Measurements of light emission from silicon avalanche photodetectors

Paulo Vinicius Pereira Pinheiro,[1,2,*] Poompong Chaiwongkhot,[1,3] Shihan Sajeed,[1,4]
Rolf T. Horn,[1] Jean-Philippe Bourgoin,[1,3] and Vadim Makarov[1,3,4]

[1] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[2] *Department of Teleinformatic Engineering, Federal University of Ceará, Campus do Pici, C. P. 6007, 60455-740, Fortaleza, Brazil*
[3] *Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[4] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*

(Dated: June 29, 2015)

Keywords: side-channel attacks on quantum key distribution, avalanche backflash, single-photon detectors

Quantum cryptography has the promise of perfect security. However the current technology is far behind the theory. In practical quantum key distribution (QKD), the most vulnerable part is the receiver which concentrates most of the attacks. Basically most of its structure has already been investigated in search for loopholes. However, light emission from photon detectors [1] has not yet been well studied. In this direction, this work investigates light emission from a QKD receiver which can leak secret information into the optical channel to an eavesdropper. The goal is to characterise the amount of emission into the channel, upper-bound the information leakage, and maintain security in the presence of leakage by applying an additional amount of privacy amplification.

Here we report preliminary experimental results of measuring emission from a silicon photodetector. Two experiments were conducted: the first quantifies the emission by direct measurements, regardless of the wavelength and multiphoton events. The second analyses the emission for two distinct spectral ranges, 532 and 808 nm, in order to compare with the spectral measurements and characterize the emission by wavelength. The amount of photons emitted per wavelength band can be useful to perform or avoid side-channel attacks. Also, those are common wavelengths used in several QKD free-space systems. The setups shown at Fig. 1 are slightly different from previous works [2], using only a few components and testing a commercial model SPCM-AQRH-12-FC from Excelitas, commonly used.

Two equal units are placed producing dark counts. Eventually, they will emit light and increase the count-rate. To clarify the origin of the clicks, the time between two unit clicks is observed and recorded. Figure 1(a) shows the units connected by 1m multi-mode fiber patch cord and to a time interval counter model SR620, which register the time between two pulses, Start and Stop. Results are shown in Fig. 2. The histogram presented resembles the avalanche breakdown current profile, with each peak represents the emission of one unit. The right peak represents backflash emission by the DUT (device under test). Three different events explain the shape

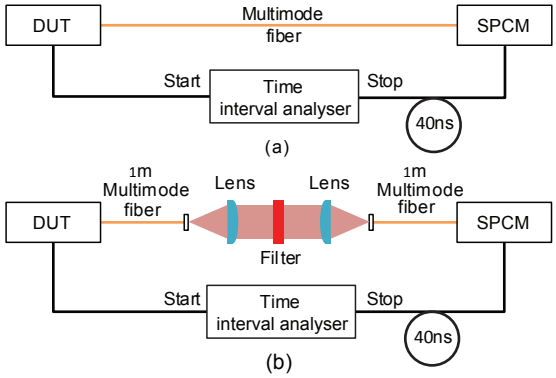

FIG. 1. (a) Setup for direct measurements and (b) setup for wavelength analysis. SPCM – single photon counter module.

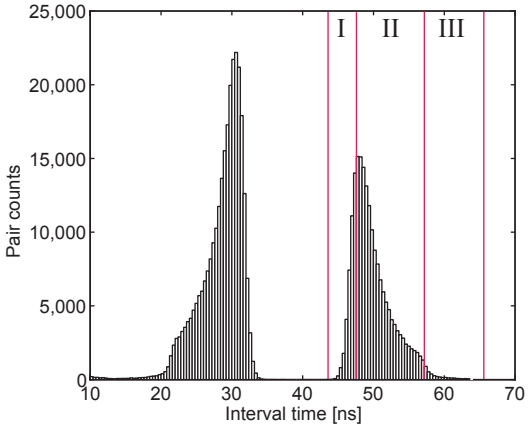

FIG. 2. Histogram of pair counts of backflash emission for 10^6 samples.

of the peak, which are properly selected and are described in time order as: (I) the avalanche process rapid development, (II) an exponential decay due a capacitor discharge, intrinsic to the photodiode and (III) the avalanche quenching by the unit electronics. In terms of security, the main factor is the probability of emission of photons per avalanche event, which in this case

is 0.35. The calculation was done taking into account the effciency of the detector, which for that wavelength is 0.55 on average.

Figure 1(b) presents a setup to check emission in specific spectrum bands by using optical filters. For the 532 nm band, two filters were used with respective bandwidths of 4 nm The probability of emission of photons per avalanche event is 1.5×10^{-4}, fairly negligible. The calculation took into account the effciency of the detector, which for that wavelength is 0.55 and the efficiency of the optical channel, that is 0.70. For 808nm, a filter with 8nm bandwidth was used. A histogram of events was observed exactly as in Fig. 2, with higher emission probability, 6.2×10^{-3}. In terms of security, some photons leaving the optical setup may provide information for a prepared eavesdropper. Most current QKD setups do not consider this backdoor. Thus, an alternative is to adequate post processing and privacy amplification to this attack.

Further experiments are currently in progress to check and measure the leakage of information in a real QKD setup and determining security bounds. A full spectral measurement was already realized, in order to determine the amount of photons emitted per wavelength and create side-channels countermeasures.

The authors would like to thank N. Lütkenhaus and T. Jennewein for valuable discussions. This work was supported by the US Office of Naval Research, Industry Canada, CFI, Ontario MRI, NSERC, Canadian Space Agency, and CryptoWorks21. P.V.P.P. acknowledges support by a Brazilian CAPES scholarship (project no. 014633/2013-02). P.C. acknowledges support by a Thai DPST scholarship. J.-P.B. acknowledges support from FED DEV.

* paulovpp@gmail.com

[1] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, J. Mod. Opt. **48**, 2039 (2001).

[2] A. Meda, H. Suk, I. Degiovanni, G. Brida, and M. Genovese, in *poster at 4th international conference on quantum cryptography, Paris, France.* (2014).