EPJ Web of Conferences **132**, 01004 (2017) DOI: 10.1051/epjconf/201713201004
SPECTROSCOPY.SU 2016

Development of the experimental setup for investigation of latching of superconducting single-photon detector caused by blinding attack on the quantum key distribution system

M.S. Elezov[1,*], R.V. Ozhegov[1], G.N. Goltsman[1], and V. Makarov[2]

[1]Moscow State Pedagogical University, 119991 Moscow, Russia
[2]Institute for Quantum Computing, University of Waterloo, N2L 3G1 Waterloo, Canada

Abstract. Recently bright-light control of the SSPD has been demonstrated. This attack employed a "backdoor" in the detector biasing scheme. Under bright-light illumination, SSPD becomes resistive and remains "latched" in the resistive state even when the light is switched off. While the SSPD is latched, Eve can simulate SSPD single-photon response by sending strong light pulses, thus deceiving Bob. We developed the experimental setup for investigation of a dependence on latching threshold of SSPD on optical pulse length and peak power. By knowing latching threshold it is possible to understand essential requirements for development countermeasures against blinding attack on quantum key distribution system with SSPDs.

As is predicted by laws of the quantum mechanics, one can transmit information from a party A ("Alice") to a party B ("Bob") securely without successful interception by a third party ("Eve"), as such an interception would be immediately detected as absence of the expected photon or inconsistency of its state [1]. Both single-photon Avalanche PhotoDiodes (APDs) and Superconducting Single-Photon Detectors (SSPDs) [2] are employed in commercial Quantum Key Distribution (QKD) systems [3].

SSPD outperforms APD by their characteristics such as low dark counts, high quantum efficiency at wavelength of 1550 nm and low jitter, which allows for increasing secret key rate, distance of quantum key distribution and for decreasing the quantum bit error rate (QBER) [4]. At the same time, development of quantum cryptography systems and their emerging to a commercial level stimulates research of potential vulnerabilities for hacking attack. One of many potential points for hacking is the superconducting single-photon detector. Some maleficent ways for remote control of an APD [5] and SSPD [6, 7] by blinding attack were demonstrated. In the blinding attack, the detector is subjected to a strong optical pulse leading to the detector being in a non-operational state for some time.

The potential vulnerability of the SSPD is the possibility of latching. After absorption of a strong optical pulse, the SSPD switches to normal state and is heated up by the bias current. The SSPD temperature is increased up to the resistive transition temperature, and the resistance of the SSPD rises up to 1 - 2 MOhm. Further increase of the SSPD

* Corresponding author: elezovms@rplab.ru

temperature occurs due to the Joule heating. The equilibrium temperature is reached when equality between the heat power and dissipated power is achieved. The SSPD stays in the normal state without imminent return to superconducting state. Such phenomenon is called latching [8], which can be used by Eve in the blinding attack. For that Eve blocks signals from Alice, blinds Bob's SSPDs by radiation at wavelength of 1550 nm and forces Bob's readout. We developed the experimental setup which is needed for investigation of latching threshold of SSPDs.

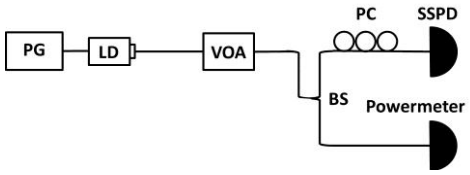

Fig. 1. Optical scheme of the experimental setup. PG – pattern generator; LD – laser diode at 1550 nm; VOA – variable optical attenuator; BS – beamsplitter 50/50; PC – polarization controller.

For measurement of the latching threshold of the SSPD we assembled the experimental setup shown in Fig. 1. In our experiment we use one SSPD of registration system. It is designed as a cryogen-free system and involves a compact low-power cold head SRDK-101D with cryostat, including a closed-cycle refrigerator, a compressor with helium lines and an SSPD control unit. The operating temperature is 2.5 K. An advantage of such a system is that closed-cycle refrigerators can operate continuously for months provided there is a reliable power source. Such a cryostat has two SMA outputs for biasing the SSPDs and reading out the output signal. Besides, the cryostat has two optical FC/PC inputs. Optical coupling is realized by means of the alignment of the 9 μm single-mode fiber core and the meander of the SSPD measuring 7×7 μm^2. The size of a meander is optimized with respect to optical matching with the core of a single-mode fiber SMF-28e. After the final alignment, the optical unit was mechanically fixed on the cold finger of the cryostat. The SSPD operates in a single-photon mode with high quantum efficiency above 20%, low dark count rate and relative bias current of about $0.95I_c$. The latching threshold of the SSPD depends on the peak power, pulse length and pulse repetition rate of the strong optical pulses. The laser diode is controlled by the pattern generator. The laser light with linear polarization at 1550 nm is sent to the beamsplitter 50/50. By means of the power meter and the variable optical fiber attenuator we will measure peak power in optical pulses incident on the SSPD. The polarization controller is needed for tuning light polarization so that the vector of polarization of the light is parallel nanowires, as it ensures the maximal quantum efficiency of the detector.

Thus, we developed the experimental setup for investigation of the SSPD latching threshold dependence on the optical pulse length and its peak power. By knowing conditions for the SSPD latching one could develop countermeasures against blinding attack on quantum key distribution system based on the superconducting single-photon detectors.

The work was supported by The Ministry of Education and Science of Russian Federation, project No. 14.586.21.0007, RFMEFI58614X0007.

References

1. N. Gisin et al., Quantum Cryptography II Rev. of Mod. Phys. **74**, 145 (2002)
2. G. Gol'tsman et al., Appl. Phys. Lett. **79**, 705 (2001)
3. http://www.idquantique.com
4. R. Ozhegov et al., Proc. of SPIE **9440**, 94401F (2014)
5. L. Lydersen et al., Nature Photonics **4**, 686 (2010)
6. L. Lydersen et al., New J. Phys. **13**, 113042 (2011)
7. M.G. Tanner et al., Opt. Express **22**, 6734 (2014)
8. A. Annunziata et al., J. Appl. Phys. **108**, 084507 (2010)