KRAJOWA KONFERENCJA ELEKTRONIKI
Darłówko Wschodnie 03 - 07.06.2018

Jakub Niemczuk
Faculty of Microsystem Electronics and Photonics
Wrocław University of Science and Technology
ul. Janiszewskiego 11/17, 50-372 Wrocław

Ewa Popko
Department of Quantum Technologies
Wrocław University of Science and Technology
Wyb. Wyspiańskiego 27, 50-370 Wrocław

Sławomir Drobczyński
Tadeusz Martynkien
Department of Optics and Photonics
Wrocław University of Science and Technology
Wyb. Wyspiańskiego 27, 50-370 Wrocław

Cryptographic quantum random number generation using shot noise

Keywords: random number generator, shot noise, quantum cryptography, noise in semiconductor devices.

ABSTRACT

With the development of telecommunications, the demand for new, more effective encryption mechanism for communication channels has increased. Many algorithms use random numbers for seed generation encryption key generation, and their power depends on the quality of the random number generators used. Currently used generators with the highest entropy use quantum phenomena, such as: vacuum fluctuation, photoluminescence, radioactive decay, Raman phenomenon. The resented method for generating random numbers is based on shot noise generated in semiconductors. The aim of this project was to produce a random number generator that would be resistant to external factors, and would be based on the phenomenon of electroluminescence and shot noise generated in a photodiode operating in a photoconductive mode.