# Thermal blinding of gated detectors in quantum cryptography

**Lars Lydersen,**[1,2,*] **Carlos Wiechers,**[3,4,5] **Christoffer Wittmann,**[3,4] **Dominique Elser,**[3,4] **Johannes Skaar,**[1,2] **and Vadim Makarov**[1]

[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-Str. 1/Bau 24, 91058 Erlangen, Germany*
[4]*Institut für Optik, Information und Photonik, University of Erlangen-Nuremberg, Staudtstraße 7/B2, 91058 Erlangen, Germany*
[5]*Departamento de Física, Universidad de Guanajuato, Lomas del Bosque 103, Fraccionamiento Lomas del Campestre, 37150, León, Guanajuato, México*
[*]*lars.lydersen@iet.ntnu.no*

**Abstract:** It has previously been shown that the gated detectors of two commercially available quantum key distribution (QKD) systems are blindable and controllable by an eavesdropper using continuous-wave illumination and short bright trigger pulses, manipulating voltages in the circuit [Nat. Photonics **4**, 686 (2010)]. This allows for an attack eavesdropping the full raw and secret key without increasing the quantum bit error rate (QBER). Here we show how thermal effects in detectors under bright illumination can lead to the same outcome. We demonstrate that the detectors in a commercial QKD system Clavis2 can be blinded by heating the avalanche photo diodes (APDs) using bright illumination, so-called *thermal blinding*. Further, the detectors can be triggered using short bright pulses once they are blind. For systems with pauses between packet transmission such as the plug-and-play systems, thermal inertia enables Eve to apply the bright blinding illumination *before* eavesdropping, making her more difficult to catch.

© 2010 Optical Society of America

**OCIS codes:** (040.1345) Avalanche photodiodes (APDs); (040.5570) Quantum detectors; (270.5568) Quantum cryptography; (270.5570) Quantum detectors.

## References and links

1. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in "Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing," (IEEE Press, New York, Bangalore, India, 1984), pp. 175–179.
2. A. K. Ekert, "Quantum cryptography based on bell theorem," Phys. Rev. Lett. **67**, 661–663 (1991).
3. H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science **283**, 2050–2056 (1999).
4. P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441–444 (2000).
5. D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, "High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres," N. J. Phys. **11**, 075003 (2009).
6. Commercial QKD systems are available from at least two companies: ID Quantique (Switzerland), `http://www.idquantique.com`; MagiQ Technologies (USA), `http://www.magiqtech.com`.

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010


This paper was published in Optics Express and is made available as an electronic reprint with the permission of OSA. The paper can be found on OSA website at http://www.opticsinfobase.org/oe/abstract.cfm?uri=oe-18-26-27938 Systematic or multiple reproduction or distribution to multiple locations via electronic or other means is prohibited and is subject to penalties under law.

7. D. Mayers, "Advances in cryptology," in "Proceedings of Crypto'96," , vol. 1109, N. Koblitz, ed. (Springer, New York, 1996), vol. 1109, pp. 343–357.
8. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Inf. Comput. **4**, 325–360 (2004).
9. H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," Eur. Phys. J. D **41**, 599–627 (2007).
10. C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, "Security proof of quantum key distribution with detection efficiency mismatch," Quantum Inf. Comput. **9**, 131–165 (2009).
11. L. Lydersen and J. Skaar, "Security of quantum key distribution with bit and basis dependent detector flaws," Quantum Inf. Comput. **10**, 0060 (2010).
12. Ø. Marøy, L. Lydersen, and J. Skaar, "Security of quantum key distribution with arbitrary individual imperfections," Phys. Rev. A **82**, 032337 (2010).
13. A. Vakhitov, V. Makarov, and D. R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," J. Mod. Opt. **48**, 2023–2038 (2001).
14. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," Phys. Rev. A **73**, 022320 (2006).
15. V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," Phys. Rev. A **74**, 022313 (2006).
16. V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems: erratum," **78**, 019905 (2008).
17. V. Makarov and J. Skaar, "Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols," Quantum Inf. Comput. **8**, 0622 (2008).
18. B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," Quantum Inf. Comput. **7**, 73–82 (2007).
19. 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).
20. A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," Opt. Express **15**, 9388–9393 (2007).
21. S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, "Information leakage via side channels in freespace BB84 quantum cryptography," N. J. Phys. **11**, 065001 (2009).
22. C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, "Phase-remapping attack in practical quantum-key-distribution systems," Phys. Rev. A **75**, 032314 (2007).
23. F. Xu, B. Qi, and H.-K. Lo, "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system," N. J. Phys. **12**, 113026 (2010).
24. Precisely, the quantum bit error rate (QBER) is the fraction given by the number of bits which differ in Alice's and Bob's raw key, divided by the length of the raw key.
25. H. F. Chau, "Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate," Phys. Rev. A **66**, 060302 (2002).
26. D. Gottesman and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications," IEEE Trans. Inf. Theory **49**, 457–475 (2003).
27. V. Makarov, "Controlling passively quenched single photon detectors by bright light," N. J. Phys. **11**, 065003 (2009).
28. V. Makarov, A. Anisimov, and S. Sauge, "Quantum hacking: adding a commercial actively-quenched module to the list of single-photon detectors controllable by Eve," e-print arXiv:0809.3408v2 [quant-ph] .
29. 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).
30. C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "After-gate attack on a quantum cryptosystem," e-print arXiv:1009.2683 [quant-ph] .
31. I. Gerhardt, Q. Liu, J. Skaar, A. Lamas-Linares, C. Kurtsiefer, and V. Makarov, "Perfect eavesdropping on a quantum cryptography system," e-print arXiv:1011.0105 [quant-ph] .
32. I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "Free-space quantum key distribution with entangled photons," Appl. Phys. Lett. **89**, 101122 (2006).
33. M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, "Daylight operation of a free space, entanglement-based quantum key distribution system," N. J. Phys. **11**, 045007 (2009).
34. Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Avoiding the detector blinding attack on quantum cryptography," Nat. Photonics **4**, 800–801 (2010).
35. S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, "Evolution and prospects for single-photon avalanche diodes and quenching circuits," J. Mod. Opt. **51**, 1267–1288 (2004).
36. All references to the APD bias voltage are absolute valued, thus an APD biased "above" the breakdown voltage is in the Geiger mode. In practice the APDs are always reverse-biased.
37. V. Makarov and D. R. Hjelme, "Faked states attack on quantum cryptosystems," J. Mod. Opt. **52**, 691–705 (2005).
38. V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010
(C) 2010 OSA

splitting attacks for weak laser pulse implementations," Phys. Rev. Lett. **92**, 057901 (2004).
39. W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," Phys. Rev. Lett. **91**, 057901 (2003).
40. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
41. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
42. S. Cova, A. Longoni, and A. Andreoni, "Towards picosecond resolution with single-photon avalanche diodes," Rev. Sci. Instrum. **52**, 408–412 (1981).
43. D. S. Bethune and W. P. Risk, "An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light," IEEE J. Quantum Electron. **36**, 340–347 (2000).
44. A. Tomita and K. Nakamura, "Balanced, gated-mode photon detector for quantum-bit discrimination at 1550 nm," Opt. Lett. **27**, 1827–1829 (2002).
45. Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, "High speed single photon detection in the near infrared," Appl. Phys. Lett. **91**, 041114 (2007).
46. Osterm, PE4-115-14-15, `http://osterm.ru/PAGE/MULTISTAGE.HTM`, visited 3. August 2010.
47. When the temperature increases, the lattice vibrations in the APD increase. This increases the probability that the electron collides with the lattice, and therefore reduces the probability that the electron gains enough energy to trigger ionization of a new electron-hole pair. Therefore, to ensure that the electron gains ionization energy, the electric field must be larger, and thus the breakdown voltage is increased.
48. S. M. Sze and K. K. Ng, *Physics of semiconductor devices* (Wiley-Interscience, 2007).
49. Marlow, NL4012, `http://www.marlow.com/media/marlow/product/downloads/nl4012t/NL4012.pdf`, visited 3. August 2010.
50. The detectors do not have any dark counts and are assumed blind at a temperature of about $-40\,^{\circ}\mathrm{C}$ at the cold plate, or when the bias voltage is decreased by 0.97 V. If one assumes that the APD temperature is equal to the cold plate temperature, this means that heating the detectors by 10 K is equivalent to decreasing the bias voltage by about 1 V.
51. G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, "Automated 'plug & play' quantum key distribution," Electron. Lett. **34**, 2116–2117 (1998).
52. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," N. J. Phys. **4**, 41 (2002).
53. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
54. S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov. in preparation.
55. G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, "Fast and user-friendly quantum key distribution," J. Mod. Opt. **47**, 517–531 (2000).
56. The system actually sends the qubits in frames of 1075 qubits each. We initially made a mistake when counting them and used 1072 qubits, which is very close and does not affect the results.
57. We picked the second bit to simplify synchronization in our measurement setup. The results for the first bit should be very similar to the results for the second bit.
58. S. L. Braunstein and P. van Loock, "Quantum information with continuous variables," Rev. Mod. Phys. **77**, 513–577 (2005).
59. U. L. Andersen, G. Leuchs, and C. Silberhorn, "Continuous-variable quantum information processing," Laser Photon. Rev. **4**, 337 (2010), ArXiv:1008.3468v1 [quant-ph].

## 1. Introduction

In theory quantum mechanics allows two parties, Alice and Bob, to grow a private, secret key, even if the eavesdropper Eve can do anything permitted by the laws of nature [1–4]. The field of quantum key distribution (QKD) has evolved rapidly in the last two decades, with transmission distance increasing from a table top demonstration to over 250 km in the laboratory [5], and commercial QKD systems available from several vendors [6].

However the components used for the experimental realizations of QKD have imperfections. As for any security technology, it is crucial to scrutinize the implementations in order to obtain a high level of practical security. The discovery of security loopholes does not prove that QKD is insecure, but rather that principles of QKD are not sufficiently well implemented.

Numerous imperfections have been addressed in security proofs [7–12]. For some loopholes it took several years from their discovery until they were covered by security proofs, for instance the Trojan-horse [13, 14] loophole and detector efficiency mismatch [15–17]. The latter was exploited in the time-shift attack [18] on a commercial QKD system [19]. Other loopholes

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010
(C) 2010 OSA

include a variety of side-channels [20–23].

Common to the loopholes mentioned so far is that the corresponding attacks are not implementable in practice, leave Eve with a probabilistic advantage, or introduce a QBER close to the tolerable limit. For instance, the implementation of the time-shift attack [19] gave Eve a probabilistic, information-theoretic advantage. With probability 0.04 the unconditional security is broken; however, extra information is needed and a nontrivial computational task remains to obtain the secret key. In the practical phase-remapping attack [23], Eve caused 19.7% QBER [24] compromising the rarely used two-way post-processing protocol which produces secure key at QBER up to 20% [25, 26].

There is however one class of attacks which stands out in terms of implementability, Eve's information and QBER: The *blinding attacks* [27–29] are fully implementable with current technology, and give Eve the whole raw key while causing zero additional QBER. The latter is essential as the QBER is measured to reveal Eve's presence. In these attacks, the APDs are tricked to exit the single-photon sensitive Geiger mode, and are so-called *blind*. Eve uses a copy of Bob's apparatus to detect Alice's signals, but resends bright trigger pulses instead of single photons, as in the after-gate attack [30]. When the detectors are blind, Bob will only detect the bright trigger pulses if he uses the same basis as Eve. Otherwise his detectors remain silent. Hence Eve gets a full copy of the raw key while causing no additional QBER. Both passively quenched detectors [27], actively quenched detectors [28] and the gated detectors of two commercially available QKD systems [29] have been shown to be vulnerable to blinding. In the case of the passively-quenched detectors, this loophole has been exploited in the first full-scale implementation of an eavesdropper [31], which was inserted in the middle of the 290 m transmission line in an experimental entanglement-based QKD system [32, 33], and recovered 100% of the raw key.

Previously the gated detectors in the commercially available system Clavis2 from manufacturer ID Quantique were subject to continuous-wave (CW) blinding [29]. The blinding illumination caused the bias voltage at the APDs to drop due to the presence of DC impedance of the bias voltage supply, and therefore the APDs were never in Geiger mode. Shortly after the result was published, Yuan *et al.* proposed that removing the bias voltage impedance or lowering the comparator threshold in the detectors would hinder blinding in gated detectors [34]. However, in this paper we show how the same detectors, regardless of the impedance of the bias voltage supply, can be blinded by heating the APD, so-called *thermal blinding*. Furthermore we show how the AC-coupling of the detectors allows a blinding technique which may blind the detectors even if the comparator threshold is lowered. We show that thermal blinding is more sophisticated form of attack than previously reported CW-blinding [29] because the APD can be heated well in advance of the detection times, and is as such harder to catch. Especially for Clavis2, all the detector parameters such as temperature of the cold plate, bias voltage and APD current indicate single photon sensitivity while the detectors are in fact blind.

In this paper we first briefly review how APDs in the linear mode can be exploited to eavesdrop on QKD systems (Section 2). Then the detector design in Clavis2 is discussed (Section 3) before we show how it is possible to thermally blind and trigger the detectors (Section 4). Finally we briefly discuss countermeasures in Section 5 and conclude in Section 6.

## 2. Eavesdropping exploiting APDs in linear mode

In this section we briefly review how APDs in the linear mode can be exploited to eavesdrop on QKD systems [28, 29].

In Geiger mode operation, an electron-hole pair produced by an absorbed single photon is amplified to a large current in the APD, which exceeds a current comparator threshold and reveals the photon's presence. This is referred to as a *click* [35].

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010
(C) 2010 OSA