Setting best practice criteria for self-differencing avalanche photodiodes in quantum key distribution

Alexander Koehler-Sidki[1,2], James F. Dynes[1], Marco Lucamarini[1], George L. Roberts[1,2], Andrew W. Sharpe[1], Seb J. Savory[2], Zhiliang Yuan[1], and Andrew J. Shields[1]

[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

ABSTRACT

In recent years, the security of avalanche photodiodes as single photon detectors for quantum key distribution has been subjected to much scrutiny. The most prominent example of this surrounds the vulnerability of such devices to blinding under strong illumination. We focus on self-differencing avalanche photodiodes, single photon detectors that have demonstrated count rates exceeding 1 GCounts/s resulting in secure key rates over 1 MBit/s. These detectors use a passive electronic circuit to cancel any periodic signals thereby enhancing detection sensitivity. However this intrinsic feature can be exploited by adversaries to gain control of the devices using illumination of a moderate intensity. Through careful experimental examinations, we define here a set of criteria for these detectors to avoid such attacks.

Keywords: Quantum key distribution, Avalanche photodiodes, Implementation security

1. INTRODUCTION

Progress in the development of quantum computers, in addition to number theory, can potentially render the security of current cryptographic techniques obsolete. As such, it has become necessary to consider other means for secure communication. Quantum key distribution (QKD) promises information theoretic secure communication which is guaranteed by the laws of physics.[1] Such a technique would thus be immune to any eavesdropping attempts, whether by a quantum or so-called classical computer. The technology has rapidly been brought to maturity during the past decade, with secure key rates exceeding 1 Mbit/s [Ref. 2] and communication distances covering hundreds of kilometers.[3]

However, the components used for its implementation can deviate from their ideal behaviour and this can create loopholes which an eavesdropper, conventionally known as Eve, can exploit to gain knowledge of a final key by means of a side-channel attack.[4] Such loopholes can be removed through the development of new QKD protocols which consider imperfections in practical QKD implementations. One prominent example is the decoy state protocol, which permits efficient key distribution with attenuated laser sources and is secure against photon number splitting attacks.[5,6] A complementary and equally important approach is to develop a set of best practice criteria for QKD manufacturers and users in order to implement and operate QKD in a secure manner.[7] For example,in Refs. 8 and 9 criteria to prevent the Trojan-horse attack targeting imperfections in the modulation optics have been developed and successfully applied.

Attacks on single photon detectors have attracted significant research attention,[10–13] because they are central to a QKD system and are naturally exposed to Eve's optical manipulation through the quantum channel. In the so-called blinding attacks, Eve forces the receiver's, known as Bob, semiconductor avalanche photodiodes (APDs) to lose their single photon sensitivity by injecting strong laser light into the quantum channel. This attack was demonstrated to be effective against early commercial QKD systems containing MHz gated InGaAs

Further author information: (Send correspondence to A. K-S)
A. K-S.: E-mail: Alex.Koehler-Sidki@crl.toshiba.co.uk

detectors.[10] These attacks are avoidable due to the intrinsic gain modulation effect in gated InGaAs APDs when the detector circuits are appropriately set.[14,15]

Significant advances have been achieved recently in single photon detection technologies using semiconductor InGaAs APDs.[16] With sine-wave gating[17] and self-differencing (SD) techniques,[18] InGaAs APDs can now be gated at a clock rate exceeding 1 GHz and have a single photon detection efficiency up to 55%.[19] Gigahertz gated InGaAs APDs have thus drastically improved the QKD secure key rate.[20–24] To ensure the security of these systems, it is necessary to develop a set of criteria for correctly setting these detectors, thus avoiding similar attacks that successfully targeted early QKD systems. Here, we approach this goal by carefully characterising gigahertz-clocked SD detectors under strong continuous wave illumination. We pay particular attention to the chosen discrimination level and how to correctly choose this value. We go on to show that, if this prescription is followed, the blinding described above cannot succeed.

2. GEIGER MODE OPERATION AND ITS VULNERABILITY TO BLINDING ATTACKS

In this section we briefly review Geiger mode APDs and the technique used to blind them. Original implementations of these devices involved the use of passive quenching. This involved the placing of a resistor in series between the DC source and the APD.[25] Its purpose was the suppression of avalanches which would otherwise be self-sustaining and forbid the APD from further detection. Due to the long hold-off time of this technique, gating was developed in order to improve the count rates. This method involves applying a DC voltage just below the device's breakdown voltage and then periodically biasing it above and below this value with an AC signal, shown in a circuit diagram in Figure 1. The periodic gating is in itself the quenching mechanism as the act of bringing the bias below the breakdown voltage suppresses further avalanches, therefore making the use of an additional resistor redundant. The amount of voltage applied over the breakdown voltage is known as the excess voltage, V_{ex}.

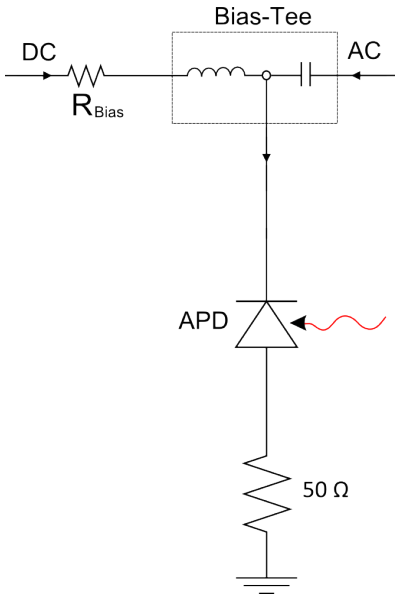

Figure 1. Circuit diagram of a conventional gated Geiger mode APD

Attacks on these detectors have exploited the impedance existing in the DC path, labeled as R_{Bias} in Figure 1. By illuminating the detector with very intense light, the product of the generated photocurrent and the aforementioned impedance causes the bias to the APD to lower such that no excess voltage can be achieved and therefore the detector never enters Geiger mode. Consequently it is no longer sensitive to single photons and behaves as a photocurrent detector. Eve can then apply her own strong pulses and thus control when the detector registers a click.[10] It has however been shown that if these detectors are operated appropriately such

an attack cannot succeed. In this context, this required removing the unnecessary bias resistor in the circuit (or at least reducing its impedance) and setting an appropriate discrimination level.[15]

3. PRINCIPLE OF THE SELF-DIFFERENCING CIRCUIT

In contrast to conventional gated mode operation, the self-differencing circuit cancels out the APD capacitive response and therefore SD APDs can detect extremely weak avalanches thereby allowing gigahertz clocked operation. This involves taking the output signal of a gated APD and splitting it in two. One arm is then delayed by one gating period, i.e. 1 ns for a 1 GHz gated APD as in this study. The two arms are then combined by means of a differencer. This results in the cancellation of the capacitive response leaving only the avalanche, which is a positive and negative peak, in the remaining signal, as shown in Figure 2.

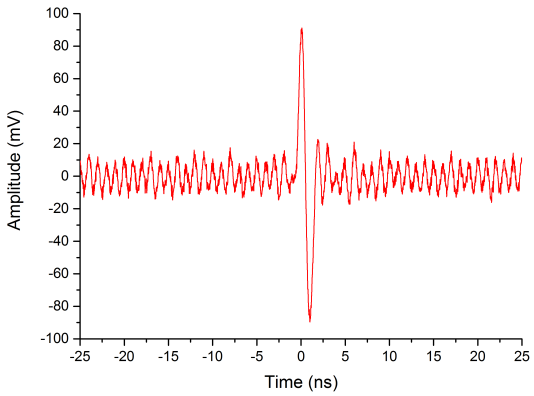

Figure 2. Example waveform showing a self-differenced avalanche.

However, the background cancellation technique can also affect the avalanche signals themselves. It is impossible to discriminate two consecutive, identical avalanches by a SD detector, because of cancellation by the SD. In theory, this effect can allow Eve to completely blind the detector with a moderate optical power. By illuminating the APD with CW light of sufficient intensity, it is possible to deterministically produce an avalanche with each gate, thereby forcing a complete cancellation of avalanche signals and bringing the detection count rate to zero.[13,26] Assuming identical avalanche amplitudes, the detection probability (P_{det}) can be simulated using

$$P_{det} = (1 - e^{-\mu\eta}) \cdot e^{-\mu\eta}, \tag{1}$$

where the first term is the probability that an avalanche occurs in a gate. The following term is then the probability of no avalanche occurring in the following gate. It can be seen that as $\mu\eta$ becomes very large the second term, and therefore the whole expression, tends to zero.

We can estimate the optical power required to blind a conventional gated detector with the mechanism described in section 2. The actual excess voltage whilst the APD is under illumination can be described with the following

$$V'_{ex} = V_{ex} - I \cdot R_{bias}, \tag{2}$$

where I is the generated photocurrent. This shows that if both I and R_{bias} are reasonably large, it is possible to make V'_{ex} zero or negative. This highlights the importance of making R_{bias} as small as possible. However removing the bias resistor does not cause this to be zero as an intrinsic resistance exists in the circuit which

we measure to be approximately $1k\Omega$. Assuming an excess voltage of 4.4 V, an incident optical power of larger than 4.4 mW is required to bring the APD out of Geiger mode. By examining equation 1, we can see that an incident optical power of just under 60 nW is sufficient to blind a 1 GHz gated SD detector (assuming a pulsed laser of the same repetition frequency and a detection efficiency of 10 %), nearly 5 orders of magnitude smaller. Since the required optical power for blinding is much smaller, it makes detection of an eavesdropper through monitoring of the photocurrent[15] less straightforward.

4. OPERATING AND CHARACTERISING THE APD

Figure 3 shows the schematic for the charcterisation setup for self-differencing detectors. A commercial InGaAs/InP APD is electrically biased through a bias-T with a square wave input clocked at of 1 GHz applied using a pulse generator as the AC input, superimposed on top of a constant DC bias provided by a source measure unit. The APD is thermo-electrically cooled to - 30 ° C. The APD is illuminated by a laser, the intensity of which is controlled by a cascade of two variable optical attenuators providing 120 dB intensity variation range. The output of the APD signal is fed into a self-differencing circuit before being measured by either an oscilloscope or a photon counter.

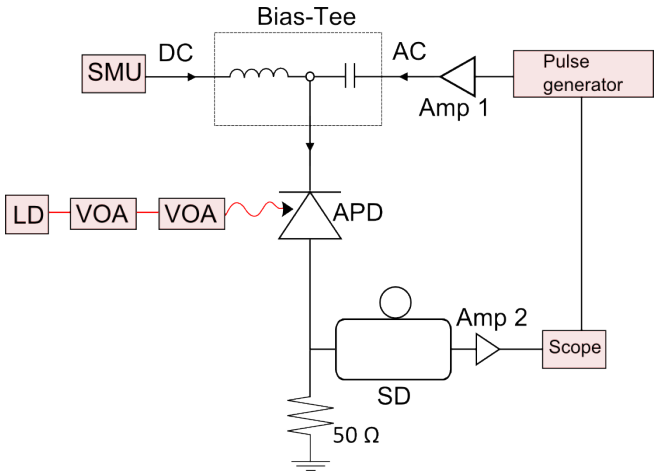

Figure 3. Schematic of the experimental set-up. SMU: Source Measure Unit; LD: Laser Diode; VOA: Variable Optical Attenuator: SD: Self-differencer.

When first setting up the detector it is important to carry out a series of steps in order to systematically arrive at the most appropriate way of operating it. This prescription is given as follows:

- Determine the APD's breakdown voltage. This is taken as the point at which the generated current exceeds 10 μA[27] when the APD is biased with the DC signal only and without optical illumination. The breakdown voltage of the APD under test is found to be 51.8 V.
- Set the initial DC and AC biases. The initial DC bias is set just below the breakdown voltage. An AC signal is set at a sufficient level to enable single photon avalanches, i.e., approximately 5-10 V. In the present case, we choose 51.6 V ($V_{DC}^{(1)}$) and 4.6 V ($V_{AC}^{(1)}$) for DC and AC signals, respectively.
- Set a coarse discrimination level. This is set by lowering the DC bias such that the APD never experiences any excess bias and therefore does not produce any single-photon or dark counts. Under this condition, the SD output contains only the uncanceled background signal. The coarse discrimination level is set as the lowest level with which the counting electronics produces a count rate of zero such that all of the background is neglected. This coarse discrimination level can then be used when varying the DC and AC signals to find the optimum detector characteristics as in the next step.
- Optimise the biasing conditions. This involves adjusting the DC and AC levels around $V_{DC}^{(1)}$ and $V_{AC}^{(1)}$ to optimise the detector performance, such as detection efficiency, dark count rate and afterpulse probability.

The detailed procedure for this step can be found in a previous publication.[19] We refer to the optimised bias values as $V_{DC}^{(2)}$ and $V_{AC}^{(2)}$.

- Set the final discrimination level under the optimal biases of $V_{DC}^{(2)}$ and $V_{AC}^{(2)}$. This step is necessary because the capacitance of an APD is bias dependent and so is the uncancelled capacitive signal background. Under dark conditions, the detector count rate is measured as a function of the discrimination level. An example result is shown in Fig. 4. The point where the count rate changes dramatically signals the detection of the noise floor. Therefore, one should choose a discrimination level just above this to ensure an optimal detection efficiency while rejecting all uncancelled capacitive background contributing to the dark counts.

Following the above steps, the discrimination level for the APD under test is set to 18 mV. The corresponding detection efficiency and dark count rate are determined to be 26% and 22 kHz, respectively.

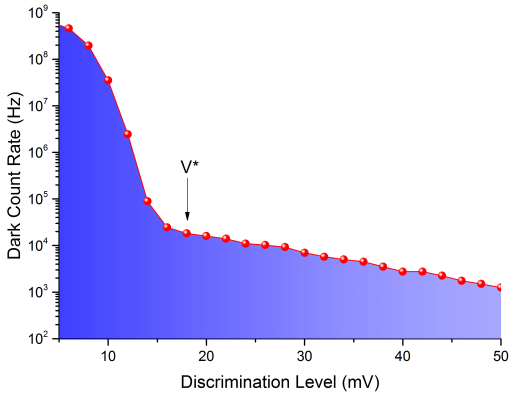

Figure 4. A graph showing the count rate as a function of discrimination level. V* indicates the value corresponding to an appropriate choice of level.

5. SD APD UNDER STRONG ILLUMINATION

Having set the operating conditions and determined the APD's characteristics, we then examine the behavior of the SD APD under strong optical illumination. A 1606 nm continuous wave diode laser is used for illumination. This wavelength laser was chosen because it can offer the optical power that is required to achieve strong illumination. At this illumination wavelength, the APD was found to exhibit a similar quantum efficiency to the more standard telecom wavelength of 1550 nm. We measure the photon count rate as a function of the incident photon flux ranging from 10^{-5} to 10^{8} photons per ns for two different discrimination levels. The first of these is set appropriately at 18 mV whereas the second one is very inappropriately set at 35 mV. The measurement results are shown in Figure 5.

At low photon fluxes (<10 photons per ns), the photon count rates show a linear dependence with the incident optical power, suggesting that the APD is behaving as a single photon detector. Further increasing the incident optical power leads first to count rate saturation and then the count rate drop for photon fluxes exceeding 10^4 per ns. This drop is a result of SD cancellation, as predicted by equation 1. However, when using an appropriate discrimination level, the count rate does not drop to zero, contrary to the aforementioned prediction. The count rate even recovers at very high photon fluxes.

We note that the experimentally measured count rates drop much slower than the prediction in 1 at photon fluxes > 10. As has previously been reported,[13,26] part of the reason for this disagreement is that the simulation assumes the avalanche amplitudes are photon number independent. In reality this is not true as such detectors have even been shown to have photon number resolving capabilities.[28] This means that since adjacent avalanches may have different amplitudes they may not always cancel to below the set discrimination level.

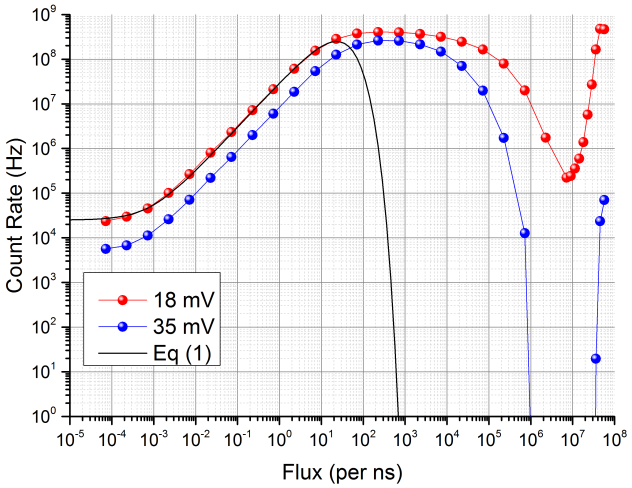

Figure 5. Count rate as a function of incident flux for discrimination levels of 18 and 35 mV with a plot of the simulation in equation 1

We attribute the count rate recovery to the intensity fluctuation of the laser diode, which we measure to be 0.6%. We further confirm this attribution by reducing the bias current to our laser so that the intensity fluctuations are now 9.2% we find that recovery occurs sooner.

In the case when the inappropriate discrimination level of 35 mV is used, the detector can be completely blinded, i.e., the count rate falling to zero, for photon fluxes between 10^6 and 5×10^7. This highlights that the detector has become vulnerable to blinding attacks.

6. DISCUSSION

In the previous section, we demonstrated that the behavior of the detector under strong illumination is closely linked to the choice of discrimination level as well as the intensity stability of the laser used for the blinding attack. Under an inappropriately high discrimination level, it is straightforward to blind a SD detector with a continuous-wave laser of moderate power, suggesting that incorrectly set detectors exhibit security loopholes. We therefore stress the importance of following the procedure given in section 4. Once this prescription is followed, it is significantly harder for Eve to blind the detector. A small intensity fluctuation existing in the laser output can effectively prevent the detector from being blinded because of the sensitivity of self-differencing circuits to non-periodic signal variations. Even with a perfectly stable laser source, it may still be difficult for Eve to blind a SD detector in a QKD setup due to the instability in Bob's interferometer which may cause fluctuations in the optical signal reaching the detectors. For example, QKD that employs active basis choice can easily bring an intensity fluctuation of signals reaching an individual detector.

In conclusion we have examined how to best operate and characterise an SD APD. We have established the best procedure for setting an appropriate discrimination level and have shown that this ensures the self-differencer cannot be completely blinded with an ordinary diode laser with fluctuating intensity output.

REFERENCES

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

[2] Lucamarini, M., Patel, K. A., Dynes, J. F., Fröhlich, B., Sharpe, A. W., Dixon, A. R., Yuan, Z. L., Penty, R. V., and Shields, A. J., "Efficient decoy-state quantum key distribution with quantified security," *Opt. Express* **21**, 24550–24565 (Oct 2013).

[3] Korzh, B., Lim, C. C. W., Houlmann, R., Gisin, N., Li, M. J., Nolan, D., Sanguinetti, B., Thew, R., and Zbinden, H., "Provably secure and practical quantum key distribution over 307km of optical fibre," *Nature Photonics* **9**, 163168 (Sep 2015).

[4] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M., "The security of practical quantum key distribution," *Reviews of Modern Physics* **81**, 1301–1350 (Sept. 2009).

[5] Lo, H.-K., Ma, X., and Chen, K., "Decoy state quantum key distribution," *Phys. Rev. Lett.* **94**, 230504 (Jun 2005).

[6] Wang, X.-B., "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.* **94**, 230503 (Jun 2005).

[7] Allaume, R., Degiovanni, I. P., Mink, A., Chapuran, T. E., Lütkenhaus, N., Peev, M., Chunnilall, C. J., Martin, V., Lucamarini, M., Ward, M., and Shields, A., "Worldwide standardization activity for quantum key distribution," in [*2014 IEEE Globecom Workshops (GC Wkshps)*], 656–661 (Dec 2014).

[8] Lucamarini, M., Choi, I., Ward, M., Dynes, J., Yuan, Z., and Shields, A., "Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution," *Physical Review X* **5**, 031030 (Sept. 2015).

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

[10] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., and Makarov, V., "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics* **4**, 686–689 (Oct. 2010).

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

[12] da Silva, T. F., Xavier, G. B., P. Temporão, G., and von der Weid, J. P., "Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems," *Opt. Express* **20**, 18911–18924 (Aug 2012).

[13] Jiang, M.-S., Sun, S.-H., Tang, G.-Z., Ma, X.-C., Li, C.-Y., and Liang, L.-M., "Intrinsic imperfection of self-differencing single-photon detectors harms the security of high-speed quantum cryptography systems," *Physical Review A* **88**, 062335 (Dec. 2013).

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

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

[16] Zhang, J., Itzler, M. A., Zbinden, H., and Pan, J.-W., "Advances in InGaAs/InP single-photon detector systems for quantum communication," *Light: Science & Applications* **4**, e286 (May 2015).

[17] Namekata, N., Sasamori, S., and Inoue, S., "800 MHz single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating," *Opt. Express* **14**, 10043–10049 (Oct 2006).

[18] Yuan, Z. L., Kardynal, B. E., Sharpe, A. W., and Shields, A. J., "High speed single photon detection in the near infrared," *Applied Physics Letters* **91**(4), 041114 (2007).

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

[20] Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W., and Shields, A. J., "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," *Opt. Express* **16**, 18790–18797 (Nov 2008).

[21] Namekata, N., Takesue, H., Honjo, T., Tokura, Y., and Inoue, S., "High-rate quantum key distribution over 100 km using ultra-low-noise, 2-GHz sinusoidally gated InGaAs/InP avalanche photodiodes," *Opt. Express* **19**, 10632–10639 (May 2011).

[22] Walenta, N., Lunghi, T., Guinnard, O., Houlmann, R., Zbinden, H., and Gisin, N., "Sine gating detector with simple filtering for low-noise infra-red single photon detection at room temperature," *Journal of Applied Physics* **112**(6), 063106 (2012).

[23] Yoshino, K., Ochi, T., Fujiwara, M., Sasaki, M., and Tajima, A., "Maintenance-free operation of wdm quantum key distribution system through a field fiber over 30 days," *Opt. Express* **21**, 31395–31401 (Dec 2013).

[24] Fröhlich, B., Lucamarini, M., Dynes, J. F., Comandar, L. C., Tam, W. W.-S., Plews, A., Sharpe, A. W., Yuan, Z., and Shields, A. J., "Long-distance quantum key distribution secure against coherent attacks," *Optica* **4**, 163–167 (Jan 2017).

[25] Gallivanoni, A., Rech, I., and Ghioni, M., "Progress in Quenching Circuits for Single Photon Avalanche Diodes," *IEEE Transactions on Nuclear Science* **57** (Dec. 2010).

[26] Dynes, J. F., Yuan, Z. L., Sharpe, A. W., and Shields, A. J., "A high speed, postprocessing free, quantum random number generator," *Applied Physics Letters* **93**(3), 031109 (2008).

[27] Jiang, X., Itzler, M. A., Ben-Michael, R., and Slomkowski, K., "InGaAsP-InP Avalanche Photodiodes for Single Photon Detection," *IEEE Journal of Selected Topics in Quantum Electronics* **13**(4), 895–905 (2007).

[28] Kardynal, B. E., Yuan, Z. L., and Shields, A. J., "An avalanche photodiode-based photon-number-resolving detector," *Nature Photonics* **2**(7), 425–428 (2008).