09.2;09.5;09.7

Study of the vulnerability of device based on collapsing mirror used in quantum key distribution systems

© S.V. Alferov[1], K.E. Bugai[2,3], I.A. Pargachev[1], Yu.V. Ivanova[2]

[1] AO „InfoTeKS“, Moscow, Russia
[2] Bauman Moscow State Technical University, Moscow, Russia
[3] OOO „SFB Laboratoriya“, Moscow, Russia
E-mail: Kirill.Bugay@sfblaboratory.ru

Received October 20, 2022
Revised October 20, 2022
Accepted December 29, 2022

An attack on equipment with laser damage of optical components called “laser damage attack“, can allow the eavesdropper to reduce the attenuation of optical elements and compromise distributed keys. A method of protection against this attack based on a device with a collapsing mirror has been considered. The conclusion based on experimental data about the effectiveness of the proposed method of protection has been made..

Keywords: quantum key distribution, laser damage attack, eavesdropper, symmetric cryptography.

DOI: 10.21883/TPL.2023.03.55682.19399

In theory, the security of quantum key distribution (QKD) systems is guarantees by fundamental laws of quantum mechanics [1]. However, such systems implemented in practice have various vulnerabilities that depend on the architecture of these systems and the type of equipment used [2]. Any actions of an illegitimate user aimed at obtaining the encryption key are called an attack. In most QKD systems, optical pulses attenuated to a quasi-single-photon level by an optical attenuator are used to prepare quantum states. The mean photon number (MPN) in quantum states should not exceed the value specified by the safety conditions for the QKD protocol guaranteeing the security of the produced key. An attack with laser damage of optical components (laser damage attack, LDA) allows one to increase the transmission coefficient of the attenuator, thus raising the MPN in quantum states. An eavesdropper may thus obtain the key and remain undetected [3].

Note that certain types of attenuators resistant to LDA were demonstrated in [4,5]. However, the authors of these studies point out that an LDA against this attenuators may be efficient at higher radiation powers or longer exposures. Indeed, since these optical components are designed to attenuate transmitted radiation, the blocking element may potentially be damaged under the indicated conditions in such a way as to enhance the transmission coefficient.

In the present study, we propose a radiation attenuator that may be built entirely from fiber-optic elements. In contrast to the mentioned attenuators, our device operates by reflecting radiation from a mirror, which collapses in the course of LDA; thus, attacking radiation exits through the mirror and does not reach the protected equipment. The diagram of the counter-LDA device is presented in Fig. 1.

Optical pulses used to prepare quantum states are fed to the device input and routed to the input port of a fiber-optic 2×2 splitter (*1* in Fig. 1) that splits radiation into two parts. The first part is transmitted through the splitter, is directed to absorber *2*, and dissipates as heat. The second part is directed to mirror *3*. Light reflected from the mirror propagates back to the optic splitter; one part of it is fed to the device output, and the other is routed in the return direction to the input.

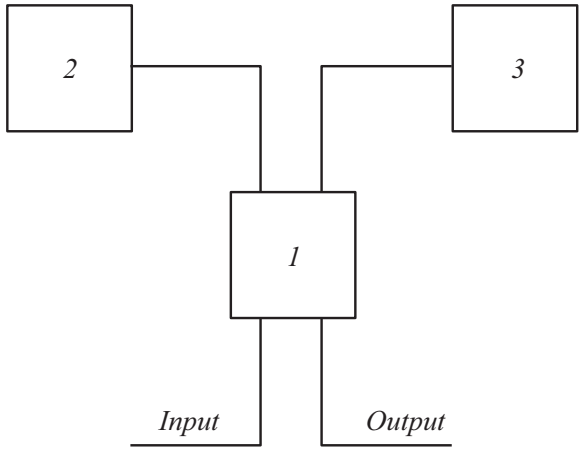

Figure 1. Diagram of the device with a collapsing mirror. *1* — Fiber-optic 2×2 splitter; *2* — absorber; *3* — collapsing mirror.

Regardless of the light propagation direction (from the input to the output or the other way around), the attenuation of light (in dB) is

$$A = -10\lg\big((0.25 - \Delta k^2)(R_a + R + \Delta R)\big), \qquad (1)$$

where $\Delta k \in (-0.5; 0.5)$ is the deviation of light division ratio in the optical splitter from 0.5; $R \in (0; 1]$ is the coefficient of power reflection from the mirror; $\Delta R \in (-R; 1 - R]$ is the possible variation of the coefficient of power reflection

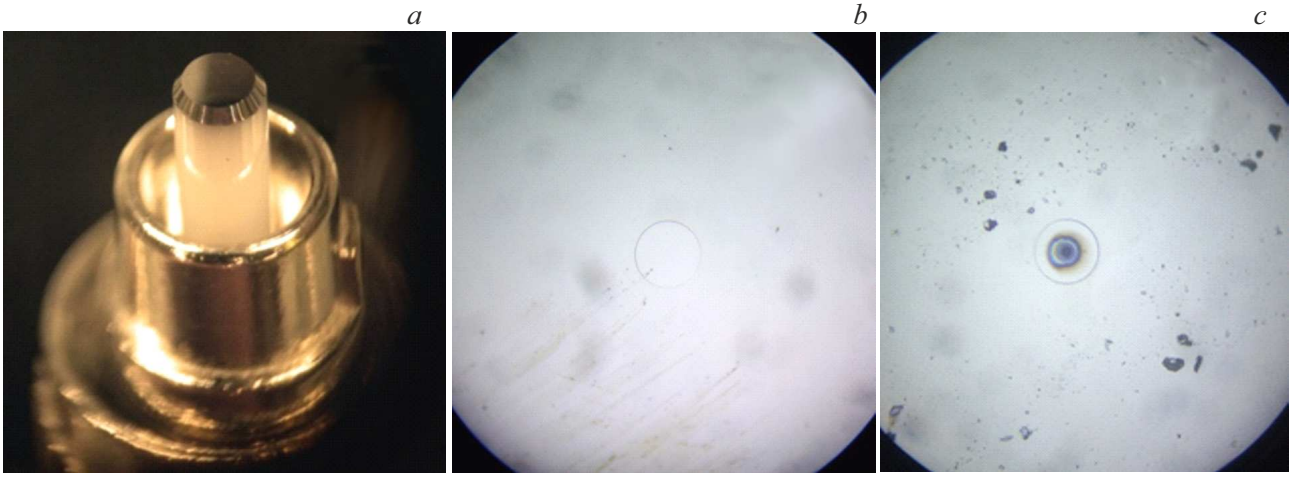

Figure 2. *a* — Metal mirror at the end face of a ferrule with straight polishing (PC); *b* — microscopic image of the mirror prior to tests; *c* — microscopic image of the mirror after tests.

from the mirror under attack by an eavesdropper; and $R_a \in [0;1]$ is the coefficient of power reflection from the absorber. The discussed device is a Michelson interferometer with the absorber in one of its arms and the mirror in the other. Note, however, that the lifetime of quantum states is limited. Thus, setting a sufficient length difference between the splitter–mirror and splitter–absorber optical paths, one may make it so that reflections from the mirror and the absorber do not interfere. The interference term may then be neglected in the derivation of formula (1). In what follows, we assume that $\Delta k \neq 0$, $R_a = 0$, and $\Delta R = 0$ prior to the exposure of the device to high-power radiation. In the course of LDA, these parameters may change in such a way that the attenuation decreases, making the system vulnerable to attack. This implies that the limits of variation of these parameters need to be estimated experimentally or theoretically at the design phase. Taking these limits into account, one should then calculate attenuation A using formula (1) and compare it to attenuation A_0 under zero influence. If difference $\Delta A = A - A_0$ satisfies the criterion (e.g., $\Delta A \geqslant 0$) set by the design engineer, the device is considered resistant to LDA. In the contrary case, optical elements specifying parameters Δk, R_a, and ΔR should be substituted with such elements that would satisfy the criterion.

Note that the degree of light attenuation by the device decreases as deviation Δk approaches zero; therefore, the initial value of the division ratio at the wavelength used in quantum states should be as close to 0.5 as possible to achieve better security against LDA. The discussed device may be combined with other attenuators to set the needed MPN in quantum states at the transmitter output.

Four prototype devices with collapsing metal mirrors were constructed as part of the research into vulnerability of QKD systems to LDA. Mirrors were fabricated by magnetron deposition of chromium onto the end face of a ferrule of a fiber-optic connector (Fig. 2, *a*). The thickness of the mirror metal film was 150 ± 50 nm, and the coefficients of reflection of radiation with wavelength $\lambda = 1550$ nm were $R \approx \{0.14; 0.12; 0.1; 0.1\}$ for prototypes Nos. 1–4, respectively. The introduced attenuation was approximately 16 dB.

Chromium mirrors have an advantage in that their spectral reflection and absorption characteristic is flat [6] in a wide wavelength range, thus making it harder for an eavesdropper to affect the device operation by manipulating the radiation wavelength. It also makes it possible to use identical mirrors in devices intended for operation at different wavelengths (with light attenuation in normal conditions being preserved at the same level). In addition, the device is designed so that radiation does not need to be coupled out of a fiber; this relaxes the production requirements and helps makes the device itself smaller.

The measurement setup and procedure used to tests the constructed prototypes corresponded to the ones detailed in [4,5]. The primary difference was in the use of a lower reference laser power that did non induce mirror collapse in measurements of the initial attenuation. Images of the end face of a ferrule with a deposited mirror before and after the experiment are presented in Figs. 2, *b*, *c*.

Figure 3 shows the dependences of attenuation of the studied prototypes on the power of attacking radiation. The values on the ordinate axis correspond to the initial attenuation measured with the attacking laser switched off. It can be seen that the attenuation of all prototypes increased by no less than 24 dB and did not fall below the initial value within the entire power range of attacking radiation.

Thus, it was found that the attenuation of devices with a collapsing mirror increases from 25 to 37.4 dBm throughout the entire power range of attacking radiation. Note that the discussed attack is the simplest in terms of implementation in the sense that much more sophisticated and subtle ways to affect the operation of optical components of the hardware part of a QKD system are known.

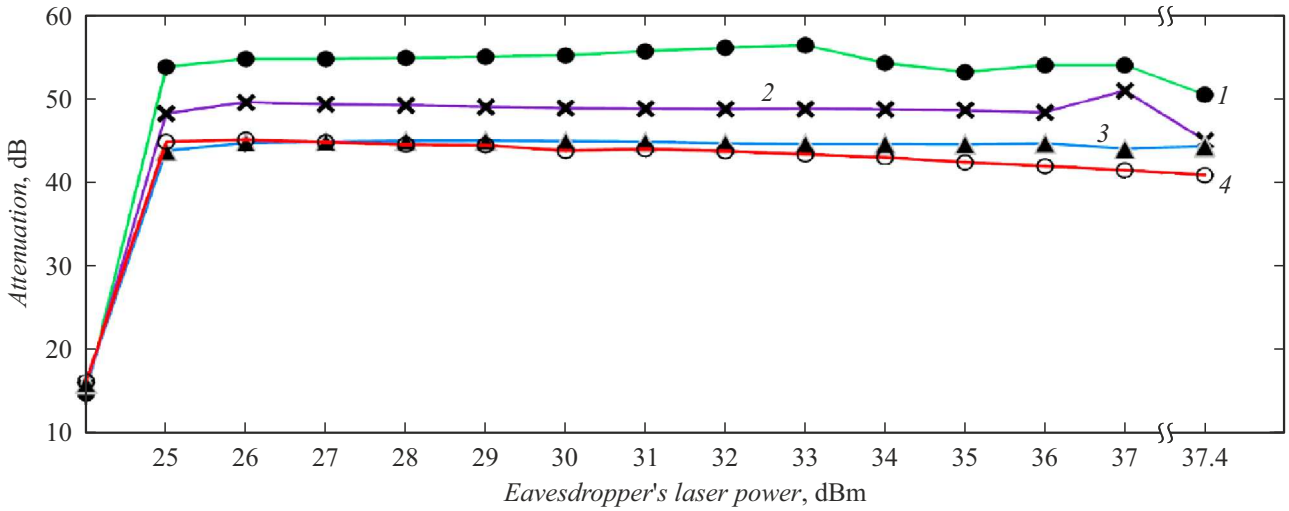

Figure 3. Dependence of attenuation of devices with different coefficients of reflection from the mirror on the power of attacking radiation. The numbers next to curves correspond to the numbers of prototype devices.

Acknowledgments

The authors wish to thank the personnel of AO „InfoTeKS“ (Quantum Technology Division and Research and Advanced Development Center), OOO „SFB Laboratoriya“ (Advanced Research and Development Division), and the Bauman Moscow State Technical University (Subdepartment of Mathematical Modelling and Subdepartment of Laser and Optoelectronic Special-Purpose Systems) for meaningful discussions.

Conflict of interest

The authors declare that they have no conflict of interest.

References

[1] I.M. Arbekov, *Elementarnaya kvantovaya kriptografiya dlya kriptografov, ne znakomykh s kvantovoi mekhanikoi* (URSS, M., 2022), p. 21 (in Russian).
[2] A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, V. Makarov, Phys. Rev. Appl., **13** (3), 034017 (2020). DOI: 10.1103/PhysRevApplied.13.034017
[3] S.N. Molotkov, JETP, **133** (3), 272 (2021). DOI: 10.1134/S1063776121080136.
[4] K.E. Bugai, A.P. Zyzykin, D.S. Bulavkin, S.A. Bogdanov, I.S. Sushchev, D.A. Dvoretskiy, in *2022 Int. Conf. Laser Optics (ICLO)* (St. Petersburg, 2022), p. 1. DOI: 10.1109/ICLO54117.2022.9839749
[5] S.V. Alferov, K.E. Bugai, I.A. Pargachev, JETP Lett., **116** (2), 123 (2022). DOI: 10.1134/S0021364022601117.
[6] A. Sytchkova, A. Belosludtsev, L. Volosevičienė, R. Juškėnas, R. Simniškis, Opt. Mater., **121**, 111530 (2021). DOI: 10.1016/j.optmat.2021.111530