Forced control of single-photon negative-feedback avalanche diodes using bright illumination

Nigar Sultana[1,2,*], Anqi Huang[1,2,3], Vadim Makarov[4,5,6], Thomas Jennewein[1,2,7]

*[1]Institute for Quantum Computing, [2] University of Waterloo, [3]Institute for Quantum Information & State Key Laboratory of High Performance Computing,[4]Russian Quantum Center,[5]National Laboratory for Physical Sciences at Microscale and CAS Center for Excellence in Quantum Information,[6]NTI Center for Quantum Communications,[7]Quantum Information Science Program, Canadian Institute for Advanced Research**

Any quantum key distribution (QKD) system trusts the detectors used for measuring the single-photons. However, in real world, their performance deviates from an ideal detector. Imperfections in the devices leave loopholes in the system that can lead to security threats. An eavesdropper Eve can get valuable partial or complete information on the key by exploiting various types of attacks such as photon number splitting (PNS) attack [1], time-shift attack [2], and blinding attack [3]. Here, we report blinding control of free-running negative feedback avalanche diodes (NFADs) [4]. These detectors are promising for long distance QKD applications because of their high quantum detection efficiencies at 1550 nm and low afterpulsing probability [5].

In the blinding attack, Eve blinds Bob's detectors using a bright illumination to bring them into the linear mode where diodes are not sensitive to single photons. Then controlled bright laser pulses are superimposed with the blinding power forcing Bob to detect exactly the same outcome when measured at the matching bases as Eve prepared, whereas Bob detects nothing when measured in the wrong bases. Eve can gain a full copy of the raw key without being noticed by Bob though this attack.

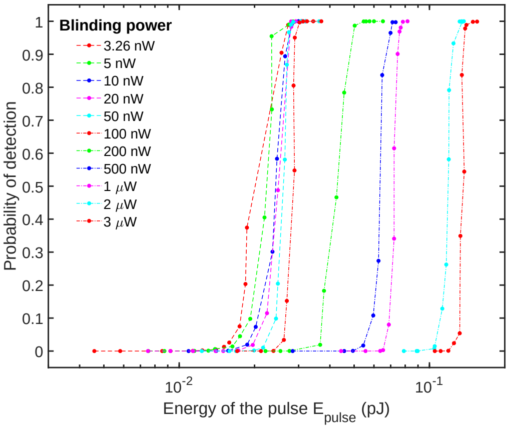

FIG. 1. Probability to force a detection as a function of the trigger energy for an NFAD.

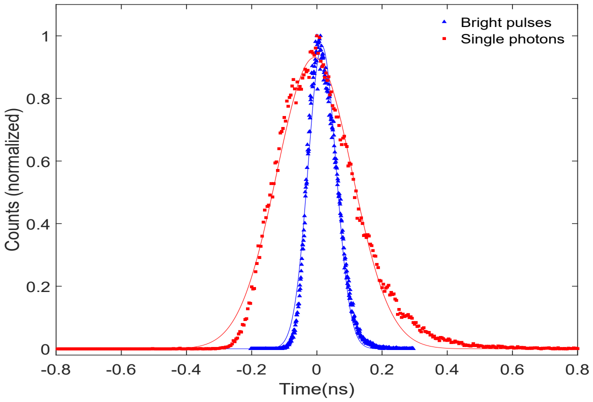

FIG. 2. Time Jitter for bright pulse and single-photons for an NFAD. Bright pulse jitter is 100.6 ps full-width-half-maximum (FWHM), while it is 271.8 ps FWHM for single photons.

For blinding control, we used two NFADs from Princeton Lightwave, and a custom made readout to sense the detection signals [6]. Fig.1 shows the detection probability ρ_d of an NFAD for various trigger pulse energies at different blinding power. With a deadtime of 20 μs and a trigger pulse rate of 40 kHz, we see in Fig.1, above certain blinding power, there is a sharp transition between E_{never} below which ρ_d is '0' and E_{always} above which ρ_d is '1'. For ideal control, $E_{never} > E_{always}/2$ and ρ_d must be '1', which can be less for larger distances. In addition, jitter for bright pulses must be smaller than the jitter at single photon, which is demonstrated in Fig.2. Both of our NFAD samples demonstrated similar results showing their susceptibility to blinding attacks.

—References—

[1] Huttner, B *et al.*, *PhysRevA* 51:1863 (1995).

[2] Qi, Bing *et al.*, *arXiv:quant-ph/0512080* 0512080 (2007).

[3] Makarov, V *et al.*, *New J Phys* 11:065003 (2009).

[4] Gras, G., Sultana, N., Huang, A., Jennewein, T., Bussières, F., Makarov, V., Zbinden, H. (*Manuscript in preparation).*

[5] Korzh, B *et al.*, *APL* 104:081108 (2014).

[6] Sultana, N., Jennewein, T. (*Manuscript in preparation).*

[*] n6sultan@uwaterloo.ca