Protecting QKD sources against light-injection attacks

Daria Ruzhitskaya,[1, 2] Anastasiya Ponosova,[1, 2] Friederike Jöhlinger,[3, 4] Poompong Chaiwongkhot,[5, 6]
Vladimir Egorov,[7] Djeylan Aktas,[3] John Rarity,[3] Chris Erven,[3, 8] Vadim Makarov,[1, 2, 9] and Anqi Huang[10]

[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] *Quantum Engineering Technology Labs, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Tyndall Avenue, Bristol BS8 1FD, United Kingdom*
[4] *Quantum Engineering Centre for Doctoral Training, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1FD, United Kingdom*
[5] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[6] *Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[7] *Faculty of Photonics and Optical Information, ITMO University, Kadetskaya line 3b, 199034 St. Petersburg, Russia*
[8] *KETS Quantum Security Ltd, Unit DX, St Philips Central, Albert Road, St. Philips, Bristol BS2 0XJ, United Kingdom*
[9] *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*
[10] *Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer, National University of Defense Technology, Changsha 410073, People's Republic of China*

(Dated: April 17, 2020)

In the age of measurement-device-independent quantum key distribution (MDI QKD) and twin-field QKD (TF QKD), the source units of these QKD schemes may become a new "Achilles' heel" of the whole system because an adversary, Eve, can inject lasers to conduct various attacks on the sources, i.e., the laser damage attack, Trojan-horse attack, and the laser seeding attack [1–6]. In these attacks, the power of Eve's injection laser is limited by the laser-induced damage threshold of the quantum channel. For example, as a quantum channel, the standard single-mode fiber is able to tolerate several watts of continuous-wave (cw) laser before a fiber fuse happens. However, some components in the QKD source may be damaged by such an injected laser [3, 4].

In this work, we have made progress in searching for a reliable solution to protect QKD sources from the injected high-power laser. Components that act as sacrificial ones under high-power illumination may protect other components behind it in a QKD source from being inoperative. Three classes of components have been examined – fiber-optic isolators, fiber-optic circulators, and integrated optics chips of a QKD source. The isolators and circulators show a significant decrease in isolation, while, however, they are still functional with tens-of-decibel remaining isolation. Thus, the isolators and circulators may be a good passive countermeasure against the attacks listed above. Moreover, we have found that a promising candidate for a QKD source, the integrated photonic chip, only loses the function of the entrance coupler before any changes are observed in other components on the chip, which indicates it may be relatively robust under high-power illumination.

Experimental setup and testing procedure. Our experimental setup and procedure simulate a hacking scenario in which Eve attacks the system through the quantum channel. Therefore, we perform measurements on components that can be used as the last ones at Alice's output, which means the first ones that Eve's high-power laser reaches and manipulates. Samples of fiber-optic isolators and circulators are tested in case of fiber-based systems. In the integrated optics sources, we directly apply the high-power laser light to an indium phosphide (InP) QKD transmitter through its coupling ports.

For high-power illumination, we use a cw high-power laser pigtailed with the standard single-mode fiber to operate at a wavelength of 1550 nm, whose output power is adjustable from 0.16 to 9 W [4]. Our laser is equipped with a fiber fuse monitor, which shuts the high-power laser down automatically if the fiber fuse is detected, and thus it prevents the extensive damage of the laser source.

The testing procedure is the following for each component. First, the initial key parameters, i.e., insertion loss and isolation, of the tested sample are characterized before illumination. Then each sample is illuminated by the high-power laser with a constant power, and meanwhile the temperature of the sample is monitored by a thermal imager. After shutting down the high-power laser, the insertion loss and isolation are characterized again. At this point, one testing cycle is finished. If no change happened, the power of high-power laser is increased, and this testing cycle is repeated until the sample is destroyed. The dependencies of components' characteristics on the applied laser power are obtained for each sample.

Testing results for fiber-optic isolators and circulators. Usage of isolators or circulators at a QKD source's output is supposed to protect other components in the source from laser damage attacks [3, 4]. Our study shows that the high-power laser decreases the isolation of both fiber-optic isolators and fiber-optic circulators. However, before the isolator or the circulator is totally destroyed, a significant isolation remains at all times.

We have tested four models of fiber-optic isolators (ISO) from real QKD systems. The samples marked with PM are polarization dependent, and all the others are polarization insensitive. Each tested sample exhibits a tem-

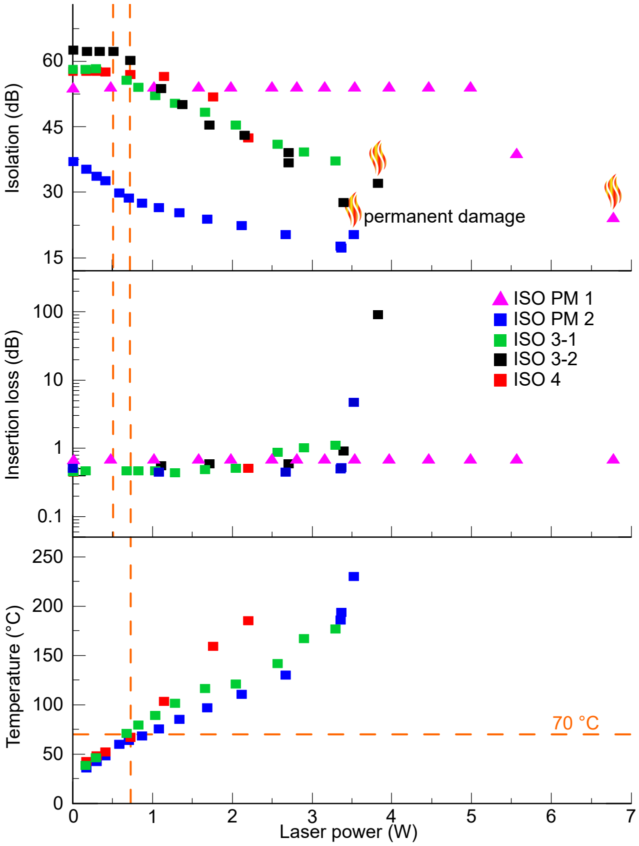


FIG. 1: Experimental data of isolators testing. Maximum specified operation power is marked by the leftmost dashed vertical line. The maximum specified operation temperature is marked by the second dashed vertical line and the dashed horizontal line.

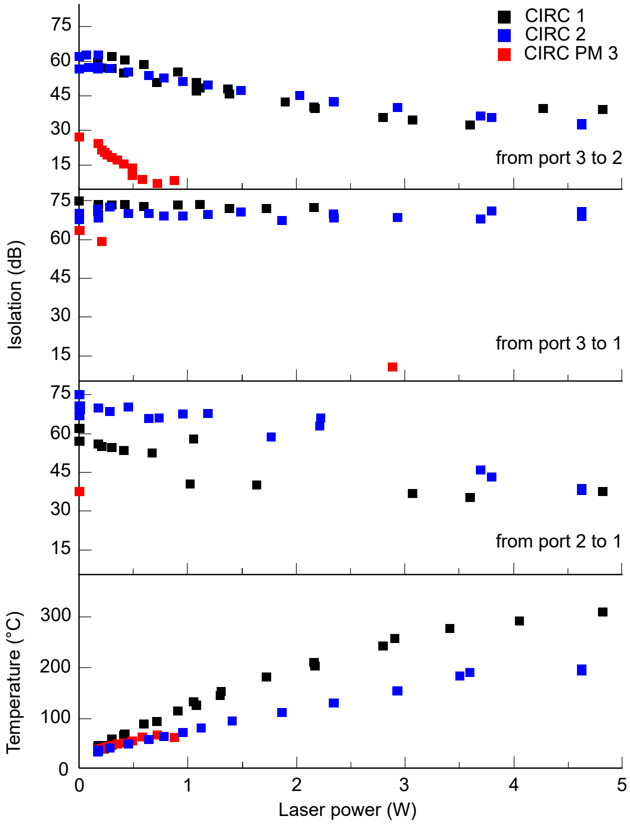


FIG. 2: Experimental data of circulators testing.

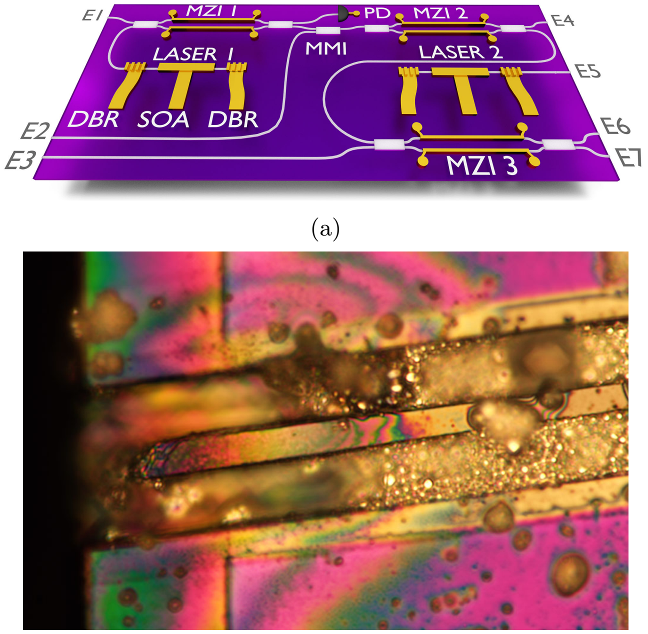
porary reduction of isolation by 15–30 dB at a certain illumination power, while 15–40 dB isolation remains. Figure 1 illustrates experimental data for all tested isolators, which includes three graphs showing dependences of the isolation, insertion loss and hot-spot temperature on the applied laser power. Presented experimental points correspond to minimum isolation values achieved at each applied laser power. After illumination, isolation come back closely to its initial value. Several points in the figure are marked as permanent damage, which means a very high insertion loss. This is a safe outcome, as the QKD system goes out of service and the adversary can not obtain any secret information.

Three models of circulators (CIRC) obtained from real QKD system are tested. The circulator's behavior under high-power laser is similar to that of the isolators. A summary of the laser damage results is presented in Fig. 2. The high-power laser is launched into the port 3 of each tested sample. We observe temporary isolation reduction by about 30 dB not only between ports that have been exposed (from the port 3 to the port 2), but also from the port 2 to the port 1. The isolation remains about 10–40 dB from the port 3 to the port 2 and around 30 dB from the port 2 to the port 1.

The experimentally observed isolation change is likely induced by heating rather than optical damage. Thus, after samples cool to room temperature, the isolation recovers to its initial value.

The isolator or the circulator can act as a sacrificial component to protect the next component behind it from a change of its function under the laser damage attack. In an attempt to further increase the illumination power, it fails permanently into a state of a very high insertion loss, which results in a denial of service and thus protects against the loss of secret information. The isolation required for protection against Trojan-horse and other light insertion attacks that actually steal the information [7] should be calculated starting from the component behind the sacrificial isolator or circulator.

Testing results for integrated photonics chips. Integrated photonic circuits are ultracompact, which should allow on-chip QKD systems to be more widely available and more energy efficient. The technology of intergrated photonics provides an alternative QKD source. Its reliability should be tested against Eve's attack. Thus, we have conducted the laser damage attack on an indium phosphide (InP) QKD transmitter [8] (Figure 3(a)). The high-power laser is injected into the chip through its coupling ports, spot size converters (SSCs) E1 to E7. During our experiments, the transmitted power of high-power laser and the parameters of chip's internal



(a)

(b)

FIG. 3: InP QKD transmitter chip. (a) Schematic of the chip containing two lasers using distributed Bragg reflectors (DBRs), various Mach-Zehnder interferometers (MZIs), a multimode interferometer (MMI), spot size converters (E1...E7), a photodiode (PD), distributed Bragg reflectors (DBRs) (b) Laser-damaged spot size converter E1.

components are monitored.

Only a destruction of SSCs is observed at laser powers of 1.6 to 5.6 W, rather than any changes in the chip's parameters. The damage of SSC E1 at the power of 1.6 W is shown in Fig. 3(b). This leads to the breaking of the quantum channel and stops the light entering the chip. Furthermore, we only achieve the increase of chip temperature when the laser power is higher than 4 W. At lower laser power, the chip temperature controller fully compensated the heating from the laser emission. However, the temperature increase will be detected by Alice, and an adversary will be disclosed. The testing results indicate that the integrated photonics circuit may be robust against the laser damage attack.

Conclusion. The experimental results show that the tested components may be a good passive countermeasure against all the known attacks that rely on light injection into the QKD source (laser-damage, Trojan-horse, and laser-seeding). However, we caution that these good candidates should be further tested in a pulsed regime and at different wavelengths, to ensure their reliability as the protection. The possibility for Eve to affect the internal components in the photonics chip in these other regimes should also be checked.

[1] Nitin Jain, Elena Anisimova, Imran Khan, Vadim Makarov, Christoph Marquardt, and Gerd Leuchs, "Trojan-horse attacks threaten the security of practical quantum cryptography," New J. Phys. **16**, 123030 (2014).

[2] Shi-Hai Sun, Feihu Xu, Mu-Sheng Jiang, Xiang-Chun Ma, Hoi-Kwong Lo, and Lin-Mei Liang, "Effect of source tampering in the security of quantum cryptography," Phys. Rev. A **92**, 022304 (2015).

[3] 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).

[4] 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).

[5] Anqi Huang, Álvaro Navarrete, Shi-Hai Sun, Poompong Chaiwongkhot, Marcos Curty, and Vadim Makarov, "Laser-seeding attack in quantum key distribution," Phys. Rev. Appl. **12**, 064043 (2019).

[6] Xiao-Ling Pang, Ai-Lin Yang, Chao-Ni Zhang, Jian-Peng Dou, Hang Li, Jun Gao, and Xian-Min Jin, "Hacking quantum key distribution via injection locking," Phys. Rev. Appl. **13**, 034008 (2020).

[7] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, "Practical security bounds against the Trojan-horse attack in quantum key distribution," Phys. Rev. X **5**, 031030 (2015).

[8] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. OBrien, and M. G. Thompson, "Chip-based quantum key distribution," Nat. Commun. **8**, 13984 (2017).