Laser damage of photodiodes helps the eavesdropper

Audun Nystad Bugge[1], Sebastien Sauge[2], Aina Mardhiyah M. Ghazali[3], Johannes Skaar[1,4], Lars Lydersen[1,4] and Vadim Makarov[5]

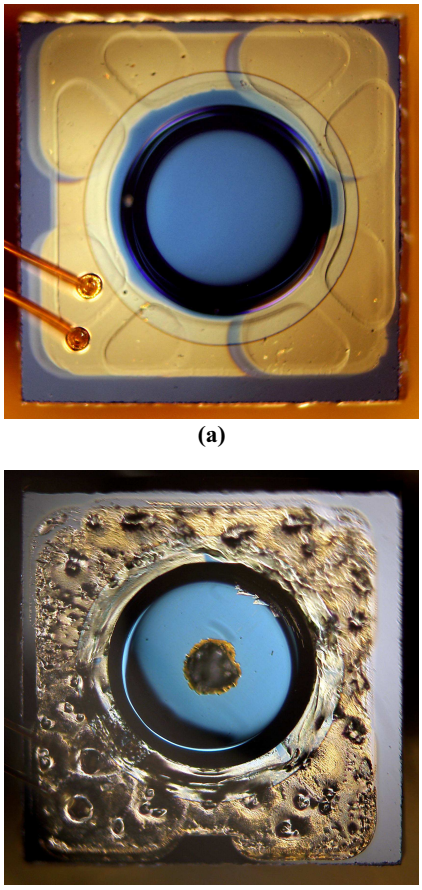
[1]*Department of Electronics and Telecommunications, Norwegian University of Science and Technology, Trondheim, Norway*
[2]*School of Information and Communication Technology, Royal Institute of Technology (KTH), Kista, Sweden*
[3]*Department of Science in Engineering, Faculty of Engineering, International Islamic University Malaysia, Kuala Lumpur, Malaysia*
[4]*University Graduate Center, Kjeller, Norway*
[5]*Institute for Quantum Computing, University of Waterloo, Waterloo, Canada*

Quantum key distribution, although secure in principle, suffers from discrepancies between the simplified model of apparatus used in its security proof, and the actual hardware being used. Often, such discrepancies can be exploited by an eavesdropper to steal the secret key.

One of the assumptions about the apparatus made in the security proof is that the eavesdropper, in general, *cannot* arbitrarily and permanently change the characteristics of the legitimate parties' apparatus. Here we disprove this assumption experimentally, by permanently damaging and thus changing the photonic and electrical characteristics of silicon avalanche photodiodes using high-power illumination. Such one-time change can open the quantum key distribution system to eavesdropping.

We exposed PerkinElmer C30902SH silicon avalanche photodiodes to a focused 807 nm continuous-wave laser radiation at a range of powers up to 3 W [1]. The photodiodes were characterized between exposures. After about 1 W power, the photodiodes permanently developed a large dark current, which made them blind to single photons in a passively-quenched detector scheme, yet deterministically controllable by bright light pulses, allowing eavesdropping [2]. Above 1.7 W power exposure, the photodiodes lost photosensitivity and became electrically either a resistor or an open circuit, accompanied by visible structural changes (Fig. 1).

This attack immediately applies to quantum key distibution schemes operating over a free-space channel. Future studies should investigate laser damage to actively-quenched avalanche photodetectors, optical scheme components other than photodiodes, various fibre-optic components, as well as contermeasures to this new class of attacks.



(a)

(b)

Figure 1: Microscope images of PerkinElmer C30902SH avalanche photodiode. **(a)** undamaged photodiode (bright field illumination). **(b)** photodiode after exposure to 3 W focused light for 60 s. A hole melted through the chip in the center, and the gold electrode melted (photodiode sample different from image (a); dark field illumination).

References

[1] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen and V. Makarov, *unpublished.*

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