Automated testbench for checking vulnerability of single-photon detectors to bright-light attack

Konstantin Zaitsev,[1, 2, *] Polina Acheva,[1, 3] and Vadim Makarov[1, 4, 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] *Moscow State University of Geodesy and Cartography, 105064 Moscow, Russia*
[4] *Shanghai Branch, National Laboratory for Physical Sciences at Microscale and CAS Center for Excellence in Quantum Information, University of Science and Technology of China, Shanghai 201315, People's Republic of China*

In recent years, quantum key distribution systems have received much attention for their reliability and safety, based on the laws of quantum mechanics. However the practical implementation of such systems has a number of vulnerabilities that an attacker can take advantage of. One of the most defenseless elements of quantum key distribution schemes is the single photon detector, which is used in most implementations as a receiver. There are several attacks that can be applied to almost all detectors. The most common of them is the bright-light detector control attack [1–3]. Therefore, before including the detector in the quantum key distribution scheme, it should be checked for resistance to this method of hacking. If countermeasures to this attack are implemented in the detector [4, 5], their quality needs to be tested.

For this purpose, we are developing an automated testbench. Its task is to study the detector behavior under laser irradiation of various power levels and temporal shapes. In other words, the testbench simulates the behavior of an eavesdropper Eve conducting an attack with bright light. We foresee implementing automated analysis of the measurement results, such that a computer can draft a conclusion about the susceptibility of the device to the attack.

We are currently assembling the testbench setup shown in Fig. 1. The setup uses two lasers, one pulsed and another continuous-wave. Light from each of them passes through an isolator for stability reasons. The power of light from the continuous-wave laser is controlled by a programmable attenuator. Light from the pulsed laser passes a 90 : 10 fiber-optic beam splitter. One of the outputs of the beam splitter is connected to an optical-to-electrical converter connected to an oscilloscope. The second output of the beam splitter is connected to a programmable attenuator. Attenuated light from both lasers is then combined on another 90 : 10 beam splitter (90:10), whose outputs are connected to an optical power meter and the detector under test. A signal generator provides synchronisation to the pulsed laser and the detector. The computer controls all the devices, runs a testing algorithm and analyses the data.

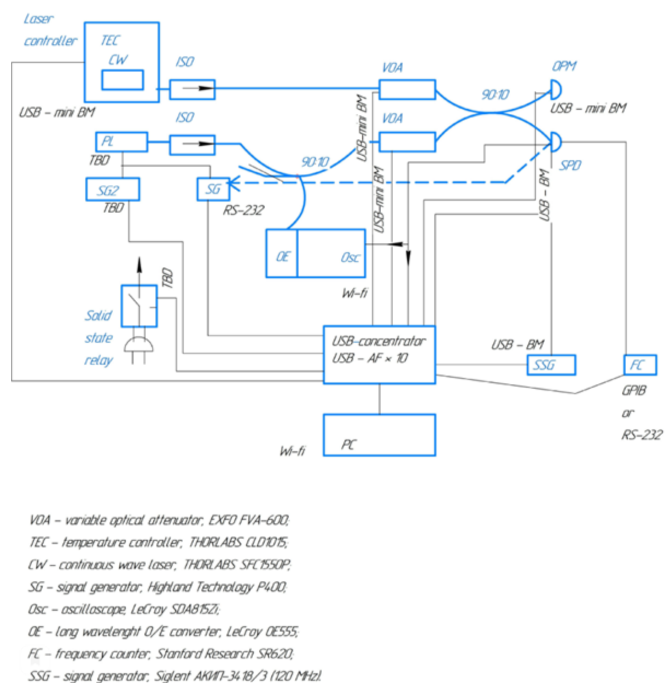

FIG. 1: Experimental setup.

[1] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[2] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18**, 27938 (2010).
[3] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, New J. Phys. **13**, 113042 (2011).
[4] A. Koehler-Sidki, M. Lucamarini, J. F. Dynes, G. L. Roberts, A. W. Sharpe, Z. Yuan, and A. J. Shields, Phys. Rev. A **98**, 022327 (2018).
[5] Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Optica **6**, 1178 (2019).

* zaitsev20k@gmail.com