502G bits/s quantum random number generation with simple and compact structure

JINLU LIU[1], JIE YANG[1], ZHENGYU LI[2], WEI HUANG[1], BINGJIE XU[1*]

[1]*Science and Technology on Security communication Laboratory, Institute of Southwestern Communication, Chengdu 610041, China*
[2]*State Key Laboratory of Advance Optical Communication Systems and Networks, Center for Computational Science & Engineering (CCSE) and Center for Quantum Information Technology, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, China*
**Corresponding author: xbjpku@pku.edu.cn*

Based on measuring quantum phase fluctuation of a laser diode, we propose a new approach of quantum random number generation (QRNG) with simple and compact structure. The theoretical model of the QRNG is established and the simulation results agree with the experimental data. Finally, 502G bits/s random bits generation rates can be obtained, which can pass the ENT, Diehard and NIST-STS random statistic test.

Experimental setup of the proposed QRNG is shown in Fig.1. A DFB laser diode (LD) emits continuous-wave (CW) beam. To maximize the phase fluctuation, the LD is operated around its threshold level. By a 50/50 polarization-maintaining beam splitter (BS), the CW beam is split into two paths. One beam is directly coupled into a 40GHz photo-detector (PD). The other beam is coupled into a fiber loop, composed by the BS and a delay line (DL), and recirculates inside the loop. Employing a high speed build-in-8-bit ADC in an oscilloscope to sample the output of the PD, raw random bits are generated.

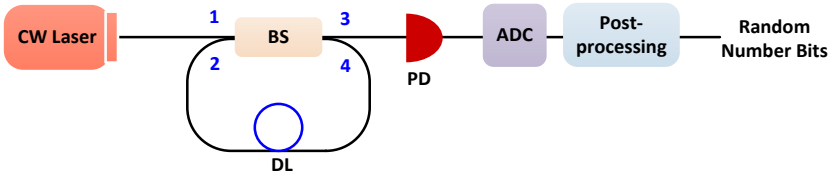

Fig.1 Experimental setup of the proposed QRNG

A theoretical model of the QRNG setup is established. As shown in Fig.2, simulation results fit well with the experiment measured data. Furthermore, the min-entropy of the raw data is 6.27 per byte. As the bandwidth of PD is 40GHz and the sampling rate of ADC is 80GSa/s, the final random bits generation rate reaches up to 502Gbits/s, which passes NIST-STS, Diehard and ENT tests. As an example, the NIST-STS test result is shown in Fig.3.

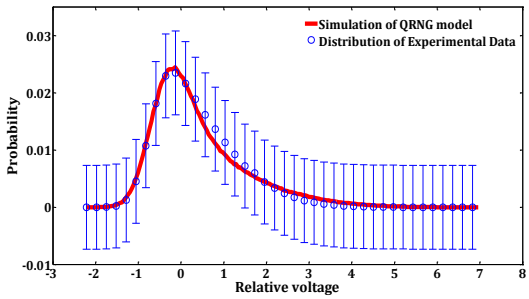

Fig.2 The normalized distribution of experimentally measured interference intensity and simulation result of the theoretical model for the proposed QRNG

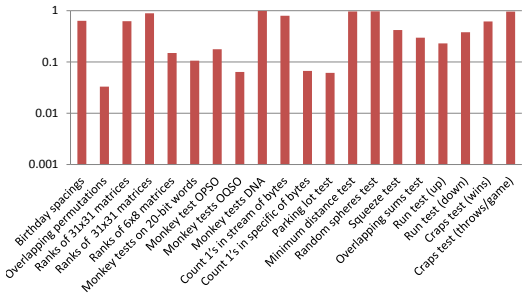

Fig.3 The NIST-STS test result

In summary, we propose and experimentally establish a simple and compact QRNG, and the random bit generation rate can be significantly upgraded to 502G bits/s.

Reference

1. *Nie, Y. Q., Huang, L., Liu, Y., Payne, F., Zhang, J., & Pan, J. W. (2015). The generation of 68 Gbps quantum random number by measuring laser phase fluctuations. Review of Scientific Instruments, 86(6), 063105.*
2. *Xu, F., Qi, B., Ma, X., Xu, H., Zheng, H., & Lo, H. K. (2012). Ultrafast quantum random number generation based on quantum phase fluctuations. Optics express, 20(11), 12366-12377.*
3. *Guo, H., Tang, W., Liu, Y., & Wei, W. (2010). Truly random number generation based on measurement of phase noise of a laser. Physical Review E, 81(5), 051137.*