EPJ Web of Conferences **103**, 10002 (2015)
DOI: 10.1051/epjconf/201510310002

Countermeasures Against Blinding Attack on Superconducting Nanowire Detectors for QKD

M.S. Elezov[1a], R.V. Ozhegov[1], Y.V. Kurochkin[2], G.N. Goltsman[1], and V.S. Makarov[3]

[1]*Moscow Pedagogical State University, 29 Malaya Pirogovskaya Str. Moscow 119991, Russia*
[2]*Russian Quantum Center, 100 Novaya Str. Skolkovo, Moscow 143025, Russia*
[3]*Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L~3G1, Canada*

Abstract. Nowadays, the superconducting single-photon detectors (SSPDs) are used in Quantum Key Distribution (QKD) instead of single-photon avalanche photodiodes. Recently bright-light control of the SSPD has been demonstrated. This attack employed a "backdoor" in the detector biasing technique. We developed the autoreset system which returns the SSPD to superconducting state when it is latched. We investigate latched state of the SSPD and define limit conditions for effective blinding attack. Peculiarity of the blinding attack is a long non-single photon response of the SSPD. It is much longer than usual single photon response. Besides, we need follow up response duration of the SSPD. These countermeasures allow us to prevent blind attack on SSPDs for Quantum Key Distribution.

Keywords: quantum cryptography, information security, superconducting single-photon detector, blinding attack.

Quantum cryptography is actively developing field of physics. It is at the turn of quantum mechanics and informatics. We can transmit some secure information from a point A ("Alice") to a point B ("Bob") without interception by third point ("Eve"). It is possible due to using laws of quantum mechanics [1].

There are commercial quantum key distribution systems [2] with single-photon Avalanche PhotoDiodes (APDs) or Superconducting Single-Photon Detector (SSPD) [3]. Employment of SSPDs instead of APDs are become possible due to low dark counts < 10 s^{-1}, high quantum efficiency > 30 % at wavelength 1550 nm and low jitter < 35 ps. It is allowed essentially to increase secure key rate, distance of a quantum key distribution and to decrease quantum bit error rate (QBER) [4]. At the same time evolution of quantum cryptography systems and conversion to a commercial level makes important research into potential vulnerabilities for hacking attack. One of potential points for hacking is superconducting single-photon detector. Early it was presented the ways for remote control of an APD [5] and SSPD [6, 7] by blinding attack.

The potential vulnerability of the SSPD is the possibility to latch. After absorption of the strong light pulse, the SSPD keeps in resistive state without spontaneous return to superconducting state. Such phenomenon is known as latching [8]. Eve can use this feature of SSPD for hacking attack. After

[a] Corresponding author: elezovms@rplab.ru

blocking signals from Alice Eve blinds the SSPD by radiation at wavelength 1550 nm and forces Bob's readout to response at wanted time.

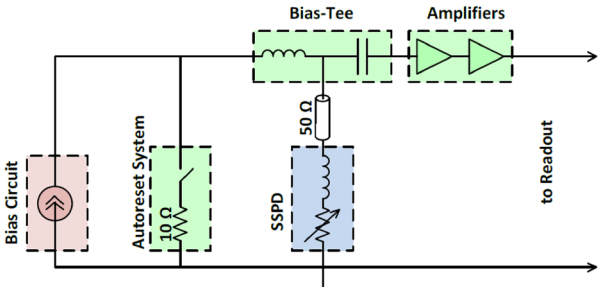

Figure 1. Bias scheme of SSPD with the autoreset system.

We suppose to use the autoreset system for prevention blind attack to quantum cryptography system with SSPD. The autoreset system forcibly returns the SSPD to superconducting state after latching and alarms to Bob about a probable attack. Bias scheme of SSPD with the autoreset system is shown in Fig 1. The autoreset system monitors an average voltage on the SSPD. At once after latching, resistance of the SSPD sharply increases and, at the same time, the voltage on it increases too. The autoreset system short-circuits the SSPD on the resistance 10 Ohm. Bias current drops through the detector. After that the detector is effectively cooled as joule heating is off. The SSPD returns to superconducting state. Either actuation of the autoreset system may alarm to us about blinding attack.

The autoreset system only limits the blinding attack, i.e. the SSPD can absorp strong light pulse without latching after that. We defined common conditions for effective blind attack:

1. Secure key rate (between Eve and Bob) and QBER under an attack must agree closely with secure key rate (between Alice and Bob) and QBER without an attack.
2. The blinded SSPD must not latch, otherwise the autoreset system will actuate.
3. Duty cycle must be maximal, in order to have highest possible secure key rate using a blind attack.
4. Blind pulse repetition frequency is minimal for decreasing QBER.

We experimentally defined optimal parameters for effective blind attack. The SSPD has quantum efficiency 26 %, dark counts 57 cps at operation temperature 2.5 K. We find out that blinding radiation must have parameters: length of the blinding optical pulses ≤ 5 μs; optimal pulse repetition frequency 1 kHz; minimal peak power for the SSPD blinding ~20 nW.

Also for prevention blinding attack we should follow up response length of the SSPD together with using the autoreset system. It is necessary, because response length of the SSPD dependences from pulse length with high optical power.

The work was supported by The Ministry of Education and science of Russian Federation, project No. 14.586.21.0003, unique identifier for Scientific Research (project) RFMEFI58614X0003.

References

1. N. Gisin et al. Quantum Cryptography II Rev. of Mod. Phys. **74**. PP. 145-175 (2002).
2. http:// http://www.idquantique.com/
3. G. Gol'tsman et al., Appl. Phys. Lett., **79**, p. 705 707 (2001).
4. R. Ozhegov et al, Proc. SPIE 9440, International Conference on Micro- and Nano-Electronics 2014, 94401F (December 18, 2014).
5. L. Lydersen et al, Nature Photonics, **4**, Issue 10, p. 686-689 (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).