Quantum
24-27 June 2018
Aberdeen, UK

Cryptographic Quantum Random Number Generation Using Shot Noise

Jakub Niemczuk[1*], Ewa Płaczek – Popko[2], Sławomir Drobczyński[2] and Tadeusz Martynkien[2]

[1]*Faculty of Microsystem Electronics and Photonics, Wrocław University of Science and Technology,*
Janiszewskiego 11/17, 50-372 Wrocław, Poland
[2]*Faculty of Fundamental Problems of Technology, Wrocław University of Science and Technology,*
Wyb. Wyspiańskiego 27, 50-370 Wrocław, Poland

The demand for fast, high entropy, randomness sources in fields like physics or mathematics was always high; despite this the quality of random numbers generated by software algorithms or hardware generators was not so important. But today along with the development of more efficient digital communication the need of stronger and stronger encryption arose. Almost all commonly used encryption protocols require a source of random numbers.

A good source of randomness are quantum uncertainty effects like the probability of radioactive decay, vacuum fluctuations, Raman scattering, photon emission in photoluminescence or, covered in this work, shot noise. Shot noise arises from the fact that electric current is not continuous but it is made of discrete particles, for example in metals the electric current is carried by electrons. Shot noise exists in every electronic device that has some type of barrier and electric current flows through it. If the long time rate of current flow through a barrier is continuous there is a chance that in smaller time intervals the number of carriers passing through that barrier will differ.

To avoid doubts if Schottky noise or avalanche noise is a type of quantum shot noise our device was build around a photodiode and a light emitting diode so that the shot noise is created from the probability of photon emission from the LED semiconductor, photon absorption in the photodiode semiconductor material and the probability of electron – hole pair generation through photon absorption.

This work describes the build of a secure, tamper-proof, hardware quantum random number generator, ideal for quantum cryptography; that is build around the shot noise phenomenon in semiconductor devices. Special care was put in the shot noise extraction to ensure that only it contributed in the generation of random number sequences.

Keywords: random numbers, quantum cryptography, shot noise