Automated setup for testing Single-Photon Detectors countermeasures with bright-light attacks

Polina Acheva[1,2*], **Konstantin Zaitsev**[1,3], **Vadim Makarov**[1,3,4]
[1]Russian Quantum Center, Skolkovo, Moscow 121205, Russia
[2]Moscow State University of Geodesy and Cartography, 105064 Moscow, Russia
[3]NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, 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

*achevap17@yandex.ru

Abstract. Quantum key distribution (QKD) is a novel technology that has developed from idea to growing industry in a part 30 years. Although the most QKD problems are shown both theoretically and experimentally, the lack of certification standards slows down industry growth. In the recent work we show an approach of automated QKD component testing. We have chosen Single-Photon Detector (SPD) as the most vulnerable element for QKD scheme. We test it with bright-light attacks. Also, we update setup for testing photocurrent flow as SPD countermeasure.

1. Introduction

The idea of quantum key distribution was first announced 1983 by Bennet and Brassard [1] and first proof-of-principle was shown in 1992 [2]. But increasing interest to technology was obtained after Shor has shown the threat of classical cryptography by quantum computer concept [3]. Now a lot of companies suggest QKD realizations on the market.

However real implementations often have distinctions with perfect devices in theory. For example, Single-Photon Detectors (SPD) were shown to be totally controlled with bright light more than 10 years ago [4]. For the past decade a lot of ideas to close this loophole were suggested [], however their efficiency is still a debate matter. Here we present an automated setup to test SPDs with or without countermeasures. We show setup in Section 2 and discuss results in the next section.

2. Setup

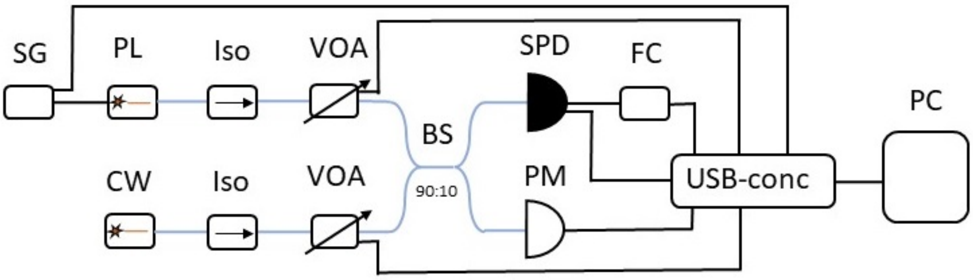

Fig.1 Experimental setup. SG – signal generator, PL – pulse laser, CW – continuous laser, Iso – isolator, VOA – variable optical attenuator, BS – beamsplitter, SPD – single-photon detector, PM – power meter, FC – frequency counter, USB-conc – USB concentrator, PC – personal computer.

The automated setup is shown on the fig. 1. We apply continuous wave laser to blind detector and apply pulse laser to control it. Variable optical attenuators allow to control lasers power, that is observed with power meter. SPD outputs are observed with frequency counter and personal computer. A Labview program varies attenuation, collects data, builds graphs and prepares a report on SPD safety automatically.

3. Results

Fig. 2 shows SPD behavior under bright-light attack. Subplot (a) shows that detector can be blinded, while subplot (c) shows SPD countermeasure response. Subplot (b) shows that detector can be controlled by bright pulses and subplot (d) shows SPD countermeasure response on bright pulses. It can be seen that SPD countermeasure reacts on bright-light attack.

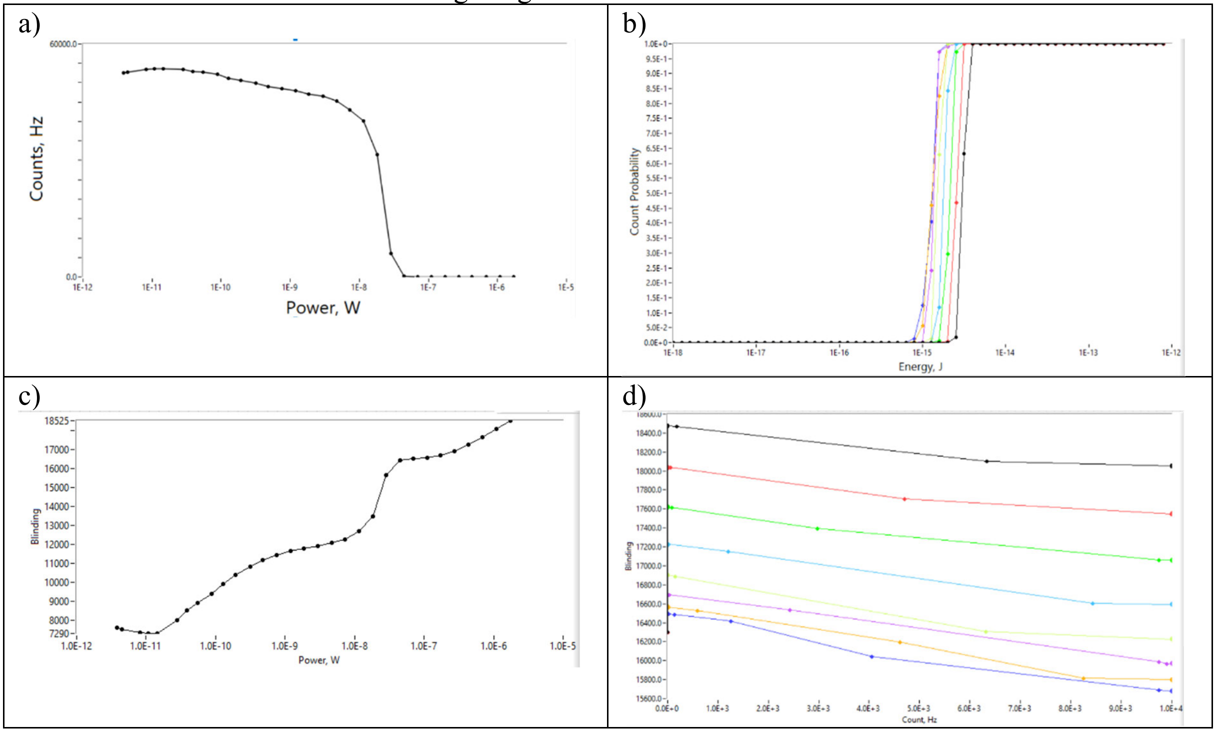

Fig. 2. Graphs obtained by automated testbench. a – SPD counts vs continuous laser power; b – SPD counts probability vs pulse energy; c – SPD countermeasure value (arbitrary units) vs continuous laser power; d - SPD countermeasure value (arbitrary units) vs SPD counts.

Acknowledgments

This work was supported by Russian Science Foundation (project № 21-42-00040).

References

[1] Bennett C H and Brassard G 1984 Proc. IEEE International Conf. on Computers, Systems, and Signal Processing (Bangalore, India)(New York: IEEE Press) pp 175–9.

[2] Bennett, C. H., F. Bessette, G. Brassard, L. Salvail, and J. Smolin, 1992, ‘‘Experimental quantum cryptography,’’ J. Cryptology 5, 3–28.

[3] P. Shor, Proc. 35th Ann. Symp. Found. Comp. Sci. (IEEE Comp. Soc. Press, Los Alamitos, California, 1994), p. 124.

[4] Lydersen, L., Wiechers, C., Wittmann, C. et al. Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photon 4, 686–689 (2010).

[5] Z. L. Yuan, J. F. Dynes, and A. J. Shields, “Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography,” Appl. Phys. Lett. 98, 231104 (2011).

[6] Yong-Jun Qian, De-Yong He, Shuang Wang, Wei Chen, Zhen-Qiang Yin, Guang-Can Guo, and Zheng-Fu Hans, “Robust countermeasure against detector control attack in a practical quantum key distribution system,” Optica 6, 1178–1184 (2019).