Enabling high-speed quantum random number generation by optically injection-locking a pulsed laser

Anastasiya Ponosova,[1,2] Dmitry Shkrabin,[3] Daria Ruzhitskaya,[1,2]
Maxim Fadeev,[1] Vadim Makarov,[4,1,2] and Roman Shakhovoy[2,3]

[1] *Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[2] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*
[3] *QRate, Skolkovo, Moscow 143026, Russia*
[4] *Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*

(Dated: June 2, 2025)

Random numbers are indispensable in modern information processing, including cryptography, modeling and simulation, etc. During the last decade, researchers have invested significant effort into designing practical quantum random number generators (QRNGs). QRNGs are particularly appealing because they utilize quantum entropy sources, which inherently provide true randomness.

QRNG that utilizes the interference of adjacent laser pulses with random phases is a promising candidate for practical applications [1]. A long list of investigations predicts extremely high random number generation rates of such QRNGs, up to 100 Gb/s. However, recent studies have shown that there are several phenomena that prevent extracting pure quantum randomness from interference of laser pulses [2, 3]. They are classical noise, chirp, jitter, and relaxation oscillations in the laser pulses. At the same time, Comandar and his coworkers [4] have designed an optically injection locked (OIL) source to improve interference visibility in measurement-device-independent quantum key distribution systems.

Here we present a comparative study of QRNG implementations with a single laser diode (LD) and OIL configuration of the laser pulse source. We experimentally demonstrate that the single-LD source limits the rate of bit generation owing to degradation of interference when the laser pulses get shorter. Meanwhile the OIL source provides an almost ideal interference visibility.

Experiment. We implement QRNG based on interference of laser pulses with random phase. Figure 1 shows our setup. The optical scheme includes a source of laser pulses and an unbalanced Michelson interferometer. The laser source consists of two identical 1550-nm LDs—master and slave—connected via a fiber-optic circulator. By switching the master LD on and off, we investigate and compare interference properties of the pulses emitted by the single LD and by OIL source configuration. At the output of the optical scheme, we take long waveform recordings using a high-speed oscilloscope and photodetector, and analyse histograms of pulse-area measurement. In addition, we extract a raw bit sequence from the waveforms using a Python script that imitates the measurement and processing parts of QRNG device.

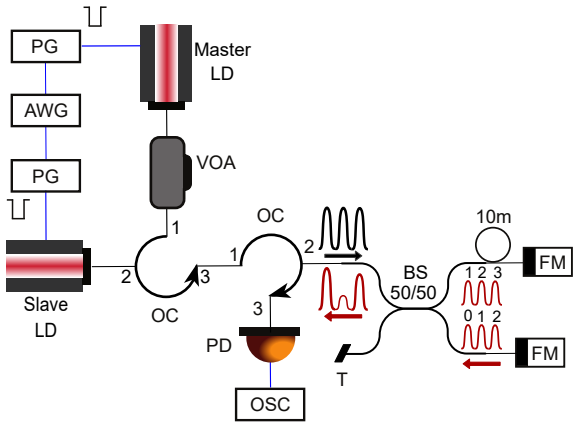

FIG. 1. Experimental setup. AWG, arbitrary waveform generator; BS, fiber-optic beam-splitter; FM, Faraday mirror; LD, laser diode; OC, fiber-optic circulator; OSC, oscilloscope; PD, photodetector; PG, pulse generator; T, beam trap; VOA, variable optical attenuator.

Figure 2 shows the experimental probability distribution of the interference signal (i.e., its probability density function, PDF) for OIL configuration and for the single LD with different pulse durations. In the top plot, OIL configura-

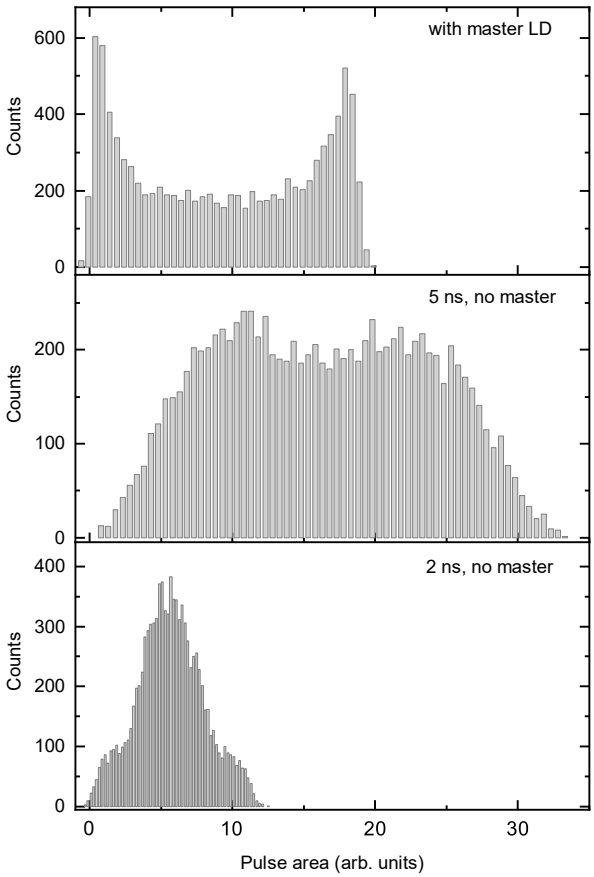

FIG. 2. Probability density function of the interference signal of the OIL source (top plot) and single LD with different pulse durations (middle and bottom plots). The duration of driving electrical pulses is given in the legend.

tion provides an almost ideal bimodal PDF. Its signatures at the interval's ends are damped, owing to noise in our measurement equipment. In the middle plot, a single LD with a sufficiently long pulse already shows that the peaks move towards the center of PDF, because of worse interference visibility owing to chirp, jitter, and relaxation oscillations of the laser pulses. The bottom plot shows that the interference of shorter laser pulses is destroyed.

Summary. Our study shows that the speed of random number generation by QRNG based on interference of laser pulses is limited. To increase generation rate, the laser pulses need to be shortened. However, the interference of short laser pulses from the single LD is problematic, due to jitter and phase modulation (chirp). The OIL configuration originally proposed for measurement-device-independent quantum key distribution [4] does not have the above disadvantages and therefore enables the design of QRNG with a high speed of random number generation.

[1] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode, Opt. Express **22**, 1645 (2014).

[2] R. Shakhovoy, D. Sych, V. Sharoglazova, A. Udaltsov, A. Fedorov, and Y. Kurochkin, Quantum noise extraction from the interference of laser pulses in an optical quantum random number generator, Opt. Express **28**, 6209 (2020).

[3] R. Shakhovoy, V. Sharoglazova, A. Udaltsov, A. Duplinskiy, V. Kurochkin, and Y. Kurochkin, Influence of chirp, jitter, and relaxation oscillations on probabilistic properties of laser pulse interference, IEEE J. Quantum Electron. **57**, 2000307 (2021).

[4] 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 **24**, 17849 (2016).