Superlinear threshold detectors in quantum cryptography

Lars Lydersen,[1,2,*] Nitin Jain,[3,4] Christoffer Wittmann,[3,4] Øystein Marøy,[1,2] Johannes Skaar,[1,2] Christoph Marquardt,[3,4] Vadim Makarov,[1,2] and Gerd Leuchs[3,4]

[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]*Max Planck Institute for the Science of Light, Günther-Scharowsky-Strasse 1/Bau 24, DE-91058 Erlangen, Germany*
[4]*Institut für Optik, Information und Photonik, University of Erlangen-Nuremberg, Staudtstraße 7/B2, DE-91058 Erlangen, Germany*
(Received 10 June 2011; published 15 September 2011)

We introduce the concept of a superlinear threshold detector, a detector that has a higher probability to detect multiple photons if it receives them simultaneously rather than at separate times. Highly superlinear threshold detectors in quantum key distribution systems allow eavesdropping the full secret key without being revealed. Here, we generalize the detector control attack, and analyze how it performs against quantum key distribution systems with moderately superlinear detectors. We quantify the superlinearity in superconducting single-photon detectors based on earlier published data, and gated avalanche photodiode detectors based on our own measurements. The analysis shows that quantum key distribution systems using detector(s) of either type can be vulnerable to eavesdropping. The avalanche photodiode detector becomes superlinear toward the end of the gate. For systems expecting substantial loss, or for systems not monitoring loss, this would allow eavesdropping using trigger pulses containing less than 120 photons per pulse. Such an attack would be virtually impossible to catch with an optical power meter at the receiver entrance.

I. INTRODUCTION

Single-photon detectors [1] can be regarded as essential parts of quantum information processing hardware, and are certainly crucial components in quantum key distribution (QKD) systems [2–7]. In QKD, the communicating parties Alice and Bob exploit the properties of quantum mechanics to reveal any eavesdropping attempt by the eavesdropper Eve. The security of QKD has been proven for perfect devices [4,5]. However, when the security of QKD is to be proven for practical systems [8–16], it is necessary to construct models based on assumptions about the practical devices, and hence also about the single-photon detectors.

With a few exceptions [17,18], most single-photon detectors suitable for QKD systems are threshold detectors that cannot resolve the number of photons in a pulse. They rather have a binary response distinguishing between zero, and "one or more" photons, where a detection event is often referred to as a "click." Threshold detectors are usually characterized by their quantum efficiency η, which is the probability to detect a single photon. For multiphoton pulses, a very common assumption is that each photon within the pulse is detected individually with probability η. Then, the detection probability of a n-photon Fock state can be expressed as

$$p_{\text{det}}(n) = 1 - (1 - \eta)^n. \tag{1}$$

We refer to threshold detectors with a multiphoton detection probability higher than the one given by Eq. (1) as *superlinear* threshold detectors. A superlinear threshold detector has a larger probability to detect multiple photons if it receives them nearly simultaneously, than if it receives each of the photons separately at different times. This effect is well known in multiphoton absorption by atoms [19], where the multiphoton

absorption rate can be much higher for chaotic light than for laser light with the same mean intensity. Meanwhile for threshold detectors, superlinear response may also originate from how the entire device converts individual excitations into the macroscopic detection event.

The photon number of a coherent state follows a Poisson distribution with probability $p_n = \mu^n e^{-\mu}/n!$, where μ is the mean photon number. Therefore, if the detection probability of a n-photon Fock state is given by Eq. (1), a coherent state with mean photon number μ is detected with probability

$$p_{\text{det}} = \sum_{n=0}^{\infty} \frac{\mu^n e^{-\mu}}{n!} p_{\text{det}}(n) = 1 - e^{-\mu\eta}. \tag{2}$$

Note that for a coherent state with mean photon number μ, a superlinear threshold detector with quantum efficiency η will have a higher detection probability than the one given by Eq. (2).

Insufficient models of single-photon detectors have caused numerous security loopholes [15,20–30] in QKD. For instance, the time-shift attack [21] based on detector efficiency mismatch [20] has been shown to break the security of a commercial QKD system [24]. More recently, the detector control attack [25–30] allows the eavesdropper to capture the full key without revealing her presence (via errors in the key). Specifically, the attack introduces zero quantum bit error rate (QBER). Furthermore, this attack, which is based on bright illumination, is implementable with current technology. Two commercial QKD systems were shown to be vulnerable to the attack [25–27], and a full eavesdropper has been implemented to capture the full key of an experimental QKD system under realistic conditions [29]. However, the power level (more than 500 μW) of the eavesdropper's illumination has led to discussions of whether an optical power meter at the entrance of Bob can be used to detect these attacks [31–34].

___

*lars.lydersen@iet.ntnu.no

In this paper we propose and analyze an attack against QKD systems with superlinear detectors (Sec. II). Note that the previously published detector control attack [25] is based on an extreme superlinear behavior of the detectors, and can therefore be considered a special case of the "imperfect" detector control attack presented here. Then we discuss how the attack would perform against superconducting single-photon detectors [35,36], which have been reported to exhibit superlinear behavior (Sec. III). In Sec. IV we show that avalanche photodiode (APD)-based gated detectors have a substantial superlinear response at the end of the gate. The superlinear behavior at the end of the gate allows eavesdropping with very faint trigger pulses [25,32]. This *faint after-gate attack* will be virtually impossible to catch with an optical power meter at the entrance of Bob. At least one security proof covers QKD systems with superlinear detectors [16]. In Sec. V we show how the detector control attack relates to the security proof, and discuss possible countermeasures. Finally, we conclude in Sec. VI.

II. THEORY OF SUPERLINEAR DETECTOR CONTROL

The core of the previously proposed detector control attacks is the following [25]: in the Bennett-Brassard 1984 (BB84) [2] family of protocols, Eve uses a random basis to measure the quantum state from Alice. Then she resends her measurement result, not as a single photon, but rather as a bright pulse, called a trigger pulse, with a carefully selected optical power. Then, if Eve uses Bob's measurement basis, her trigger pulse is *always* detected by Bob. On the contrary, if Eve uses a basis not matching Bob's to measure the quantum state from Alice, her trigger pulse is *never* detected. This is possible because Bob's detectors are very superlinear: for less than a factor of two (3 dB) increase in trigger pulse power, the detection probability shoots from 0 to 100%. Since Eve uses the correct basis only half of the time, the total loss between Alice and Bob is 3 dB. For the differential-phase-shift protocol [37,38] there is no basis choice, so the same factor of two (3 dB) superlinearity allows eavesdropping without extra loss [30]. The coherent one-way protocol [39,40] is also vulnerable to the detector control attacks [30], but requires a more strict relationship between the superlinearities of the detectors in the system.

The previously proposed detector control attacks allow Eve to capture the full secret key without introducing any QBER. However, Alice and Bob usually tolerate a nonzero QBER (typically less than 11%). Therefore, Eve might introduce a small QBER without getting caught. What if the superlinearity of the detector is such that when Eve selects the right basis, the trigger pulse is detected with a *high* probability, while when Eve selects the wrong basis, the trigger pulse is detected with a *low* probability? One can immediately identify two consequences of this "imperfect" detector control attack: the nonunity detection probability when Eve uses the right basis will contribute extra to the loss. On the other hand, the nonzero detection probability when Eve uses the wrong basis will introduce a nonzero QBER.

We will here consider an active basis choice BB84 implementation using two detectors. In a passive basis choice BB84 implementation [41], Eve's trigger pulse will strike the detectors in both bases simultaneously for each bit. For this case, the QBER introduced by the attack depends on how Bob handles simultaneous clicks in both bases. Assume that Bob assigns a random bit value to these events. Then, if the probability for simultaneous clicks in both bases is nonzero, the QBER introduced by an imperfect detector control attack will be higher in a passive basis choice implementation than in an active basis choice implementation. In any case, for passive basis choice implementations, the theoretical QBER derived below can be used as a lower bound.

To calculate the QBER caused by this attack, let $p_{f,i}$ be the detection probability in detector i for the trigger pulse with full power. Likewise, let $p_{h,i}$ be the detection probability at detector i with half the power. We assume Eve resends the same power regardless of her detected bit value, that double clicks are assigned to a random bit value [42], and that Eve selects Bob's measurement basis with probability $1/2$. When Eve resends in the wrong basis and Bob has a detection, the bit value will be erroneous with probability $1/2$. Therefore, the QBER caused by the imperfect detector control attack is given by

$$\text{QBER} = \frac{1}{2} \frac{\text{Bob detects and Eve used wrong basis}}{\text{Bob has a detection}}$$
$$= \frac{p_{h,0} + p_{h,1} - p_{h,0}p_{h,1}}{p_{f,0} + p_{f,1} + 2(p_{h,0} + p_{h,1} - p_{h,0}p_{h,1})}, \quad (3)$$

where dark counts have been omitted. Errors originating from dark counts would add to the errors caused by the attack. However, in a good detector design the amount of errors from dark counts is minimized. Since we require the eavesdropper to reproduce the detection probability from normal operating conditions, the dark count probability would be minimized under attack as well. A high dark count probability, and thus a high error rate without the eavesdropper would leave the attack less room for errors to be introduced. However, an equivalent restriction on the attack is easier obtained by lowering the acceptance threshold for the QBER. Therefore, our analyses is limited to the QBER introduced by the attack, and dark counts are omitted. Assuming that both detectors have equal detection probabilities, $p_{f,i} = p_f$ and $p_{h,i} = p_h$, Eq. (3) simplifies to

$$\text{QBER} = \frac{2p_h - p_h^2}{2p_f + 2(2p_h - p_h^2)}. \quad (4)$$

As discussed above, the perfect detector control attack introduces 3 dB loss when applied against BB84 QKD systems with active basis choice in Bob's implementation, because Eve only selects the correct basis half of the time. If $\min_i p_{f,i} < 1$, the attack will cause an even higher loss. On the other hand, $\max_i p_{h,i} > 0$ will reduce the loss introduced by the attack. Therefore, the transmittance T when an imperfect detector control attack is applied against a BB84 QKD system with active basis choice is given by

$$T = \tfrac{1}{4}(p_{f,0} + p_{f,1}) + \tfrac{1}{2}(p_{h,0} + p_{h,1} - p_{h,0}p_{h,1}). \quad (5)$$

Note that T refers to the transmittance between Eve and Bob. If Eve uses imperfect detectors, this will add to the total loss observed by Alice and Bob. For the remainder of the paper, we simply consider Eve to use perfect detectors. Since Eve can place her detectors close to Alice, and she

can use detectors with almost unity detection efficiency [18], this is an acceptable assumption. If both detectors have equal probabilities, Eq. (5) simplifies to

$$T = \tfrac{1}{2} p_f + \tfrac{1}{2}\left(2p_h - p_h^2\right).\qquad(6)$$

Note that in passive implementations of Bob, such as passive basis choice in BB84 [41], or in distributed phase reference protocols [37–40], there is no 3 dB loss due to basis choice. Therefore, the above expression for the transmittance T can be considered a lower bound also for such implementations.

In most cases, the eavesdropper can introduce substantial loss without getting noticed. With the notable exception of transition-edge sensors [18], the quantum efficiency of Bob's detectors is typically about 10% at telecom wavelengths [1]. Furthermore, an optical fiber usually exhibits a loss of about 0.2 dB/km at 1550 nm wavelength. Adding the loss owing to detector's quantum efficiency to the loss in the line at a typical distance of 50 km, Alice and Bob normally observe a total loss of 20 dB, corresponding to $T \sim 0.01$. In addition to this, there is loss in the optical path inside Bob's apparatus. However, Eve can always adjust the power in her trigger pulses to strike Bob's detectors with a given optical power. Therefore, by inserting her eavesdropping station into the line close to Alice's system, Eve has almost the full 20 dB at her disposal. In one case, a QKD system operating with loss up to 40 dB has been reported [43] (but the actual, tolerable loss might be less because there is no satisfactory security proof for the protocol used in Ref. [43]). Therefore, it seems that for many QKD setups, Eve can introduce loss of more than 20 dB without being revealed from the reduction in the transmittance.

III. SUPERLINEARITY OF SUPERCONDUCTING SINGLE-PHOTON DETECTORS

Superconducting single-photon detectors (SSPDs) based on superconducting nanowires [35] have been used for long-distance QKD experiments [43–47], due to their ultralow dark count rate and timing jitter. However, the need for cryogenic cooling to temperatures in the 2–4 K range has prevented them from being used in commercial QKD systems.

In SSPDs, the nanowire is cooled to the superconducting state. Then, then the nanowire is biased with a current I_b slightly lower than the critical current I_c. Because the wire is superconducting at I_b, there is no voltage drop over the device. A photon incident on the nanowire can create a normally conducting hotspot, with the effect that the whole cross section of the nanowire becomes normally conducting. This increases the voltage over the device. Afterward, the cooling restores superconductivity in the nanowire, and the current increases back to the bias current. This dead time is usually about 10 ns. The biasing current I_b can be adjusted for a trade-off between high detection efficiency and low dark count rate.

Already in the first systematic investigation of the detection efficiency of SSPDs [36], superlinear behavior due to multi-photon absorption mechanisms was reported. The superlinear behavior is wavelength dependent, and is substantial at 1550 nm, which is the wavelength suitable for long-distance experiments. Figure 1 shows the detection count data for 1550 nm extracted from Fig. 1 in Ref. [36], processed as detection probability (count rate/trigger pulse rate), and plotted
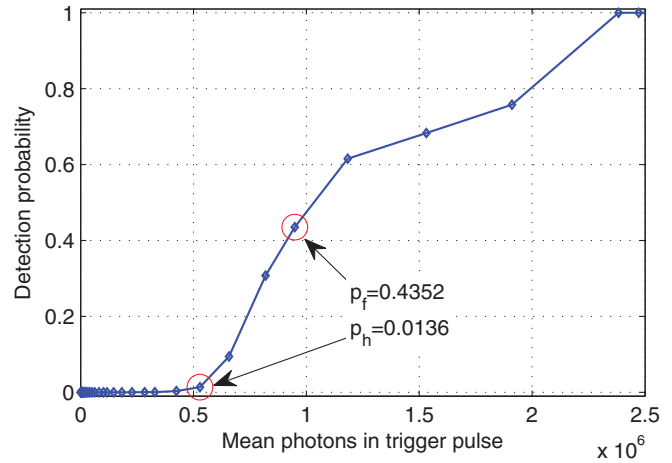

FIG. 1. (Color online) The detection probability versus mean photon number in the trigger pulse for the SSPD in Ref. [36], at 1550 nm and $I_b = 0.8I_c$. Count rates were extracted from Fig. 1 in Ref. [36], and divided by the pulse repetition frequency of 82 MHz to obtain the detection probability. The red circled data points were used to calculate the QBER and the transmittance from an attack.

on a linear scale. The SSPD was biased at $I_b/I_c = 0.8$. The superlinear behavior is suitable for eavesdropping in QKD: by increasing the photon number, the detection probability increases sharply. Using trigger pulses containing 10^6 photons per pulse, Eq. (4) predicts a QBER of less than 3%, and Eq. (6) predicts a transmittance $T > 0.20$ (assuming reasonable errors in extracting the numerical data from the plot in Ref. [36]). Therefore, a QKD system using this SSPD would clearly be vulnerable to a detector control attack.

Judging by the low detection probability at one photon per pulse for this SSPD, the QKD experiments would use a higher bias current to get better sensitivity. Unfortunately, few publications seems to report the detection probabilities for pulses above the single-photon level, especially for 1550 nm wavelength. The available literature shows that SSPDs are less superlinear at shorter wavelengths [36], and also less superlinear at higher bias currents [48]. However, note that any superlinear detector response must be handled in the security proof. Therefore, the reported data on SSPDs [36,48] clearly shows that such a security proof is necessary for QKD systems using SSPDs.

IV. SUPERLINEARITY OF GATED APD-BASED DETECTORS

The gated APD-based detectors in the QKD system Clavis2 by ID Quantique exhibit substantial superlinear behavior far after the gate [27], or when blinded by bright illumination [25,26]. However, as pointed out before [25,31], the bright trigger pulses might be revealed by an optical power meter at the entrance of Bob. Here, we show that at the end of the gate, when the APD is biased close to the breakdown voltage, the superlinear response allows Eve to use very faint trigger pulses.

The detection probability during the gate was measured as follows: the gated InGaAs detectors in the QKD system Clavis2 were run with factory settings, but with the gating
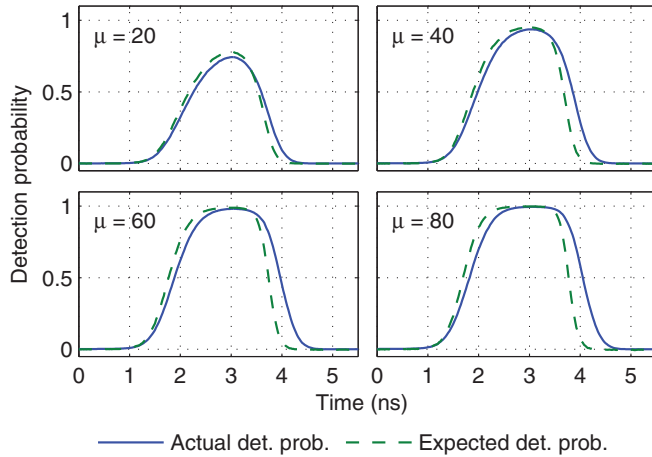
FIG. 2. (Color online) The measured detection probability for a coherent state with $\mu = 20, 40, 60$, and 80, compared to the expected detection probabilities predicted by Eq. (2). Data points are 25 ps apart. Data for detector 0 is shown; detector 1 behaved very similarly. When the mean photon number μ is increased, deviation between the expected detection probabilities and the actual measured detection probabilities increases, especially at the end of the gate. See also Fig. 3.

frequency reduced from 5 MHz to 98 kHz. The reduced frequency corresponds to the factory frequency with a detection in every gate, and afterpulse blocking (forced 10 μs dead time after detection events to reduce dark counts) enabled. A short-pulsed laser (see the Appendix for the pulse shape) was attenuated to the appropriate mean photon number and connected directly to the fiber pigtail of each detector. Then, the laser pulse was scanned through the gate in steps of 25 ps, and the detection probability was recorded in each step. The "quantum efficiency" η was measured by applying a coherent state $\mu = 1$, and solving η from Eq. (2). In fact, the detector is slightly superlinear, but a coherent state with $\mu = 1$ contains only a small fraction of multiphoton pulses.[1]

Once the quantum efficiency η is known, Eq. (2) can be used to calculate the expected detection probability for a coherent state with any mean photon number, assuming that each photon is detected individually. Figure 2 shows the detection probability of a coherent state for various mean photon numbers predicted by Eq. (2), compared to the actual detection probabilities measured in our experiment.

The measurement data matches the expected detector response fairly well until the falling edge of the gate. There, the measured detection probability becomes superlinear. One possible explanation for this could be the following: an avalanche, started by a photon in a localized spot, laterally spreads over time to encompass the entire junction area of the APD [49]. For detection events before the falling edge of the gate, the avalanche has sufficient time to spread and therefore the current reaches the same amplitude regardless of

the number of photons absorbed in the APD [17]. At the end of the gate, an avalanche from a single-photon absorption does not have sufficient time to spread to the entire junction area, and therefore only causes a small current insufficient of crossing the comparator threshold. However, multiple photon absorptions in different spots across the junction can start multiple small avalanches that together provide enough current to cross the comparator threshold. This is exactly the process exploited to make photon-number-resolving APD-based detectors [17]. Avalanche spreading assisted by secondary photons reemitted by the APD, has already been used to explain avalanche development [49,50]. Similarly, multiple photon absorptions caused by the multiphoton pulse could speed up the avalanche development.

For the gated APD-based detectors, the superlinear response can be exploited in a faint version of the after-gate attack [27]. From Eve's perspective, the original after-gate attack has some drawbacks. The attack may cause a substantial amount of errors in the key, because the bright pulses cause afterpulses with a random bit value. Furthermore, in principle, an optical power meter can be used to catch Eve's bright pulses. Also, removing gates randomly or as a part of afterpulse blocking (to avoid excessive dark counts) would reveal the attack because the trigger pulses would cause clicks regardless of the presence of a gate. Then, detection events without a gate applied would indicate the presence of the eavesdropper. Similarly, it has been noted that in the original after-gate attack could be countered by ignoring detection events outside the gate [33], while for this faint after-gate attack, the detections happen within the gate [34].

As discussed in Sec. II, having a "high" detection probability for a given trigger pulse power, and a "low" detection probability for a 3 dB dimmer trigger pulse is suitable for Eve's attack. Figure 3 shows the measured and expected detection probability at a single point at the falling edge of the gate. For less than 40 photons per trigger pulse, the APDs clearly exhibit superlinear response in favor of the eavesdropper.

The detection probability curve of the detector 0 (the results are very similar for detector 1) was used when calculating
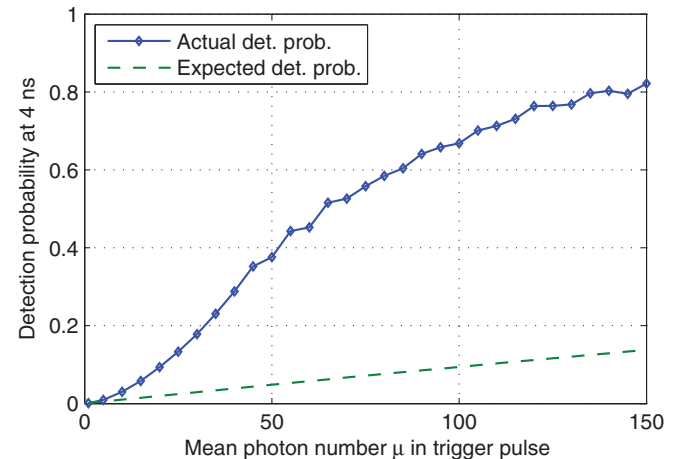

FIG. 3. (Color online) Detection probability at the falling edge of the gate (at the 4 ns point in Fig. 2). For $\mu < 40$, the shape of the actual detection probability is clearly superlinear, in contrast to the nearly linear expected detection probability.

---

[1]The coherent state with $\mu = 1$ was obtained by shining much brighter pulses into a power meter and calculating the energy per pulse. Then a controlled amount of optical attenuation was introduced to decrease the energy level of each pulse to $\mu = 1$.
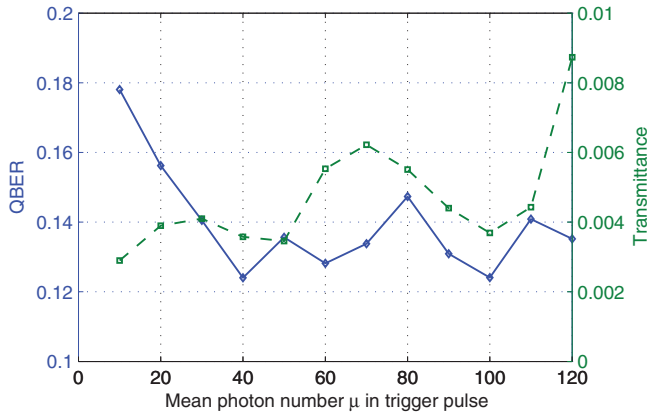
FIG. 4. (Color online) The minimum QBER (solid curve) caused by trigger pulses with various mean photon numbers calculated from Eq. (4) and the corresponding transmittance (dashed curve) calculated from Eq. (6). The data contains some noise due to fluctuations in applied power and/or fluctuations in the detection efficiency.

QBER and transmittance from Eqs. (4) and (6). Figure 4 shows the resulting QBER and the corresponding transmittance for various mean photon numbers in the trigger pulse, when the trigger pulse timing was optimized to minimize the QBER. The data indicates that a faint after-gate attack could cause a QBER around 13% with a transmittance of about 0.005, corresponding to 23 dB loss (for instance, for $\mu = 40$, $p_f = 0.0054$ and $p_h = 0.00089$ at the point 4.525 ns in Fig. 2). As discussed in Sec. II, this transmittance corresponds to Bob's detectors having 10% quantum efficiency, a line loss corresponding to about 50 km of fiber and another 3 dB loss in Bob's apparatus, which are reasonable values.

While most QKD systems do not accept QBER above 11% [5], there are postprocessing protocols which accept QBER up to 20% [51]. Also note that the QBER introduced by the attack may be significantly lower with yet shorter trigger pulses, since they would better resolve the superlinear behavior at the falling edge of the gate. Our relatively wide pulse (see the Appendix) arrives at both linear and superlinear regions of the gate. Therefore the superlinear response to it must be less than that to a narrower pulse arriving only at the most superlinear point in the gate.

The detectors in Clavis2 have been shown to exhibit detection efficiency mismatch [20,24,52]. Therefore, in general, one would have to use different timings and/or different powers depending on the bit value, to avoid skewing the bit value distribution in the raw key. Also, the superlinearity could be exploited in other attacks, such as the faked-state attack [52,53] and conventional quantum attacks, to make them more efficient [15]. ID Quantique has been notified about this loophole, prior to submission of the paper.

V. COUNTERMEASURES AND PROOF OF SECURITY

The security of QKD systems with arbitrary nonlinearities in Bob's system, and therefore superlinear threshold detectors, has already been proved [16]. Without source imperfections

and with symmetry in the two bases, the secret key rate is given by [16]

$$R \geqslant -h(\text{QBER}) + \eta[1 - h(\text{QBER})], \qquad (7)$$

where $h(\cdot)$ is the binary entropy function, and η is the smallest detection probability of a nonvacuum state. If one further assumes that the probability to detect a multiphoton state is higher than a single photon, η is simply the quantum efficiency (the probability to detect a single photon).

As for the detector control attack, let us assume the worst-case superlinearity, namely, that a single photon is detected with probability η, while a two-photon state is detected with probability 1. Then, Eve can use trigger pulses with two photons, and Eq. (4) simplifies to

$$\text{QBER} = \frac{2\eta - \eta^2}{2 + 2(2\eta - \eta^2)}. \qquad (8)$$

Figure 5 shows Eq. (7) for $R = 0$ and Eq. (8), comparing the "imperfect" detector control attack with the bounds derived in the security proof [16]. It shows that a sufficiently high detection probability, and thus quantum efficiency, allows extraction of secret key regardless of any superlinear detector response. For instance, if the QBER is 5%, a quantum efficiency $\eta > 0.4$ allows the extraction of secret key. Note that a high quantum efficiency does not remove the superlinear effect, but then the security proof makes it possible to remove any knowledge Eve could have obtained exploiting the superlinear response, by (a large amount of) extra privacy amplification [54].

For gated systems, one possible countermeasure might be bit-mapped gating [55]. Then, the basis selector is used to randomize all detection events outside the center of the gate. Therefore, trigger pulses timed at the falling edge of the gate
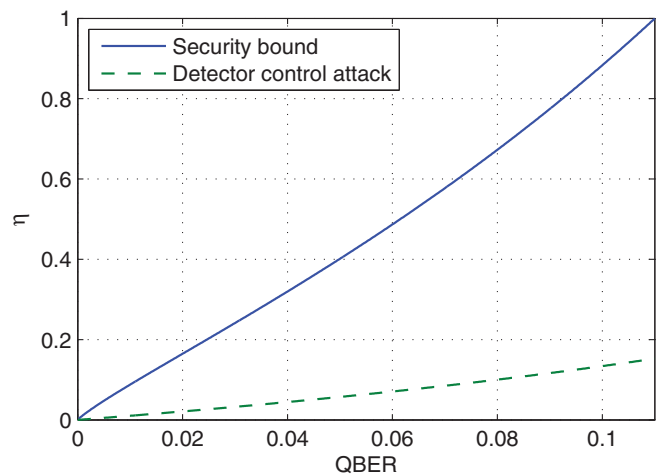

FIG. 5. (Color online) Comparison of the detector control attack and the bound from the security proof [16]. The region to the left of the security bound curve (solid curve) allows extraction of a secure key. The region to the right of the detector control attack curve (dashed curve) is clearly insecure, because the attack presented in Sec. II can be applied. The region between the curves should be assumed insecure.

would cause random detections and thus a QBER of 50%. This would reveal Eve's presence. However, the security analysis for bit-mapped gating requires that each photon is detected individually during the transition of the basis selector. In practice, this means that the detectors must have a detection probability given by Eq. (2) in the center of the gate. Figure 2 shows that this is nearly the case. It might be possible to detect each photon completely individually in the middle of the gate by expanding the gate, or by shaping the applied electrical gate appropriately.

VI. SUMMARY AND CONCLUSION

In this paper we have analyzed the security of QKD systems using superlinear threshold detectors. The detector control attack previously reported [25] is based on very superlinear detection probability: when the amplitude of the trigger pulses is increased, the detection probability sharply increases from 0 to 100%. This allows eavesdropping the full key without causing any errors; the only side effect is 3 dB total loss. Here, the detector control attack is generalized to moderately superlinear detectors by accepting a limited amount of errors in the key and/or accepting a higher loss. Note that in practice, a total loss of about 20 dB may be tolerable, as discussed in Sec. II.

Nanowire SSPDs [35] have been reported to have superlinear detection probability [36]. We have shown that by carefully selecting the trigger pulse amplitude, an eavesdropper would introduce a QBER of less than 3% when attacking the SSPD in Ref. [36]. The total loss caused by the eavesdropping would be less than 6 dB. Therefore, a QKD system using this detector would clearly be insecure.

Figures 2 and 3 show that the response of the APD-based gated detector is superlinear at the falling edge of the gate. Therefore, it is possible to attack the gated detectors with faint trigger pulses, with less than 120 photons per pulse. From the measurements, the attack would cause a QBER of about 13% and about 23 dB loss. Most QKD systems do not accept a QBER above 11% [5], but there are postprocessing protocols allowing a QBER up to 20% [51]. Furthermore, we suspect that both the QBER and the loss could be reduced by using shorter trigger pulses.[2] Finally, even if the attack is not directly applicable to some QKD systems due to the QBER and/or loss threshold, the superlinear response of the APD-based detector shows that ordinary security proofs no longer apply to these systems. Therefore, these systems must use advanced security proofs to bound and remove Eve's partial knowledge from the moderate superlinear response.

The faint after-gate attack does not suffer from the limitations of the original after-gate attack [27]. In the faint after-gate attack, the afterpulsing is negligible. Furthermore, with less than 120 photons per pulse, the trigger pulses should be nearly impossible to catch with an optical power meter at the entrance of Bob. Also, removing gates randomly or due to after-pulse blocking will not expose the attack [27] since such trigger pulse will not cause a click unless there is a gate present.

Furthermore, the timing of the trigger pulse detection will be very similar to a normal detection inside the gate, and therefore difficult to discard based on timing [33].

If the detectors have an increasing detection probability for increasing photon number, a sufficiently high quantum efficiency makes it possible to remove Eve's knowledge using privacy amplification [54]. For gated APD-based detectors, bit-mapped gating [55] can be used if each photon is detected individually in the center of the gate.

Quantum key distribution has been proven secure, so currently the challenge is to make a secure implementation. We believe that weeding out loopholes caused by the implementation is a necessary step toward achieving practical secure QKD, and that this work is crucial because it fully exposes the nature of the detector control attack.

APPENDIX: PULSE SHAPE OF ID300

Figure 6 shows the pulse shape of the id300 short-pulsed laser [56]. This is the particular laser sample used in this experiment; other samples of this laser model may have a different pulse shape.
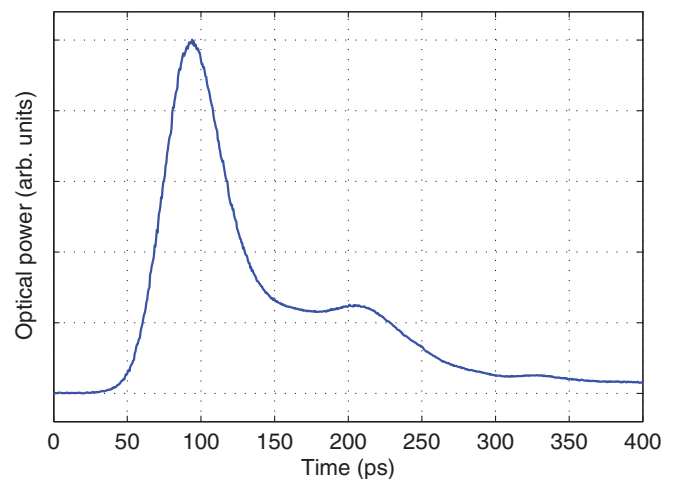

FIG. 6. (Color online) Pulse shape of the id300 short-pulsed laser, measured with a 45 GHz optical probe on a 12.5 GHz sampling oscilloscope at a pulse repetition rate of 100 kHz.

---

[2]Unfortunately we did not have a laser with shorter pulse-width at our disposal for this experiment.

[1] R. H. Hadfield, Nat. Photonics **3**, 696 (2009).

[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.

[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[4] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[8] D. Mayers, in *Proceedings of Crypto'96*, edited by N. Koblitz (Springer, New York, 1996), Vol. 1109, pp. 343–357.

[9] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).

[10] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).

[11] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[12] H.-K. Lo and J. Preskill, Quantum Inf. Comput. **7**, 431 (2007).

[13] Y. Zhao, B. Qi, and H.-K. Lo, Phys. Rev. A **77**, 052327 (2008).

[14] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **9**, 131 (2009).

[15] L. Lydersen and J. Skaar, Quantum Inf. Comput. **10**, 60 (2010).

[16] Ø. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010).

[17] B. E. Kardynal, Z. L. Yuan, and A. J. Shields, Nat. Photonics **2**, 425 (2008).

[18] A. E. Lita, A. J. Miller, and S. W. Nam, Opt. Express **16**, 3032 (2008).

[19] B. R. Mollow, Phys. Rev. **175**, 1555 (1968).

[20] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006); **78**, 019905 (2008).

[21] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73 (2007).

[22] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007).

[23] V. Makarov and J. Skaar, Quantum Inf. Comput. **8**, 622 (2008).

[24] Y. Zhao, Chi-Hang Fred Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).

[25] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[26] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18**, 27938 (2010).

[27] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011).

[28] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, e-print arXiv:0809.3408.

[29] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).

[30] L. Lydersen, J. Skaar, and V. Makarov, J. Mod. Opt. **58**, 680 (2011).

[31] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nat. Photonics **4**, 800 (2010).

[32] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 801 (2010).

[33] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Appl. Phys. Lett. **98**, 231104 (2011).

[34] L. Lydersen, V. Makarov, and J. Skaar, e-print arXiv:1106.3756.

[35] G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski, Appl. Phys. Lett. **79**, 705 (2001).

[36] A. Verevkin, J. Zhang, R. Sobolewski, A. Lipatov, O. Okunev, G. Chulkova, A. Korneev, K. Smirnov, G. N. Gol'tsman, and A. Semenov, Appl. Phys. Lett. **80**, 4687 (2002).

[37] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).

[38] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003).

[39] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, e-print arXiv:quant-ph/0411022v1.

[40] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).

[41] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).

[42] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).

[43] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nat. Photonics **1**, 343 (2007).

[44] R. H. Hadfield, J. L. Habif, J. Schlafer, R. E. Schwall, and S. W. Nam, Appl. Phys. Lett. **89**, 241129 (2006).

[45] D. Rosenberg *et al.*, New J. Phys. **11**, 045009 (2009).

[46] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).

[47] Y. Liu *et al.*, Opt. Express **18**, 8587 (2010).

[48] M. K. Akhlaghi and A. H. Majedi, IEEE Trans. Appl. Supercond. **19**, 361 (2009).

[49] A. Spinelli and A. L. Lacaita, IEEE Trans. Electron Devices **44**, 1931 (1997).

[50] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, J. Mod. Opt. **51**, 1267 (2004).

[51] H. F. Chau, Phys. Rev. A **66**, 060302 (2002).

[52] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. (to be published), e-print arXiv:1103.2327.

[53] V. Makarov and D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005).

[54] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[55] L. Lydersen, V. Makarov, and J. Skaar, Phys. Rev. A **83**, 032306 (2011).

[56] id300, datasheet: [http://www.idquantique.com/images/stories/PDF/id300-laser-source/id300-specs.pdf], visited 28, April 2011].