Optical control of single-photon negative-feedback avalanche diode detector

View Online   Export Citation   CrossMark

Gaëtan Gras,[1,2,a)] ID Nigar Sultana,[3,4,b)] Anqi Huang,[3,4,5,c)] Thomas Jennewein,[3,6] Félix Bussières,[1,2]
Vadim Makarov,[7,8,9] and Hugo Zbinden[2]

AFFILIATIONS

[1] ID Quantique SA, CH-1227 Carouge, Switzerland
[2] Group of Applied Physics, University of Geneva, CH-1211 Geneva, Switzerland
[3] Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
[4] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
[5] Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer,
National University of Defense Technology, Changsha 410073, People's Republic of China
[6] Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
[7] Russian Quantum Center, Skolkovo, Moscow 121205, Russia
[8] Shanghai Branch, National Laboratory for Physical Sciences at Microscale and CAS Center for Excellence in Quantum
Information, University of Science and Technology of China, Shanghai 201315, People's Republic of China
[9] NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia

Note: This paper is part of the special collection on Materials for Quantum Technologies: Computing, Information, and Sensing.
a)**Author to whom correspondence should be addressed:** gaetan.gras@idquantique.com
b)**Electronic mail:** n6sultan@uwaterloo.ca
c)**Electronic mail:** angelhuang.hn@gmail.com

ABSTRACT

We experimentally demonstrate optical control of negative-feedback avalanche diode detectors using bright light. We deterministically generate fake single-photon detections with a better timing precision than normal operation. This could potentially open a security loophole in quantum cryptography systems. We then show how monitoring the photocurrent through the avalanche photodiode can be used to reveal the detector is being blinded.

Published under license by AIP Publishing. https://doi.org/10.1063/1.5140824

I. INTRODUCTION

Quantum key distribution (QKD) allows two parties, Alice and Bob, to share a secret key. The first proposal of QKD was done by Bennett and Brassard in 1983.[1] Since then, this field has evolved rapidly. Unlike classical cryptography that makes assumptions on the computational power of an eavesdropper Eve, security proofs in QKD are based on the laws of quantum mechanics.[2,3]

However, imperfections in practical systems can open loopholes that can be used by a malicious third party to get some information on the key. Attacks of various types have been proposed, for example, photon number splitting (PNS) attack,[4] detector efficiency mismatch

attack,[5] Trojan-horse attack,[6] and time-shift attack.[7] In this paper, we are interested in a detector blinding attack, which belongs to the class of faked-state attacks.[8] In this attack, Eve uses bright light to take control of the detectors in the QKD system to force the outcome of the measurement to be the same as her own. Such blinding on individual detectors has been demonstrated for single-photon avalanche diodes (SPADs)[9–13] and for superconducting nanowire single-photon detectors (SNSPDs).[14–16]

Here, we show that negative-feedback avalanche diode (NFAD) detectors can be controlled with bright light. Such detectors are promising thanks to their high efficiency and low afterpulsing probability.[17] We also show that diode current monitoring can be used to

TABLE I. Characteristics of our NFAD devices.[18]

Designation	Model number	Diameter (μm)	Coupling
D1	E2G6	22	Capacitive
D2	E3G3	32	Capacitive
D3	E2G6	22	Inductive
D4	E3G3	32	Inductive

uncover the presence of blinding. We have tested four diodes made by Princeton Lightwave.[18] Two of them are integrated in a commercial single-photon detector from ID Quantique (model ID220[19]) and two are used with a custom readout circuit made at the University of Waterloo.[20]

II. EXPERIMENTAL SETUP

The characteristics of the four NFAD devices are given in Table I. The electronic circuit of the detectors is shown in Fig. 1. It is similar for both setups except for the coupling to the amplifier, which is capacitive in D1 and D2 and inductive in D3 and D4. This differing part of the circuit is shown in dashed boxes. Under normal conditions, the NFAD works in a Geiger mode; i.e., the avalanche photodiode (APD) is biased with a voltage V_{bias} greater than the breakdown voltage V_{br}. When a photon is absorbed, it creates an avalanche generating an electrical pulse. This analog signal is then converted into a digital signal by using a comparator with a
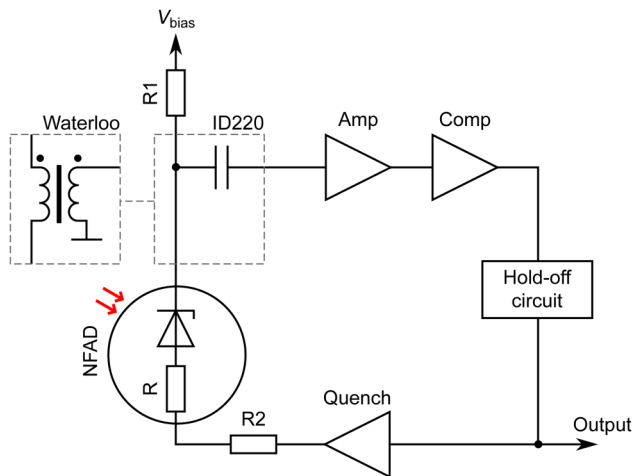

FIG. 1. Scheme of the electrical readout. After detection of a photon by the APD, the avalanche signal is coupled to an amplifier (Amp) through a capacitor in ID220 or a pulse transformer in a custom readout (Waterloo). Then, it goes through a comparator (Comp). The hold-off circuit outputs a gate with a pre-set width. The feedback loop is used to quench the avalanche by applying a +5 V (ID220) or a +4 V (custom readout) voltage to the anode of the NFAD for dead-time τ_d. By applying this voltage, we reduce the voltage across the APD below its breakdown voltage. R = 1.1 MΩ is a resistor integrated into the NFAD.[18] In ID220, R1 = 1 kΩ and R2 = 50 Ω; for Waterloo, R1 = 1 kΩ and R2 = 100 Ω.
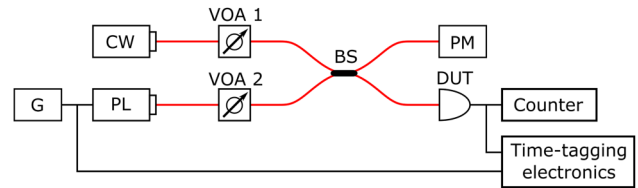

FIG. 2. Experimental setup for testing blinding and control of the detectors. The optical power of the continuous-wave laser (CW) and the pulsed laser (PL) is adjusted using variable optical attenuators (VOAs). The pulsed laser is triggered by a pulse generator (G). The two lasers are combined on a 50:50 beam splitter (BS). The light is sent to the device-under-test (DUT) and to a power meter (PM).

threshold voltage V_{th}. To take control of the detector, Eve needs first to blind it so that it becomes insensitive to single photons.[11] To do so, she sends continuous bright light on the APD, which then generates a photocurrent. As the APD is connected in series with resistors R, R1, and R2 (see Fig. 1), the voltage across the APD will be reduced. If Eve sends enough light, she can then bring the voltage across the APD below V_{br} and put the detector into a linear mode. In this mode, the detector is no longer sensitive to single photons but instead works as a linear photodetector. Eve can now force the detector to click at the time of her choosing by superimposing optical pulses (trigger pulses) to her blinding laser.

To test for blinding and control, we use a setup shown in Fig. 2. For the attack, we use two lasers at 1550 nm.[11] The first laser (blinding laser) is working in a continuous-wave mode to make the detector enter its linear mode and hence become insensitive to single photons. The second laser is generating optical pulses of 33 ps full-width at half-maximum (FWHM) for the tests on detectors D1 and D2 and 161 ps for the detectors D3 and D4. The two laser signals are then combined on a 50:50 beam splitter.

III. DETECTOR CONTROL

A. Blinding

First, we test our four devices to see if they are blindable. For this, we increase the continuous-wave optical power $P_{blinding}$ arriving on the APD, and we measure the rate of detection. Once it reaches 0, the detector is blinded. For our four devices, this happens at an optical power of a few nanowatts, and we have tested that they stay blinded up to several milliwatts.

B. Forced detections

Once Eve has blinded the detector, she can send optical trigger pulses to generate electrical pulses. The amplitude of the signal will be proportional to the energy of the trigger pulse E_{pulse}. As there is a comparator in the readout circuit, not all pulses are necessarily detected. If the amplitude of the signal is below the comparator threshold, no click will be registered. Therefore, by controlling E_{pulse}, Eve can force the detector to click with a probability $p \in [0, 1]$. We can then define E_{never} as the maximum energy of the optical pulse that never generates a click and E_{always} as the energy above which the detector always clicks. To avoid introducing

errors in the key, Eve must carefully choose the energy of her pulse. In the case of the BB84 protocol,[1] if Eve and Bob measure in different bases, the pulse energy will be divided equally between Bob's two detectors.[11] In this case, Eve does not want Bob's detectors to click; thus, she must choose her $E_{pulse} < 2E_{never}$. If Eve's and Bob's bases are the same, all the light will be directed to one detector, which will click with a probability p. For short distances, Bob will expect a high detection rate. Eve must then force Bob to click with a high probability; hence, the transition region between E_{never} and E_{always} must be sufficiently narrow. On the other hand, for long-distance QKD, Bob expects a low detection rate; therefore, Eve can afford to have Bob's detector clicking with a low probability.

Figure 3 shows the probability to get a detection depending on the energy of the trigger pulse for various blinding powers. For this experiment, we set the deadtime τ_d of the detector at $18\,\mu s$ ($20\,\mu s$), which corresponds to a maximum detection rate of $\sim 55\,kHz$ ($50\,kHz$) for detectors D1 and D2 (D3 and D4) and send trigger pulses at a rate of $40\,kHz$. As we can see in Fig. 3, there is a

transition region where the detection probability monotonically increases from 0 to 1. The changing width of this transition region can be seen in Fig. 4 for D1 and D2 and in Fig. 5 for D3 and D4.

For high blinding power, the detector is in the linear mode, and the APD gain decreases with the optical power because the voltage across the APD drops. In order to get the same amplitude of the signal at the input of the comparator and get a click, we then need to increase the energy of the trigger pulse. For low blinding power, the detector is in the transition between the linear mode and the Geiger mode.[13] In this region, the probability to generate a macroscopic signal even with a low energy pulse is non-zero, which explains why E_{never} decreases when we reduce the blinding power. As seen in Fig. 4(a), when we increase the efficiency of D1 from 10% to 20%, the curves are shifted to the right. This is because the bias voltage is higher for 20% efficiency; hence, we need higher $P_{blinding}$ to reduce the voltage across the APD to the same value. The detector D3 exhibits a similar effect as seen in Fig. 5(a). Now, if we compare detectors D1 and D2 with the same efficiency, we
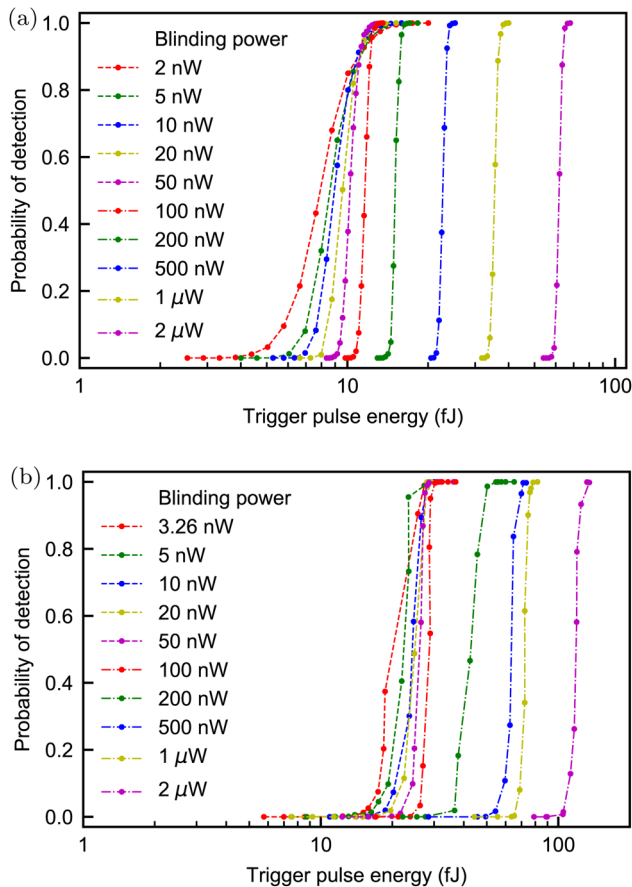

FIG. 3. Probability to force a detection as a function of the pulse energy for (a) detector D1 with 10% photon counting efficiency and (b) detector D3 with a 2 V excess bias above V_{br}. The measurements were made by sending trigger pulses at a frequency of 40 kHz.
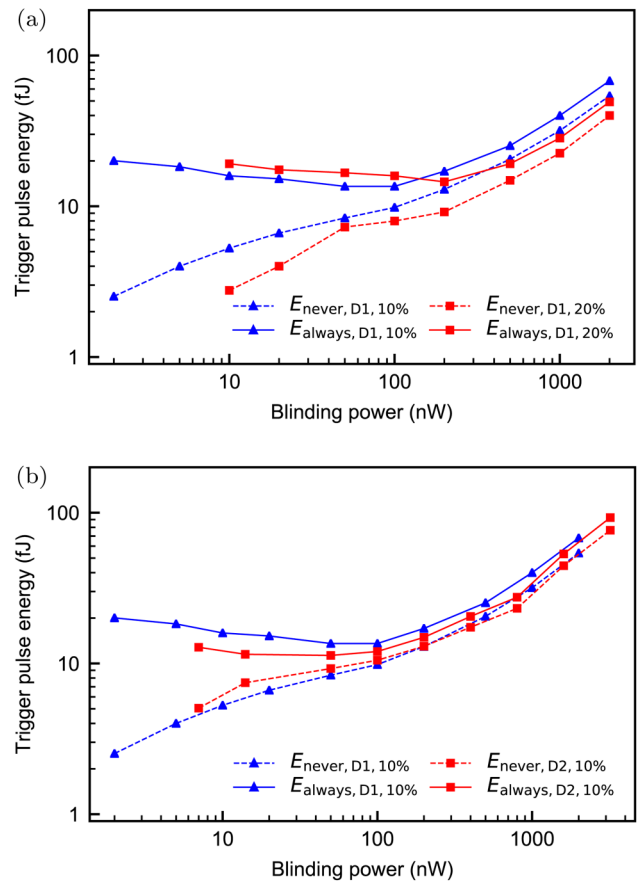

FIG. 4. Dependence of E_{always} and E_{never} on the blinding power. (a) Thresholds for detector D1 with 10% and 20% efficiency (corresponding to 1.3 V and 4.1 V excess biases). (b) Comparison of detectors D1 and D2 with the efficiencies set at 10%.
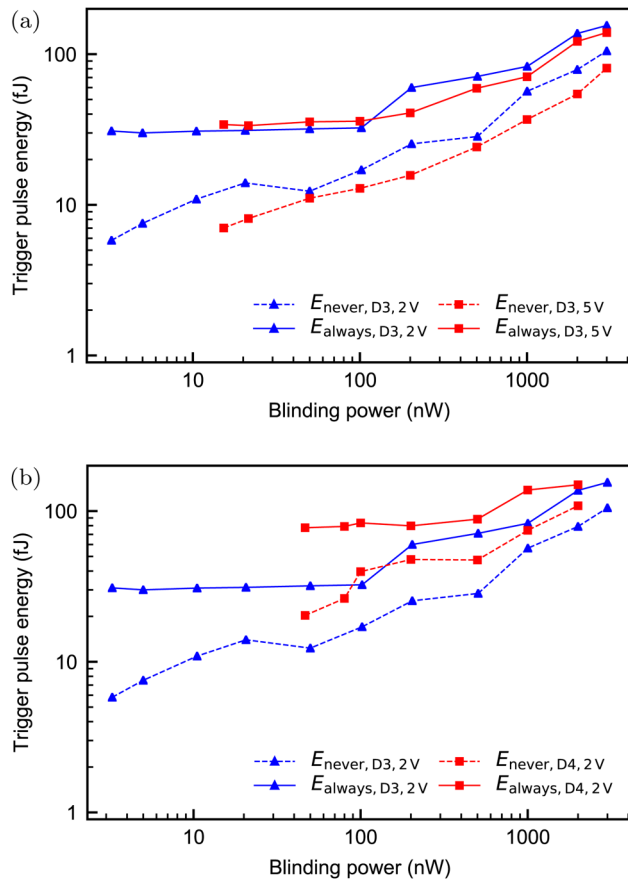
FIG. 5. Dependence of E_{always} and E_{never} on the blinding power for the Waterloo detectors. (a) Thresholds for detector D3 with 2 V and 5 V excess biases. (b) Comparison of detectors D3 and D4 with the same excess voltage of 2 V.

see in Fig. 4(b) that both of them have similar triggering energies. The main difference is in the minimum blinding power, which is higher for D2 by a factor of 3. The detectors D3 and D4 require higher triggering energy. This can come from the fact that the detection threshold was set to a higher value due to higher noise in the circuit. We also note that D4 has ≈ 14 times higher minimum blinding power than D3 [Fig. 5(b)]. Thus, for both pairs of detectors, higher minimum blinding power correlates with a larger active area.

For low blinding power, the transition is too wide for an eavesdropper to attack the entire key in a short distance BB84 protocol.[10] Eve has then two possibilities: either she increases the blinding power to have a transition region sufficiently narrow or she attacks only a small part of the key such that Bob's detection rate is not impacted.[21]

C. Timing jitter

Another important parameter for Eve is the jitter of the detector's response to her trigger pulse.[10] Ideally, it should be narrower

than a single-photon detection jitter. For our measurements, we use a time-correlated single-photon counting with the trigger signal for the pulsed laser as a time reference. We perform timing measurements with single photons and bright pulses. For detector D2, we use a 33 ps FWHM laser for bright pulses and a single-photon jitter measurement; for detector D3, we use 161 ps FWHM bright pulses and 147 ps FWHM attenuated pulses for a single-photon jitter measurement. Results are shown in Fig. 6.

As we can see, under control, the jitter of the detection is greatly reduced compared to single-photon detection. Eve is then able to perfectly control in which time bin she wants to make Bob's detector clicks. In order to reproduce the larger jitter of single-photon detections, Eve can artificially increase the jitter of her bright pulses.
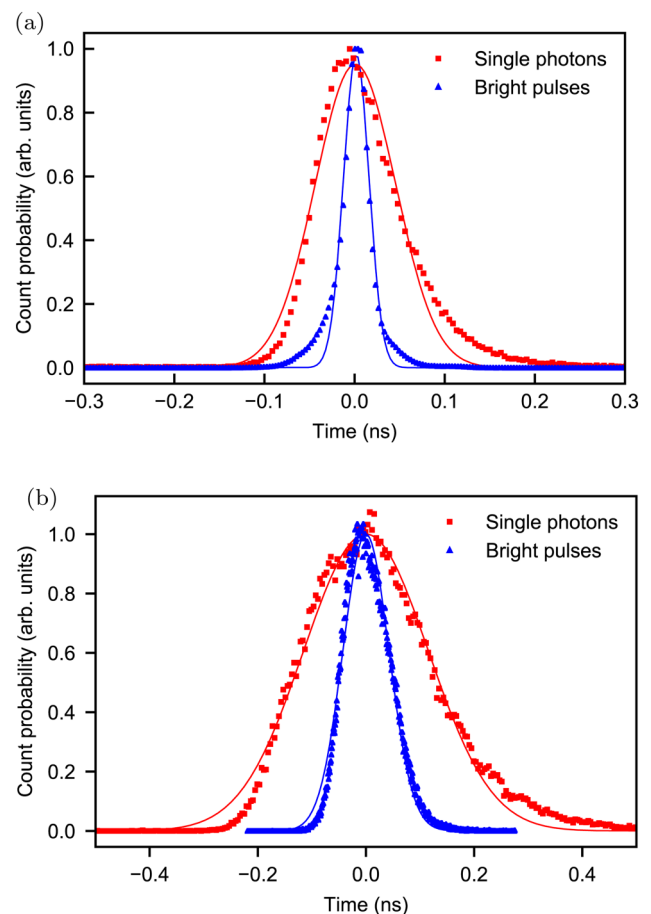

FIG. 6. Comparison of the jitter for the detection of a single photon and a bright pulse. The relative time shift between the distributions is not shown; the distributions have been centered. (a) Jitter of detector D2 with the efficiency set at 10%. The Gaussian fits (solid lines) give a FWHM of 33.4 ps for the detection of a faked state ($P_{blinding} = 7$ nW, $E_{pulse} = 12.8$ fJ) and 104.9 ps for the detection of single photons. (b) Jitter of detector D3 with a 2 V excess bias. The detection of a faked state ($P_{blinding} = 3.3$ nW, $E_{pulse} = 30.9$ fJ) has 100.6 ps FWHM, and the detection of single photons has 271.8 ps FWHM.

The detector response to the trigger pulse is probably slightly time-shifted relative to its single-photon response. We have not measured this time shift. However, this should not hinder Eve in most situations because she controls the arrival time of her trigger pulse.

IV. COUNTERMEASURES

It is a general assumption in cryptography, called Kerckhoffs's principle,[22] that Eve knows everything about the cryptographic setup and its parameters (detector characteristics under the bright-light control, deadtime, etc.). We, therefore, have to design a countermeasure that detects the attack even if Eve knows about our countermeasure and tries her best to circumvent it.

One possible way to detect this attack is to monitor the current through the APD. A monitoring circuit is already implemented in ID220. A voltage converter chip biasing the APD has a monitoring pin giving a current equal to 20% of the average current flowing through the APD, thanks to a current mirror. This current is measured using a 24-bit analog-to-digital converter. In the actual implementation, its value is sampled once per second. We have performed tests of this current monitoring using detector D2 with τ_d set at $18\,\mu s$. We have first only blinded the detector without sending trigger pulses.

In normal conditions, the mean current through the APD is very small since the only contribution comes from avalanches due to the detection of a photon. Under control, the blinding laser forces the APD to be continuously conductive. In this case, the mean current should be greater than under normal use. This can be seen in Fig. 7. At more than 10^{10} incident photons per second, the count rate of the detector drops and reaches 0 (the detector is blinded), while the mean current I increases significantly.

We have then tested the countermeasure while fully controlling the detector. For this, we used CW blinding and the 33 ps FWHM pulsed laser to generate the forced detections. In this case, we see that the mean current through the detector is reduced and depends on the rate of the trigger pulses (see Table II).
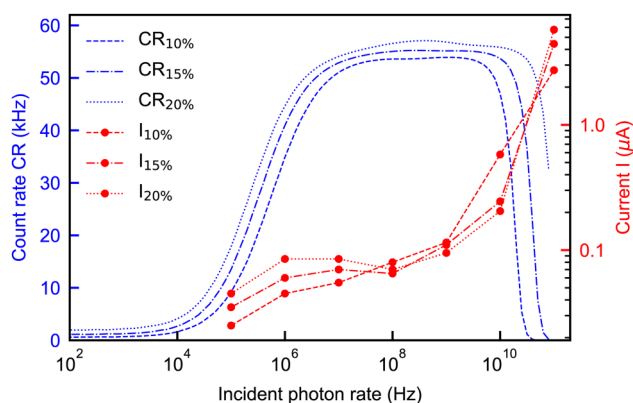
TABLE II. Current values measured for detector D2 under blinding for different efficiencies and trigger pulse rates.

Efficiency (%)	Pulse rate (kHz)	Current (μA)
10	40	0.87
10	50	0.38
10	55	0.15
20	40	2.39
20	50	1.23
20	55	0.71

The explanation comes from the working principle of the detector. Indeed, after a detection, the voltage across the APD is reduced to limit the afterpulsing. During this deadtime ($18\,\mu s$ in our case), the gain of the APD is smaller so that the current due to the blinding is reduced. This gives a mean current smaller than that with only the blinding laser.

The lowest current we could reach was 150 nA by saturating the detector. This is still higher than the values measured with up to 10^8 incoming photons per second, which never exceed 100 nA (Fig. 7). By setting the threshold of the current to a proper value (which would depend on τ_d and the detection rate), Bob can thus detect the blinding of his detector by Eve. However, this countermeasure is only guaranteed to work provided the blinding is continuous as in our tests and not a more advanced pulsed one.[15,23]

In order to reduce the impact of her attack on the mean photocurrent, Eve has the possibility to take advantage of the detector deadtime to minimize the overall illumination. Indeed, during the deadtime, the voltage across the detector is reduced below V_{br} but is still several tens of volts, and the blinding laser will unnecessarily generate a current. Hence, by stopping the blinding while the
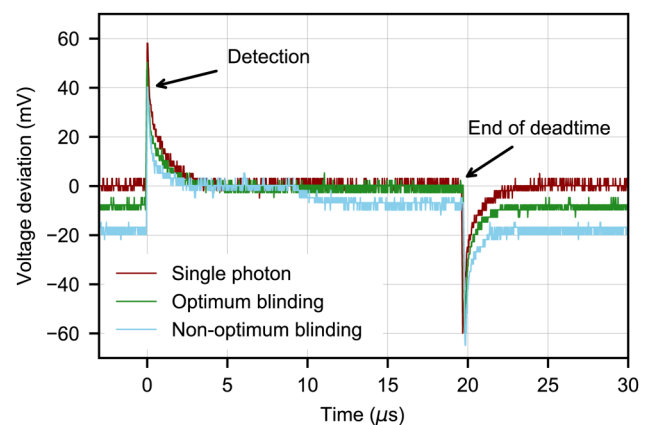

FIG. 7. Dependence of the detector D2 count rate and bias current on the incident photon rate. Unlike measurements done with an Si detector in Ref. 10, here, we observe a plateau for the count rate due to the deadtime.

FIG. 8. Fluctuations of the bias voltage due to the detection of a single photon (a dark red oscilloscope trace) and under the blinding attack (green and blue oscilloscope traces). For an optimum blinding, we use the minimum blinding power, and the blinding laser is switched on just at the end of the deadtime. For non-optimum blinding, the laser is switched on in the middle of the deadtime and has higher power.

detector is inactive and forcing the detection shortly after its recovery, we can reduce the mean current slightly below 100 nA, making the attack hardly distinguishable from the normal conditions. To detect these short periods of blinding and keep the system secure against the blinding attack, a high-bandwidth measurement is necessary. For this, we use an oscilloscope probe to monitor the output of the bias voltage source (point marked V_{bias} in Fig. 1). Due to the photocurrent generated by the attack and the non-zero output impedance of the bias voltage source, small voltage drops are observed at this point.

Figure 8 shows the deviation of V_{bias} from its nominal value for detector D2. On each curve, we see two peaks (one positive and one negative) separated by the duration of the deadtime. These are due to high-frequency components of the applied quenching voltage. After the deadtime, we see a voltage drop but only in the case where we blind the detector. This drop comes from the photocurrent induced by the blinding of the detector and lasts as long as the detector is blinded. The deviation of the voltage from its nominal value gives us information on the state of the detector in real time. The detection of this voltage drop may be used to unveil the presence of an eavesdropper even in the case of more sophisticated attacks such as the one proposed here and could give Bob information on the bits potentially compromised by this attack.

V. CONCLUSION

We have demonstrated the control of four free-running single-photon NFAD detectors by using bright light, which could be used to attack QKD. Mean current monitoring allows us to detect the presence of continuous blinding but might be insufficient in the case of blinding with varying intensities. In the latter case, we have shown that a high-bandwidth measurement of the current flowing through the APD can be used to monitor the state of the detector in real time. This is a step toward constructing a hack-proof single-photon detector for QKD.

ACKNOWLEDGMENTS

REFERENCES

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

[2]H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science **283**, 2050–2056 (1999).

[3]P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441–444 (2000).

[4]B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," Phys. Rev. A **51**, 1863 (1995).

[5]V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," Phys. Rev. A **74**, 022313 (2006); erratum ibid. **78**, 019905 (2008).

[6]N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Trojan-horse attacks threaten the security of practical quantum cryptography," New J. Phys. **16**, 123030 (2014).

[7]Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," Phys. Rev. A **78**, 042333 (2008).

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

[9]S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, "Controlling an actively-quenched single photon detector with bright light," Opt. Express **19**, 23590–23600 (2011).

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

[11]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).

[12]L. Lydersen, J. Skaar, and V. Makarov, "Tailored bright illumination attack on distributed-phase-reference protocols," J. Mod. Opt. **58**, 680–685 (2011).

[13]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).

[14]M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, and M. Sasaki, "Characteristics of superconducting single photon detector in DPS-QKD system under bright illumination blinding attack," Opt. Express **21**, 6304–6312 (2013).

[15]M. G. Tanner, V. Makarov, and R. H. Hadfield, "Optimised quantum hacking of superconducting nanowire single-photon detectors," Opt. Express **22**, 6734–6748 (2014).

[16]L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, "Controlling a superconducting nanowire single-photon detector using tailored bright illumination," New J. Phys. **13**, 113042 (2011).

[17]B. Korzh, N. Walenta, T. Lunghi, N. Gisin, and H. Zbinden, "Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency," Appl. Phys. Lett. **104**, 081108 (2014).

[18]M. A. Itzler, X. Jiang, B. M. Onat, and K. Slomkowski, "Progress in self-quenching InP-based single photon detectors," Proc. SPIE **7608**, 760829 (2010).

[19]See https://marketing.idquantique.com/acton/attachment/11868/f-023d/1/-/-/-/-/ID220˙Brochure.pdf for "ID220 infrared single-photon detector datasheet" (accessed 14 February 2019).

[20]N. Sultana, J. P. Bourgoin, K. Kuntz, and T. Jennewein, "A simple photon counting module for free-running negative-feedback avalanche diodes with active suppression of afterpulses" (unpublished).

[21]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).

[22]A. Kerckhoffs, "La cryptographie militaire," J. Sci. Mil. **IX**, 5–38 (1883).

[23]M. Elezov, R. Ozhegov, G. Goltsman, and V. Makarov, "Countermeasure against bright-light attack on superconducting nanowire single-photon detector in quantum key distribution," Opt. Express **27**, 30979 (2019).