Uniwersytet Gdański
Centrum Transferu Technologii

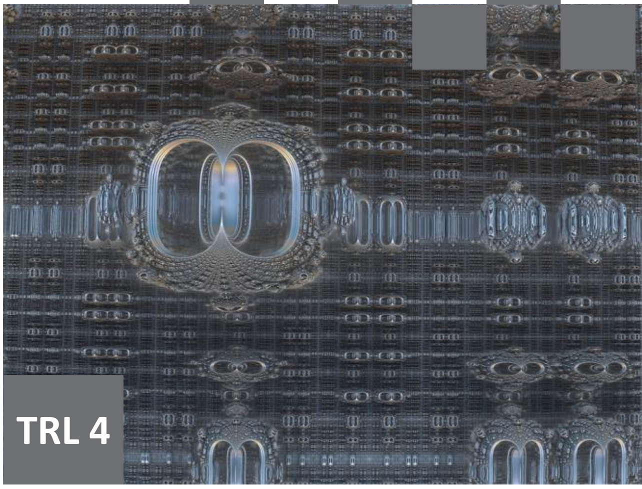
physics

Single-photon-based self-testing quantum random number generator

Brief description of the invention

Random number generation is a crucial aspect of various fields of study, including cryptography, statistical analysis, and simulations. Random numbers are used to generate cryptographic keys, to simulate stochastic events, and to ensure the fairness of games and lotteries, among other applications. However, generating truly random numbers is a challenging task.
Most computer-based random number generators rely on algorithms that are deterministic and thus in practice predictable, and thus produce only pseudo-random numbers.

The **invention** refers to **self-testing quantum devices** allowing generation of truly **random bit strings**.
A features of quantum random number generators (QRNGs) is the possibility of self-testing of the device. A self-testing device can monitor the output statistics to verify the quality of the obtained randomness, and further based on this knowledge improve on this quality.
In QRNGs quantum measurements of physical quantities like photon polarization are used to **generate random numbers** that cannot be predicted or reproduced by an attacker. These devices offer high levels of security, making them ideal for applications for which security is critical.



Authors

Konrad Schlichtholz, PhD Std
Bianka Wołoncewicz, PhD Std
PhDTamoghna Das
PhD Marcin Markiewicz
Prof. Marek Żukowski

IP protection

The invention is the subject of a European patent application EP23199255.3

Possible cooperation

- Partnership in further Research
- Licensing
- Selling the technology

Dedicated for sectors

- communication
- cryptography
- computer Monte Carlo simulations
- password generation
- banking encryption
- lotteries and casinos
- video-computer games

biuro@ctt.ug.edu.pl
ul. Wita Stwosza 63,
80-308 Gdańsk
www.ctt.ug.edu.pl

Judyta Gawryś
☎ +48 725 991 257

Technology offer
No 111/24/2024