Laser-pumping attack on QKD sources

M. Fadeev[1,2], A.A. Ponosova[1], R. Shakhovoy[3,4,5], V. Makarov[1,5,6]
[1]*Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[2]*ITMO University, St. Petersburg, 197101, Russia*
[3] *QRate, Skolkovo, Russia*
[4] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*
[5] *Moscow Technical University of Communications and Informatics, Moscow, Russia*
[6] *University of Science and Technology of China, Shanghai 201315, People's Republic of China*
mfadeev2022@gmail.com

***Abstract*—For the first time, we demonstrate a new type of attack on QKD systems based on laser pumping of a photon source. It includes injection of cw-laser emission into a source at a wavelength shorter than the system operating one. In particular, we show that laser emission at 1310 nm induces an increase in photon number at 1550 nm, changes in pulse shape and width. The QKD risk evaluation due to laser-pumping attack is presented.**

***Index Terms*—QKD source loopholes, vulnerabilities, laser-pumping attack, quantum hacking**

I. Introduction

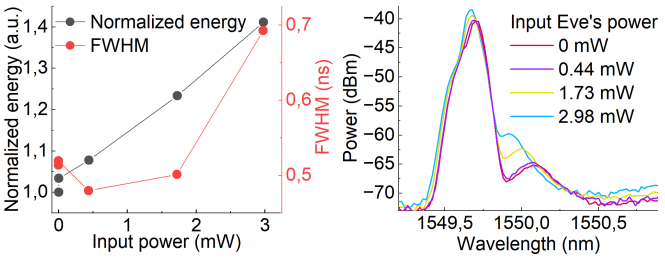
Semiconductor distributed-feedback laser diodes used in QKD systems have electrical pumping, where an electrical current generates electron-hole pairs, afterward, theirs relaxation results in photons emitting. However, some semiconductor materials might also be pumped optically. Typically, optical pumping is possible at a somewhat shorter wavelength than the operating one. While the most producers do not disclose information about semiconductor composition, more often, for lasers in 1300 and 1550 nm wavelength range, the active material is InGaAsP-based quaternary compound [1], which might be pumped optically [2]. Our study is focused on risk evaluation in presence of laser-pumping attack on semiconductor diodes of QKD systems.

II. Experiment

To simulate a quantum hacking scenario, we have implemented a simple experimental setup in which 1310-nm Eve's light injects into a target photon source via a fiber-optic circulator and, next, output characteristics at 1550 nm of a source are measured at the third circulator port. As Alice source, we used semiconductor LD without internal isolator. It generates 510-ps optical pulses with a repetition rate of 10 MHz. Eve's LD at 1310 nm operates in the continuous-wave regime. Its power at the entrance of the source under test ranges from 1.17 μW to 2.98 mW. The pulse envelope and spectra are measured under different injection powers. The pulse energy is then calculated by integrating the recorded pulse envelope. To better understand, we have also studied the watt-ampere characteristic of 1550-nm LD in the CW mode when pumped by 1310-nm emission.

III. Results

We observe changes in spectral, power and amplitude-time characteristics (Fig. 1). Each of them might be used by Eve to obtain additional information about the secret key. However, the increase in pulse energy is the most likely due to the unnoticed increase in intensity that can compromise the security of QKD, as was theoretically shown [2] for the prepare-and-measure decoy-state BB84 and MDI QKD protocols. We show the maximum magnification of 1.4 at the pump power of about 2.98 mW. To prevent the attack, adequate isolation should be provided throughout the spectral range.



(a) (b)

Fig. 1: Changes in photon source characteristics depending on 1310-nm injection power: normalized pulse energy and pulse width (a); output spectra (b).

IV. Summary

We have shown that a practical source based on a semiconductor laser diode is vulnerable to a laser-pumping attack, in which light at a somewhat shorter wavelength injected from the communication line into the QKD source results in an increase of the intensities of the prepared states.

References

[1] Z. Fang, H. Cai, G. Chen, R. Qu, Single Frequency Semiconductor Lasers, 1st ed. Springer Singapore, 2017.
[2] H. Temkin, G.J. Dolan, and R.A. Logan, "Optically pumped InGaAsP/InP distributed feedback lasers." J. Appl. Phys., vol. 56, pp. 2183–2186, 1984.
[3] A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, "Laser-seeding attack in quantum key distribution," Phys. Rev. Appl., vol. 12, pp. 064043, 2019.