Backflash attack in different gating regimes of single-photon detectors

Alexey Shilko[1,2,3,*], Boris Nasedkin[4], Vladimir Chistiakov[4], and Vadim Makarov[1,5,2]
[1]*Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[2]*NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*
[3]*QRate LLC, Skolkovo, Moscow 121205, Russia*
[4]*ITMO University, St. Petersburg 199034, Russia*
[5]*Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*
(Dated: June 7, 2025)
e-mail *alexeyshilko 1996@list.ru*

Keywords: quantum key distribution, backflash, single-photon detector

Quantum key distribution (QKD) is an advanced communication method, the security of which is guaranteed by the laws of quantum mechanics [1]. However, real QKD systems have vulnerabilities related to the component base or to the implementation of the transmitters (Alice) or receivers (Bob) [2].

One of such imperfection is the secondary photon emission (backflash) from the receiver [3]. The point of the at-tack is as follows: when the single photon detector (SPD) is triggered, there is an increase in the photocurrent in the avalanche photodiode (APD). This process leads to backflash that the detector emits. This radiation carries information about the detector on which the trigger oc-curred [4]. Then it gets into the quantum channel, where an eavesdropper (Eve) has access to it.

This type of attack has already been considered for SPD operating in the near-infrared wavelength range used in telecommunications [5]. Here we investigate the amount of leakage through this channel for a sinusoidally-gated detector and compare detectors in different gating regimes. We test SPDs operating in free-running (QRate), rectangular-gated (ID Quantique), and sinusoidally-gated (QRate) regimes.

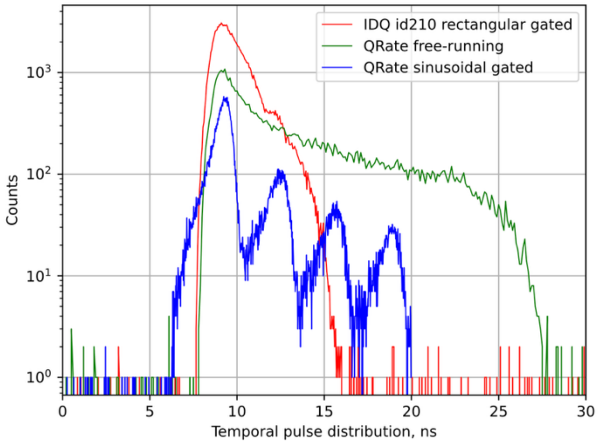

FIG. 1 Backflash photons measured from ID Quantique id210 (red), QRate free-running (green), and QRate sin-gated (blue) detectors. The measurement of backflash from sin-gated is performed only up to the fourth gate.

The experimental scheme consists of the detector under test (DUT) connected via a single-mode fiber patch-cord to another measuring SPD. While no external light is introduced into the scheme, both detectors have dark counts. The optical backflash travels from DUT to the measuring SPD, causing it to detect a photon. Electri-cal outputs of both detectors are connected to an oscilloscope, which builds a time histogram of backflash photon registrations relative to the trigger click from DUT, see Fig. 1

Based on the conclusion that the probability of backflash photon leaking from DUT equals fractional secret key leakage [4], we use the following estimate for secret key leakage $P_L = P_{BF} = N_{BF}/(N_{DC}\eta_{det}\eta_{ch})$, where N_{BF} is the number of recorded clicks of the measuring SPD, N_{DC} is that of DUT during the measurement, η_{det} is quantum efficiency of the measuring SPD, and η_{ch} is the channel transmittance between the detectors.

The estimated key leakage differs by more than an order of magnitude between the detectors: 7% for ID210, 0.23% for QRate free-running and 0.23% for QRate sin-gated.

In this work, we estimated the leakage of key for SPD as part of a commercial QKD system. We also propose and test a countermeasure consisting of isolators installed at Bob's entrance that block most of the spectral range of backflash.

[1] C. H. Bennett and G. Brassard, in Proc. Int. Conf. on Computers, Systems, and Signal Processing (IEEE Press, New York, Bangalore, India, 1984) pp. 175–179.

[2] C. Marquardt et al., BSI technical report, https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Studien/QKD-Systems/Implementation_Attacks_QKD_Systems_node.html, visited 4 Jun 2025

[3] C. Kurtsiefer et al., J. Mod. Opt. 48, 2039–2047 (2001).

[4] P. V. P. Pinheiro et al., Opt. Express 26, 21020–21032 (2018).

[5] Meda et al., Light Sci. Appl. 6, e16261 (2017).