Transmission spectra of fiber optic components used in quantum key distribution systems for protection against Trojan-horse attacks

Alina Borisova[1], **Boris Garmaev**[2], **Ivan Bobrov**[2]

[1] *JSC "InfoTeCS", Moscow, Russia*
[2] *Lomonosov Moscow State University, Quantum Technologies Center, Moscow, Russia*
*E-mail: borisova_alina_95@mail.ru

As with any cryptographic system, various types of attacks can be carried out on quantum key distribution (QKD) systems. To avoid leakage of information to the eavesdropper (Eve) special protective measures are developed for each type of attack. The report considers the counteraction to attacks associated with the illumination of the system by powerful laser pulses: the Trojan-horse, which is an optical probe, as well as Laser damage attack. Protection against these attacks is performed by setting the isolating passive optical components: isolators (OI), circulator (CIRC) etc.

Since Eve has unlimited technical capabilities in terms of power level and spectrum of the probe radiation, in order to construct effective protective measures, it is necessary to know the minimum required level of isolation and take into account the spectral transmission characteristics of the optical components. The transmission spectra of some optical elements are given in [1, 2], from the analysis of which it was concluded that the use of a single optical isolator or circulator for protection against radiation probe in a wide spectral range is inefficient. In addition, when selecting components for protection against Trojan-horse attacks, it is necessary to consider the transmission spectra of both the main isolating elements and other components located in the path of the probe pulses. It should also be noted that the characteristics of optical elements of different manufacturers may differ significantly from each other.

This report presents the measured transmission spectra of various fiber optic components from different manufacturers: isolator, circulator, WDM, bandpass spectral filters, attenuator. The principle of calculating the required level of isolation of the QKD system is also shown, which provides effective protection against Trojan-horse attacks, based on the maximum technical Eve's capabilities: the maximum power of the probe pulses (N = 1020 photon/s/50 μm2) and the minimum mean photon number ($\mu = 10^{-6}$) registered by Eve [3].

In the hardest conditions for the sides of the QKD and the most conducive for Eve, the isolation should exceed 150 dB in the entire spectral range allowed for propagation in optical fiber. As an example, there is shown that the required isolation level in the spectral range from 1260 nm to 1640 nm can be achieved by using a combination of the following components: circulator, mirror, attenuator (50 dB), and WDM. Optical circuit and the transmission spectra of this combination are shown in fig. 1.

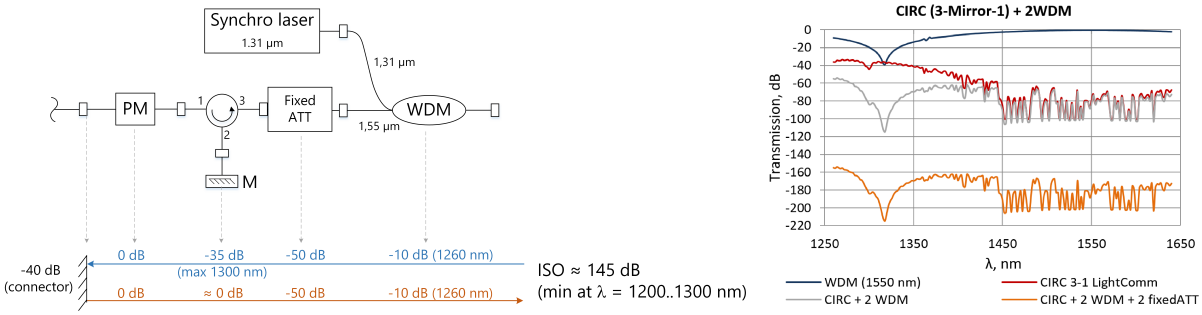

Figure 1: The optical scheme for calculating the isolation of the phase modulator (left) and the transmission spectra of this scheme in a double pass: to the phase modulator and backward (right). Designations: PM — phase modulator, M — mirror, Fixed ATT — attenuator with a fixed attenuation coefficient, WDM — spectral multiplexer 1310/1550, CIRC — circulator.

The reported study was funded by RFBR according to the research project 19-37-80007.

References

[1] *N. Jain, B. Stiller, I. Khan, V. Makarov, Ch. Marquardt, G. Leuchs*, Risk analysis of Trojan-horse attacks on practical quantum key distribution systems. IEEE Journal of Selected Topics in Quantum Electronics. 21, 3 (2014).

[2] Deliverable D5-1 Best practice guide on characterization of counter-measures to side-channel and Trojan-horse attacks [Electronic resource] Access mode: http://projects.npl.co.uk/MIQC/documents/MIQC_BPG_v1.pdf.

[3] *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, 3, 031030 (2015).