

PQRNG 150

Quantum Random Number Generator

- Quantum Random Number Generator based on photon arrival times
- Bit rate: 150 Mbits/s
- Interface: USB 2.0
- Software: Driver and user library (DLL) for Windows™ XP, Vista and 7; DLL demos and simple GUI for data retrieval to files

Applications

- Monte Carlo simulations
- Secure data encryption
- Gaming and lotteries



Randomness is an invaluable resource in many areas of science and technology ranging from Monte Carlo simulations to secure encryption methods. While computer generated random numbers can be used for some applications, they remain fundamentally non-random in the sense that anything generated by an algorithm is at least in principle predictable. However, quantum physics provides randomness with unpredictability based on the fundamental laws of nature.

An accessible and convenient source of quantum randomness is ubiquitously available in the form of a stream of single photons. Several photon based random number generators utilizing quantum indeterminism have been proposed and realized in the recent past. However, with respect to commercial availability, not many implementations so far were reliable and/or cost efficient enough for routine use outside the physics laboratory.

The PQRNG 150 is a new Quantum Random Number Generator (QRNG) based on the quantum randomness of photon arrival times. It provides turn-key usability, provable and long term statistical quality, and high speed. The design creates a new quality in the sense that it offers substantially higher bit rates than previous solutions available to the public. This has become possible by exploiting most recent photon timing instrumentation and state-of-the-art data processing in hardware. The post-processing algorithm applied to the raw data is based on solid predictions from information theory, which guarantee conservation of randomness. This allows for the use of the delivered random numbers in unconditionally secure encryption schemes. The random numbers delivered by the PQRNG 150 have successfully passed the most stringent testing possible today. Results are published in Applied Physics Letters, Vol. 098, 171105 (2011).

Single chunks of random data generated by the PQRNG 150 can be downloaded directly from a dedicated webserver (<https://qrng.hu-berlin.de>), which also provides continuous streams of random data by means of DLLs for access to the server.

Specifications

Bit rate	150 Mbits/s
Interface	USB 2.0
Software	driver and user library (DLL) for Windows™ XP, Vista and 7 DLL demos and simple GUI for data retrieval to files
Size	310 × 235 × 140 mm
PC requirements	min. 1 GHz CPU clock, 512 MB memory
Power consumption	< 50 W, at 100 VAC to 240 VAC



PicoQuant GmbH
Rudower Chaussee 29 (IGZ)
12489 Berlin
Germany

Phone +49-(0)30-1208820-0
Telefax +49-(0)30-1208820-90
Email info@picoquant.com
Web www.picoquant.com