Secure laser source for QKD systems

M. Fadeev[1,2], A.A. Ponosova[1], A. Huang[3], R. Shakhovoy[4,5,6], V. Makarov[1,5,7]
[1] *Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[2] *ITMO University, St. Petersburg, 197101, Russia*
[3] *National University of Defense Technology, Changsha 410073, People's Republic of China*
[4] *QRate, Skolkovo, Russia*
[5] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*
[6] *Moscow Technical University of Communications and Informatics, Moscow, Russia*
[7] *University of Science and Technology of China, Shanghai 201315, People's Republic of China*
mfadeev2022@gmail.com

***Abstract*—In practical quantum key distribution systems, single photon sources take laser-seeding attacks. Typically, some amount of isolation is recommended as the countermeasure against these attacks. Here, we demonstrate a new approach of QKD system protection against laser seeding based on internally seeded photon source scheme, resilient to external perturbations.**

***Index Terms*—single photon source, QKD, laser-seeding attack, quantum hacking, countermeasure**

I. Introduction

Practical QKD systems use strongly attenuated laser pulses from semiconductor laser diodes (LD) rather than truth single-photon sources due to the lasts do not enable practical key rates. However, as LDs are very sensitive to external perturbations, there are several laser-seeding attacks which open up back doors for Eve. Previous study has shown that an injection power of 100 nW could be enough to control the intensity of Alice's pulses [1] and about 1 nW might be enough to partially control the phase [2]. Here, we investigate an internally seeded photon source configuration under external laser-seeding attack.

II. Experiment

We implemented an optical injection-locked light source proposed by L.C.Comandar et al. [3]. It includes the master laser diode that injects pulses into the slave laser diode via a fiber-optic circulator. Both LDs' temperature and time of drive electric pulses were matched well to provide injection locking and chirpless bell-shaped laser pulses. The source operates at 10.035 MHz repetition rate with pulse duration of about 850 ps. To investigate resilience of the source, the attacker's CW seed laser emission is inserted into the source through the third circulator port (Alice's output). Our experimental setup allow Eve's laser power from 100 mW to 1.1 W and spectral tunability of about several nanometers near to 1550 nm. Due to losses in the circulator for Eve's light, the maximum Eve's laser power is about 1.3 μW at the slave entrance (in comparison, the average power of the master LD at the slave entrance is 7 μW). The average power, spectra, pulse shapes, pulse intensity stability and statistic of interference of two following each other pulses are characterized before and under attack using different Eve's laser wavelengths.

III. Results

The source under attack shows high stability of its spectral and amplitude-time characteristics. However, we found an increase in average output power by 7.5%. According to data analysis, it results from amplification of Eve's emission in the slave LD. Figure 1 shows output spectra for different seed laser wavelengths. It can be seen that amplification is the most notable when Eve's wavelength differs from Alice's one. While Eve might conduct a wavelength-dependent attack using DWDM to obtain additional information about the secure key, this attack might be easy closed using a narrowband spectral filter.

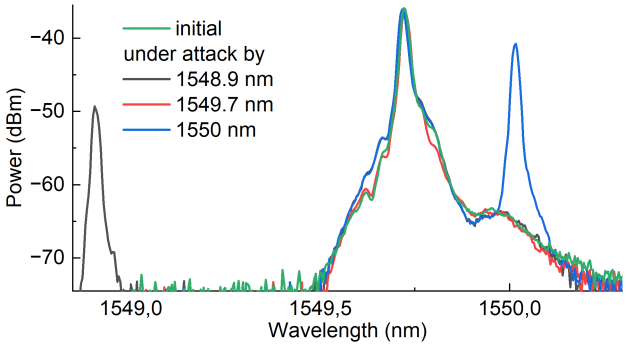

Fig. 1. QKD source output spectra when seeding power at the slave entrance is about 700 nW. (The spectra of reflected Eve's emission are rejected from the measured output spectra.)

IV. Summary

We show experimentally that the injection-locked source is resilience against laser-seeding attacks and might be used as an effective countermeasure in QKD sources.

References

[1] 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.
[2] 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., Vol. 20, pp. 044005, 2023.
[3] L.C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, Z.L. Yuan, and A.J. Shields, "Near perfect mode overlap between independently seeded, gain-switched lasers," Opt. Express. vol. 24, pp. 17849–17859, 2016.