Controlling an actively-quenched single photon detector with bright light

Sebastien Sauge,[1] **Lars Lydersen,**[2,3] **Andrey Anisimov,**[4]
Johannes Skaar[2,3] **and Vadim Makarov**[2,3*]

[1]*School of Information and Communication Technology, Royal Institute of Technology (KTH),
Electrum 229, SE-16440 Kista, Sweden*
[2]*Department of Electronics and Telecommunications, Norwegian University of Science and
Technology, NO-7491 Trondheim, Norway*
[3]*University Graduate Center, NO-2027 Kjeller, Norway*
[4]*Radiophysics Department, St. Petersburg State Polytechnical University, Politechnicheskaya
street 29, 195251 St. Petersburg, Russia*

[*]makarov@vad1.com

Abstract: We control using bright light an actively-quenched avalanche single-photon detector. Actively-quenched detectors are commonly used for quantum key distribution (QKD) in the visible and near-infrared range. This study shows that these detectors are controllable by the same attack used to hack passively-quenched and gated detectors. This demonstrates the generality of our attack and its possible applicability to eavsdropping the full secret key of all QKD systems using avalanche photodiodes (APDs). Moreover, the commercial detector model we tested (PerkinElmer SPCM-AQR) exhibits two new blinding mechanisms in addition to the previously observed thermal blinding of the APD, namely: malfunctioning of the bias voltage control circuit, and overload of the DC/DC converter biasing the APD. These two new technical loopholes found just in one detector model suggest that this problem must be solved in general, by incorporating generally imperfect detectors into the security proof for QKD.

© 2011 Optical Society of America

OCIS codes: (270.5568) Quantum cryptography; (040.1345) Avalanche photodiodes (APDs); (270.5570) Quantum detectors.

References and links

1. Commercial QKD systems are available from at least two companies: ID Quantique (Switzerland), http://www.idquantique.com; MagiQ Technologies (USA), http://www.magiqtech.com.
2. R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," Nat. Phys. **3**, 481–486 (2007).
3. D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," New J. Phys. **11**, 075003 (2009).
4. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature **299**, 802–803 (1982).
5. D. Mayers, "Advances in cryptology," in *Proceedings of Crypto'96,* vol. 1109, N. Koblitz, ed. (Springer, New York, 1996), vol. 1109, pp. 343–357.
6. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quant. Inf. Comp. **4**, 325–360 (2004).
7. Ø. Marøy, L. Lydersen, and J. Skaar, "Security of quantum key distribution with arbitrary individual imperfections," Phys. Rev. A **82**, 032337 (2010).
8. M. Koashi, "Simple security proof of quantum key distribution based on complementarity," New J. Phys. **11**, 045018 (2009).

9. 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).

10. C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "After-gate attack on a quantum cryptosystem," New J. Phys. **13**, 013043 (2011).

11. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Thermal blinding of gated detectors in quantum cryptography," Opt. Express **18**, 27938–27954 (2010).

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

13. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Reply to 'Avoiding the blinding attack in QKD'," Nat. Photonics **4**, 801 (2010).

14. 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**, 231104 (2011).

15. L. Lydersen, V. Makarov, and J. Skaar, "Comment on 'Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography'," arXiv:1106.3756 [quant-ph].

16. Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Reply to "Comment on 'Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography'"," arXiv:1109.3149 [quant-ph].

17. 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).

18. PerkinElmer SPCM-AQR single photon counting module, data sheet, PerkinElmer (2005).

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

20. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in "Proc. IEEE International Conference on Computers, Systems, and Signal Processing" (IEEE Press, New York, Bangalore, India, 1984), pp. 175–179.

21. J. G. Rarity, P. C. M. Owens, and P. R. Tapster, "Quantum random-number generation and key sharing," J. Mod. Opt. **41**, 2435–2444 (1994).

22. M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, "Daylight operation of a free space, entanglement-based quantum key distribution system," New J. Phys. **11**, 045007 (2009).

23. R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," New J. Phys. **4**, 43 (2002).

24. C. Erven, C. Couteau, R. Laflamme, and G.Weihs, "Entangled quantum key distribution over two free-space optical links," Opt. Express **16**, 16840–16853 (2008).

25. S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, "Evolution and prospects for single-photon avalanche diodes and quenching circuits," J. Mod. Opt. **51**, 1267–1288 (2004).

26. T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**, 010303 (1999).

27. M. Hillery, "Quantum cryptography with squeezed states," Phys. Rev. A **61**, 022309 (2000).

28. M. D. Reid, "Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations," Phys. Rev. A **62**, 062308 (2000).

29. M. Heid and N. Lütkenhaus, "Security of coherent-state quantum cryptography in the presence of Gaussian noise," Phys. Rev. A **76**, 022313 (2007).

30. S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, "Field test of a continuous-variable quantum key distribution prototype," New J. Phys. **11**, 045023 (2009).

31. G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski, "Picosecond superconducting single-photon optical detector," Appl. Phys. Lett. **79**, 705–707 (2001).

32. A. Verevkin, J. Zhang, R. Sobolewski, A. Lipatov, O. Okunev, G. Chulkova, A. Korneev, K. Smirnov, G. N. Gol'tsman, and A. Semenov, "Detection efficiency of large-active-area NbN single-photon superconducting detectors in the ultraviolet to near-infrared range," Appl. Phys. Lett. **80**, 4687–4689 (2002).

33. V. Makarov, "Controlling passively quenched single photon detectors by bright light," New J. Phys. **11**, 065003 (2009).

34. R. T. Thew, H. Zbinden, and N. Gisin, "Tunable upconversion photon detector," Appl. Phys. Lett. **93**, 071104 (2008).

35. R. T. Thew, D. Stucki, J.-D. Gautier, H. Zbinden, and A. Rochas, "Free-running InGaAs/InP avalanche photo-diode with active quenching for single photon counting at telecom wavelengths," Appl. Phys. Lett. **91**, 201114 (2007).

36. id210 advanced system for single photon detection, data sheet, ID Quantique (2011), http://www.idquantique.com/images/stories/PDF/id210-single-photon-counter/id210-specs.pdf (accessed on 1 August 2011).

37. H. Dautet, P. Deschamps, B. Dion, A. D. MacGregor, D. MacSween, R. J. McIntyre, C. Trottier, and P. P. Webb, "Photon counting techniques with silicon avalanche photodiodes," Appl. Opt. **32**, 3894–3900 (1993).

38. PerkinElmer SPCM-AQ4C single photon counting module array, data sheet, PerkinElmer (2005).

39. K. J. Gordon, V. Fernandez, P. D. Townsend, and G. S. Buller, "A short wavelength gigahertz clocked fiber-optic quantum key distribution system," IEEE J. Quantum Electron. **40**, 900–908 (2004).

40. L. Lydersen, V. Makarov, and J. Skaar, "Secure gated detection scheme for quantum cryptography," Phys. Rev.

A **83**, 032306 (2011).

41. L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "Superlinear threshold detectors in quantum cryptography," Phys. Rev. A **84**, 032320 (2011).
42. H.-K. Lo, M. Curty, and B. Qi, "Measurement device independent quantum key distribution," arXiv:1109.1473 [quant-ph].
43. S. L. Braunstein and S. Pirandola, "Side-channel free quantum key distribution," arXiv:1109.2330 [quant-ph].
44. L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, "Controlling a superconducting nanowire single-photon detector using tailored bright illumination," arXiv:1106.2396 [quant-ph].

1. Introduction

Over the past twenty years, quantum key distribution (QKD) has progressed from a tabletop demonstration to commercially available systems [1], with secure key exchange demonstrated up to 144 km in free-space [2] and 250 km in optical fibers [3]. Security of these cryptosystems is based on the impossibility, in principle, to reliably copy an *a priori* unknown quantum state, as accounted for by the no-cloning theorem [4]. However, security also relies on the assumption that the optical and electro-optical devices which are part of quantum cryptosystems do not deviate from model assumptions made to establish security proofs [5–8].

Recently, it has been demonstrated that both commercial QKD systems available on the market in 2009 could be fully cracked [9–11]. A tailored bright illumination was employed to remote-control gated avalanche photodiodes (APDs) used to detect single photons in these QKD systems. Note that these publications raised discussions regarding technique's applicability to QKD systems from other developers [12, 13], as well as how such loopholes should be tackled [14–16]. In another work, a full eavesdropper has been implemented on a research system using passively-quenched APDs [17]. The overall purpose of the work reflected in this paper is two-fold. First, we establish the generality of this attack, by extending its validity to QKD systems employing actively-quenched APDs. Second, we demonstrated two new control mechanisms in just one detector model (a commonly used commercial module, PerkinElmer SPCM-AQR [18]). The latter finding supports the opinion that efficient countermeasures must rely on a general security proof based on a sufficiently general detector model, as opposed to incremental 'intuitive' technical patches.

The paper is organized as follows. In the next section, we recap the general scheme of attack which can in principle be implemented using this detector vulnerability. In sections 3–5, we demonstrate that this particular detector, as other models tested before, fulfills the general conditions proposed for 100% eavesdropping of the cryptographic key. We discuss countermeasures in section 6, and conclude in section 7.

2. Proposed attack

From eavesdropper's point of view, the *intercept-resend attack* provides a general framework to exploit unaccounted non-idealities or operating modes of components. In this attack, we assume that the eavesdropper Eve owns an exact replica of receiver Bob's detection apparatus, with which she intercepts and measures the state of each qubit sent by Alice. To successfully eavesdrop, Eve must resend faked states [19] that will force her detection results onto Bob's in a transparent way. Ideally, the faked state should make the target detector click controllably (with unity probability and near zero time-jitter) while keeping any other detector blind (no click). In the Bennett-Brassard 1984 (BB84) [20] and similar four-state protocols, Bob must detect two bit values in two bases, which can be implemented with two pairs of detectors. One pair detects bit values "0" and "1", and a second pair (not necessary with active basis choice) detects in the conjugate measurement basis, which is randomly selected prior to detection of each qubit in order to guarantee security against eavesdropping. Thus in 50% of the cases, the qubit resent by Eve will be measured by Bob in the conjugate basis, resulting in a random outcome. Similarly, if
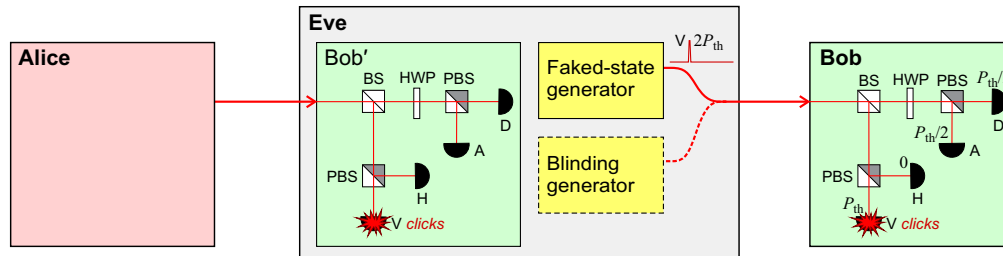
Fig. 1. Intercept-resend (faked-state) attack Eve could launch against a QKD system which runs a four-state protocol with polarization coding and passive choice of basis [21–24]. In the example, Eve targets the detector recording vertically polarized qubits in the horizontal/vertical (H/V) basis. We assume here that detectors click controllably when illuminated by an optical pulse with peak power $\geq P_{th}$, and that they are blind (or kept blind) at power $\leq P_{th}/2$ (characteristics of the 'blinding generator' potentially needed to bring detectors in this working mode will be described later). To address the target detector, Eve sends a faked state with V polarization and power $2P_{th}$, thus the V detector receives power P_{th} after basis choice, and clicks. The detectors recording polarized qubits in the conjugate (45°-rotated, D/A) basis each receive a pulse of power $P_{th}/2$, and thus remain blinded. In the diagram: BS, 50:50% beamsplitter; PBS, polarizing beamsplitter; HWP, half-wave plate rotated 22.5°.

the photonic qubit is replaced by a classical pulse of peak power P_{th}, an incompatible choice of basis will result in arrival of pulses of power $P_{th}/2$ at both detectors [9, 17]. Let us now assume that under some conditions, detectors remain blind at power $P_{th}/2$ and click controllably at threshold power P_{th}. With the latter pulse, Eve can selectively address the target detector without causing a click in the conjugate basis. This is illustrated in Fig. 1 in the case of a QKD system running a four-state protocol with polarization coding and passive choice of basis at Bob's side. After Bob reveals in which bit slots he has registered detections, Eve will have the same raw key bit sequence as Bob. Eve thus can extract the final secret key by listening to the classical public communication between Alice and Bob and doing the same post-processing operations as Bob [9, 17]. Thus, providing that the above assumption of the detector threshold behavior is satisfied, QKD systems using such detectors are vulnerable.

Let us now explain how this assumption can be fulfilled. Most QKD systems today use *avalanche photodiodes* (APDs) to detect single photons [25]. (The two notable exceptions are continuous-variable QKD systems [26–30] and those using superconducting detectors [3, 31, 32].) For single-photon sensitivity, APDs are operated in so-called Geiger mode, i.e., they are biased above the breakdown voltage so that an absorbed photon triggers an avalanche. (In case of gated-mode operation, the APD is biased above breakdown only during the gate time to limit noise [9, 25].) The avalanche current is sensed by a comparator before the avalanche is quenched to reset the diode. Quenching is achieved by lowering (passively or actively) the bias voltage below breakdown [25]. In the latter condition, however, the APD is no longer in the single-photon detection mode but behaves as a classical photodiode generating photocurrent proportional to the optical illumination. It is thus insensitive to single photons, but also to noise sources (dark counts, afterpulses). However, it is still possible to make the APD click controllably since in this classical photodiode mode, the comparator threshold translates to a classical optical power threshold P_{th}. Providing the threshold is well-defined, no click will ever occur at power $P_{th}/2$, and Eve has at her disposal a very general attack for breaking the security of most APD-based QKD systems.

3. Blinding and controlling an actively-quenched single-photon detector

In the case of the two recently-hacked commercial QKD systems operating at telecom wavelengths [9], transition from Geiger to classical photodiode mode was achieved by using continuous-wave (c.w.) bright illumination to reduce APD bias voltage below breakdown. Equivalently, raising the breakdown voltage above the fixed bias voltage by heating the APDs also led to blinding and control of the detectors [11].

In this paper, we illustrate further the generality of the attack by taking full control of a commercial actively-quenched detector model PerkinElmer SPCM-AQR module [18]). Until recently, the SPCM-AQR has been the only commercially available unit among actively-quenched modules. The latter account for about half of the 28 QKD experiments using non-gated detectors reported in the literature (the other half uses passively-quenched detectors) [33]. It thus makes the SPCM-AQR an obvious choice for testing. Moreover, such detectors may be used after upconverting telecom-wavelength qubits into the visible and near-infrared range, where Si modules have better detection characteristics [34]. Free-running, actively-quenched InGaAs/InP APDs for telecom wavelenghts have also recently been introduced [35, 36]. Obviously, one would rather study security and control mechanisms of actively-quenched detectors before (rather than after) they get incorporated into commercial QKD systems.

In the case of SPCM-AQR detector model, we achieved transition to classical photodiode mode by applying not c.w. (as for gated detectors) but instead bright pulsed illumination at the level of less than $10\,\mathrm{mW}$ at $\geq 70\,\mathrm{kHz}$ repetition rate. Between the pulses, the detector is blind to single photons, and does not produce dark counts or afterpulses. However, it clicks controllably if a classical light pulse $\geq P_{\mathrm{th}}$ is applied, as illustrated in Fig. 2.

4. Blinding mechanisms

Figure 3(a) shows at which optical pulse frequencies blinding of the detector is achieved, and the corresponding bias voltage at the APD. We identified three distinct mechanisms responsible for blinding. Each mechanism is activated in a different range of control pulse frequencies, as
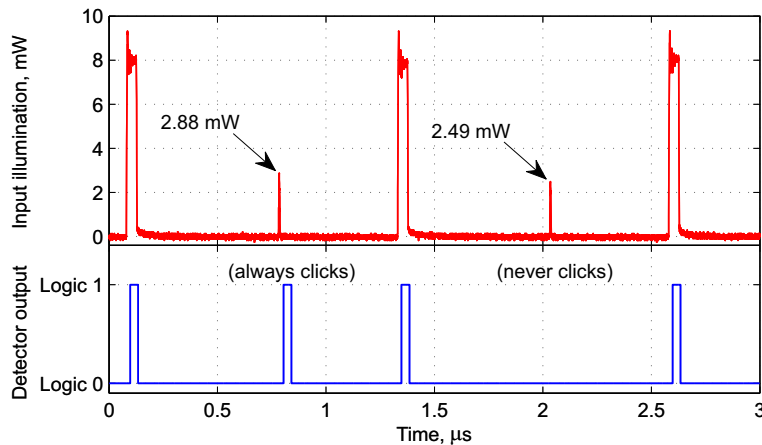

Fig. 2. Oscillogram at detector output (lower trace) illuminated by bright optical pulses (upper trace) made of control pulses ($808\,\mathrm{nm}$, $8\,\mathrm{mW}$, $50\,\mathrm{ns}$ wide, $800\,\mathrm{kHz}$ repetition rate) to blind the detector, and of weaker trigger pulses ($8\,\mathrm{ns}$ wide). The trigger pulses make the detector click with unity probability and sub-nanosecond time jitter *only* above a certain power threshold. In the example, detector always clicks at $P_{\mathrm{th}} = 2.88\,\mathrm{mW}$ peak power trigger pulses, never clicks at $\leq 2.49\,\mathrm{mW}$.
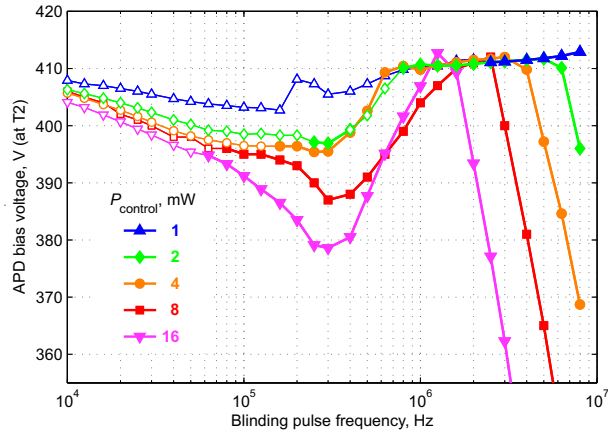
(a)
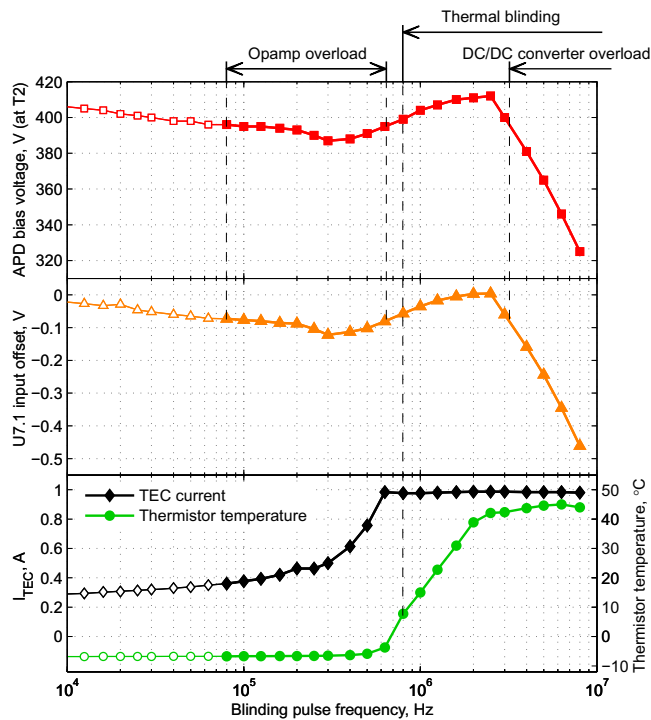
(b)

Fig. 3. Detector blinding: (a) APD bias voltage vs. frequency and peak optical power $P_{control}$ of rectangular 50 ns wide input optical pulses. Normal bias voltage at low count rate for this detector sample is 410 V (the other detector sample we tested had bias voltage of 350 V). Filled symbols denote pulse parameters at which the detector got completely blind between the control pulses. (b) Parameters in the circuit vs. frequency of optical pulses with peak power $P_{control} = 8$ mW. Behavior of these parameters reveals three blinding mechanisms summarized over the top of the chart. The middle chart shows static voltage difference between the inputs of opamp, controlling the APD bias voltage (as similarity of the two top charts confirms). The lower chart shows current of the thermoelectric cooler (TEC) and the temperature of the APD as measured by a thermistor mounted nearby at the cold plate of the TEC.
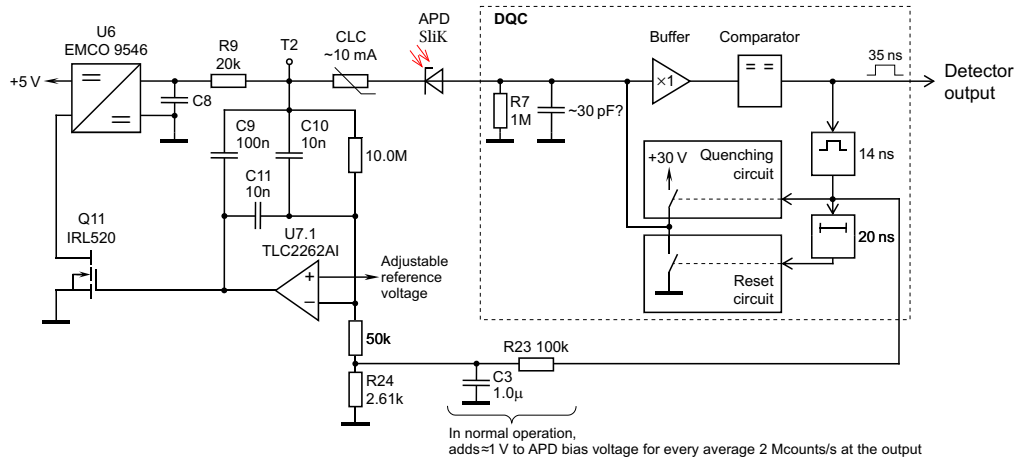
Fig. 4. Simplified reverse-engineered circuit diagram of PerkinElmer SPCM-AQR module. In normal operation, the cathode of the APD (superlow-k (SliK) type [37]) is biased at a constant high voltage, stabilized by a feedback loop containing an opamp U7.1 (Texas Instruments TLC2262), field-effect transistor Q11 and high-voltage DC/DC converter module U6 (EMCO custom model no. 9546). The anode of the APD is connected to a detection and quenching circuit (DQC). The DQC senses charge flowing through the APD during the avalanche, then briefly connects the APD anode to $+30\,$V to lower the voltage across the APD below breakdown and quench the avalanche. The APD anode voltage is subsequently reset to $0\,$V, and the detector becomes ready for the next avalanche. (Note: the circuit diagram has been greatly simplified for the paper; do not use this figure for attempting detector repair or modification.)

discussed below.

The first blinding mechanism corresponds to transition from Geiger to classical photodiode mode by lowering the APD bias voltage below breakdown. As the frequency of optical pulses increases, control first appears when the APD bias voltage drops by 12–15 V (Fig. 3(a)). To understand why it drops, let's consider the detector electrical circuit depicted in Fig. 4. When the APD is illuminated by a bright optical pulse, the current through it is not interrupted by the detection and quenching circuit (DQC) and is much larger than during an ordinary single-photon avalanche. A current limiting circuit (CLC) kicks in and limits the current pulse to about 10 mA. This current is drawn from the capacitor C9, whose other end is connected to the output of a low-power opamp U7.1. This opamp has a specified maximum load current significantly smaller than 10 mA. It gets overloaded by the current pulses, and unexpectedly develops a large static voltage offset between its inputs (see Fig. 3(b), middle chart), which may be a behavior specific to this particular opamp integrated circuit. Yet, this negative offset effectively adds to the pre-set reference voltage at the opamp non-inverting input, and the feedback loop lowers the APD bias voltage proportionally.

At higher control pulse frequencies $\sim$1 MHz, however, the disrupted opamp gets back into normal operation. At these frequencies, the duty cycle of the current pulses at the opamp output gets closer to 1/2. Since the opamp output is AC-loaded, its sourcing peak current decreases while its sinking peak current grows; they become close in magnitude and now apparently better suit opamp load capability. As a result, its large input offset disappears and the circuit raises the APD bias voltage back to the nominal value. Yet, the detector remains blind. This occurs because the APD produces more heat through electrical power dissipated in it, as the frequency of control pulses increases. In normal operation, the APD is cooled to $-7\,^{\circ}$C with a thermo-
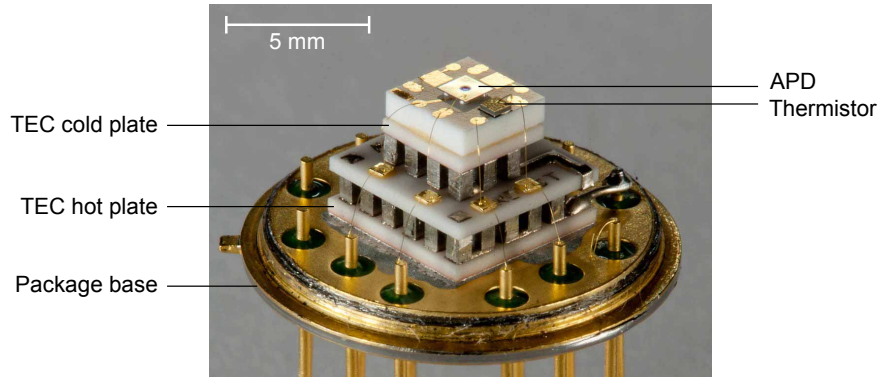
Fig. 5. APD package decapsulated: the cover and fibre coupling optics have been cut off. The dark dot in the center of the APD is its photosensitive area. The APD and thermistor are mounted on the cold plate of a two-stage thermoelectric cooler (TEC). In the assembled detector, the package base is in thermal contact with an aluminum detector outer case serving as a heatsink.
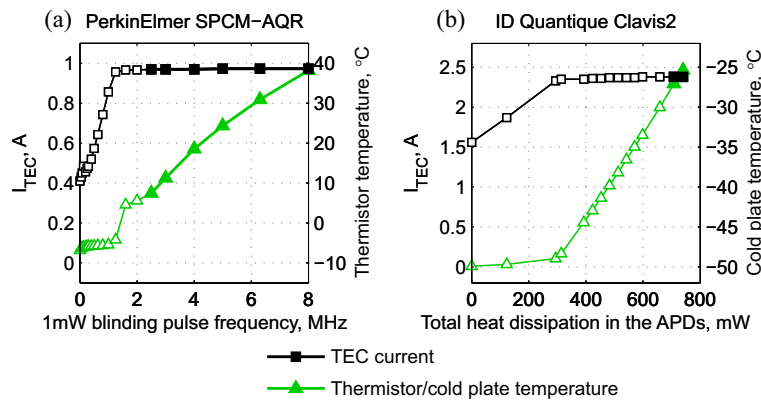

Fig. 6. Comparison of thermal blinding characteristics of the PerkinElmer SPCM-AQR detector (a) to the ones reported for ID Quantique's Clavis2 commercial QKD system [11] (b). Filled symbols denote regime in which the detector got completely blind between the control pulses. For the SPCM-AQR, characteristics at $P_{control} = 1\,mW$ are shown, because at this power thermal blinding is the only blinding mechanism.

electric cooler (TEC), see Fig. 5. The TEC heat removal capability and maximum current are inherently limited. As can be seen in the lower chart in Fig. 3(b), after a temperature controller reaches the maximum TEC current, the APD temperature quickly rises. The raised APD temperature in turn raises its breakdown voltage (by $\approx 1.2\,V/^\circ C$) above the bias voltage, which also leads to blinding. The same thermal blinding behaviour has been observed before [11]: the detectors in the commercial QKD system Clavis2 operate at a different wavelength (1550 nm) and use gating instead of active quenching. Yet, as seen in Fig. 6, they have a similar response: after reaching the maximum TEC current, the APD temperature starts increasing. Eventually, after a sufficient increase in temperature, the detectors become blind. This temperature-induced increase of the breakdown voltage makes thermal blinding an attack generic in principle to all avalanche single-photon detectors.

At even higher pulse frequencies, the bias voltage drops again below breakdown, while the

detector is still under control. This is due to load capacity exhaustion of the high-voltage DC/DC converter U6 biasing the APD.

Above, we have demonstrated three distinct blinding modes in the SPCM-AQR detector model [18]. Some QKD experiments [24] use a four-channel version of this detector module, PerkinElmer SPCM-AQ4C [38]. Our preliminary analysis indicates that it has a different bias control circuit that is not susceptible to the first blinding mechanism (opamp overload). However, it is likely susceptible to both thermal blinding and DC/DC converter overload, because it uses the same APD package and the same model of DC/DC converter.

The data sheets of both detector models [18,38] state that exposure to intense light will reduce the count rate to zero. We could reproduce a similar effect with only one out of the two SPCM-AQR samples we tested under up to 8–16 mW peak power, both c.w. and pulsed at various duty cycles and repetition rates. In that sample, a power-line monitoring circuit incorporated in the detector module (not shown in Fig. 4) powered down the entire detector for 1–1.5 s following a brief time period when it was forced to count at the saturation rate of ~ 15 MHz. The detector produced zero counts while it was powered down indeed, then recovered. Another peculiarity of the SPCM-AQR model is that if a weak c.w. illumination is present while it is being powered up (when it either recovers as above or being manually powered up by the experimenter), the DQC would latch into a 'forbidden logic state' with a permanent logic high at the detector output. The detector recovers instantly from this state when the c.w. illumination is reduced below a certain level. (The SPCM-AQ4C circuit however seems to have no forbidden logic states.) However, we could not get controllable clicks from the detector in these blinded modes.

5. Side effects

There are many interesting changes that can be monitored in the circuit (Fig. 3), however the only electrical signal an unmodified detector module currently provides to the QKD system is the detector output signal (Fig. 4). The only side effect that betrays our attack at the detector output are clicks caused by blinding pulses with a rate of at least 70 kHz (Fig. 2). In a general case, these clicks may increase the quantum bit error rate (QBER) observed by the legitimate parties, and a further analysis whether this attack would work is required. However, in many QKD systems Eve can arrange for these clicks to be always ignored by the legitimate parties as falling outside their post-processing gating time window. For instance, when attacking an entanglement-based system [24] where Eve can intercept both photons of a pair, she can arrange timing of the clicks caused by the blinding pulses to never register as coincidences between Alice and Bob. In this case, the control pulses will have zero contribution to the QBER. Similarly, if the system uses a pulsed source [23, 39], the clicks can be timed to fall outside Bob's qubit time window and thus will not increase the QBER. In free-space systems operating in daylight [22, 23], the clicks may be masked as a normal background count rate; note that the blinding pulses can be irregularly spaced to make them look more like background counts. We remark that the blinded state has some inertia (especially in the case of thermal blinding [11]) that should in principle allow Eve to apply the blinding pulses in bursts interleaved with quiet periods when only the trigger pulses are applied.

Both APDs used in the present study died suddenly, after many days of extensive testing during which they worked normally and showed no advance signs of the coming failure. This may indicate that at least some of these control regimes reduce APD lifetime, although no reliable conclusions can be drawn from our limited testing. A study of failure mechanisms caused by bright light may be interesting, however it is much more challenging and expensive, and thus lies completely outside the scope of this paper. While we have exceeded the absolute maximum rating on the peak light intensity of the detector module [18], note that Eve is never limited by manufacturer's specifications.

6. Countermeasures

The major difference between public-key cryptography and quantum key distribution is that there are security proofs for the latter. However, these security proofs are based on models of the devices used in quantum key distribution. The fact that bright illumination attacks are applicable against a detector implementation, shows that this detector implementation is not within the device model of any security proof. However, the abovementioned difference from the public-key cryptography also requires loopholes to be closed differently than before. Rather than just avoid the specific attack, one must alter the implementation and/or the security proofs to re-ensure that the devices are within the models of the security proofs. Otherwise, the quantum key distribution implementation is no longer provably secure, and thus has no advantage over key distribution based on classical cryptography.

Countermeasures have been extensively discussed for gated APD-based detectors [9, 11–16, 40]. That discussion shows clearly that avoiding specific attacks does not necessarily re-establish security. The most frequently proposed countermeasure to prevent blinding consists of using an optical power meter (or the APD itself as an optical power meter [12, 14, 16]) with a classical threshold at Bob's entrance [9, 12–14, 16]. For such a countermeasure, the classical threshold for the optical power must originate from a more general security proof [9], otherwise the provable security is not re-established. In fact, a recent study [41] has shown that for gated APD-based detectors, control can be achieved with faint trigger pulses containing less than 120 photons per pulse, already making the attack very difficult to detect with an optical power meter. For gated detectors, the so-called "bit-mapped gating" scheme [40] seems to make the implementation compatible with certain security proofs [7], and may thus re-establish security. One possible way of further development down this path would be to test single-photon sensitivity of Bob's APDs at random times by a calibrated light source placed inside Bob [40]. The results from this testing may then be used as an input to a security proof that incorporates detector deficiencies and non-linearities [7]. Alternatively, countermeasures for all detectors considered may also include monitoring the APD bias voltage, current and temperature [11], with the efficiency of each countermeasure to be assessed in the framework of a general security proof. Although development of countermeasures has begun [9, 12, 40, 42, 43], no definite countermeasure has been finalized and tested by hacking at this time [13].

If one simply wishes to avoid the specific bright-illumination attacks without re-establishing provable security, there are numerous options. One could replace the APD with a beamsplitter distributing photons to two APDs, and to look for coincidences as a signature of eavesdropping. One could also monitor any of the parameters presented in Fig. 3, or any other parameter such as the background detection rate, revealing detector control attempts. However we don't see why anybody would then prefer this QKD system that is not provably secure, over cheaper and much more convenient classical cryptography systems.

7. Conclusion

In view of this study, complemented by the ones made on other APD models [9–11, 17], we estimate that most of the QKD systems existing today are potentially vulnerable to our attack. The only 'detector-dependent' aspect here is the type of bright illumination (none, c.w., or pulsed) required to bring a particular APD into the classical photodiode regime. We remark that very similar bright-light control method is also applicable to a superconducting nanowire based single photon detector [44]. While we have not analysed actively-quenched detectors of manufacturers other than PerkinElmer, the above experience suggests that there is a chance they may be vulnerable to some of the already studied, as well as new yet-to-be-found blinding and control mechanisms.

While bright-light detector control is, strictly speaking, not equivalent to the hack of a QKD

system, we note that for one of the APD models, a full eavesdropper based on bright-light detector control has previously been implemented and tested under realistic conditions on a 290 m experimental entanglement-based QKD system [17]. In view of this demonstration, we consider that closing the exposed loopholes in a provable way should take precedence over confirming that a full eavesdropper can be built for all APD models.

Our work emphasizes the need to investigate thoroughly vulnerabilities originating from unaccounted physical non-idealities of QKD components.

Acknowledgements