Optical-pumping attack on a laser source in quantum key distribution

Maxim Fadeev,[1,2] Irina Zhluktova,[3] Vladimir Kamynin,[3] Roman Shakhovoy,[4,5] Vladimir Tsvetkov,[3] Vadim Makarov,[6,1,4] and Anastasiya Ponosova[1,4]

[1] *Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[2] *ITMO University, St. Petersburg 197101, Russia*
[3] *Prokhorov General Physics Institute of Russian Academy of Sciences, Moscow 119991, Russia*
[4] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*
[5] *QRate, Skolkovo, Moscow 143026, Russia*
[6] *Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*

(Dated: May 10, 2024)

The technology of quantum key distribution (QKD) can provide secret key distribution over an untrusted channel between two or more participants [1]. It uses single photons to distribute quantum states between Alice and Bob, who are authorised users. The usage of such particles provides security by laws of quantum physics such as the no-cloning theorem [2], which proves that such quantum states cannot be perfectly copied by an eavesdropper Eve.

Real implementations of QKD systems may contain several side-channels that can be used by Eve. For example, she might use a Trojan-horse attack to measure modulation states applied by Alice or Bob [3]. Or, she can perfectly control a detector at the receiver side to successfully implement an intercept-resend attack [4]. Recent research in the exploration of side-channels in QKD systems focuses on exploiting weaknesses of laser sources. These are called laser-seeding attacks [5]. To implement this attack, Eve injects light into the source of coherent light to change its output power, shape of the output pulse, or even its wavelength, by using a laser with wavelength close to the source laser's operating wavelength. In addition, the laser-seeding attack can induce phase correlations in output radiation that can provide knowledge of key information to Eve [6]. Here we propose a new kind of attack on the laser source in QKD systems that we call an *optical-pumping attack*. In this attack, Eve's radiation is absorbed by the active medium in the source's laser cavity. This energy contributes to an additional population inversion that leads to increased output power. In this attack, Eve can inject wavelength far remote from the operating wavelength in order to affect the output of the laser source.

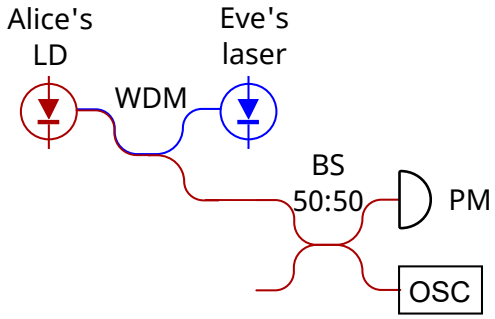

FIG. 1. Optical scheme of experiment. LD, laser diode; WDM, wavelength-division multiplexer; BS, 50:50 beamsplitter; PM, power meter; OSC, oscilloscope.

Experiment. We test a 1550-nm Alice's laser diode (LD) without a built-in isolator. It works in a gain-switched mode, biased by 3 mA constant current and driven by an electrical pulse generator at 10 MHz repetition rate. It produces 730-ps wide optical pulses. We illuminate this Alice's laser source by several Eve's cw lasers with wavelengths of 1064, 1310, 1480, and 2000 nm (Fig. 1). These lasers were connected via suitable wavelength-division multiplexers (1060/1550, 1310/1500, 1480/1550, and 2000/1550 nm).

We measure several characteristics under Eve's radiation: watt-ampere characteristic of Alice's LD in cw mode, its pulse shape and energy, and average output power. The latter is shown in Fig. 2. It can be seen that the efficiency of attack depends on Eve's illumination wavelength. In our case, the maximum increase in average power is observed under 1310-nm illumination. The pulse energy increases similarly. That is, Eve can possibly increase the mean photon number emitted by Alice, compromising the

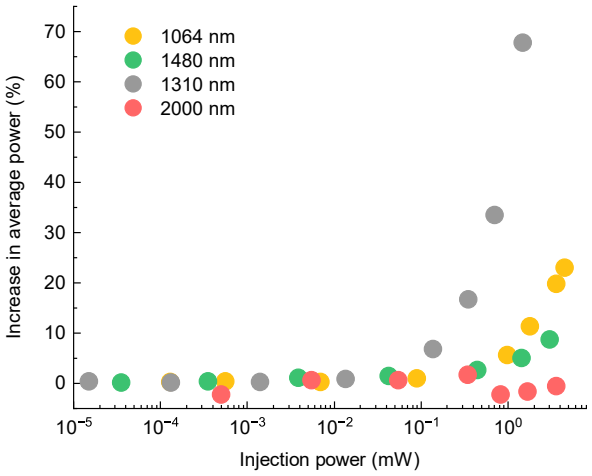

FIG. 2. Change in average output power of Alice's pulsed laser under Eve's cw illumination.

security of QKD [5].

Comparing with the laser-seeding attacks, our optical pumping attack requires a significantly higher power, on the order of milliwatts in our experiment. Many industrial QKD systems use optical isolators and dense-wavelength-division-multiplexer filters as passive countermeasures to prevent light-injection attacks. Eve has to apply high power at Alice in order to overcome the attenuation and inject the required amount of power into Alice's LD. However, these filtering elements are not perfect and their isolation is changing with wavelength. The optical-pumping attack allows Eve to use different wavelengths that match weak spots where the insertion loss, caused by the countermeasures, is the lowest.

Summary. We have proposed a new kind of attack against the laser sources used in real QKD systems. It might be performed even through existing passive countermeasures. While this attack may require a high-power laser to be successful, it should be considered as a possible threat to the security of QKD systems, especially those with a passive state preparation [7].

[1] Charles H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett. **68**, 3121–3124 (1992).

[2] Bernard Zygelman, "No-cloning theorem, quantum teleportation and spooky correlations," in *A First Introduction to Quantum Computing and Information* (Springer International, Cham, 2018) pp. 125–147.

[3] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," Phys. Rev. A **73**, 022320 (2006).

[4] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Thermal blinding of gated detectors in quantum cryptography," Opt. Express **18**, 27938–27954 (2010).

[5] 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).

[6] V. Lovic, D.G. Marangon, P.R. Smith, R.I. Woodward, and A.J. Shields, "Quantified effects of the laser-seeding attack in quantum key distribution," Phys. Rev. Appl. **20**, 044005 (2023).

[7] Wenyuan Wang, Rong Wang, Chengqiu Hu, Victor Zapatero, Li Qian, Bing Qi, Marcos Curty, and Hoi-Kwong Lo, "Fully passive quantum key distribution," Phys. Rev. Lett. **130**, 220801 (2023).