Energy–time attack on detectors in quantum key distribution

Vadim Makarov[1,2], Vladimir Bizin[1], Jialei Su[3,4], Dmitriy Kuzmin[5], Anqi Huang[3], Konstantin Zaitsev[2]

[1]*Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[2]*Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*
[3]*College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, People's Republic of China*
[4]*School of Automation, Central South University, Changsha 410083, People's Republic of China*
[5]*QRate, Skolkovo, Moscow 143025, Russia*

Quantum key distribution is unbreakable in theory but may be hacked via imperfections in its hardware implementations. While many imperfections have been mitigated by countermeasures and advanced security proofs, several remain unsolved. One of these is a superlinear behaviour in single-photon detectors, when the click probability rises faster with the photon number of an incoming light pulse than expected from individual independent photon detections [1]. Here we test for superlinearity three models of sinusoidally-gated avalanche single-photon detectors: one gated at 312.5 MHz from QRate [2] and two gated at 1.25 GHz from unidentified vendors [3]. The click probabilities of all three detectors are moderately superlinear. However, we notice that the click timing depends strongly on the incoming pulse energy. The click occurs progressively earlier, shifting more than 60% of the gate period as the energy rises over a wide 50-dB range [2,3]. This effect is observed both in and between the detector gates (Fig. 1). An attacker might use this energy–time effect to conditionally toggle the click between adjacent key bit slots, violating an implicit assumption in the security proofs and rendering them inapplicable. We propose two attacks that exploit this flaw, one of them for a specific industrial quantum key distribution system [2]. We also propose certification methodology for the superlinearity and energy–time effect.

The energy–time effect is a vulnerability in quantum cryptography that is not covered by any existing security proof. We have observed it in seven samples of three different detector models, which suggests this behaviour is intrinsic to the single-photon detectors; we show that it is electrical in origin [3]. It thus needs attention of both the theory and experimental community.

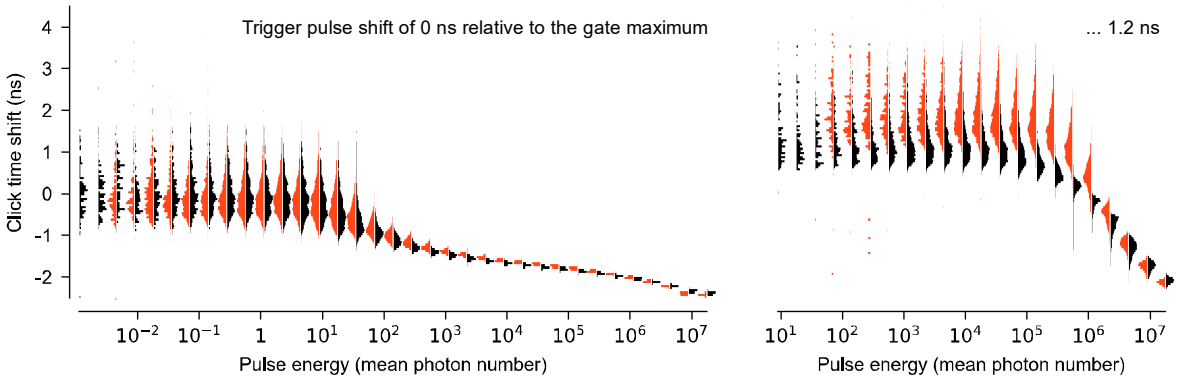

Fig. 1: *Click time distributions in sample 1 (red) and sample 2 (black) of 312.5-MHz detector. The click is caused by a short trigger pulse of varying energy that is aligned to the gate (left plot) or between the gates (right plot). Each histogram is normalised individually. See [2] for details.*

References

[1] L. Lydersen et al., Phys. Rev. A 84, 032320 (2011).
[2] K. Zaitsev, V. Bizin, D. Kuzmin, and V. Makarov, e-print arXiv:2603.07538 (2026).
[3] V. Bizin, J. Su, V. Makarov, and A. Huang, unpublished manuscript (2026).