Laser damage attack against optical attenuators in quantum key distribution

Anqi Huang,[1, 2] Ruoping Li,[3] Serguei Tchouragoulov,[4] Vladimir Egorov,[5] and Vadim Makarov[6, 3]

[1] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[2] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[3] *Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[4] *QGLex Incorporation, 105 Schneider Road, Suite 111, Ottawa, ON, K2K 1Y3 Canada*
[5] *Department of Photonics and Optical Information Technology, ITMO University, St. Petersburg, 199034, Russia*
[6] *Russian Quantum Center and MISIS University, Moscow*

Implementation flaws in quantum key distribution (QKD) systems can be exploited by an eavesdropper Eve to learn the secret key. Eve's capability to compromise the security of QKD systems was shown [1–4], especially against single-photon detectors [2, 3]. Measurement-device-independent QKD (MDI QKD) was proposed [5] to protect QKD system from all detector loopholes. However, the source stations, Alice and Bob, are still assumed to be in secure laboratories, which might not be satisfied in a practical scenario. Here we experimentally show that Eve can decreasing the attenuation of optical attenuators by shining a high-power laser at Alice. She thus increases the mean photon number emitted by the source in the QKD system, and creates a side channel.

The experimental setup is shown in Fig. 1. The test laser acts as Alice's laser, providing 5 mW c.w. light. The input of this optical attenuator is connected to the test laser through a 50:50 beamsplitter (BS). The output of the optical attenuator under test is connected to a laser amplifier, which can provide up to 9 W c.w. power, through a 99:1 BS. Power meter A and power meter B work as monitors. Power meter C serves to check the attenuation of the optical attenuator before and after optical damage. The amplifier applies high power starting from 316 mW for at least 10 s. Afterwards, we turn off the high-power laser and record the attenuation value. If no attenuation change has occurred, the laser power is increased by 0.5–1 dBm, and the steps above are repeated. Once a change in attenuation is registered, the testing stops. If the maximum power, 9 W, is applied, but still no change in attenuation, the testing stops.

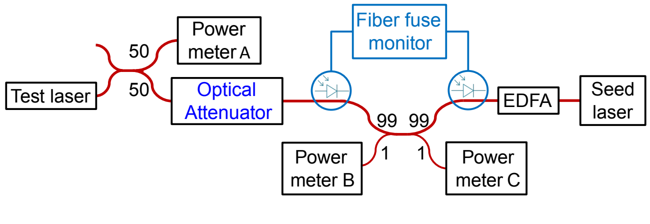

FIG. 1: Simplified diagram of experimental setup, with the optical attenuator as a replaceable testing target. The output of fiber amplifier is fusion-spliced to the 99% arm of the beamsplitter. All fibers used are standard single-mode.

TABLE I: Results after optical damage for tested attenuator types. Third column gives the number of successfully attacked samples out of their total number.

Type	N.	N.	N. crit.	Avg. success	Avg. attack
	total	success	failure	ΔAtt. (dB)	thresh. (dBm)
Manual VOA	2	0	0	–	–
Fixed	12	4	6	−1.37	34.0
MEMS VOA	13	8	4	−5.34	36.2
VDMC VOA	25	18	0	−9.59	34.5

We have tested four types of optical attenuators from different QKD systems. A manual variable attenuator with a screw tip appears to be essentially unaffected up to 9 W. A fixed attenuator consistently shows a short-term temporary decrease in attenuation, but no permanent decrease. Remarkably, the other two attenuator types exhibit permanent decrease in attenuation. These are a variable optical attenuator (VOA) using micro-electro-mechanical-system (MEMS) and a programmable VOA employing a glass disk covered with variable density metal coating (VDMC). A complete summary of the laser damage results is presented in Table I.

In detail, out of 13 tested samples of MEMS VOAs, we have been successful in permanently decreasing the attenuation for 8 samples with an average decline of 5.34 dB at their default setting after laser damage. For the VDMC VOA, we performed in total 25 measurements over different areas of the glass disk. Out of these, 18 testing points demonstrate permanent decrease in attenuation, with mean decrease of 9.59 dB.

In summary, this laser damage attack on optical attenuators shows that the mean photon number can be tampered with by Eve, which effectively breaks the fundamental assumption about the mean photon number in a QKD system.

[1] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).

[2] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[3] A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, and V. Makarov, IEEE J. Quantum Electron. **52**, 8000211 (2016).

[4] V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, Phys. Rev. A **94**, 030302 (2016).

[5] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).