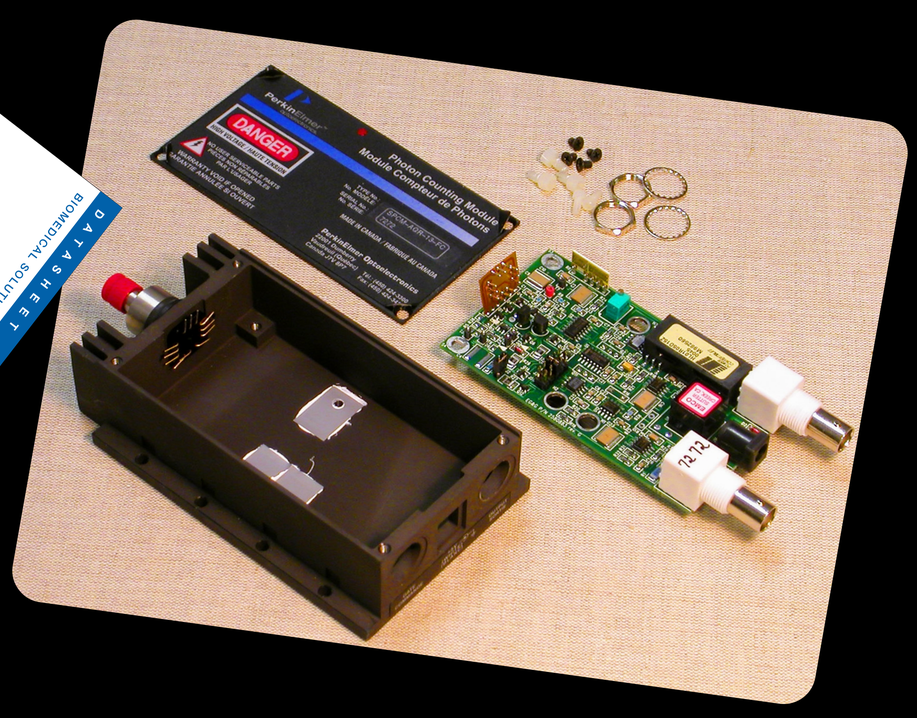
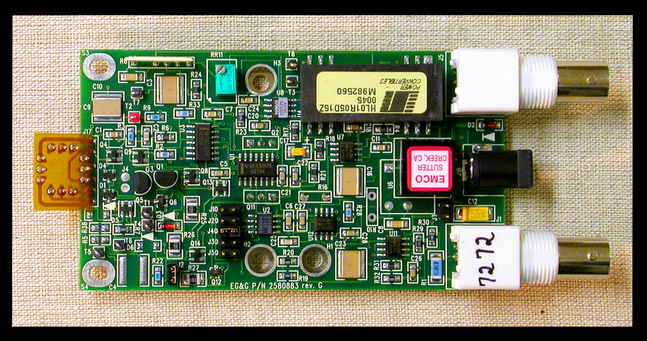
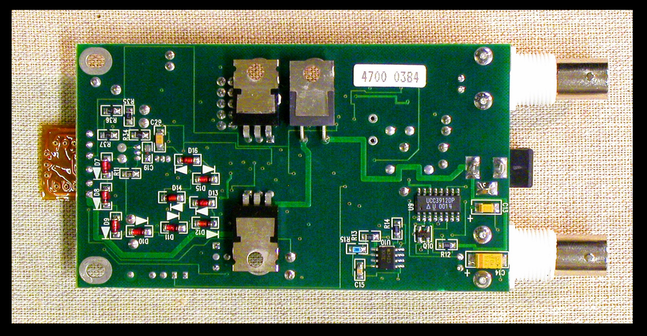
# Can Eve control PerkinElmer actively-quenched detector?

**V. Makarov** (1), **A. Anisimov** (2), **S. Sauge** (3)
1: Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway; makarov@vad1.com
2: Radiophysics Department, St. Petersburg State Polytechnic University, Russia
3: Department of Microelectronics and Information Technology, Royal Institute of Technology (KTH), Sweden

## I. The suspect, reverse-engineered

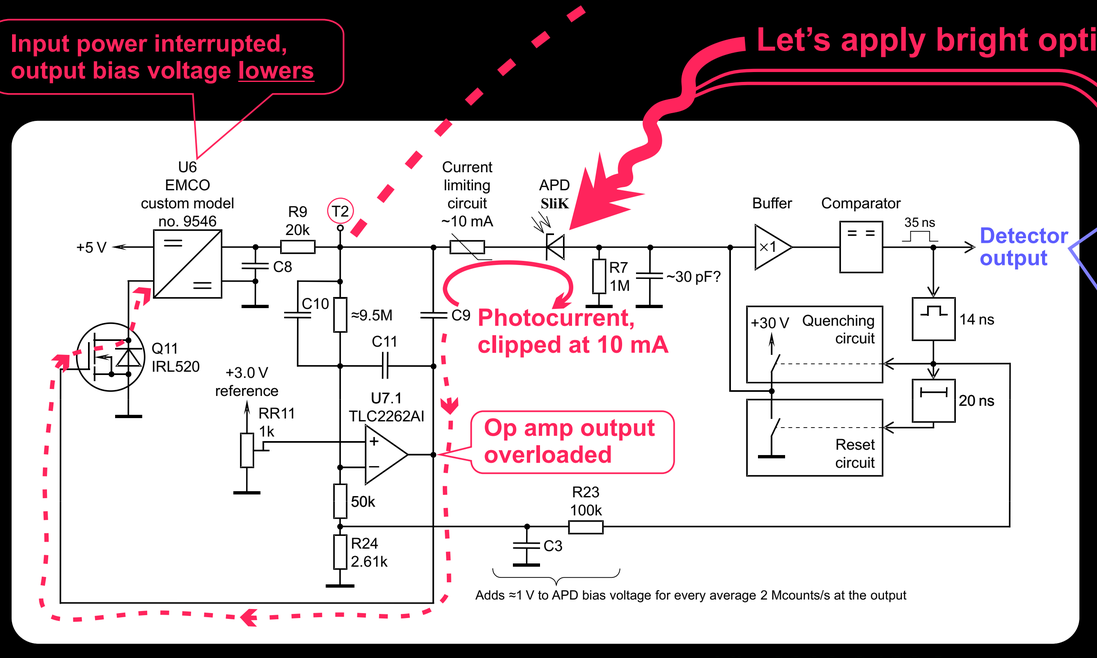



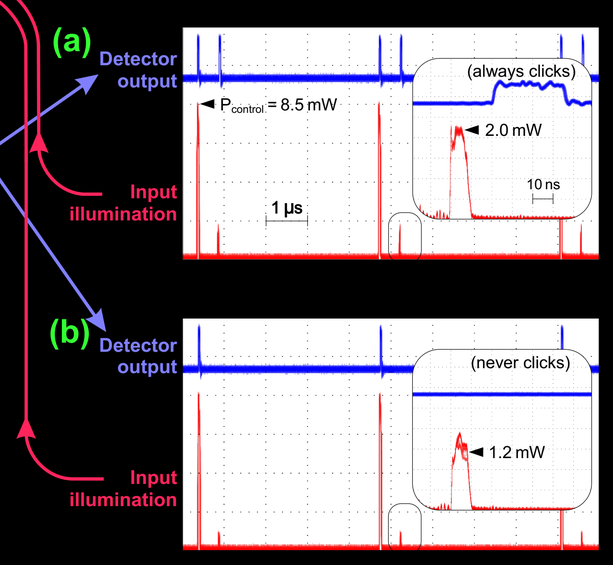


## II. Control method №4

**Let's apply bright optical control pulses, 50 ns wide**

**Input power interrupted, output bias voltage lowers**



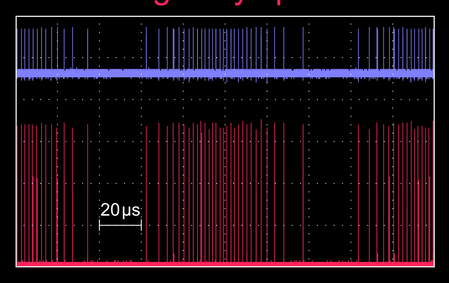







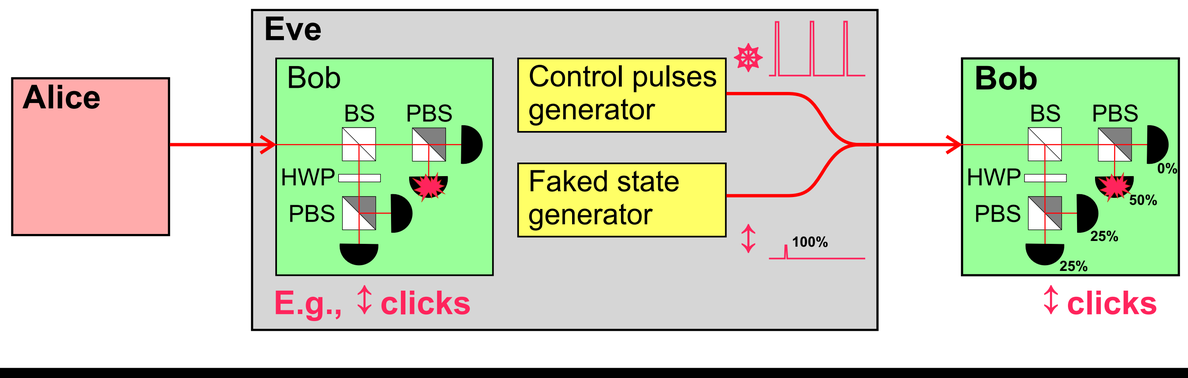
**Filled symbols: full control, no spontaneous counts, detector only reacts to bright pulses**

**Note**: control pulses can be irregularly spaced:




arXiv:0809.3408 [quant-ph]

## III. Proposed attack




**Side effect**: simultaneous clicks from control pulses, >70 kHz. Eve can try to masquerade them as out-of-sync clicks or as background counts.

## Possibly affected experimental quantum cryptosystems

1. C. Erven *et al.,* arXiv:0807.2289 [quant-ph].
2. V. Fernandez *et al.,* IEEE J. Quantum Electron. **43**, 130 (2007); K. J. Gordon *et al.,* Opt. Express **13**, 3015 (2005); IEEE J. Quantum Electron. **40**, 900 (2004).
3. X. Shan *et al.,* Appl. Phys. Lett. **89**, 191121 (2006).
4. K. J. Resch *et al.,* Opt. Express **13**, 202 (2005).
5. W. T. Buttler *et al.,* Phys. Rev. Lett. **84**, 5652 (2000); *ibid.* **81**, 3283 (1998); Phys. Rev. A **57**, 2379 (1998).

There may be a few more... people don't always specify which model of detector they use.

NTNU Det skapende universitet · KTH VETENSKAP OCH KONST · SPbSPU

Presented at SECOQC international conference in Vienna, October 8–10, 2008