Laser Damage Attack on an Integrated Optics Chip for Quantum Key Distribution

Daria Ruzhitskaya*[1,2], Friederike Jöhlinger[3,4], Anastasiya Ponosova[1,2], Anqi Huang[5], Chris Erven[3,6], John Rarity[3], Vadim Makarov[1,2,7]

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

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

[3] *Quantum Engineering Technology Labs, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Bristol, 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, United Kingdom*

[5] *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*

[6] *KETS Quantum Security Ltd, Unit DX, Bristol, United Kingdom*

[7] *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*

*E-mail: dariaruzh@yandex.ru

Quantum key distribution (QKD) has been demonstrated as a promising method to share secret keys for symmetric encryption algorithms in the post-quantum world using single photons or attenuated pulses sent over a quantum channel [1]. Today one of the most important development directions in this area is related to the progress in integrated optics. Integrated photonic devices provide a scalable robust platform for quantum technologies [2]. Photonic integrated circuits are ultracompact in size with traditional discrete bulky components. They will also provide a way of making QKD systems more widely available and more energy efficient.

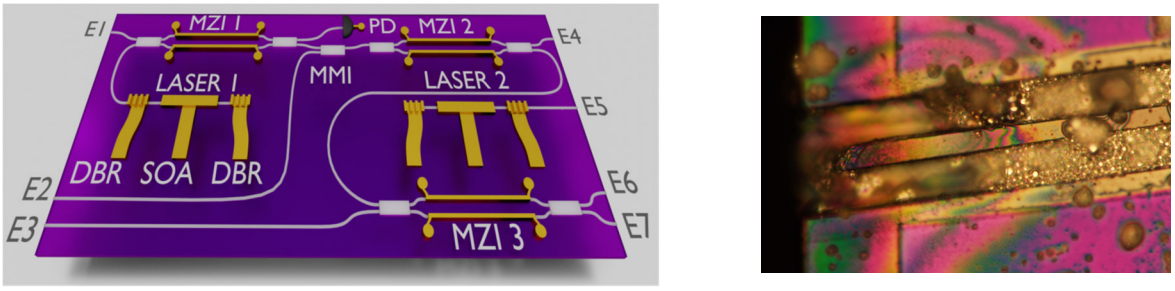
However, despite the high efficiency of integrated photonic components, they might be vulnerable to quantum attacks. Because some class of quantum attacks demonstrated vulnerabilities of discrete QKD systems using fiber components [3], it might be interesting to consider the possible attacks to integrated QKD system. Here we tried to find the potential vulnerabilities of integrated components to laser damage [4].

In this work we present the preliminary results of a laser damage attack on an indium phosphide (InP) QKD transmitter [5]. We found that the irradiation from a high-power laser (HPL) caused a failure in the coupler between the chip and the quantum channel without any changes in internal components in the chip. This means that the integrated photonic circuit has demonstrated robustness to the laser damage attack.

Our experimental setup had two main parts: the first one was the chip-setup (this part is

shown in fig 1a) and the second one was a HPL. The HPL used in our experiments was a continuous-wave single-mode fiber laser with an operating wavelength of 1550 nm [6]. The available laser output power was from 0.16 W to 2.5 W. The emission of external laser was introduced into the chip through output ports, or spot size converters (SSCs) E1 to E7. We tested the internal components shown in fig.1a. During our experiments, the transmitted power of HPL and parameters of internal components were monitored. In such way we achieved the destruction only of SSCs at the power of HPL 1.6 W and 2.5 W.

Using the HPL, we achieved the destruction of the SSCs. The damage of one of the SSCs (E1) at the power of HPL 1.6 W is shown in fig. 1b. This leads to breaking of the quantum channel and stops the light entering the chip.



a) b)

Figure 1: a) An InP QKD transmitter chip with two lasers, various Mach-Zehnder interferometers (MZIs), made from multimode interferometers (MMIs) and phase modulators (PH MODs), spot size converts (E1...E7), a photodiode (PD), distributed Bragg reflectors (DBRs); b) A damaged SSC (E1).

The chip-based QKD systems have thus shown an essential difference from QKD systems using fiber components to laser damage. If in the latter the modification of parameters some component was observed in fiber-based system it could keep working. In the case of integrated QKD systems, when the coupler was damaged, the system would no longer be operational. This means the chip-based QKD systems are more secure in the case of laser damage attack because they don't allow the operation of a compromised system. Future work should estimate the possibility for Eve to affect the internal components and show possible vulnerabilities in the photonic chip.

References

[1] *C. H. Bennett, G. Brassard*, in Proc. IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India) pp. 175-179 (1984).

[2] *M.G. Thompson, A. Politi, J.C.F. Matthews, J.L. O'Brien*. Integrated waveguide circuits for optical quantum computing. IET Circuits, Devices & Systems, 5(2), pp. 94-102 (2011).

[3] *V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagn´e, T. Jennewein, S. Kaiser, R. Kashyap, M. Legr´e, C. Minshull, and S. Sajeed*. Creation of backdoors in quantum communications via laser damage. Phys. Rev. A 94, 030302 (2016).

[4] *R. M. Wood,* Laser-Induced Damage of Optical Materials. CRC Press. (2013).

[5] *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. O'Brien, M. G. Thompson.* Chip-based quantum key distribution. Nat. Commun. 8, 13984 (2017).

[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).