Creation of loopholes in QKD systems using high-power pulsed laser

Daria Ruzhitskaya,[1,2] Irina Zhluktova,[3,4] Mikhail Petrov,[1] Konstantin Zaitsev,[1,2] Polina Acheva,[1] Nikolay Zunikov,[1] Alexey Shilko,[1] Djeylan Aktas,[5] Daniil Trefilov,[1] Anastasiya Ponosova,[1,2,3] Vladimir Kamynin,[3] and Vadim Makarov[1,2,6]

[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]*Prokhorov General Physics Institute of Russian Academy of Sciences, Moscow 119991, Russia*
[4]*MIREA – Russian Technological University, Moscow 119454, Russia*
[5]*RCQI, Institute of Physics, Slovak Academy of Sciences, Dúbravská Cesta 9, 84511 Bratislava, Slovakia*
[6]*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*

(Dated: June 17, 2022)

Quantum key distribution (QKD) is a promising method to establish secret keys between remote users in a post-quantum world, as QKD protocols are theoretically proved to be unhackable even by a quantum computer. However, real QKD implementations might have loopholes, similar to "side-channels" in classical cryptography.

One particular known quantum-hacking strategy involves changing QKD system characteristics by illuminating it with external intense laser light through a quantum channel—the laser-damage attack [1–4]. In our previous study, we have shown that an extra isolation component at QKD source output is a good countermeasure against such a hacking strategy when an eavesdropper uses the continuous-wave high-power laser to manipulate the QKD system characteristics [4]. However, according to the laser-damage theory, three mechanisms of laser-induced damage might be observed depending on a high-power laser oscillating mode. These include heating (under the exposure to continuous-wave lasers, lasers with a pulse duration of more than 1 ns, and high-repetition-rate pulsed lasers), avalanche ionization (under the exposure to short laser pulses of 1 ps to 1 ns), and multiphoton ionization (under the exposure to laser pulses with a duration of less than 1 ps) [5].

Here we extend our study to QKD isolation components' resilience against pulsed high-power lasers [6]. In this study, we consider the influence of short-pulsed laser radiation on fiber-optic isolators.

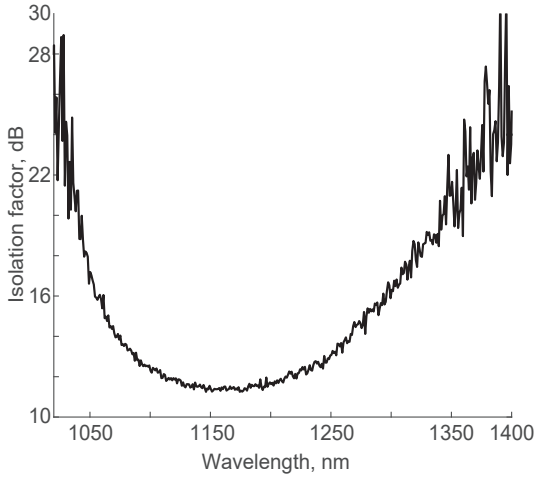

FIG. 1: Typical wavelength-dependent dip in isolation of a fiber-optic isolator designed for operation at 1550 nm.

Experimental setup and testing procedure. We have tested several samples of polarization-independent fiber-optic isolators that are widely used in commercial QKD systems. They provide losses of more than 50 dB to light propagating backwards in an isolator at 1550 nm and thus protect a QKD source against light-injection attacks.

The experimental setup provided exposure of isolators to pulsed laser radiation with a pulse duration of several hundred picoseconds and a mean power up to 840 mW in four different pulse generation modes [6]. A high-power laser at a wavelength of 1064 nm was of choice as it corre-

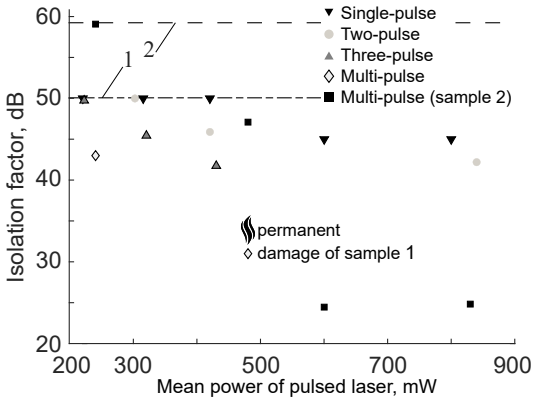

FIG. 2: The isolation at 1550 nm versus the applied power of the pulsed laser. Lines 1 and 2 are the initially measured values of isolation for the sample 1 and 2.

sponds to the transparency window of the isolators (Fig. 1) and thus minimises the heating of the component under test by absorption inside it. The pulsed laser was developed in the laboratory of solid-state lasers active media of the General Physics Institute of the Russian Academy of Sciences [7].

The isolation coefficient and insertion loss of tested samples were monitored using a laser diode with a wavelength of 1550 nm and average power of 10.5 mW. In addition, the sample's temperature was monitored using a thermocouple placed on the surface of the isolator.

Testing results. We show a summary of experimental results [6] for the first two tested samples in Fig. 2. The minimum achieved isolation coefficient was 24.7 dB, while the device specification guaranteed 59.1 dB. The experimentally observed isolation change is likely induced by optical damage than heating, because the temperature monitoring indicated that the isolator was within its operating temperature range. Moreover, contrary to the experimental results with a continuous-wave high-power laser, the isolation does not recover to its initial value after the end of the exposure. We remark that the isolators pass enough light at 1064 nm that may damage other components installed behind the last isolator in the QKD source.

Summary. We show that loopholes in a QKD system might be induced by a variety of laser oscillating regimes. Our results [6] can be used to prepare the standards for certification procedures for assessing the security of quantum communication systems.

Acknowledgements. Friederike Jöhlinger of the University of Bristol participated in this study and obtained these results [6] prior to the Russia's war with Ukraine. Pursuant to the ensuing sanctions by the U.K. Government, our collaboration has been suspended and her name can not appear in the author list of this poster abstract.

[1] Audun Nystad Bugge, Sebastien Sauge, Aina Mardhiyah M. Ghazali, Johannes Skaar, Lars Lydersen, and Vadim Makarov, "Laser damage helps the eavesdropper in quantum cryptography," Phys. Rev. Lett. **112**, 070503 (2014).

[2] Vadim Makarov, Jean-Philippe Bourgoin, Poompong Chaiwongkhot, Mathieu Gagné, Thomas Jennewein, Sarah Kaiser, Raman Kashyap, Matthieu Legré, Carter Minshull, and Shihan Sajeed, "Creation of backdoors in quantum communications via laser damage," Phys. Rev. A **94**, 030302 (2016).

[3] Anqi Huang, Ruoping Li, Vladimir Egorov, Serguei Tchouragoulov, Krtin Kumar, and Vadim Makarov, "Laser damage attack against optical attenuators in quantum key distribution," Phys. Rev. Appl. **13**, 034017 (2020).

[4] Anastasiya Ponosova, Daria Ruzhitskaya, Poompong Chaiwongkhot, Vladimir Egorov, Vadim Makarov, and Anqi Huang, "Protecting fiber-optic quantum key distribution sources against light-injection attacks," arXiv:2201.06114 [quant-ph].

[5] Roger M. Wood, *Laser-Induced Damage of Optical Materials* (CRC Press, 2003).

[6] D. D. Ruzhitskaya, I. V. Zhluktova, M. A. Petrov, K. A. Zaitsev, P. P. Acheva, N. A. Zunikov, A. V. Shilko, D. Aktas, F. Johlinger, D. O. Trefilov, A. A. Ponosova, V. A. Kamynin, and V. Makarov, "Vulnerabilities in the quantum key distribution system induced under a pulsed laser attack," Sci.Tech. J. Inf. Technol. Mech. Opt. **21**, 837–847 (2021).

[7] Irina V. Zhluktova, Serafima A. Filatova, Anton I. Trikshev, Vladimir A. Kamynin, and Vladimir B. Tsvetkov, "All-fiber 1125 nm spectrally selected subnanosecond source," Sci.Tech. J. Inf. Technol. Mech. Opt. **59**, 9081–9086 (2020).