**Article:**

Koehler-Sidki, A, Dynes, James F, Paraiso, T K et al. (4 more authors) (2020) Backflashes from fast-gated avalanche photodiodes in quantum key distribution. Applied Physics Letters. 154001. ISSN 0003-6951

https://doi.org/10.1063/1.5140548

Applied Physics Letters

# Backflashes from fast-gated avalanche photodiodes in quantum key distribution

Cite as: Appl. Phys. Lett. **116**, 154001 (2020); https://doi.org/10.1063/1.5140548
Submitted: 01 December 2019 . Accepted: 15 March 2020 . Published Online: 13 April 2020

A. Koehler-Sidki, J. F. Dynes, T. K. Paraïso, M. Lucamarini, A. W. Sharpe, Z. L. Yuan, and A. J. Shields

COLLECTIONS

This paper was selected as Featured

This paper was selected as Scilight

View Online Export Citation CrossMark

Applied Physics Letters ARTICLE scitation.org/journal/apl

# Backflashes from fast-gated avalanche photodiodes in quantum key distribution

Cite as: Appl. Phys. Lett. **116**, 154001 (2020); doi: 10.1063/1.5140548
Submitted: 1 December 2019 · Accepted: 15 March 2020 ·
Published Online: 13 April 2020

View Online Export Citation CrossMark

A. Koehler-Sidki,[1,2,a)] J. F. Dynes,[1,b)] T. K. Paraïso,[1] M. Lucamarini,[1] A. W. Sharpe,[1] Z. L. Yuan,[1] and A. J. Shields[1]

## AFFILIATIONS

[1]Toshiba Research Europe Ltd., Cambridge Research Laboratory, 208 Cambridge Science Park, Milton Road, Cambridge CB4 0GZ, United Kingdom
[2]Engineering Department, University of Cambridge, 9 J. J. Thomson Avenue, Cambridge CB3 0FA, United Kingdom

[a)]Author to whom correspondence should be addressed: amks31@outlook.com
[b)]Electronic mail: james.dynes@crl.toshiba.co.uk

## ABSTRACT

InGaAs single-photon avalanche photodiodes (APDs) are key enablers for high-bit rate quantum key distribution. However, the deviation of such detectors from ideal models can open side-channels for an eavesdropper, Eve, to exploit. The phenomenon of backflashes, whereby APDs reemit photons after detecting a photon, gives Eve the opportunity to passively learn the information carried by the detected photon without the need to actively interact with the legitimate receiver, Bob. While this has been observed in slow-gated detectors, it has not been investigated in fast-gated APDs where it has been posited that this effect would be lessened. Here, we perform the first experiment to characterize the security threat that backflashes provide in a GHz-gated self-differencing APD using the metric of information leakage. We find that, indeed, the information leakage is lower than that reported for slower-gated detectors, and we show that its effect on the secure key rate is negligible. We also relate the rate of backflash events to the APD dark current, thereby suggesting that their origin is the InP multiplication region in the APD.

Quantum key distribution (QKD) promises information theoretic security that is guaranteed by the laws of physics.[1] This property has spurred significant efforts in this research area, culminating in a number of field trials.[2–8] With the recent deployment of QKD outside of the lab, avalanche photodiodes (APDs) have presented themselves as the most promising single-photon detectors due to their ability to operate at room temperature,[9] excellent detection efficiency,[10] and short dead-times.[11]

While perfectly secure in theory, deviations of components from their ideal behavior can create security loopholes. Detectors are the most vulnerable devices in a QKD system as they are exposed through the optical channel and therefore are the most accessible components to Eve. One example exists in the form of the faked-state attack,[12] of which the most notable implementation is the blinding attack. Demonstrations of this attack have been presented on a variety of individual detectors and systems,[13,14] although several of these have only been possible due to inappropriate operation rather than a genuine security weakness.[15,16]

The aforementioned attacks are all examples of Eve actively interacting with the QKD system, both by measuring Alice's qubits and then illuminating Bob's detectors. This presents a significant chance of their presence being detected. It has been shown that APDs are susceptible to emitting light after detection, known as backflashes.[17–21] Backflashes can then allow Eve to act in a more passive way and thus ascertain which of Bob's detectors has clicked without having to interact with any components in the QKD system. However, no studies have yet been performed on fast-gated detectors that are used in state-of-the-art QKD systems.[11] While it has been suggested that faster gating, resulting in shorter gates and subsequently avalanches with less charge, would result in fewer backflashes,[17] this hypothesis has not been experimentally verified.

In this paper, we present the first study on backflashes in GHz-gated self-differencing APDs, key enablers in high bit rate QKD.[11] Our finding supports the hypothesis that faster gating, resulting in narrower gates and smaller avalanche charges, results in fewer backflashes. Using the technique in Ref. 17, we quantify the information leakage and find it to be 0.5%, which is an order of magnitude lower than the value measured for a MHz-gated detector. Such a low information leakage has a negligible effect on the secure key rate.

To determine the potential vulnerability of a fast-gated APD, we perform a simple experiment. An InGaAs/InP APD is chosen as the device under test. It is thermoelectrically cooled to $-30\,^{\circ}$ C where the breakdown voltage is 62.16 V. When driven with a constant DC bias of 59.66 V and a peak-to-peak 1 GHz AC signal of 10 V with 50% duty cycle corresponding to 500 ps "ON" and "OFF" times, respectively, the APD exhibits a detection efficiency of 17% at a wavelength of 1550 nm, a dark count probability of $1.9 \times 10^{-6}$, and an afterpulse probability of 5%.

For investigating the effect of backflashes on the security of QKD, the APD is illuminated with a 1550 nm pulsed laser diode (LD) with a pulse width of approximately 30 ps and a repetition frequency of 1/64 of the APD gating frequency (15.625 MHz). We use this laser repetition frequency to only illuminate every 64th gate as this allows us to mitigate the addition of afterpulses when determining the number of legitimate APD counts. If a faster frequency were used, afterpulses could raise the APD detections and thus artificially lower the information leakage. The flux is controlled using a variable optical attenuator (VOA). We illuminate the APD with 0.1 photons/pulse, a flux typical for QKD, at the start of the APD gate. The reasons for the placement of the pulse in this temporal location are twofold. First, this simulates the behavior of the legitimate users, as the detection efficiency is the greatest at the start of the gate. Second, placing the pulse at the start of the gate gives the avalanches the longest time to grow and therefore provides a maximum value of the backflash probability and is therefore the more conservative estimate of information leakage. The light enters port 1 of a circulator, and port 2 is connected to the APD. Emitted backflashes then re-enter the circular and exit via port 3, after which they are measured with a superconducting nanowire single-photon detector (SNSPD). The detected APD counts and backflashes are interpreted with a time-tagging single-photon counter. This is illustrated in Fig. 1(a).

In an ideal case, any light detected by the SNSPDs can be attributed to backflashes. However, in the optical path, backreflections are also detected and can artificially raise the SNSPD count rate. An example of this is shown in the histogram of SNSPD detection events with the APD DC and AC disabled (see red bars in Fig. 1(b)). The peak features at approximately 17 and 49 ns can be attributed to backreflections from the APD surface and connector between the APD and circulator, and they dominate the SNSPD detection events when the APD is single-photon insensitive, shown as the red bars in the same figure. The blue bars corresponding to backflashes are reasonably uniformly distributed across the histogram, with the exception of the second backreflected peak. At this point of approximately 49 ns, the blue bars have a much larger amplitude (around 100 rather than 40), which suggests that this peak corresponds to reflection from the APD surface itself and that the backflashes are strongly correlated with APD detection events.

To quantify the effect of backflashes on QKD security, we use the metric of information leakage, defined in Ref. 17, as

$$P_L = \frac{N_B}{N_A \eta_{det} \eta_{ch}}, \tag{1}$$

where $N_B$ is the number of detected backflashes (neglecting backreflections and dark counts), $N_A$ is the number of detected valid APD counts (i.e., neglecting dark counts), $\eta_{det}$ is the detection efficiency of the monitoring detector (80% for the SNSPD used), and $\eta_{ch}$ is the channel loss between the APD under test and the monitoring detector, measured to be 0.78.

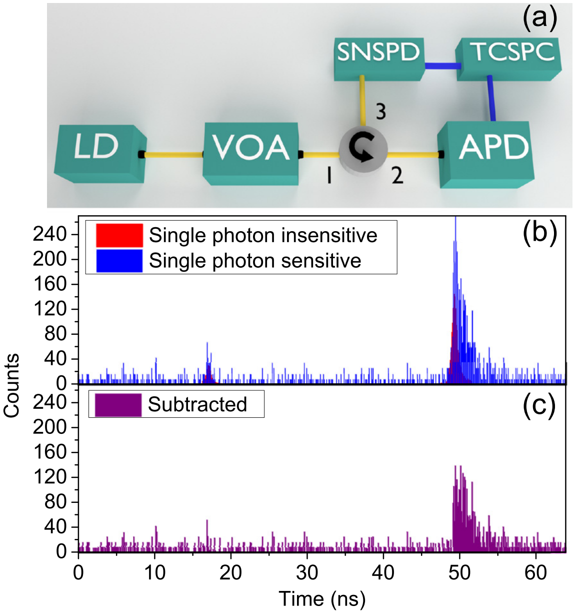

**FIG. 1.** (a) Schematic of the experiment used to investigate APD backflashes. LD: laser diode, VOA: variable optical attenuator, SNSPD: superconducting nanowire single-photon detector, and TCSPC: time-correlated single-photon counter. (b) Histograms of the detection events on the SNSPD when the APD is illuminated with a 0.1 photons/pulse where the total measurement time is 10 s. The x-axis refers to the effective delay with respect to the laser trigger pulse. The APD is biased under two different DC biases: single photon sensitive (blue bars) and single photon insensitive (red bars). (c) Subtracted histogram with backreflections removed, leaving only backflashes.

In order to obtain a true measure of the information leakage, it was necessary to isolate the backreflections. A simple technique for this is simply to neglect them in post processing. This was done by subtracting the SNSPD histogram with the APD turned off so that only backflashes were measured, shown in Fig. 1(c). This large peak also at around 49 ns supports the hypothesis given above that the backflashes are correlated with APD clicks. Measurements were performed for different detection efficiencies by varying the DC bias to the APD, and the subsequent information leakage was then calculated and is plotted as a function of detection efficiency in Fig. 2 alongside the value measured in Ref. 17 for the ID 201 detector. The APD detection efficiency was determined at each point using the technique outlined in Ref. 22.

The data appear initially very noisy at low efficiency. This is due to the SNSPD count rate being similar to its dark count rate, which suggests that the rate of backflashes is very low. We note that it was not possible to extend the measurement time to smooth out the statistics due to the instability of the APD's temperature over time. The data then appear much smoother from an efficiency of 10% as the rate of backflashes increases. As the information leakage remains more or less constant from then on, this suggests that the relationship between backflashes and APD counts is linear. By comparing this to the ID 201 detector, we see an order of magnitude improvement in the information leakage, which supports the hypothesis that shorter gates will emit fewer backflashes.

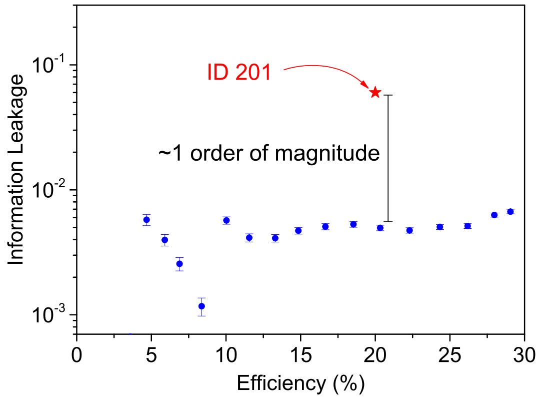

**FIG. 2.** Information leakage plotted as a function of the APD single-photon detection efficiency. The red star indicates the corresponding information leakage for a commercially available APD, ID 201, reported in the literature.[17] The detector under test exhibits an order of magnitude smaller than information leakage, supporting the hypothesis that faster-gated APDs emit fewer backflashes.

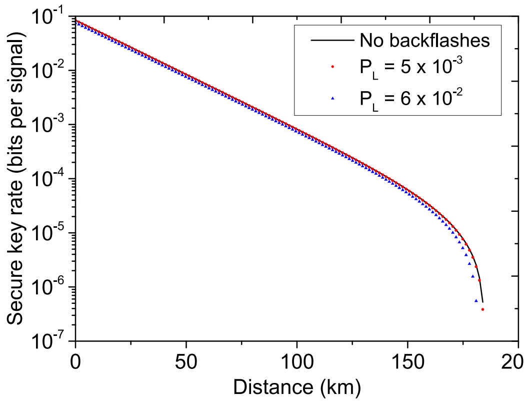

**FIG. 3.** Secure key rate plotted in the absence of backflashes, with the measured information leakage and previous state-of-the-art. Even with $P_L = 6\%$, the effect on the key rate is negligible, as the term $P_L$ gives the exact amount by which the key rate is reduced.

Using the value for information leakage, which is a direct measurement of Eve's information, we can derive a new secure key rate in the presence of backflashes. This has been partially investigated in Ref. 18 where the authors approach the derivation of the key rate from a photon number splitting perspective and treat the information leakage as "tagged" bits but originating from Bob rather than Alice.[23,24] However, the authors in Ref. 18 assume that the backflash probability, and therefore information leakage, remains constant over all distances, which means that they obtain a very pessimistic estimate for the secure key rate. This is because they use the conditional backflash probability (i.e., the probability of a backflash if there is an APD click), whereas the raw, absolute backflash probability would have been more appropriate. In reality, as the information leakage is dependent on an APD click, the APD click probability should also be incorporated into this analysis so that the key rate is affected by the same proportion, regardless of the distance. We use a modified version of the key rate given in Ref. 18 considering single-photon BB84 as follows:

$$R \geq qP_{click}\left[(1 - P_L)\{1 - h(e)\} - \{fh(e)\}\right], \qquad (2)$$

where $q$ is the basis choice probability, $P_{click}$ is the probability of a click on a detector, $P_L$ is the information leakage [defined in Eq. (1)], $h(x)$ is the binary Shannon entropy, $e$ is the quantum bit error rate, and $f$ is the error correction efficiency. It is interesting to note that by simply multiplying the information leakage term by the click probability in the key rate definition from Ref. 18, thereby including a dependence of the backflash probability on the APD detection probability, the equation reduces to Eq. (2).

Using detector characteristics from this study, we plot the key rate as a function of the distance for several values of information leakage, namely, zero, $5 \times 10^{-2}$, which was the previous state-of-the-art, and $5 \times 10^{-3}$, as measured in our own setup, as shown in Fig. 3.

As an information leakage of 0.5% has a negligible effect on the key rate, an isolator would not be needed as a countermeasure since even with a very low insertion loss of 0.2 dB, it would have a greater impact on the key rate. This result provides strong evidence that backflashes are not a significant threat to QKD, even for slower gated detectors where the information leakage is potentially larger. We note, however, that characterizing the spectrum of the backflashes is also important for enforcing this point in order to more accurately determine the information leakage. While this has been partially explored in previous studies,[18–20] these have not corrected for the spectral response of the measurement apparatus. We believe that this is an important avenue for future work, not only from a security perspective but also to shed light on the precise origin of backflashes within APDs.

While we have shown that backflashes have a small effect on the secure key rate, they can still pose a security risk. As shown in Ref. 17, the temporal profile of backflashes appears to be unique for different APDs. This can provide Eve with information on the detectors used by Bob, allowing her to use a tailored attack that is dependent on the type of APD in Bob's system. Therefore, the use of an isolate may still be desirable as a countermeasure.

As a second experiment to probe the origin of the APD backflashes, we switch off the laser and measure the backflashes with the APD kept under dark conditions. We measure the SNSPD count rate

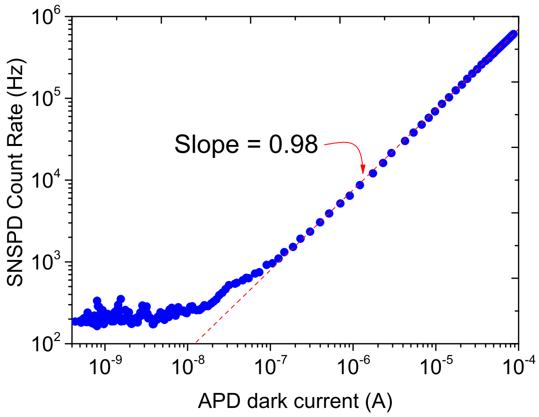

**FIG. 4.** SNSPD count rate as a function of APD dark current. The linear relationship between the two strongly points to backflashes originating in the InP multiplication region.

as a function of the APD dark current by adjusting the DC bias to the APD. The result is given in Fig. 4.

Initially, the SNSPD count rate remains at the dark count level until the APD current reaches a value of approximately 10 nA. After about 100 nA, the data appear to follow a linear trend, and this is confirmed by fitting the data points. This finding supports the hypothesis that backflashes arise from carriers in the multiplication region; a higher dark current arises from the larger electric field increasing the avalanche probability, thereby generating more carriers, which cause backflashes.

In conclusion, we have investigated backflashes in GHz-gated self-differencing InGaAs APDs. By performing the first characterization of the backflash rate in these devices using high efficiency SNSPDs, we have found evidence that supports the hypothesis that shorter gates lead to fewer backflashes. We have shown that the information leakage as a result of backflashes has a negligible effect on the secure key rate in QKD and is, as such, of minimal concern in QKD systems. We have performed characterization, which indicates that backflashes originate in the detector's InP multiplication region.

A.K.-S. gratefully acknowledges the financial support from Toshiba Research Europe Ltd. and the Engineering and Physical Sciences Research Council through an Industrial CASE studentship.

## REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 9–12 (1984), pp. 175–179.

[2] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, 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. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," New J. Phys. **11**(7), 075001 (2009).

[3] 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).

[4] J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, M. Fujiwara, M. Sasaki, and A. J. Shields, "Stability of high bit rate quantum key distribution on installed fiber," Opt. Express **20**(15), 16339–16347 (2012).

[5] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, Q. Zhang, J. Zhang, T.-Y. Chen, and J.-W. Pan, "Integrating quantum key distribution with classical communications in backbone fiber network," Opt. Express **26**(5), 6010–6020 (2018).

[6] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, W. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, "Quantum key distribution with hacking countermeasures and long term field trial," Sci. Rep. **7**(1), 1978 (2017).

[7] D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein, D. Trotter, A. Starbuck, A. Pomerene, S. Hamilton, F. N. C. Wong, R. Camacho, P. Davids, J. Urayama, and D. Englund, "Metropolitan quantum key distribution with silicon photonics," Phys. Rev. X **8**, 021009 (2018).

[8] W. Sun, L.-J. Wang, X.-X. Sun, Y. Mao, H.-L. Yin, B.-X. Wang, T.-Y. Chen, and J.-W. Pan, "Experimental integration of quantum key distribution and gigabit-capable passive optical network," J. Appl. Phys. **123**(4), 043105 (2018).

[9] L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Room temperature single-photon detectors for high bit rate quantum key distribution," Appl. Phys. Lett. **104**(2), 021101 (2014).

[10] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution without detector vulnerabilities using optically seeded lasers," Nat. Photonics **10**(5), 312–315 (2016).

[11] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. Sharpe, A. Dixon, E. Lavelle, J. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, "10-Mb/s quantum key distribution," J. Lightwave Technol. **36**(16), 3427–3433 (2018).

[12] V. Makarov and D. R. Hjelme, "Faked states attack on quantum cryptosystems," J. Mod. Opt. **52**(5), 691–705 (2005).

[13] 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**(10), 686–689 (2010).

[14] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," Nat. Commun. **2**, 349 (2011).

[15] Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Avoiding the blinding attack in QKD," Nat. Photonics **4**(12), 800–801 (2010).

[16] Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography," Appl. Phys. Lett. **98**(23), 231104 (2011).

[17] A. Meda, I. P. Degiovanni, A. Tosi, Z. Yuan, G. Brida, and M. Genovese, "Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution," Light: Sci. Appl. **6**, e16261 (2017).

[18] P. V. P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R. T. Horn, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, "Eavesdropping and countermeasures for backflash side channel in quantum cryptography," Opt. Express **26**(16), 21020–21032 (2018).

[19] L. Marini, R. Camphausen, B. J. Eggleton, and S. Palomba, "Deterministic filtering of breakdown flashing at telecom wavelengths," Appl. Phys. Lett. **111**(21), 213501 (2017).

[20] Y. Shi, J. Z. J. Lim, H. S. Poh, P. K. Tan, P. A. Tan, A. Ling, and C. Kurtsiefer, "Breakdown flash at telecom wavelengths in InGaAs avalanche photodiodes," Opt. Express **25**(24), 30388–30394 (2017).

[21] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, "The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks?," J. Mod. Opt. **48**(13), 2039–2047 (2001).

[22] L. C. Comandar, B. Fröhlich, J. F. Dynes, A. W. Sharpe, M. Lucamarini, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Gigahertz-gated InGaAs/InP single-photon detector with detection efficiency exceeding 55% at 1550 nm," J. Appl. Phys. **117**(8), 083109 (2015).

[23] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Inf. Comput. **4**(5), 325–360 (2004). Available at http://www.theory.caltech.edu/~preskill/pubs/preskill-2004-imperfect.pdf.

[24] H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," Eur. Phys. J. D **41**(3), 599 (2007).