Overview of recent results on the optical-pumping attack on quantum key distribution sources

Maxim Fadeev,[1,2] Irina Zhluktova,[3] Serafima Filatova,[3] Vladimir Kamynin,[3] Anatoliy Sotnikov,[1,4] Roman Shakhovoy,[5,6] Vladimir Tsvetkov,[3] Vadim Makarov,[7,1,5] and Anastasiya Ponosova[1,5]

[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] *Moscow Institute of Physics and Technology, Moscow 141701, Russia*
[5] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*
[6] *QRate, Skolkovo, Moscow 143026, Russia*
[7] *Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*

(Dated: April 9, 2025)

Introduction. Quantum key distribution (QKD) technology [1] uses single photon states to distribute a secret key between two parties - Alice and Bob. However, due to lack of practical true sources of single photons, commercial QKD systems use laser radiation attenuated to a single photon level. These photons are Poisson distributed [2]. An average photon number emitted by Alice is crucial for the security of QKD systems. To guarantee secrecy of key distribution, it always has to be unchanged. Recent research shows an effective attack on a typical QKD source based on a single laser diode. It is the laser seeding. Eavesdropper (Eve), injects her light at wavelength 1550-nm into Alice's laser [3]. This allows Eve to increase output power of Alice's laser, change shape of its pulses, or even wavelength [4, 5]. However, this attack can be prevented by enough isolation for light incoming from quantum channel [6]. In this work, we overview the latest research results of a new type of attack on practical Alice photon sources that could be performed to bypass existing countermeasures. It is named the optical-pumping attack. We show that both typical source configurations, a single distributed feedback laser diode and optically injection-locked laser diodes, are vulnerable to it. They emit higher output power when exposed to a light at shorter wavelengths. We investigated spectral dependency of optical-pumping attack on DFB laser. The novelty of this work lies in the demonstration of the effect of increasing the average number of photons when pumping with other wavelengths without an optical injection locking mechanism, that is used in [4]. The use of different wavelengths poses a major threat since standard optical components can pass some wavelengths almost without loss [7, 8].

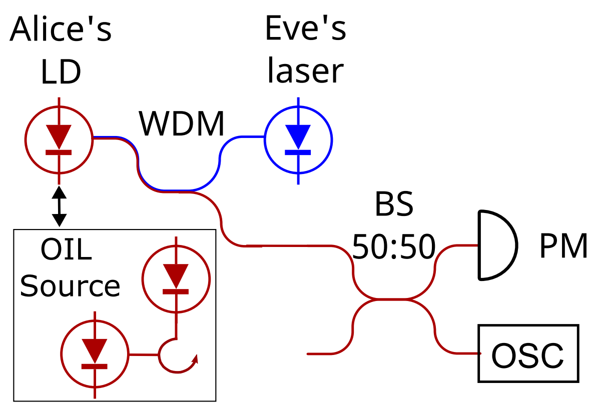

FIG. 1. Experimental setup used for optical-pumping attack

Optical-pumping attack To implement this attack, Eve injects light at a shorter wavelength than Alice by using WDM filter. There, the Eve radiation is absorbed by laser's medium, and this absorption increases output power of laser. Combined with imperfections in transmission spectrum of elements that are used for protection against attacks, optical-pumping attack can be performed more easily compared to the laser-seeding. We used a standard off the shelf Fabry-Perot laser with wavelength 1310 nm and tuned its power in a range from 23 nW to 1.6 mW by a variable optical attenuator. We measured several characteristics of Alice's output radiation, such as light-current dependency, average output power and energy of emitted pulses. Normalized pulse energy is demonstrated

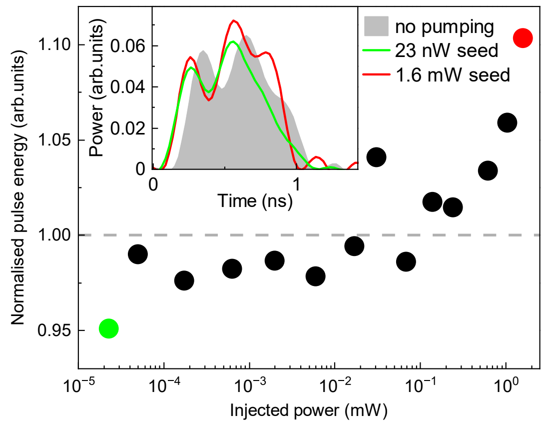

FIG. 2. Pulse energy of laser pulses under Eve's illumination, normalized to their energy without pumping (reprinted form [9]).

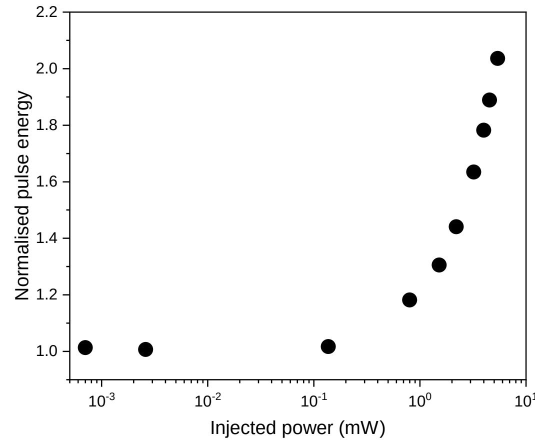

FIG. 3. Pulse energy of laser pulses emitted by OIL configuration under Eve's illumination, normalized to their energy without pumping

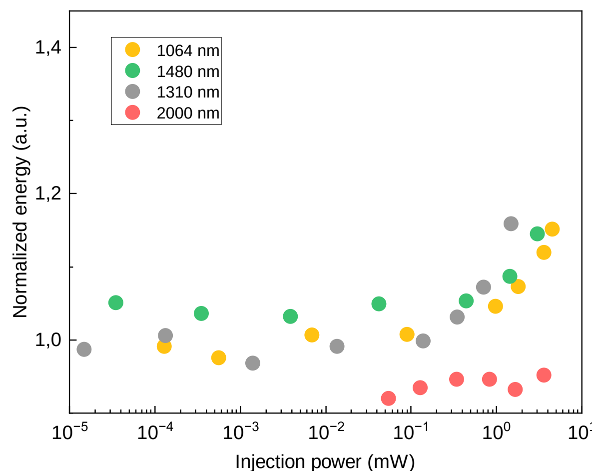

FIG. 4. Change in average output power of Alice's pulsed laser under Eve's cw illumination.

Figure 2. In this case, we managed to increase the energy of output pulses by 10%. In addition, this attack increased the differential quantum efficiency by 5% and the average output power by 21%. Increase in average photon number as a result of increased output power leads to overestimation of secret key rate by about 10% at distance of 50 km for BB84 decoy-states protocol.

Optical-pumping attack on laser source with optical injection locking. Optical injection locking (OIL) is a technique that is used to improve characteristics of output radiation of laser. It reduces spectral width of radiation, stabilizes its wavelength, reduces jitter of emitted pulses and reduces oscillations within pulses. Such laser source contains two laser sources: master and slave. Master injects its radiation through an optical circulator into slave's cavity to seed it. This method is used in measurement-device independent protocols. We used the same 1310-nm attackers laser to hack the OIL configuration of Alice source.. In this case, power of Eve's laser changed from 0.7 μW to 5.6 mW. We measured average output power of Alice's laser, energy of pulses and pulse waveforms. As a result, the optical-pumping attack increased energy of pulses by 2 times, average power increased by 2.25 times; it is demonstrated in figure 3. Increase in pulse energy for QKD applications leads to increase in photon number. This is also leads to overestimation of secret key rate in comparison to SKR with average photon number specified by the protocol. This allows Eve to get more bits of secret key.

Spectral dependency of optical-pumping attack. InGaAsP crystals have wide absorption spectra, that can be used by Eve to perform the optical-pumping attack. We investigated efficiency of the optical-pumping attack with lasers at different wavelengths. For this purpose we used several laser sources with wavelengths 1064 nm, 1310 nm, 1480 nm and 2000 nm. For each Eve's wavelength we measured average output power and pulse energy. Results for each wavelength are demonstrated in Figure 4. For pump at

1064 nm increase in average power is 23% and for pulse energy is 15%, for 1310 nm pump average power increased by 21% and pulse energy increased by 10%, for 1480 nm average output power increased by 8.7% and pulse energy by 14%. However, under pumping by 2000 nm illumination we measured a decrease in average output power by 8% and pulse energy decreased by 0.5% Those results show that Eve can use broad spectral range to implement the optical-pumping attack. The most effective wavelength is 1064 nm because it increases the energy of the pulses.

Conclusion In this work we presented new kind of attack on technical implementation of QKD system called "optical-pumping" attack. This attack allows Eve to increase average photon number, emitted by Alice. It leads to overestimation of the secret key rate. Here we demonstrate that this attack can be performed to single DFB-lasers as well to DFB-laser source with optical injection locking. Also we demonstrated that this attack can be performed by using several wavelengths. 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.

[1] Gilles Brassard and Louis Salvail, "Secret-key reconciliation by public discussion," Lect. Notes Comp. Sci. **765**, 410 (1994).

[2] Oxborrow M and Alastair G Sinclair, "Single-photon sources," Contemporary Physics **46**, 173–206 (2005).

[3] Zhixin Liu and Radan Slavík, "Optical injection locking: From principle to applications," Journal of Lightwave Technology **38**, 43–59 (2020).

[4] 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).

[5] 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).

[6] M. Fadeev, A.A. Ponosova, A. Huang, R. Shakhovoy, and V. Makarov, "Secure laser source for qkd systems," in *2024 International Conference Laser Optics (ICLO)* (2024) pp. 571–571.

[7] A. V. Borisova, B. D. Garmaev, I. B. Bobrov, S. S. Negodyaev, and I. V. Sinil'shchikov, "Risk analysis of countermeasures against the Trojan-horse attacks on quantum key distribution systems in 1260–1650 nm spectral range," Opt. Spectrosc. **128**, 1892–1900 (2020).

[8] Boris Nasedkin, Fedor Kiselev, Ilya Filipov, Darya Tolochko, Azat Ismagilov, Vladimir Chistiakov, Andrei Gaidash, Anton Tcypkin, Anton Kozubov, and Vladimir Egorov, "Loopholes in the 1500–2100-nm range for quantum-key-distribution components: Prospects for trojan-horse attacks," Phys. Rev. Appl. **20**, 014038 (2023).

[9] M. Fadeev, A. Ponosova, Q. Peng, H. Anqi, R Shakhovoy, and V. Makarov, "Optical-pumping attack on a quantum key distribution laser source," Phys. Rev. A **-**, – (2025).