Optical-pumping attack on an injection-locked semiconductor laser source of quantum key distribution system

A. Sotnikov[1,2], **M. Fadeev**[1,3], **V. Makarov**[1,4,5], **and A. Ponosova**[1,5]
[1] *Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[2] *Moscow Institute of Physics and Technology, Moscow 141701, Russia*
[3] *ITMO University, St. Petersburg 197101, Russia*
[4] *Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*
[5] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*
e-mail: *sotnikov.ak@phystech.edu*

Quantum key distribution (QKD) securely establishes a secret key between two parties, Alice and Bob. Its security relies on quantum physics rather than computational complexity. Providing unconditional security in theory, practical implementations of QKD systems have a number of vulnerabilities.

A recent study [1] demonstrated a new attack on Alice, the optical-pumping attack. It shows that an eavesdropper Eve can boost the pulse energy of a QKD source based on a single laser diode by pumping it with different wavelengths of light. Here we study this type of attack on an optically injection-locked semiconductor laser source. This type of source is indispensable for measurement-device-independent QKD systems [2]. It is also used in QKD systems with passive state preparation [3].

Figure 1(a) shows our setup. The injection-locking source is implemented using two 1550 nm semiconductor lasers—master and slave (LD1550M and LD1550S), connected via an optical circulator (CIRC) [4]. A 1310 nm laser diode LD1310E mimics Eve. Its power varies from 700 nW to 5.4 mW. Here we place a 1310/1550 wavelength division multiplexer (WDM) between the circulator and slave laser of Alice. This configuration reduces insertion loss for Eve's light, allowing us to investigate the optical-pumping attack with a low-power LD1310E. At the same time, it maintains seeding of the slave laser by the master laser emission, as in the original Alice source.

We measure and analyze Alice's source characteristics: average power, pulse energy, and pulse shape. The optical power is characterized using an optical power meter (PM). Note that owing to WDM, back-reflected 1310 nm emission is filtered out, and we neglect it in the source power measurements. Pulse characteristics are studied using a photodiode (PD, 10 GHz bandwidth) and an oscilloscope (OSC, 16 GHz bandwidth).

We observe an increase in pulse energy and changes in the shape of Alice pulses at Eve's power above 140 μW. The pulse shape shows relaxation oscillation peaks under attack. This means that source is no longer in a stable locked regime. The pulse energy depends linearly on the pumping power [Fig. 1(b)], increasing up to 2 times under attack. These effects decrease the secure key rate [2].

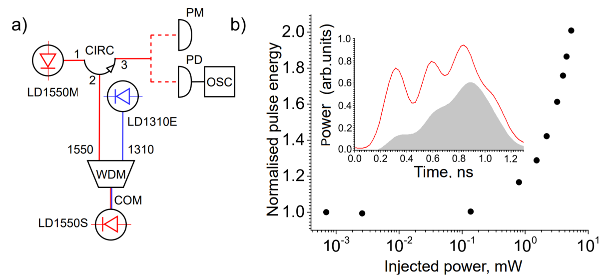

Figure 1: Optical-pumping attack. (a) Experimental setup. (b) Normalized pulse energy of Alice's pulses under Eve's illumination. Inset shows single-shot pulse shapes before and under attack at 5.4 mW.

In our work, we carry out the attack directly on the slave laser, connecting Eve inside Alice's source. Thus insertion loss for Eve's injection light is less than for attack through a quantum channel. However, this could be easily be overcome using a high-power laser, owing to the dip in isolation of circulators over the broad spectral range [2].

We have shown that the optical-pumping attack poses a threat not only to single-laser systems [1], but also to the optically injection-locked semiconductor source. This must be taken into account when designing QKD systems.

[1] M. Fadeev et al., arXiv:2503.11239 (2025).
[2] A. Huang et al., Phys. Rev. Appl. 12, 064043 (2019).
[3] J.W. Ying et al., Sci. China Phys. Mech. Astron. 68, 240312 (2025).
[4] Z.L. Yuan et al., Phys. Rev. Appl. 2, 064006 (2014).