Isolation Reduction of Quantum Cryptography Systems Induced by Continuous-Wave High-Power Laser

Anastasiya Ponosova[1,2*], Daria Ruzhitskaya[1,2], Poompong Chaiwongkhot[3,4], Vladimir Egorov[5], Vadim Makarov[1,2,6], and Anqi Huang[7]

[1] *Russian Quantum Center, Skolkovo, Moscow, Russia*

[2] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow, Russia*

[3] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON, Canada*

[4] *Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, Canada*

[5] *Faculty of Photonics and Optical Information, ITMO University, St. Petersburg, Russia*

[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, People's Republic of China*

[7] *Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer, National University of Defense Technology, Changsha, People's Republic of China*

*E-mail: nastya-aleksi@mail.ru

Over the last two decades, a lot of research efforts have been focused on security analysis of real quantum key distribution (QKD) implementations. For now, numerous hacking strategies have been demonstrated through the subversion of QKD hardware components. The development of countermeasures against known attacks provides the ongoing evolution of the QKD system designs.

One of the latest QKD improvements is the placement of an optical fiber isolator [1] or a circulator [2] at Alice's output. An "isolation countermeasure" strategy is supposed to prevent the variety of possible attacks on optical fiber-based QKD systems such as laser seeding [3], Trojan-horse [4, 5] and laser damage attacks [6].

In this work, we create loopholes of fiber-optic isolators and circulators through high-power laser illumination and propose the countermeasures against it.

The experimental setup simply simulated a hacking scenario in which Eve attacks the system by high-power laser through a quantum channel. We have tested four models of optical fiber isolators and three models of circulators from real QKD systems. The dependencies of isolation, insertion loss and temperature on exposing laser power and time were investigated for each sample. The coefficients were continuously measured both during and after exposure to the laser. The high-power laser used in our experiments was a continuous-wave single-mode fiber laser with the operating wavelength of 1550 nm. The available laser output power was from 0.16 W to 6.35 W. Temperature maps of samples were measured by a thermal imaging camera (Fluke TiS45).

Each sample exhibited a temporary reduction of isolation by 15-30 dB at a certain illumination power. Figure 1 demonstrates the typical evolution of isolation and hottest point temperature of a sample when irradiated by laser. The inferences listed below were made from our experimental results:

a. The value of isolation reduction is limited at constant illumination power. Therefore, the maximum reduction of isolation is bounded by a laser damage threshold power of a sample.
b. The isolation always returns closely to the initial value after the end of illumination, except when the sample is damaged by laser emission.
c. The temporary reduction of isolation is caused by elevated temperature produced by the laser heating.

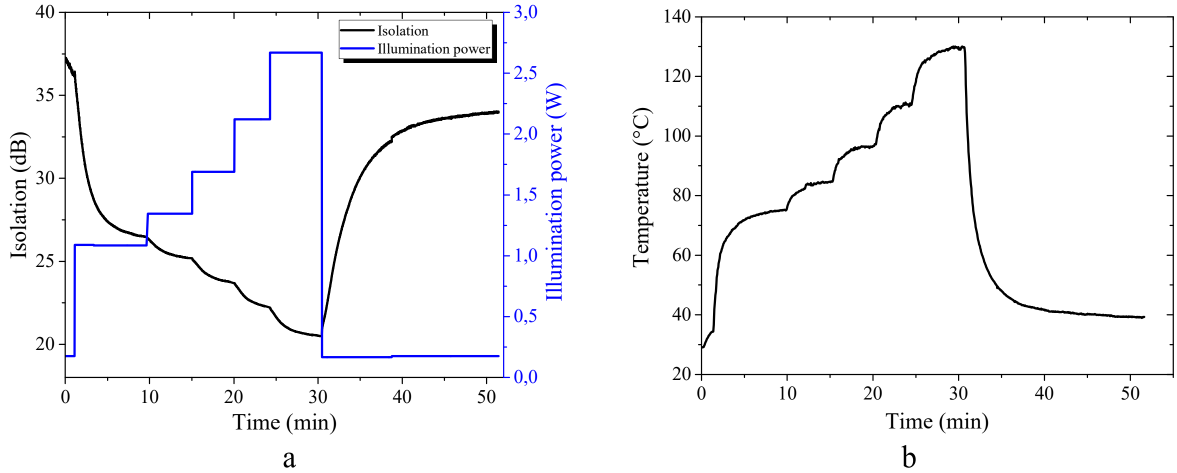

Figure 1: The typical dependencies of sample properties: a - isolation, b - temperature.

We have analyzed vulnerabilities caused by laser-induced isolation reduction. We suppose that they may be easily prevented by measuring of sample temperature or placing an optical fuse or an extra optical isolator component at Alice's output.

In summary, we have shown that the isolation of optical fiber isolators and circulators can be remotely decreased by Eve via being exposure by a high-power laser. The possible countermeasures are conceived.

References

[1] *Y. Zheng, P. Huang, A. Huang, J. Peng, and G. Zeng,* Practical security of continuous-variable quantum key distribution with reduced optical attenuation. Phys. Rev. A, 100, 012313 (2019).

[2] *C. Agnesi, M. Avesani, A. Stanco, P. Villoresi, G. Vallone*, All-fiber self-compensating polarization encoder for quantum key distribution. Optics letters, 44(10), 2398 (2019).

[3] *A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov,* Laser seeding attack in quantum key distribution, Phys. Rev. Appl. (in press).

[4] *A.R. Dixon, J.F. Dynes, M. Lucamarini, B. Fröhlich, , A.W. Sharpe, A. Plews, W. Tam, Z.L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, S. Kawamura,* Quantum key distribution with hacking countermeasures and long term field trial. Scientific reports, 7(1), 1978 (2017).

[5] *K. Tamaki, M. Curty, M. Lucamarini,* Decoy-state quantum key distribution with a leaky source, New J. Phys., 18, 1 (2016).

[6] *A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, V. Makarov,* Laser damage attack against optical attenuators in quantum key distribution., arXiv preprint, arXiv:1905.10795 (2019).