Attack-resistant quantum random number generator based on the interference of laser pulses with random phase

Violetta Sharoglazova[1,2*], Roman Shakhovoy[1,2], Alexander Udaltsov[1,2], Alexander Duplinsky[1,2], Yury Kurochkin[1,2,4]

[1] *Russian Quantum Center, Moscow, Russia 2QRate, Moscow, Russia*
[2] *QRate, Moscow, Russia*
[3] *Skolkovo Institute of Science and Technology, Moscow, Russia*
[4] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow, Russia*
*E-mail: v.sharoglazova@goqrate.com

Random numbers are an important resource for various fields of science and technology. One of the most interesting and promising areas for their use is cryptography and its everyday applications. Nowadays, the physical source of true random numbers — a quantum random number generator (QRNG) — plays a key role in cryptographic methods with a quantum key distribution (QKD).

Over the past decades, numerous QRNG schemes based on different quantum effects have been proposed [1]; however, most modern QRNGs use various methods of quantum optics, because optical QRNGs may provide high rates of random bit generation. The rapid development of this area has formed the basic approaches for extracting random numbers. At present, the main work is focused on improving existing optical schemes and creating new post-processing algorithms in order to achieve higher generation rates.

We propose QRNG, which uses an idea of M. Jofre et al. [2]. The principal scheme of the QRNG is shown in fig. 1. The laser is modulated by the pulse driver over threshold and a continuous train of pulses is sent to the Michelson interferometer, where the delay time of the longer arm is chosen to be a multiple of the pulse repetition period. The fast photodiode detects the interference of two laser pulses with random phases.

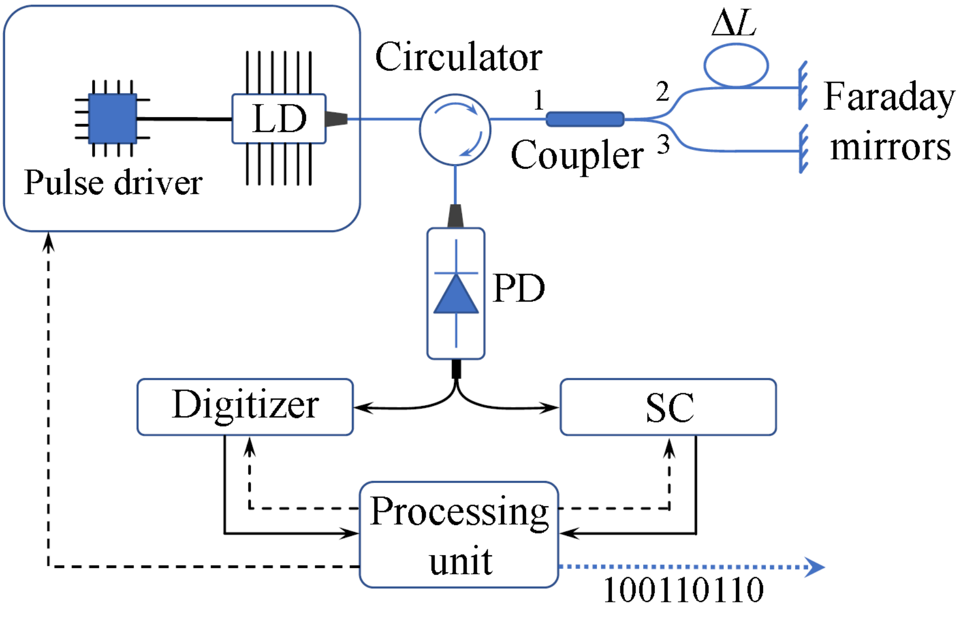

Figure 1: Principle scheme of the QRNG. Optical part includes unbalanced Michelson interferometer. ΔL — delay line. PD — photodetector, LD — laser diode, SC — statistics control unit.

The signal from the photodetector is processed in the statistical control unit, which is employed to find the probability density of the random signal. Obtained statistic is used to determine the contribution from external classical noise and possible influence of the adversary. This information is used to set up the digitizer so that it discards the potentially predictable signals. These blocks can be implemented using cheap comparators.

We demonstrated QRNG that can generate bit sequences with rate of 2.5 Gbps. Under normal operating regime, the system continuously determines (on-the-fly) the ratio of quantum and classical noise performing the self-testing and self-tuning of the QRNG. We avoid comprehensive post-processing procedures and replace them with the hardware algorithm. The proposed scheme is designed to be low-priced and optimized for potential production.

The work was supported by the Russian Science Foundation (Grant No. 17-71-20146).

References

[1] *M. Herrero-Collantes, J. C. Garcia-Escartin*, Quantum random number generators. Rev. Mod. Phys., **89**, 015004, (2017).

[2] *M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, V. Pruneri*, True random numbers from amplified quantum vacuum. Opt. Express, **19**, 20665, (2011).