68 Gbps quantum random number generation by measuring laser phase fluctuations

You-Qi Nie,[1,2] Leilei Huang,[3] Yang Liu,[1,2] Frank Payne,[3]
Jun Zhang[1,2,*] and Jian-Wei Pan[1,2]

[1]*Hefei National Laboratory for Physical Sciences at the Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[2]*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[3]*Department of Engineering Science, University of Oxford, Parks Road, Oxford OX1 3PJ, United Kingdom*

[*]*Electronic mail: zhangjun@ustc.edu.cn*

Abstract:

Random numbers have a wide range of applications such as encryption, Monte Carlo simulation, statistical analysis, and lottery. The indeterministic nature of quantum mechanics allows us to construct quantum random number generators (QRNGs) whose output cannot be predicted. The generation speed is essential for practical applications, such as high-speed quantum key distribution systems.

Here, we push the speed of a quantum random number generator to 68 Gbps [1] by operating a laser around its threshold level. To achieve the rate, not only high-speed photodetector and high sampling rate are needed but also a very stable interferometer is required. A practical interferometer with active feedback instead of common temperature control is developed to meet the requirement of stability. Phase fluctuations of the laser are measured by the interferometer with a photodetector and then digitalized to raw random numbers with a rate of 80 Gbps.

The min-entropy of the raw data is evaluated by modeling the system and is used to quantify the quantum randomness of the raw data. The bias of the raw data caused by other signals, such as classical and detection noises, can be removed by Toeplitz-matrix hashing randomness extraction [2]. The final random numbers can pass through the standard randomness tests. Our demonstration shows that high-speed quantum random number generators are ready for practical usage.

Keywords:

Random number, quantum random number generation, phase fluctuation, min-entropy, Toeplitz-matrix hashing

Reference:

[1] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang and J.-W. Pan, Rev. Sci. Instrum. 86, 063105 (2015).

[2] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Phys. Rev. A 87,062327 (2013).