Optical fuse for protection of QKD transmitters against light-injection attacks

Ekaterina Borisova,[1] Anastasiya Ponosova,[1,2] Boris Galagan,[3] Vasiliy Koltashev,[4]
Natalia Arutyunyan,[3] Elena Obraztsova,[3,5] Alexey Shilko,[1,2] and Vadim Makarov[1,6,2]

[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 the Russian Academy of Sciences, Moscow 119991, Russia*
[4]*Dianov Fiber Optics Research Center, Prokhorov General Physics*
Institute of the Russian Academy of Sciences, Moscow 119991, Russia
[5]*Moscow Institute of Physics and Technology, Dolgoprudny 141701, Russia*
[6]*Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*

(Dated: June 15, 2024)

We propose an original device that can protect quantum key distribution (QKD) systems from the effects of intense laser radiation. Carbon nanomaterials dispersed in a polymer can be used as a fuse that interrupts key distribution when Eve tries to hack the system by high-power laser emission. Moreover, it saves system components from laser damage.

In the modern world, more and more attention is being paid to QKD systems. From a theoretical point of view, they are able to ensure complete security of information transmission. However, the real equipment is not perfect, so various channels of information leakage may occur.

One of the main security issues of QKD systems is the protection against light-injection attacks. These include the Trojan-horse attacks [1], laser-seeding attack [2], laser-damage attack [3], and induced-photorefraction attack [4].

Here we demonstrate an optical element that is able to provide sufficient protection for equipment from this type of attack. It is a carboxymethylcellulose film with dispersed single-walled carbon nanotubes (CNT-CNT) [5]. Once exposed to powerful laser radiation, it behaves as a safety fuse. When placed at the exit of a QKD transmitter, it disconnects the communication line. Thus an attacker Eve will not be able to receive any information about secure keys or damage the QKD system further.

Experimental setup and testing procedure. For experiments, we assembled about ten samples of our optical fuse. The fuse has a simple design that enables a high reproducibility of manual production. It consists of the CMC-CNT composite film squeezed between standard FC/UPC fiber connectors with single-mode fiber, as shown in Fig. 1. Its attenuation at QKD operating wavelength of 1550 nm is typically 3.6 dB.

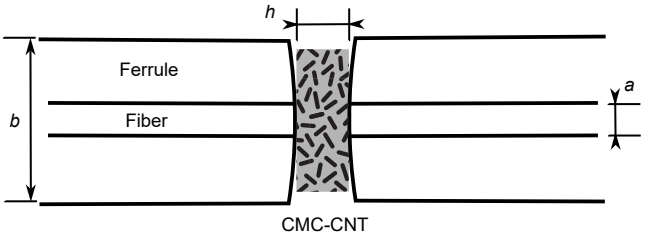

FIG. 1. The design of optical fuse (not to scale). The sample of CMC-CNT is between the ferrules of the connectors inserted into a standard bulkhead adapter. Diameter of the fiber $a = 125$ μm, ferrule diameter $b = 2.5$ mm, sample thickness $h = 5$ μm.

The experimental setup simulates the light-injection attacks on QKD source. We used a 1550-nm high-power cw laser as Eve's source, with a power tunable up to 5.5 W.

Based on the measurements of the transmitted power, we determined the attenuation of the samples under exposure. Moreover, we analysed the mechanisms of changes in the optical characteristics of the samples as a result of the exposure. The phase composition of the samples was studied by Raman spectroscopy and optical microscopy.

Testing results. The sample's optical properties depend on the incoming power. There is no change up to 70–100 mW, but when exposed to a power of 100 mW or more, an irreversible increase in attenuation occurs in all the samples. We show that changes in optical characteristics

are caused by a change in the phase composition of the sample.

At power higher than 1 W, our device ignites a fiber-fuse (a runaway destruction of the optical fiber propagating towards the light source [6]). To prevent it propagating through the communication line and destroying it, an adiabatic taper fiber device may be used [7].

In addition, we have installed our CMC-CNT prototype device at the transmitter exit in a laboratory QKD system and evaluate its effect on the main parameters of QKD operation, including QBER and key rate. The QKD system is a plug-and-play two-pass phase-coded QKD autocompensation system running the BB84 protocol. We show that this does not adversely affect system normal operation.

Summary. We have made a prototype of the system element and recommend it for protection against attacks with injection of laser radiation into QKD systems.

[1] 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).

[2] 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).

[3] Anastasiya Ponosova, Daria Ruzhitskaya, Poompong Chaiwongkhot, Vladimir Egorov, Vadim Makarov, and Anqi Huang, "Protecting fiber-optic quantum key distribution sources against light-injection attacks," PRX Quantum **3**, 040307 (2022).

[4] Peng Ye, Wei Chen, Guo-Wei Zhang, Feng-Yu Lu, Fang-Xiang Wang, Guan-Zhong Huang, Shuang Wang, De-Yong He, Zhen-Qiang Yin, Guang-Can Guo, and Zheng-Fu Han, "Induced-photorefraction attack against quantum key distribution," Phys. Rev. Appl. **19**, 054052 (2023).

[5] A. I. Chernov, E. D. Obraztsova, and A. S. Lobach, "Optical properties of polymer films with embedded single-wall carbon nanotubes," Phys. Stat. Sol. B **224**, 4231–4235 (2007).

[6] R. Kashyap and K. J. Blow, "Observation of catastrophic self-propelled self-focusing in optical fibres," Electron. Lett. **24**, 47–49 (1988).

[7] Dianov, E. M. and Bufetov, I. A. and Frolov, A. A., "Device for protecting fiber-optic lines against destruction by laser emission," RU 2 229 770 C2 (filed 2002-07-12, published 2007-05-27).