Number	Contribution type	Topic	Session info
481	Poster	EB	EB-P.14, Thursday, 13:00–14:00, Hall B0

Resilience of Quantum Key Distribution Source against Laser-Damage Attack by a Variety of Lasers

Daria Ruzhitskaya[1,2], Irina Zhluktova[3,4], Anastasiya Ponosova[1,2,3], Daniil Trefilov[1,2,5], Poompong Chaiwongkhot[6], Anqi Huang[7], Vladimir Kamynin[3], Vadim Makarov[1,2,8]

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. Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain
6. Department of Physics, Faculty of Science, Mahidol University, Bangkok, 10400 Thailand
7. Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, China
8. 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

Quantum key distribution (QKD) systems provide quantum-safe key exchange. Therefore, complete security analysis of implementations of QKD protocols is in the focus of interest of a worldwide information-security community. For today, a number of QKD loopholes are closed by countermeasures, which are also considered in emerging QKD security evaluation and certification [1–3]. However, new threats to practical QKD implementations are still found, such as the laser-damage attack, which is a powerful hacking strategy. In investigations, CW laser radiation is most often used, but in contrast to it, the interaction of pulsed laser radiation with optical materials may lead to a wide range of effects, like nonlinear effects, dielectric breakdown, etc.

Here we test fiber-optic components from QKD systems under high-power lasers at several lasing regimes and operating wavelengths. Our goal is to develop a strong countermeasure against the laser-damage attack on QKD sources and a common methodology of characterisation of fiber-optic components for QKD, including the choice of lasing regimes for certification tests. We test fiber-optic isolators under illumination by three high-power lasers: 1550-nm CW laser, 1061-nm single-pulsed laser (SPL), and 1061-nm multi-pulsed laser (MPL) [4-6]. The results are summarised in Table 1. We observe a similar temporary decrease in isolation, which recovers after illumination, in all cases. After a permanent damage by illumination, CW laser causes the loss of transparency in both directions, while the pulsed lasers lead to permanent (or very long-term) decrease in isolation by 10.8–31.4 dB without a drastic loss of transparency in the forward direction. Damage by both pulse trains and single laser pulses leads to similar changes in optical characteristics. However, changes induced by MPL might occur at lower average powers comparing to those induced by SPL. We conclude that a countermeasure proposed earlier [4], consisting of adding a sacrificial fiber-optic isolator at the QKD source's output, is still effective against the laser-damage attack by a 1061-nm sub-nanosecond laser.

This work was funded from the Ministry of Science and Higher Education of the Russian Federation (grant 075-15-2022-315) and the Russian Science Foundation (grant 21-42-00040).

Table 1: Summary of testing results of isolators [4,5]. All measurements are at 1550 nm.

Sample number	Laser regime	Initial		Temporary, under exposure		Damaged	After damage	
		Isolation (dB)	Insertion loss (dB)	Minimum isolation (dB)	Corresponding insertion loss (dB)	at average power (W)	Isolation (dB)	Insertion loss (dB)
1-1	SPL, 1 MHz	65.4	0.60	29.6	23.4	1.06	34.0	16.1
1-2	MPL, 16 MHz	59.2	0.60	24.5	2.5	0.83	40.7	16.2
2-1	SPL, 1 MHz	69.6	0.68	25.3	11.3	1.06	41.3	6.8
2-2	MPL, 16 MHz	59.8	0.53	26.8	2.7	1.05	49.0	6.2
2-3	CW	62.1	0.55	27.6	0.9	3.83	87	93.5

References

[1] S. Sajeed, P. Chaiwongkhot, A. Huang, H. Qin, V. Egorov, A. Kozubov, A. Gaidash, V. Chistiakov, A. Vasiliev, A. Gleim, and V. Makarov, "An approach for security evaluation and certification of a complete quantum communication system," Sci. Rep. **11**, 5110 (2021).

[2] ISO/IEC DIS 23837-1(en) Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements `https://www.iso.org/obp/ui/#iso:std:iso-iec:23837:-1:dis:ed-1:v1:en`

[3] ETSI White Paper No. 27. Implementation Security of Quantum Cryptography. Introduction, challenges, solutions. First edition – July 2018. `https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf`

[4] A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang, "Protecting fiber-optic quantum key distribution sources against light-injection attacks," PRX Quantum **3**, 040307 (2022).

[5] 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. V. Makarov, "Vulnerabilities in the quantum key distribution system induced under a pulsed laser attack," Sci. Tech. J. Inf. Technol. Mech. Opt. **21**, 837 (2021; in Russian).

[6] I. V. Zhluktova, S. A. Filatova, A. I. Trikshev, V. A. Kamynin, and V. B. Tsvetkov, "All-fiber 1125 nm spectrally selected subnanosecond source," Appl. Opt. **29**, 9081 (2020).