

Controlling a superconducting nanowire single-photon detector using tailored bright illumination

Lars Lydersen^{1,2,4}, Mohsen K Akhlaghi³, A Hamed Majedi³, Johannes Skaar^{1,2} and Vadim Makarov^{1,2,4}

¹ Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway

² University Graduate Center, NO-2027 Kjeller, Norway

³ Department of Electrical and Computer Engineering and Institute for Quantum Computing, University of Waterloo, Waterloo, ON N2L 3G1, Canada
E-mail: lars.lydersen@iet.ntnu.no and makarov@vad1.com

New Journal of Physics **13** (2011) 113042 (14pp)

Received 8 August 2011

Published 30 November 2011

Online at <http://www.njp.org/>

doi:10.1088/1367-2630/13/11/113042

Abstract. We experimentally demonstrate that a superconducting nanowire single-photon detector is deterministically controllable by bright illumination. We found that bright light can temporarily make a large fraction of the nanowire length normally conductive, can extend deadtime after a normal photon detection, and can cause a hotspot formation during the deadtime with a highly nonlinear sensitivity. As a result, although based on different physics, the superconducting detector turns out to be controllable by virtually the same techniques as avalanche photodiode detectors. As demonstrated earlier, when such detectors are used in a quantum key distribution system, this allows an eavesdropper to launch a detector control attack to capture the full secret key without this being revealed by too many errors in the key.

⁴ Authors to whom any correspondence should be addressed.

Contents

1. Introduction	2
2. Detector design and operation	3
3. Detector control in the latched state	5
3.1. Device physics	5
3.2. Application to eavesdropping	6
4. Detector control via deadtime extension	8
4.1. Device physics	8
4.2. Application to eavesdropping	9
5. Discussion and conclusion	12
Acknowledgments	13
References	13

1. Introduction

Quantum key distribution (QKD) allows two parties, Alice and Bob, to generate a secret random key at a distance [1–4]. The key is protected by quantum mechanics: an eavesdropper Eve must disturb the signals between Alice and Bob and therefore reveal her presence. QKD using perfect devices has been proven to be secure [5, 6].

Implementations of QKD have to use components available with current technology, which are usually imperfect. While there are numerous security proofs considering more realistic devices [7–15], these proofs assume that the imperfections are quantified in terms of certain source and detector parameters. Due to the difficulty of characterizing or upper bounding these parameters owing to limitations of these security proofs, it is common to use the more established security proofs for ideal systems also in practical implementations. With actual devices deviating from the ideal models, numerous security loopholes have therefore been identified and usually experimentally confirmed [16–27], and in some cases exploited in eavesdropping experiments with full secret key extraction by Eve [28, 29]. Finding and eliminating loopholes in implementations is crucial to obtain provable practical security.

As an example, several recent attacks have been based on bright-light control of avalanche photodiodes (APDs) [24, 25, 28–34]. Superconducting nanowire single-photon detectors (SNSPDs), studied in this paper, are based on different physics. However, as we will see, the principles of attacks on QKD systems using SNSPDs are broadly similar to attacks on QKD systems using APDs: Eve uses a faked-state attack [35], can blind the detectors [24, 25], make them click with a classical threshold using a bright pulse [25] or let one detector temporarily recover from blinding [24]; also, the detector’s response to multiphoton pulses can be superlinear [34]. We refer to these principles throughout the paper.

Although SNSPDs have been used in several QKD experiments [36–40], this detector technology is still in its infancy. No automated unattended operation of systems containing SNSPDs has been reported. Technical aspects of SNSPD operation, such as handling the latching behavior and converting the nanowire analogue response into a digital detection signal, have only been studied in the normal single-photon counting regime. So far, no study reported has considered SNSPD’s non-idealities as a vulnerability for QKD security. This study thus serves as an *early warning*. Although we have done our experiments on only one detector

sample, we show that control by bright light can be achieved through two separate mechanisms, and may thus be applicable to different detector designs⁵. Regardless of whether the control mechanisms we have identified apply to other detector designs, our experiment shows that the bright illumination response of the SNSPD is deviating from the detector model in the simple security proofs for QKD. Therefore, theoretical and/or experimental effort is required to re-establish security for QKD systems using SNSPDs.

This paper is organized as follows. In section 2, we describe the SNSPD under test. Sections 3 and 4 deal with the SNSPD in the latched and non-latched states; in each section we present the physics behind the detector's reaction to bright-light illumination and then how it can be exploited to attack QKD. We discuss our findings and conclude in section 5.

2. Detector design and operation

We performed our tests on an SNSPD of a fairly standard configuration, which has been characterized in previous publications [41–43]. The SNSPD chip was manufactured by Scotel, Moscow, and consists of a 4 nm thick, 120 nm wide NbN nanowire on a sapphire substrate, laid out in a $10 \times 10 \mu\text{m}$ meander pattern with 60% filling ratio. The chip is packaged and installed in a ~ 1 m long dipstick assembly (for details see [42]), which is lowered into a Dewar flask. During detector operation, the chip is immersed into liquid helium at 4.2 K. It is optically accessible through a single-mode fibre. The chip is connected to a room-temperature bias tee and a wideband radio-frequency (RF) amplifier via a 50Ω coaxial cable (figure 1). A battery-powered current source biases the superconducting nanowire with $I_b = 22.5 \mu\text{A}$, which is ≈ 0.85 of its critical current I_c (this I_b value provides the highest ratio of the photon detection probability at 1550 nm to the dark count rate for this particular SNSPD sample). The signal from the output of the RF amplifier travels to a 16 GHz single-shot oscilloscope (Tektronix DSA 71604) and a counter (Stanford Research Systems SR400). The detection efficiency for single photons at 1550 nm was 2.2×10^{-5} and the dark count rate was < 1 Hz, which is a typical performance for this SNSPD model (higher detection efficiency can be obtained at the expense of a much higher dark count rate; while this SNSPD was not optimized for high detection efficiency, the effects we have observed should qualitatively be the same as those with efficiency-optimized designs [44]). The detector sensitivity was polarization dependent; in all experiments in this paper, polarization was aligned to maximize the detection efficiency, using a fiber polarization controller.

One aspect of detector operation is how the analogue pulse produced by a transient hotspot (see the inset in figure 1) is converted into a detection event and assigned a particular timing. The analogue pulse is well defined, its magnitude and shape being nearly constant from one photon detection to another. Therefore almost any discriminator design would work for single-photon detection, and its implementation details (bandwidth, hysteresis, whether it is a threshold discriminator or a constant-fraction discriminator, etc) are often omitted in the literature on SNSPDs. However, as previously discussed for APDs [45, 46], these details become more important for the demonstration of detector control by bright light. We assume in this study that

⁵ Testing was restricted to one sample owing to the difficulty in gaining access to more samples. One reason for this was that high-power illumination was initially assumed to be potentially lethal to the devices. However, the sample we tested survived undamaged. In fact, the measurement in section 3.1 suggests that the maximum temperature of the nanowire under 20 mW, 1550 nm continuous-wave illumination stayed relatively low, because only a part of the nanowire rose above the superconducting transition temperature of ~ 10 K.

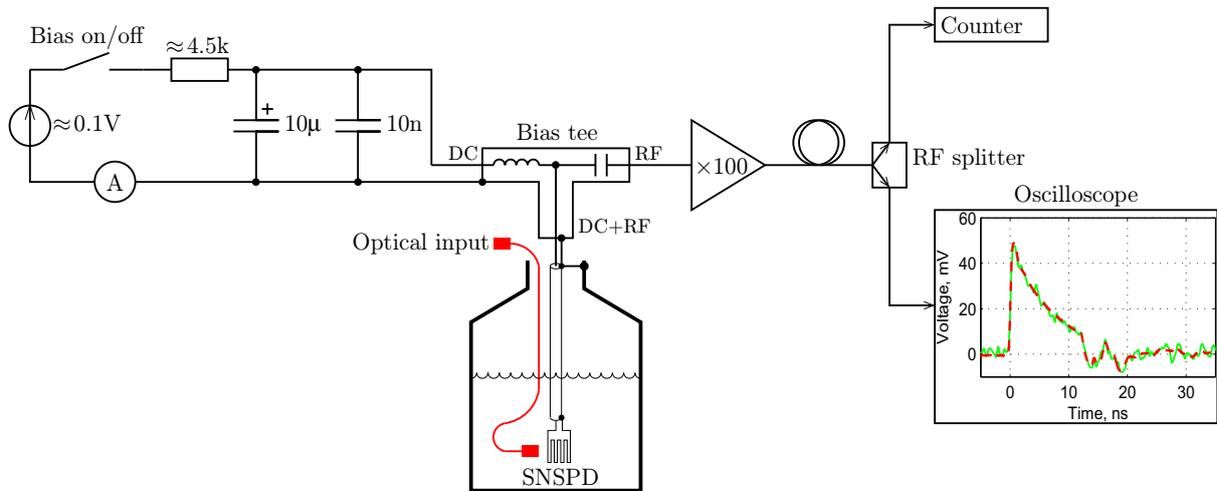


Figure 1. Detector circuit. The SNSPD is biased from a battery-powered direct current (dc) source, an equivalent circuit diagram of which is shown. Pulses produced by the SNSPD travel through a ~ 1 m coaxial cable, bias tee (0.1–6000 MHz, Mini-Circuits ZFBT-6GW+), a radio-frequency (RF) amplifier (voltage gain 100, 0.1–1500 MHz, Phillips Scientific 6954-S-100), a ~ 1.5 m coaxial cable and an RF splitter (Mini-Circuits ZN2PD-9G-S+) to the counter and oscilloscope. Inside the oscilloscope box: the normal single-photon response after the RF amplifier and splitter, shown as a single-shot trace with 2 GHz bandwidth (green solid line) and averaged over many pulses (red dashed line). Features appearing 12 ns after the leading edge are attributed to reflections due to impedance mismatch in the RF circuits.

the analogue pulse is sensed by a high-speed voltage comparator, and the detection event timing is registered by the pulse's leading edge crossing a pre-set comparator threshold. Indeed this is how our SR400 counter operates: it has an adjustable threshold set with 0.2 mV resolution. In our setup, the counter works correctly (registering one count per single-photon analogue pulse) in a wide range of threshold settings, from +4.4 to +37 mV. A detail not mentioned in the literature is what threshold level the comparator should be set at, within this working range. While the setting may not affect normal detector operation, only a part of this voltage range is reachable under bright-light control described in the following section.

Another interesting aspect of detector operation is latching. In the single-photon detection regime, the hotspot after formation shrinks quickly and the nanowire returns to the superconducting state [47]. However, the detector also has a stable *latched state*, when a larger self-heating hotspot persists indefinitely, at a steady current I_{latched} which is a fraction of I_b , and a large voltage across the SNSPD. The detector is blind to single photons and does not produce dark counts in this regime. A properly designed SNSPD does not enter the latched state after single-photon detection [47, 48]. However, it can still latch after an electromagnetic interference (which in our experiment was easily caused by switching on and off lights and other mains-powered electrical equipment in the same building). Latching also occurs after a brief bright illumination: at 1550 nm, a single 5 ms long light pulse with as little as 50 nW optical power reliably latches the device. Increasing the bias current I_b very close to I_c also leads to latching.

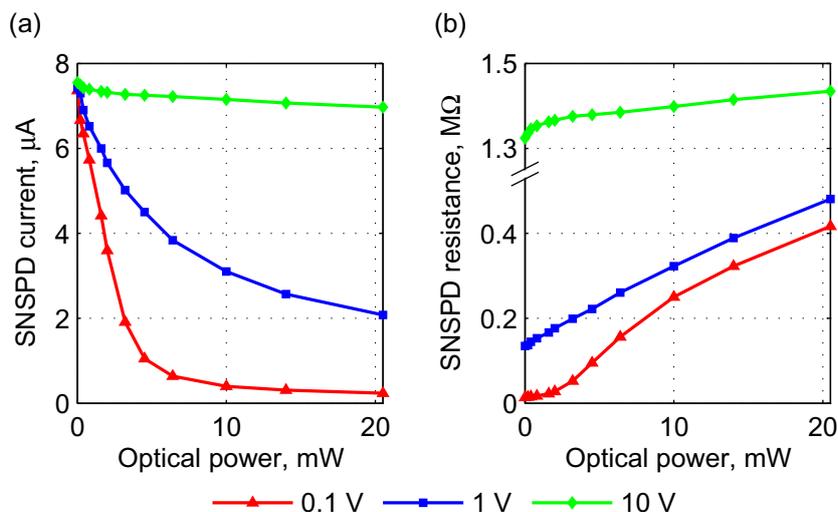


Figure 2. Response to CW light in the latched state. (a) Current I through the SNSPD versus optical power at 1550 nm, at different voltages V applied across the SNSPD. (b) SNSPD resistance $R = V/I$.

The only way to return from the latched state into the normal regime is to temporarily reduce I_b below I_{latched} . In our experiment, and supposedly in most other experiments reported in the literature, this was performed manually.

3. Detector control in the latched state

3.1. Device physics

In the latched state, the Joule heat generated in the normally conductive fraction of the nanowire exactly balances the cooling. The length of the normally conductive fraction changes with the voltage applied across the SNSPD. We investigated this by replacing the battery-powered bias source with an external bias source consisting of a constant-current source limited at a certain maximum voltage. Since the SNSPD enters and maintains latching at a current lower than the normal bias current, this bias source automatically turns into a voltage source once the device latches. In our experiment, I_{latched} was roughly 7 μA regardless of the voltage across the device, up to 10 V (we did not apply higher voltages in order to reduce the chances of electrical breakdown). At 10 V, the nanowire resistance was thus $\sim 1.4 \text{ M}\Omega$. Above the superconducting transition temperature, the resistance of the entire device is approximately constant and is $\approx 2.3 \text{ M}\Omega$ [43]. We therefore concluded that slightly over half its length was normally conductive at 10 V. During the experiment, I_{latched} would randomly assume a value in the 6–8 μA range, which could correspond to the normally conductive region shifting and ‘locking’ to the local variations of nanowire thermal characteristics along its length.

Next, we investigated what happens when bright continuous-wave (CW) light was applied in the latched state. Under illumination, the current I through the device dropped, with a different sensitivity at different voltages (figure 2(a)). When recalculated into device resistance (figure 2(b)), we see that at low source voltages the resistance increased by about the same amount (350–400 $\text{k}\Omega$ per 20 mW), while at 10 V the increase was smaller ($\sim 110 \text{ k}\Omega$). Note that depending on optical coupling, illumination may be unevenly distributed along the nanowire.

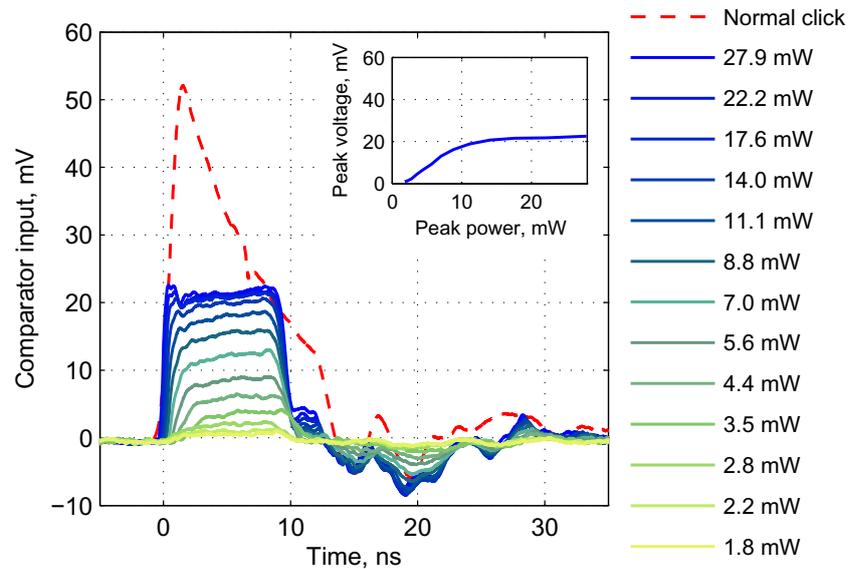


Figure 3. Electrical response in the latched state to the 10 ns, 1550 nm optical trigger pulse. All traces are averaged over 500 samples. The trigger pulse saturates at an electrical response of about 20 mV (see the inset), compared to the normal detection event, which reaches a peak amplitude of about 50 mV.

Implementation and maximum voltage of the bias source is yet another detail that varies between setups and is rarely specified in the literature. In our detector it is implemented as a ≈ 0.1 V voltage source in series with a ≈ 4.5 k Ω resistor (see figure 1), with both voltage and resistance being trimmable in a small range to set precise I_b in the normal (non-latched) regime. When the SNSPD resistance is zero, this bias circuit acts as a current source. However, in the latched state the SNSPD resistance becomes larger than the circuit output impedance; thus it acts as a voltage source. Measurements carried out with this battery-powered bias circuit closely match the 0.1 V curve in figure 2.

3.2. Application to eavesdropping

The eavesdropper Eve can latch the device by applying sufficient illumination at the SNSPD, for instance, a single > 50 nW, 5 ms long light pulse at 1550 nm. The latching causes a number of random detection events, depending on the discriminator setting and optical power of the latching pulse. However, for intense illumination, it is possible for Eve to latch the device with only a few random events (for instance, using 5 mW optical power for some ms at 20 mV discriminator threshold). Also note that Eve only has to latch the device once.

In the latched state, the SNSPD is insensitive to single photons and produces no dark counts (similarly to blinding of APDs [24, 25]). However, the nanowire's response to bright CW illumination detailed in section 3.1 also holds on a nanosecond scale for bright pulses, and can be used to produce an electrical pulse after the RF amplifier and splitter (figure 3)⁶.

⁶ The measurement in figures 3 and 4 was taken some days apart from the measurement in figure 2. Unfortunately, it seems we had an optical and/or polarization alignment problem during the former: the detector is ~ 3 times less sensitive in figures 3 and 4 than in the rest of the paper, with its behavior being otherwise consistent except for the scale factor of ~ 3 on the optical power.

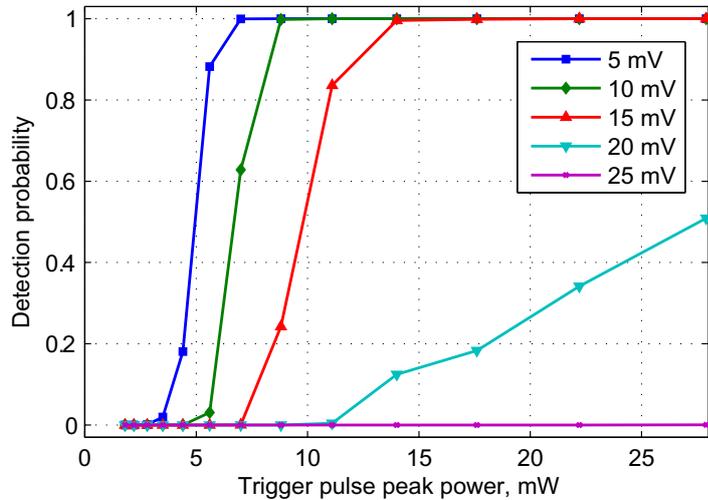


Figure 4. Detection probability of the 10 ns trigger pulse, depending on the comparator threshold. The probabilities were obtained by simulating a bandwidth-limited ideal comparator, requiring that the wideband signal recorded by the oscilloscope spent at least 3 ns above the threshold level to register a click. A measurement using a real comparator SR400 (not shown on the plot) confirmed this strong superlinearity; the jitter of SR400 comparator clicks in response to the bright pulse was ~ 0.5 ns FWHM.

The response is caused by a larger piece of the nanowire becoming normally conductive during the bright illumination, therefore causing an abrupt change in the resistance, just as a single photon causes an abrupt change in the resistance in the normal operating regime. Note that the electrical response to a bright trigger pulse saturates at ~ 20 mV when optical power > 15 mW is applied, because at this power the current through the nanowire is reduced to almost zero.

Since this analogue electrical pulse is sensed by a comparator, the detector has a highly superlinear detection probability of bright pulses [34]. By simulating an ideal bandwidth-limited comparator on recorded wideband long oscilloscope traces, we found that the detection probability would depend strongly on the comparator threshold (figure 4). If the comparator threshold is set in the 5–20 mV range, the detection probability is highly superlinear and increases quickly from negligible to a substantial value for a 3 dB increase in the optical power. A sufficient condition for a detector control attack is a large ratio of detection probabilities over a 3 dB change in the trigger pulse power [25, 34] (or 6 dB change in the trigger pulse power for distributed-phase-reference protocols [30]). Then Eve can intercept the quantum states from Alice and resend bright trigger pulses corresponding to her detection to Bob [25, 34]. If Eve used a measurement basis not matching Bob's, she wanted her pulse to remain undetected. Indeed, when the pulse is measured by Bob in a different basis, it will be split to both detectors, corresponding to a 3 dB reduction in its power, and almost never cause a click. Due to the large difference in detection probability for a 3 dB change in the trigger pulse amplitude, a detector control attack would cause negligible errors and not expose eavesdropping, for the comparator threshold settings $\lesssim 20$ mV. Above ~ 20 mV the trigger pulses stop causing clicks at all, and this attack method no longer works. However, it may be possible to reach higher threshold settings using a different attack method described in the next section.

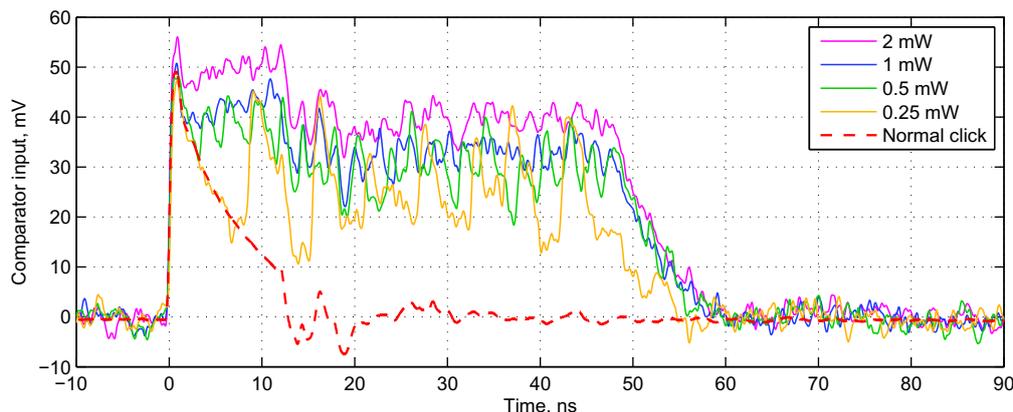


Figure 5. Electrical response in the non-latched state to the 48 ns, 1550 nm optical pulse. Single-shot traces with 2 GHz bandwidth for different pulse powers are shown, as well as an averaged normal single-photon response.

4. Detector control via deadtime extension

4.1. Device physics

In this section we consider a non-latched, single-photon-sensitive normally operating detector. The attack is based on the detector's ability to form a hotspot in response to bright light when the current I through the SNSPD is low. In addition, the hotspot formation probability at a low current is strongly superlinear. It is well known that at relatively low values of the bias current I_b , multiphoton processes dominate the detector sensitivity [34, 49, 50]. Here we demonstrate that this effect becomes extreme during the normal recovery time after a photon detection.

In normal detector operation, after the hotspot formation, I drops to a fraction of I_b [47]. Then, I exponentially recovers to I_b at a low rate, owing to a relatively large kinetic inductance of the superconducting nanowire (see the dashed trace in figure 5). During the initial part of this recovery, the SNSPD remains insensitive to single photons, but it can react to a bright illumination by forming another hotspot, with a higher illumination power being able to form a hotspot earlier in the recovery. This is illustrated in figure 5, which shows the electrical response to a 48 ns long bright pulse. At 0.25 mW pulse power, the single-shot trace clearly shows that the SNSPD forms a hotspot on average every 6 ns. At 0.5 mW, the period reduces to ~ 2.7 ns. At higher optical powers, separate hotspot formations are no longer distinguishable, but the whole electrical pulse gets higher, indicating a lower average current through the nanowire during the optical pulse. Thus, during a sufficiently bright optical pulse, the electrical signal will stay above the comparator threshold. This allows Eve to extend the detector deadtime after the first photon detection, up to 500 ns with this detector setup, without causing latching.

We further quantify the hotspot formation probability during the recovery, by applying a 53 ps full-width at half-maximum (FWHM) trigger pulse after the closing edge of the 48 ns, 2.5 mW pulse. (The recovery after the bright pulse should be similar to the recovery after a single-photon detection; however, we focus on the former for reasons that will become apparent in the next subsection.) As far as we can see, the response to this trigger pulse is probabilistic and binary: the hotspot either forms or does not (figure 6). In the former case, the recovery resets and starts anew from a certain current value; in the latter case the recovery continues

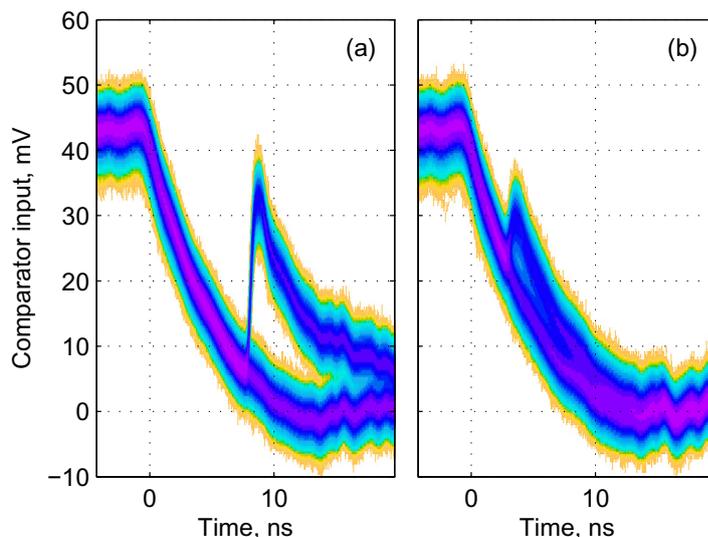


Figure 6. Accumulated 30 000 oscilloscope traces of the electrical response to the trigger pulse during the recovery from a 48 ns, 2.5 mW rectangular optical pulse. The trigger is (a) 8 ns into the recovery, 25 fJ energy and (b) 3 ns into the recovery, 78 fJ energy. In both cases, the trigger pulse causes hotspot formation with roughly 50% probability and resets the voltage to the same level. All oscillograms at trigger pulse delays ≥ 2 ns show the same behavior.

undisturbed. The probability that the trigger pulse causes a hotspot is plotted in figure 7. The measurement shows that the detection probability is reduced for at least 40 ns. It also shows that the detector is highly superlinear in at least the first 10 ns. During this time, a hotspot can be formed with unity probability using a sufficiently high energy trigger pulse (~ 150 fJ), while the same trigger pulse attenuated by 20 dB (i.e. 100 times lower pulse energy) is very unlikely to cause hotspot formation.

4.2. Application to eavesdropping

The extendability of the SNSPD's deadtime can be exploited in the previously described attack [24] on Bennett-Brassard 1984 (BB84) and similar protocols. We remark that superlinearity is not required for this attack, but is helpful and makes it easier. Here we propose a version of this attack for differential-phase-shift QKD (DPS-QKD) systems [37, 51]. We explain the key component of the attack: how Eve can control Bob's SNSPDs in the DPS-QKD system. Bob consists of an unbalanced Mach-Zehnder interferometer and two detectors, D_0 and D_1 (figure 8(a)). We assume that a properly implemented Bob will not accept clicks from both detectors for the duration of recovery after a click in one of the detectors, in order to avoid the detector deadtime and efficiency mismatch loopholes [18, 29]. As illustrated above, the expected recovery is ~ 40 ns long. Eve begins by applying to both detectors a laser pulse longer than the recovery time (figure 8(b)), with phase φ changing in steps along the pulse such that its power splits equally to the two detectors. This pulse produces a double click at the beginning, which, however, can be timed to fall in between the bit slots and be discarded by Bob (the extra clicks may affect routines that adjust the timing of Bob's acceptance windows, but note that

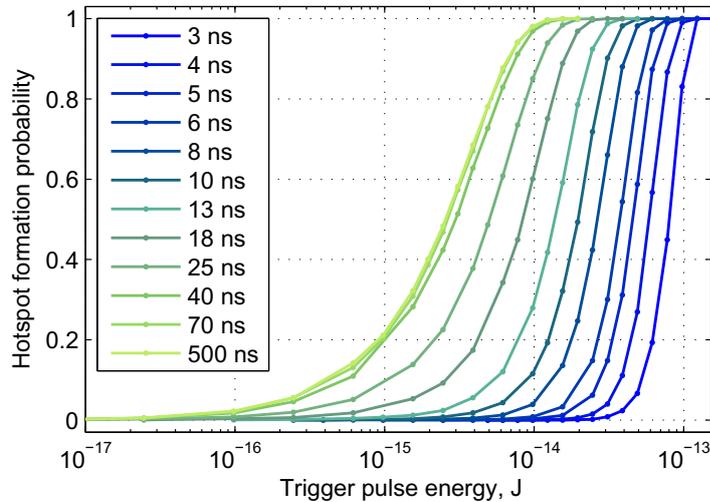


Figure 7. Hotspot formation probability versus energy of a 53 ps wide trigger pulse, for different trigger pulse delays after the closing edge of a 48 ns, 2.5 mW rectangular optical pulse (both pulses at 1550 nm). The probabilities were extracted from recorded oscillograms similar to those shown in figure 6. 10^{-13} J corresponds to 780 000 photons contained in the trigger pulse.

attacks on such calibration routines are also possible [26]). Immediately after this long pulse, Eve applies a sequence of short pulses. Their phases are chosen to steer them primarily to one of the two detectors (similarly to [30, 52]) and form hotspots in that detector only, keeping the comparator input voltage above the threshold. In the other detector, the voltage is allowed to fall below the comparator threshold. Then a pulse is applied and causes a click only in the detector that has recovered. Eve can end her control diagram here, or repeat the long pulse (as shown in figure 8(b)) and then make another controlled click. The total length of such a chained control diagram producing several controlled clicks is limited by the low-frequency cutoff of the RF components, and in the case of our setup can be up to 500 ns. We remark that the short pulsed parts of the diagram could, in principle, be replaced by a single phase-modulated long pulse; however, short pulses may be easier to steer between Bob's detectors in the case of sub-nanosecond Δt used in modern DPS-QKD systems [37].

The interferometers used for DPS-QKD are of a sufficiently good quality to allow Eve an extinction ratio of at least 20 dB when routing her short pulses between Bob's two detectors [37]. An examination of the recovery traces in figure 6 and hotspot formation probabilities in figure 7 suggests that the above control diagram will work. It should allow Eve to make clicks in Bob deterministically, or close to deterministically, in a wide range of comparator threshold voltages and Δt , even for $\Delta t = 100$ ps [37] and/or threshold voltages above 20 mV. Eve should be able to vary the number of short pulses during recovery to suit these system parameters, and still induce clicks in the correct detector most of the time.

While we did not have access to a complete DPS-QKD system to fully verify this Bob control method, we tested it experimentally by reproducing the expected power diagrams (optical power at D_0 and D_1 in figure 8(b)) at the single detector. We used $\Delta t = 5$ ns, and the threshold setting of 11.6 mV at the SR400 counter. We applied to the detector a 2 mW peak power, 53 ns long optical pulse, followed by 53 ps FWHM short optical pulses of varying

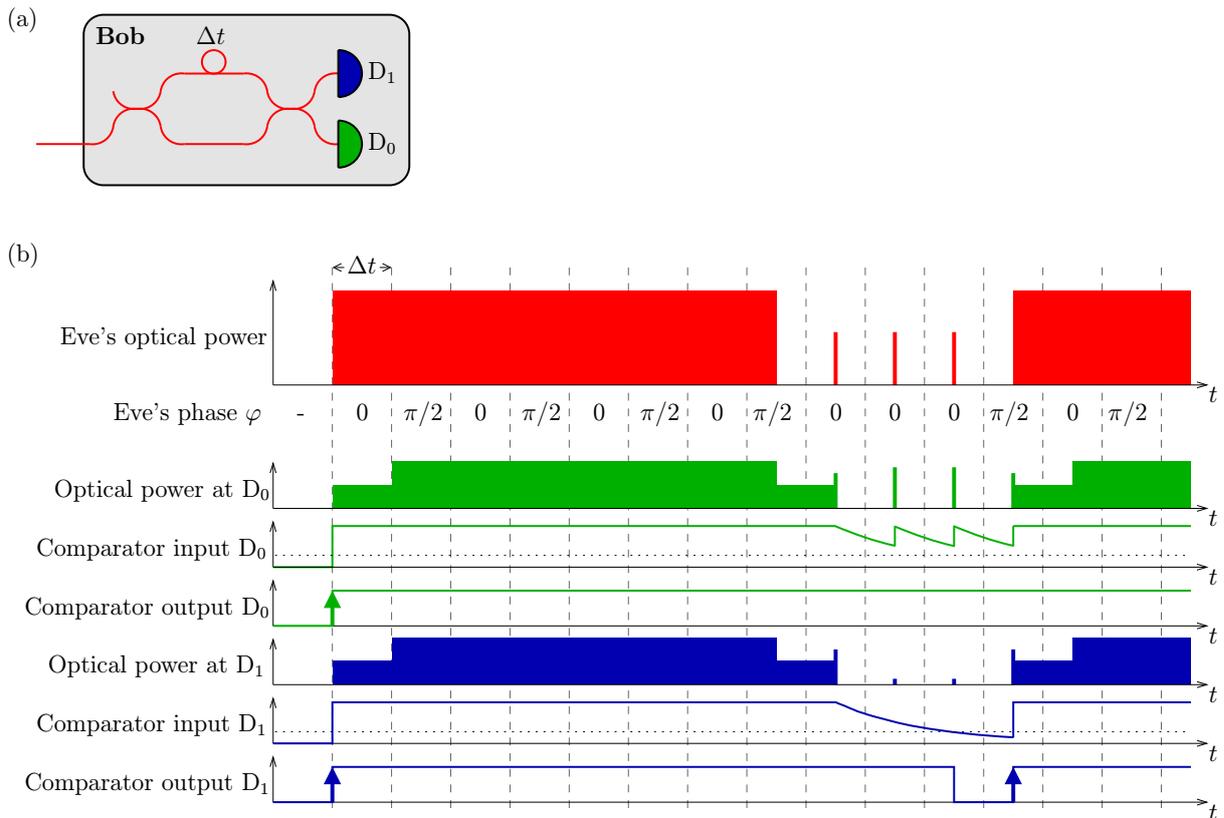


Figure 8. Proposed faked-state attack on the DPS-QKD system. (a) Bob's optical scheme. Δt is the time delay between the two interferometer arms. (b) Diagram showing Eve's optical output, how her light splits to Bob's two detectors, and how the electrical signals in each detector react to it.

energy. Measurement of the click probability while varying the short pulse energy showed that nearly perfect detector control ($<0.005\%$ click probability in the wrong detector) would be achievable if Bob's interferometer in the DPS-QKD system had a reasonable 20 dB extinction ratio, and good control ($<1\%$ click probability in the wrong detector) would be possible at a very poor 10 dB extinction ratio. The extinction ratio of Bob's interferometer determines how well Eve can suppress her short pulses from reaching the wrong detector, while making the target detector click with nearly unity probability. The jitter of the controllable click caused by the short pulse in the target detector was 250 ps FWHM, while that of the double click caused by the long pulse's leading edge was 170 ps FWHM.

One can note that Eve would need to know Bob's detector parameters rather precisely to execute this attack. In modern cryptography, according to Kerckhoffs' principle [53], the properties of the equipment are assumed to be fully known to Eve. In practice, to learn the detector parameters, Eve might, at first, try to attack intermittently a few bits at a time (which would not raise the error rate noticeably) while varying her attack parameters, and watch the public discussion between Alice and Bob [35]. One can also note that Eve's intercept-and-resend equipment would introduce an insertion delay of at least some tens of ns. However, the photon's time-of-flight is not authenticated in today's implementations of QKD, and is not

a part of the practical QKD protocols. Furthermore, in a fiber-optic line Eve can easily cancel this insertion delay by shortcutting a part of the line between her intercept and resend units with a line-of-sight RF classical link [28, 35].

5. Discussion and conclusion

The experimental results show that the control of this SNSPD is nearly perfect. Therefore, if this SNSPD were used in a QKD system, an eavesdropper could use bright illumination to capture the full raw and secret key while introducing negligible errors. Installation of the eavesdropper is fully reversible: the detector survived the bright illumination with no signs of damage or deterioration⁵.

While the SNSPD is based on a different physics than the APD single-photon detector, the similarity in how they can be controlled is startling. Latching the SNSPD using bright illumination can be considered as permanently blinding it, without the need for additional illumination to keep it blind. In the latched/blind state, the SNSPD exhibits the same superlinear response to bright trigger pulses as a blind APD. Likewise, controlling the SNSPD using deadtime extension is nearly identical to controlling the APD using deadtime extension: the only difference is that for this SNSPD the low-frequency cutoff of the RF components (and on a longer time scale the latching phenomenon) limits how long the deadtime can be extended.

Countermeasures against bright illumination attacks have been discussed extensively [24, 25, 28, 33, 45, 46, 54–56], and the conclusions are equally applicable to SNSPDs. The difference between public-key cryptography and QKD is that for the latter there exist security proofs. However, when the security is proved for systems with imperfections, models are used for the devices in the implementations. Even if this experiment is only performed on one device, *the results show that the response deviates considerably from the models* in the simple security proofs that are usually employed [5, 6, 10]. There are more advanced security proofs that could allow such a response under certain conditions [15, 34], but this would require discarding large amounts of the raw key to remove Eve's knowledge about the final key. For gated APD-based detectors, there is a proposal to bound the detector parameters by including a calibrated light source inside Bob, randomly testing and thereby guaranteeing the single-photon sensitivity at random times [54]. Another approach suggests to move detectors outside the secure devices and thus outside the security proof [57, 58].

If one only wants to avoid these specific attacks, proposals for APD-based detectors [24, 25, 28, 33, 45, 46, 54–56] should be equally efficient on SNSPDs, for instance an optical power meter at the entrance of Bob. In an installed QKD system, latching should be avoided either by an automated reset or by including a shunt resistor in parallel with the nanowire [59], but this does not guarantee that latching is precluded for all types of external input. Developing such specific countermeasures effective against *specific*, known attacks is less than satisfactory, because this introduces an unproven extra assumption into the QKD security model that the countermeasure also eliminates all *unknown* attacks exploiting the same loophole. Meanwhile, the difference between the device and its model in the QKD security proof remains. This approach would downgrade the level of the QKD security model to that of public-key cryptography, which also includes unproven assumptions (of computational complexity).

As mentioned in the introduction, SNSPDs are still in their infancy and therefore our findings might not apply to other detector designs. However, our findings clearly demonstrate that unless detector control is specially considered during design, SNSPDs may be controllable

using bright illumination, just as their APD-based cousins are. Furthermore, it could be possible to design the SNSPDs to be compliant with security proofs for QKD. This early stage of SNSPD technology is an excellent opportunity to avoid detector control vulnerability for future generations of SNSPDs. Designing hack-proof detectors will be crucial for the success of QKD.

Acknowledgments

We thank A Korneev, R Hadfield and V Burenkov for useful discussions. This work was supported by the Research Council of Norway (grant no. 180439/V30), Ontario Center of Excellence (OCE) and National Research Council of Canada (NSERC). LL and VM thank the Institute for Quantum Computing for travel support during their visit to Waterloo.

References

- [1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing* (New York: IEEE Press) pp 175–9
- [2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661–3
- [3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145–95
- [4] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
- [5] Lo H K and Chau H F 1999 *Science* **283** 2050–6
- [6] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441–4
- [7] Mayers D 1996 *Proc. Crypto '96* vol 1109 ed N Koblitz (New York: Springer) pp 343–57
- [8] Inamori H, Lütkenhaus N and Mayers D 2007 *Eur. Phys. J. D* **41** 599–627
- [9] Koashi M and Preskill J 2003 *Phys. Rev. Lett.* **90** 057902
- [10] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325–60
- [11] Lo H K and Preskill J 2007 *Quantum Inf. Comput.* **7** 431–58
- [12] Zhao Y, Qi B and Lo H K 2008 *Phys. Rev. A* **77** 052327
- [13] Fung C H F, Tamaki K, Qi B, Lo H K and Ma X 2009 *Quantum Inf. Comput.* **9** 131–65
- [14] Lydersen L and Skaar J 2010 *Quantum Inf. Comput.* **10** 60–76
- [15] Marøy Ø, Lydersen L and Skaar J 2010 *Phys. Rev. A* **82** 032337
- [16] Vakhitov A, Makarov V and Hjelme D R 2001 *J. Mod. Opt.* **48** 2023–38
- [17] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev. A* **73** 022320
- [18] Makarov V, Anisimov A and Skaar J 2006 *Phys. Rev. A* **74** 022313
Makarov V, Anisimov A and Skaar J 2008 **78** 019905 (erratum)
- [19] Qi B, Fung C H F, Lo H K and Ma X 2007 *Quantum Inf. Comput.* **7** 73–82
- [20] Zhao Y, Fung C H F, Qi B, Chen C and Lo H K 2008 *Phys. Rev. A* **78** 042333
- [21] Lamas-Linares A and Kurtsiefer C 2007 *Opt. Express* **15** 9388–93
- [22] Fung C H F, Qi B, Tamaki K and Lo H K 2007 *Phys. Rev. A* **75** 032314
- [23] Xu F, Qi B and Lo H K 2010 *New J. Phys.* **12** 113026
- [24] Makarov V 2009 *New J. Phys.* **11** 065003
- [25] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photonics* **4** 686–9
- [26] Jain N, Wittmann C, Lydersen L, Wiechers C, Elser D, Marquardt C, Makarov V and Leuchs G 2011 *Phys. Rev. Lett.* **107** 110501
- [27] Sun S H, Jiang M S and Liang L M 2011 *Phys. Rev. A* **83** 062331
- [28] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C and Makarov V 2011 *Nat. Commun.* **2** 349
- [29] Weier H, Krauss H, Rau M, Fürst M, Nauerth S and Weinfurter H 2011 *New J. Phys.* **13** 073024
- [30] Lydersen L, Skaar J and Makarov V 2011 *J. Mod. Opt.* **58** 680–5

- [31] Wiechers C, Lydersen L, Wittmann C, Elser D, Skaar J, Marquardt C, Makarov V and Leuchs G 2011 *New J. Phys.* **13** 013043
- [32] Sauge S, Lydersen L, Anisimov A, Skaar J and Makarov V 2011 *Opt. Express* **19** 23590–600
- [33] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Opt. Express* **18** 27938–54
- [34] Lydersen L, Jain N, Wittmann C, Marøy Ø, Skaar J, Marquardt C, Makarov V and Leuchs G 2011 *Phys. Rev. A* **84** 032320
- [35] Makarov V and Hjelme D R 2005 *J. Mod. Opt.* **52** 691–705
- [36] Hadfield R H, Habif J L, Schlafer J, Schwall R E and Nam S W 2006 *Appl. Phys. Lett.* **89** 241129
- [37] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 *Nat. Photonics* **1** 343–8
- [38] Stucki D, Walenta N, Vannel F, Thew R T, Gisin N, Zbinden H, Gray S, Towery C R and Ten S 2009 *New J. Phys.* **11** 075003
- [39] Rosenberg D *et al* 2009 *New J. Phys.* **11** 045009
- [40] Liu Y *et al* 2010 *Opt. Express* **18** 8587–94
- [41] Akhlaghi M K and Majedi A H 2008 *21st Annu. Meeting of the IEEE Lasers and Electro-Optics Society (2008)* pp 234–5
- [42] Orgiazzi J L F X and Majedi A H 2009 *IEEE Trans. Appl. Supercond.* **19** 341–5
- [43] Yan Z, Akhlaghi M K, Orgiazzi J L and Majedi A H 2009 *J. Mod. Opt.* **56** 380–4
- [44] Rosfjord K M, Yang J K W, Dauler E A, Kerman A J, Anant V, Voronov B M, Gol'tsman G N and Berggren K K 2006 *Opt. Express* **14** 527–34
- [45] Yuan Z L, Dynes J F and Shields A J 2010 *Nat. Photonics* **4** 800–1
- [46] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photonics* **4** 801
- [47] Yang J K W, Kerman A J, Dauler E A, Anant V, Rosfjord K M and Berggren K K 2007 *IEEE Trans. Appl. Supercond.* **17** 581–5
- [48] Annunziata A J *et al* 2010 *J. Appl. Phys.* **108** 084507
- [49] Verevkin A, Zhang J, Sobolewski R, Lipatov A, Okunev O, Chulkova G, Korneev A, Smirnov K, Gol'tsman G N and Semenov A 2002 *Appl. Phys. Lett.* **80** 4687–9
- [50] Akhlaghi M K and Majedi A H 2009 *IEEE Trans. Appl. Supercond.* **19** 361–6
- [51] Nambu Y, Hatanaka T and Nakamura K 2004 *Japan. J. Appl. Phys.* **43** L1109–L1110
- [52] Makarov V and Skaar J 2008 *Quantum Inf. Comput.* **8** 622–35
- [53] Kerckhoffs A 1883 *J. Sci. Militaires* **IX** 5–38
- [54] Lydersen L, Makarov V and Skaar J 2011 *Phys. Rev. A* **83** 032306
- [55] Yuan Z L, Dynes J F and Shields A J 2011 *Appl. Phys. Lett.* **98** 231104
- [56] Lydersen L, Makarov V and Skaar J 2011 *Appl. Phys. Lett.* **99** 196101
- [57] Lo H K, Curty M and Qi B 2011 Measurement device independent quantum key distribution arXiv:1109.1473 [quant-ph]
- [58] Braunstein S L and Pirandola S 2011 Side-channel free quantum key distribution arXiv:1109.2330 [quant-ph]
- [59] Hadfield R 2011 private communication