and intensity fluctuation.

B. QKD Operation Considering the Side Channel Effects

The side channel effects were eliminated under $I_{\mathrm{DC}} = 0.95I_{\mathrm{th}}$, as shown in Fig. 4(a). Pulses with different intervals between consecutive pulses are temporally overlapped and the intensity fluctuation becomes negligible. Thus, we can ensure that the side channels are eliminated under $I_{\mathrm{DC}} = 0.95I_{\mathrm{th}}$. However, when I_{DC} is increased close to the lasing threshold level I_{th} of the laser diodes, the QBER can be increased due to the enhanced amount of background noise photons resulting from the spontaneous emission process.

While the QBER was estimated as around 1.04% under $I_{\mathrm{DC}} = 0$, it was increased to 2.67% under $I_{\mathrm{DC}} = 0.95I_{\mathrm{th}}$, as shown in Fig. 4(b). The excess QBER was mostly due to the spontaneously emitted noise photons from the four laser diodes, which were always generated, even for unallowed time slots, due to the relatively high I_{DC}, as shown in the left part of Fig. 1. Here, the spontaneously emitted noise photons under the $I_{\mathrm{DC}} = 0.95I_{\mathrm{th}}$ condition become a dominant factor limiting the QBER performance, due to the fact that 1.63% out of a 2.67% QBER is caused by the increase of I_{DC} from 0 to $0.95I_{\mathrm{th}}$.

The probability of the detection counts due to spontaneously emitted photons C_{SE} is shown in Fig. 2. Here, temporal filtering evidently improved the QBER performance as the signal window decreased from 2.5 to 1.5 ns, because the C_{SE} outside the signal window was effectively eliminated. In such signal windows, the sifted key rate was slightly diminished, which allowed a higher gain in the final secure key rate, as shown in Fig. 4(c). For signal windows smaller than 1.5 ns, however, the QBER performance was not significantly improved, because temporal filtering reduces not only background photon noises but also true signals, which significantly reduces the sifted key rate. Note that most of the received signals were covered within approximately 1.5 ns, as shown in Fig. 2. For our QKD system, the measured optimal signal window in terms of the final secure key rate for $I_{\mathrm{DC}} = 0.95I_{\mathrm{th}}$ was approximately 1.75 ns, where the QBER was 1.51% with a sacrifice of detection events of 6.4%. Here, the secure key rate was recorded as 1.037 Mbps. Further reduction of the signal window should be discouraged as it would eliminate too many signal photons, which diminishes the final secure key rate.

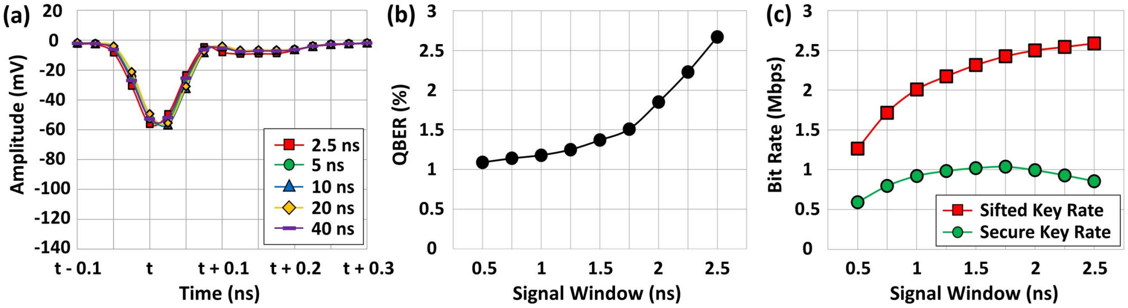

Fig. 4. Side channel effects and performance of the QKD system under $I_{\mathrm{DC}} = 0.95I_{\mathrm{th}}$. (a) Side channel effects of temporal disparity and intensity fluctuation. Second pulses out of two consecutive pulses in a 1 s time block were measured for different time intervals from 2.5 to 40 ns. Details of the measurement methods are described in [11]. (b) QBER as a function of the signal window with temporal filtering. The signal window was resized from 2.5 to 0.5 ns, with a resolution of 0.25 ns. (c) Sifted key rate and secure key rate as functions of the signal window with temporal filtering.

One can easily verify that the condition of $I_{\mathrm{DC}} = 0.95I_{\mathrm{th}}$ degrades the performance of the QBER and key rate compared with the $I_{\mathrm{DC}} = 0$ case. The final secure key rate without temporal filtering was decreased from 1.213 to 0.856 Mbps, which indicates a 29.4% drop. However, a high I_{DC} condition is necessary to close the side channels, especially for a high-speed polarization-based QKD system with multiple lasers. Under this condition, we can increase the secure key rate from 0.856 to 1.037 Mbps using temporal filtering, which results in a 21.1% improvement in the secure key rate.

4. DISCUSSION

Many previously known side channels of QKD systems can be easily avoided through simple countermeasures or simple monitoring methods without degradation of the system performance [7–10]. However, the temporal disparity and intensity fluctuation caused by random bit generation using multiple semiconductor laser diodes cannot be avoided without sacrificing the QBER performance, especially for high-speed BB84 QKD systems. Although the temporal filtering technique is definitely an effective method for improving the performance, as demonstrated in the previous sections, there could be other possible strategies for alleviating the increase of the QBER, as follows.

One of the differences between spontaneously emitted and stimulated emitted photons is the spectral characteristics, as shown in Fig. 5. We measured the spectrum for three cases of $\{I_{\mathrm{DC}}, I_{\mathrm{AC}}\}$: for $\{0.95I_{\mathrm{th}}, 0\}$, $\{0.95I_{\mathrm{th}}, I_{\mathrm{AC}}\}$, and $\{0, I_{\mathrm{AC}}\}$. Note that $I_{\mathrm{DC}} = 0.95I_{\mathrm{th}}$ generates spontaneously emitted photons and an AC pulse generates stimulated emitted photons. In a single longitudinal mode laser diode, most of the stimulated output photons are generated at a single wavelength, as shown in Fig. 5. On the other hand, photons generated by spontaneous emission show broad spectral characteristics [13]. We can easily see that the power of the sidebands is higher under $I_{\mathrm{DC}} = 0.95I_{\mathrm{th}}$ than under $I_{\mathrm{DC}} = 0$. Sidebands become negligible for $I_{\mathrm{DC}} = 0$, as shown by the dotted line in Fig. 5. Therefore, we can eliminate sidebands caused by high I_{DC} by utilizing an ultra-sharp spectral bandpass filter, which mostly functions as noise photons.

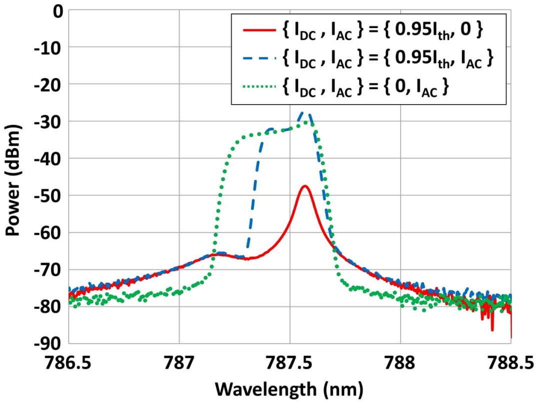

Fig. 5. Spectral characteristics of photon pulses for different DC bias and AC pulse conditions.

Reducing system jitter is another strategy for improving the performance. The QBER caused by the spontaneous emission process can be continuously decreased as we carry out more temporal filtering, as shown in Fig. 4(a). If the system jitter, including the SPD response jitter, becomes smaller, such that the received signal distribution becomes significantly narrower than that of our system, we can effectively decrease the QBER without sacrificing signal counts, which increases the final secure key rate. For our system, most of the jitter occurred at the stage of the single photon detection response.

5. CONCLUSION

In this study, we experimentally demonstrated for the first time (to our knowledge) that the noise photons caused by spontaneous emission of multiple lasers, beyond dark counts of the SPDs or system errors, can be a dominant factor limiting QBER performance in high-speed (400 MHz) QKD operation if the side channel effects of temporal disparity and intensity fluctuation are considered. We showed that the performance of the secure key rate of the QKD system decreased from 1.213 Mbps to 856 kbps due to the increase of QBER performance caused by photon noise from the spontaneous emission process, which is non-negligible under $0.95I_{\mathrm{th}}$. We showed that a secure key rate of 856 kbps can be improved up to 1.037 Mbps by utilizing the temporal filtering technique, which should be considered a desirable prerequisite for high-speed QKD systems with multiple laser diodes. In addition, we briefly discussed that using an ultra-sharp bandpass filter and reducing system jitter can be effective techniques for achieving superior system performance.

Funding. ICT R&D Program of Ministry of Science, ICT and Future Planning (MSIP)/IITP (1711035342); Electronics and Telecommunications Research Institute (ETRI).

Acknowledgment. The authors thank Dr. Haeyoung Rha for helping with data processing with a real-time FPGA system. This work was supported by the ICT R&D Program of MSIP/IITP [Development of key technologies for flexible optical node based on software-defined network (SDN)] and Electronics and Telecommunications Research Institute (ETRI) grant funded by the Korean government (Development of preliminary technologies for transceiver key components and system control in polarization based free space quantum key distribution).

REFERENCES

1. J. Y. Wang, B. Yang, S. K. Liao, L. Zhang, Q. Shen, X. F. Hu, J. C. Wu, S. J. Yang, H. Jiang, Y. L. Tang, B. Zhong, H. Liang, W. Y. Liu, Y. H. Hu, Y. M. Huang, B. Qi, J. G. Ren, G. S. Pan, J. Yin, J. J. Jia, Y. A. Chen, K. Chen, C. Z. Peng, and J. W. Pan, "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," Nat. Photonics **7**, 387–393 (2013).
2. S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, "Air-to-ground quantum communication," Nat. Photonics **7**, 382–386 (2013).
3. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of

free-space decoy-state quantum key distribution over 144 km," Phys. Rev. Lett. **98**, 010504 (2007).

4. S. K. Liao, H. L. Yong, C. Liu, G. L. Shentu, D. D. Li, J. Lin, H. Dai, S. Q. Zhao, B. Li, J. Y. Guan, W. Chen, Y. H. Gong, Y. Li, Z. H. Lin, G. S. Pan, J. S. Pelc, M. M. Fejer, W. Z. Zhang, W. Y. Liu, J. Yin, J. G. Ren, X. B. Wang, Q. Zhang, C. Z. Peng, and J. W. Pan, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," Nat. Photonics **11**, 509–513 (2017).
5. J. Yin, Y. Cao, Y. H. Li, S. K. Liao, L. Zhang, J. G. Ren, W. Q. Cai, W. Y. Liu, B. Li, H. Dai, G. B. Li, Q. M. Lu, Y. H. Gong, Y. Xu, S. L. Li, F. Z. Li, Y. Y. Yin, Z. Q. Jiang, M. Li, J. J. Jia, G. Ren, D. He, Y. L. Zhou, X. X. Zhang, N. Wang, X. Chang, Z. C. Zhu, N. L. Liu, Y. A. Chen, C. Y. Lu, R. Shu, C. Z. Peng, J. Y. Wang, and J. W. Pan, "Satellite-based entanglement distribution over 1200 kilometers," Science **356**, 1140–1144 (2017).
6. S. K. Liao, W. Q. Cai, W. Y. Liu, L. Zhang, Y. Li, J. G. Ren, J. Yin, Q. Shen, Y. Cao, Z. P. Li, F. Z. Li, X. W. Chen, L. H. Sun, J. J. Jia, J. C. Wu, X. J. Jiang, J. F. Wang, Y. M. Huang, Q. Wang, Y. L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y. A. Chen, N. L. Liu, X. B. Wang, Z. C. Zhu, C. Y. Lu, R. Shu, C. Z. Peng, J. Y. Wang, and J. W. Pan, "Satellite-to-ground quantum key distribution," Nature **549**, 43–47 (2017).
7. H. Ko, K. Lim, J. Oh, and J. K. K. Rhee, "Informatic analysis for hidden pulse attack exploiting spectral characteristics of optics in plug-and-play quantum key distribution system," Quantum Inf. Process. **15**, 4265–4282 (2016).
8. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nat. Photonics **4**, 686–689 (2010).
9. S. Nauerth, M. Furst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, "Information leakage via side channels in freespace BB84 quantum cryptography," New J. Phys. **11**, 065001 (2009).
10. K. Nakata, A. Tomita, M. Fujiwara, K. I. Yoshino, A. Tajima, A. Okamoto, and K. Ogawa, "Intensity fluctuation of a gain-switched semiconductor laser for quantum key distribution systems," Opt. Express **25**, 622–634 (2017).
11. H. Ko, B. S. Choi, J. S. Choe, K. J. Kim, J. H. Kim, and C. J. Youn, "Critical side channel effects in random bit generation with multiple semiconductor lasers in a polarization-based quantum key distribution system," Opt. Express **25**, 20045–20055 (2017).
12. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *IEEE International Conference on Computers, Systems, and Signal Processing* (1984), pp. 175–179.
13. L. A. Coldren, S. W. Corzine, and M. L. Mashanovitch, *Diode Lasers and Photonic Integrated Circuits* (Wiley, 2012).
14. M. Dusek, M. Jahma, and N. Lutkenhaus, "Unambiguous state discrimination in quantum cryptography with weak coherent states," Phys. Rev. A **62**, 022306 (2000).
15. G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," Phys. Rev. Lett. **85**, 1330–1333 (2000).
16. X. B. Wang, C. Z. Peng, J. Zhang, L. Yang, and J. W. Pan, "General theory of decoy-state quantum cryptography with source errors," Phys. Rev. A **77**, 042311 (2008).
17. M. Hayashi and R. Nakayama, "Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths," New J. Phys. **16**, 063009 (2014).
18. A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, "Finite-key security analysis of quantum key distribution with imperfect light sources," New J. Phys. **17**, 093011 (2015).
19. W. Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," Phys. Rev. Lett. **91**, 057901 (2003).
20. H. K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
21. X. Ma, B. Qi, Y. Zhao, and H. K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**, 012326 (2005).