Comment on "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography" [Appl. Phys. Lett. 98, 231104 (2011)]

Lars Lydersen,[a] Vadim Makarov, and Johannes Skaar
Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway and University Graduate Center, NO-2027 Kjeller, Norway

(Received 19 June 2011; accepted 16 October 2011; published online 11 November 2011)

Quantum key distribution (QKD) has initially been proven secure using ideal devices. However, implementations use imperfect devices available with current technology. Therefore, there are security proofs for QKD which model the devices to allow imperfections, though at the expense of a lower secure key rate. To achieve provable security, it is crucial that the devices and implementations are verified to be within the models in the security proofs.

Security loopholes have been found originating from discrepancies between the actual implementations and the models in the security proofs. For instance, one such discrepancy allows the tailored bright illumination attacks,[1–3] recently shown also to be applicable against superconducting nanowire single-photon detectors.[4,5] In this case, the loophole is caused by the response of qubit measurement devices (detectors) to swarms of qubits (bright illumination). The question is how to counter such loopholes.

In their paper, Yuan *et al.* propose to counter these bright illumination attacks by monitoring the avalanche photodiode (APD) current for "anomalously high values."[6] The robustness of this countermeasure is shown by arguing that previously proposed attacks do not work anymore. First of all, this leaves the challenge of determining what is "anomalously high." In order to achieve provable security, this threshold must originate from a security proof. Second, the fundamental issue, namely that the detector response deviates from the models in the security proofs,[7] is not solved by this countermeasure.

As discussed previously,[8,9] practical QKD cannot become provably secure by intuitive countermeasures against known attacks. This approach also requires manufacturers to make frequent, possibly costly upgrades to their systems. Loopholes should instead be countered by modifying the implementation and/or the security proofs such that the devices are within the models of the security proofs. This is the only way practical QKD can obtain the provable security that makes it superior to classical key distribution schemes. This is also how loopholes have been handled previously: for example, the photon-number splitting attack[10] led to more general security proofs[11] and eventually more efficient protocols to negate the decrease in the key rate.[12] In another example, detector efficiency mismatch,[13] enabling for instance the time-shift attack,[14,15] is now included in security proofs.[16,17] For the bright illumination attacks, we have proposed a secure detection scheme which integrates with security proofs.[18] In this scheme, a calibrated light source is used to verify the quantum efficiency in the center of the detector gate. Randomizing detection events outside the center of the gate provide a lower bound on the fraction of detections in the center of the gate. Other proposals also exist.[19,20]

In this particular case, we have already shown that an eavesdropper using temporally tailored light of short pulses containing less than 120 photons can threaten the security of QKD.[4] This faint after-gate attack would not be detectable with the countermeasure proposed by Yuan *et al.*, since the pulses would not cause an "anomalously high" current, but rather a current similar to the current caused by a single photon. Therefore, this serves as an example of the risk associated with closing loopholes in an intuitive way.

[a] Electronic mail: lars.lydersen@iet.ntnu.no.

[1] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[2] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18**, 27938 (2010).
[3] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011).
[4] L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. A **84**, 032320 (2011).
[5] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, "Controlling a superconducting nanowire single-photon detector using tailored bright illumination," New J. Phys. (in press).
[6] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Appl. Phys. Lett. **98**, 231104 (2011).
[7] There are security proofs including this detector response in their model of the receiver (for instance Ref. 17), but they predict zero secret key rate for such receivers.
[8] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nat. Photonics **4**, 800 (2010).
[9] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 801 (2010).
[10] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[11] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[12] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[13] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006), erratum *ibid.* **78**, 019905 (2008).
[14] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73 (2007).
[15] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[16] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **9**, 131 (2009).
[17] Ø. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010).
[18] L. Lydersen, V. Makarov, and J. Skaar, Phys. Rev. A **83**, 032306 (2011).
[19] H.-K. Lo, M. Curty, and B. Qi, e-print arXiv:1109.1473.
[20] S. L. Braunstein and S. Pirandola, e-print arXiv:1109.2330.

0003-6951/2011/99(19)/196101/1/$30.00