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

Konstantin Zaitsev[1,2,*], Polina Acheva[1,3] and Vadim Makarov[1,2,4]

Problem

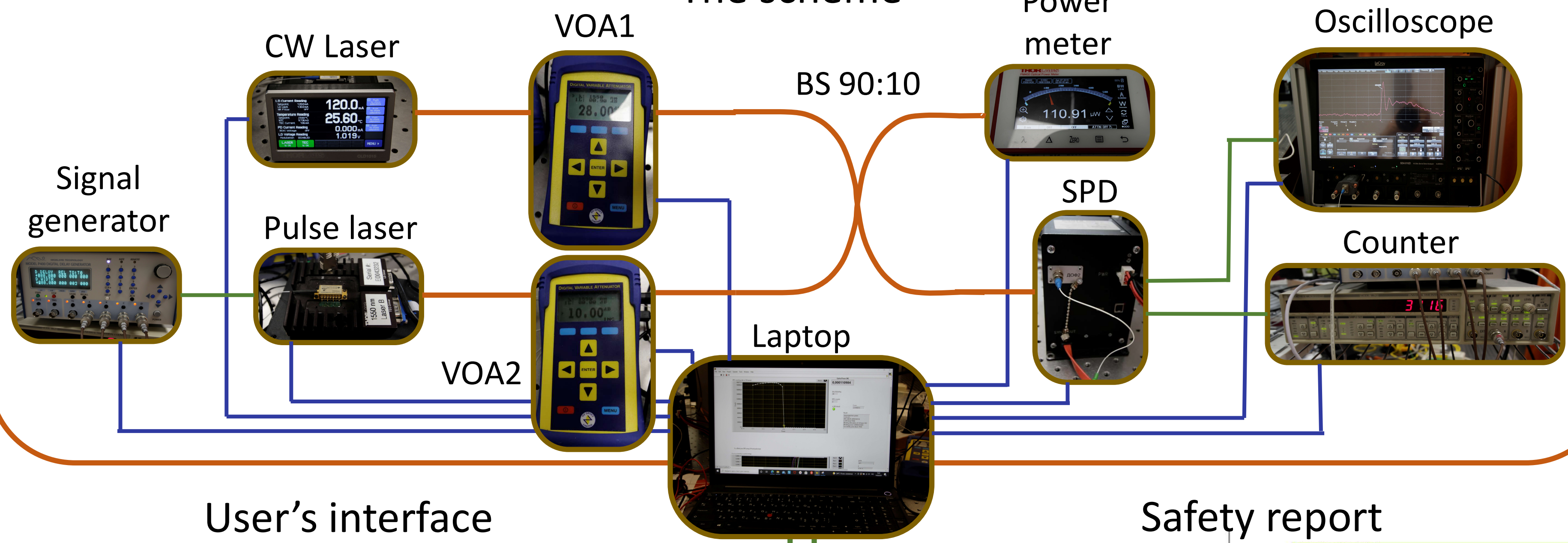
- Single photon detectors (SPDs) can be controlled by bright light attacks, see [1, 2].
- Many countermeasures suggested must be tested properly. See advanced attack at [3].
- Proper test by quantum hackers' team takes a lot of time and attention.

[1] L. Lydersen et al, Nat. Photonics 4, 686 (2010)
[2] C. Wiechers et al, New J. Phys. 13, 013043 (2011)
[3] A. Huang et al, IEEE J. Quantum Electron. 52, 8000211 (2016)

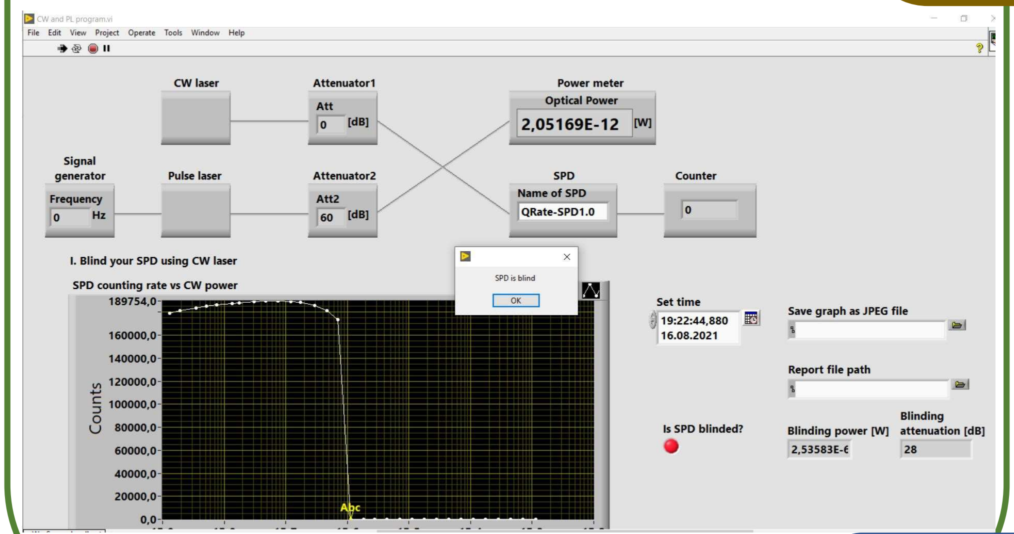
Solution

- ✓ Automated testbench that executes known bright-light attacks and their combinations.
- ✓ To apply to SPD CW light at a wide power range with 1-2 dB step (blinding attack).
- ✓ To apply to SPD pulse light at a wide energy range with 1-2 dB step (blinding\after-gate attacks).
- ✓ To observe SPD countermeasure (if any).

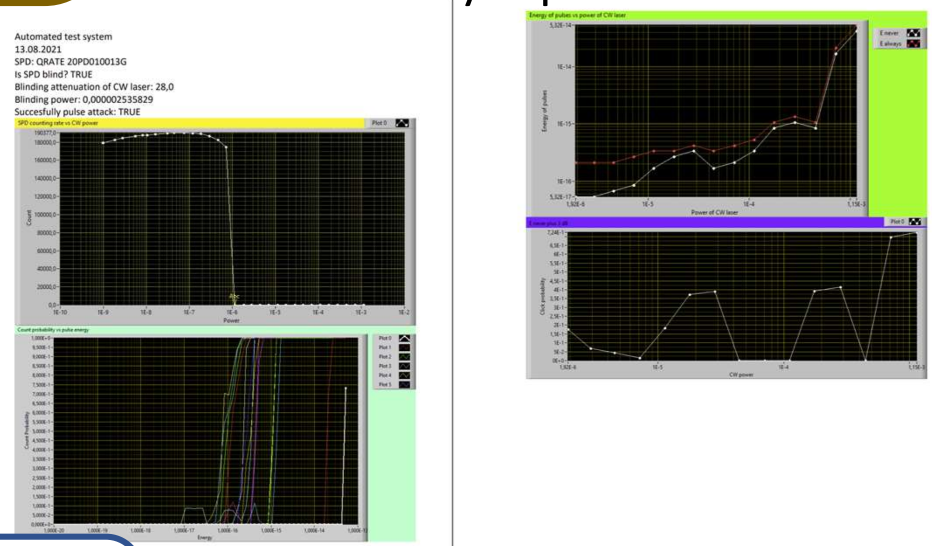
The scheme



User's interface



Safety report



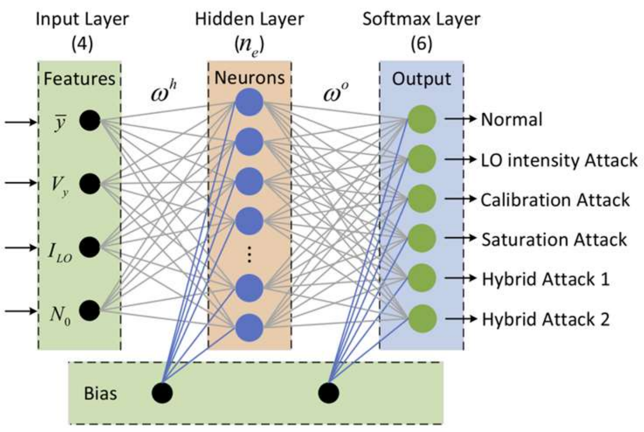
Future plans

Certification

Layer	Description
Q7. Installation and maintenance	Manual management procedures done by the manufa
Q6. Application interface	Handles the communication between the quantum c application that has asked for the service. For exampl ated key to an encryption device or key distribution nication this layer transfers secret messages from/to
Q5. Post-processing	Handles the post-processing of the raw data. For QK key data, sifting, error correction, privacy amplificati over a classical public channel involved in these steps
Q4. Operation cycle	State machine that decides when to run subsystems i nating between qubit transmission, calibration and o
Q3. Driver and calibration algorithms	Firmware/software routines that control low-level op optical devices in different regimes
Q2. Analog electronics interface	Electronic signal processing and conditioning betwe devices. This includes for example current-to-voltage frequency filtering, limiting, sampling, timing-to-dig
Q1. Optics	Generation, modulation, transmission and detection and electro-optical components. This includes both synchronization and calibration. For example, in a de include generation of weak coherent pulses with diffe mission, polarization splitting and detection, but also

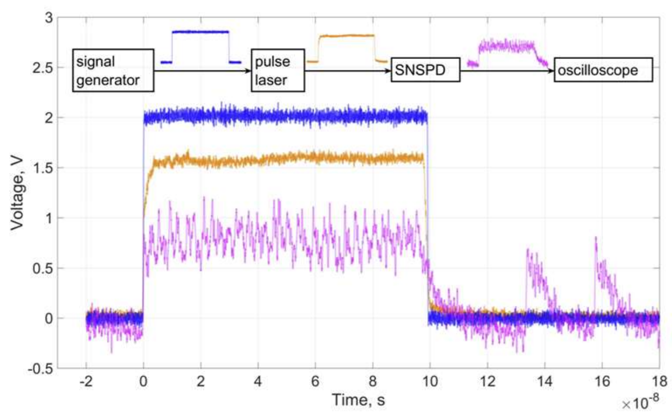
*S. Sajeed et al, Sci. Rep. 11, 5110 (2021)

Machine learning



*Yi. Mao et al, New J. Phys. 22, 083073 (2020)

Deeper understanding



*Intermediate report on SNSDP safety (2021)

[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