Technology Offer

Apparatus for Generating Random Numbers using an Optical Parametric Oscillator
Ref.-No.: 1201-5494-BC-JK

The invention relates to an apparatus for generating random numbers, using an optical parametric oscillator.

The generation of random numbers is important in information science as well as in modelling and simulation. In cryptography, for instance, random numbers are needed for encryption algorithms. Preferably, the generated numbers are true (i.e. non-predictable) and have an equal distribution.

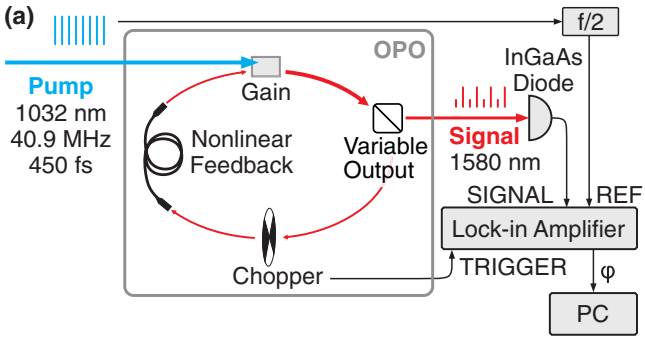
The apparatus according to the invention is based on the bi-stable outcome of an optical parametric oscillator (OPO) with nonlinear fiber feedback. A lock-in amplifier is used for determining the phase of the output signal of the OPO compared to a reference signal. Other, more simple schemes, such as a demodulator or a rf-mixer, can be used instead of the lock-in amplifier. Depending on whether the high (H) pulses or the low (L) pulses of the output signal of the OPO are synchronous with the pulses of the reference signal, the apparatus generates a 1-bit or a 0-bit. This implementation allows for a non-degenerate operation of the OPO, is simpler and has a lower noise-level than the prior art.

Advantages

- Unambiguous generation of two different output/bit states
- The bi-stability of the OPO associated with the two output states is equi-energetic and equi-probable
- No additional un-biasing or bit extraction is necessary for randomness generation
- Detector noise plays no role in detecting the output signal of the OPO
- The entropy of the generated bit stream amounts to 99.5% (11.5σ bound)
- The apparatus passes with flying colors the "Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications" provided by NIST and published on September 16, 2010, by Lawrence E. et al.
- Has the potential of miniaturization with state-of-the-art technology on a photonic chip
- With a miniaturized apparatus including a pulsed laser with a repetition rate in the GHz range and a corresponding OPO random bit rates in the MHz range can be achieved

Applications

- In cryptography for providing encryption keys to secure communication, money transfer and storage of sensitive data
- In modelling and simulation for providing random numbers
- In gambling for providing the complete randomness necessary for the outcome of chance-based digital games (online casinos)



Background

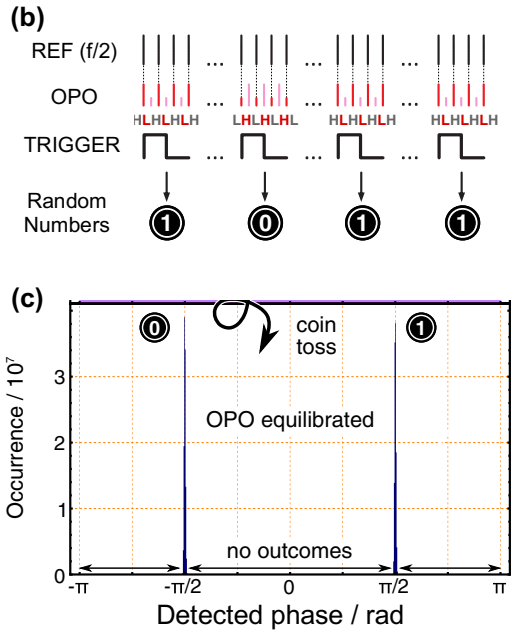
Random number generators can be based on algorithms. However, these generators can emit only cycles of seemingly random bits; and therefore are referred to as pseudo number generators (PRNG). True random number generators (TRNG) are based on hardware, such as a die, a coin, a chaotic system or an electrical component. The numbers generated by TRNGs are considered unpredictable, although it is difficult to prove this. This fundamental problem of TRNGs can be overcome by quantum random number generators (QRNG). These are based on quantum mechanical processes, whose observation is inherently random. Quantum mechanical processes in optical systems are preferred in view of speed, power losses, heat generation and wiring. However, in some of the conventional optical QRNGs the measured output signal is not unambiguously binary and/or exhibits an unbalanced distribution. In order

Max-Planck-Innovation GmbH
Amalienstr. 33
80799 München
www.max-planck-innovation.de

to overcome these drawbacks, additional extensive processing of the measured output signal is necessary. This additional processing can be avoided by using OPOs as part of the optical system. Conventional optical QRNGs that use OPOs are operated in a degenerate state with phase-sensitive amplification. This mode of operation requires additional stabilization mechanisms with sub-micrometer precision, which complicates the structure of the apparatus and makes it more expensive.

Technology

The apparatus for generating random numbers according to the invention comprises an OPO, a phase determination unit, an evaluation unit, a switching means and a trigger means. The OPO is pumped by a pulsed laser with a predetermined pump power and a predetermined pulse repetition rate, wherein the OPO operates in a period multiplication state (PMS) for providing an oscillator output signal of light pulses with alternating pulse energy. The oscillator output signal has a pulse repetition rate that is 1/N of the predetermined pulse repetition rate of the pulsed laser, where N is an integer and N > 1. Figure a) shows an implementation for N=2. In this figure the oscillator output signal is red colored. The phase determination unit determines the phase (φ) of the oscillator output signal with respect to the reference signal (REF), wherein the reference signal has a pulse repetition rate that is 1/N of the predetermined pulse repetition rate of the pulsed laser. In the implementation shown in figure a) a lock-in amplifier is used as the phase determination unit. The evaluation unit generates at least one random number based on the determined phase (φ). Preferably, the evaluation unit generates a 0-bit when the determined phase (φ) is below a threshold value, and a 1-bit when the determined phase (φ) is above the threshold value. In figure a) the oscillator output signal is a pulse train of alternating high and low pulses, and accordingly the evaluation unit generates a 1-bit when the high pulses are synchronous with the pulses of the reference signal, and generates a 0-bit when the low pulses are synchronous with the pulses of the reference signal. This is illustrated in figure b). A chopper is used as switching means in the implementation of figure a). This alternately switches the OPO on and off. After switching the OPO on, this undergoes a transient phase until it reaches a stable phase of the PMS. The trigger means provides a trigger pulse (TRIGGER) in the stable phase of the PMS. In response to the trigger pulse, the phase determination unit determines the phase (φ), and the evaluation unit generates the corresponding bit. The determined phase (φ) is mainly due to quantum effects occurring in the transient phase of the starting OPO, especially vacuum fluctuations. As these are of random nature, also the phase (φ) and its associated bit are of random nature. Figure c) shows phases (φ) which have been determined in the stable phase of consecutive on-states of the OPO. The outcomes are centered around -π/2 and π/2, respectively. The width (1σ) of each peak is 0.0023 rad, and the peaks are separated by 400 standard deviations. In the implementation shown in Figure a) the random bit generation rate is limited by the sample rate of the chopper, which is limited to 10 kHz. However, when using a fiber-optic electro-optic modulator instead of the chopper, the random bit generation rate is mainly limited by the duration of the transient phase of the PMS. This is approx. 300ns, and hence random bit generation rates above 1 MHz can be achieved.



Contact

Dr. Franz Gadelmeier
Patent- & License Manager
Physicist
Phone: 0171-6569140
eMail: gadelmeier@max-planck-innovation.de

Patent Publications:

WO 2019/086093 A1
EP 3 704 570 A1
US 2020/0257502 A
(Notice of Allowability has been received)

Further Publication:

Tobias Steinle et al., Unbiased All-Optical Random-Number Generator, Phys. Rev. X 7, 041050 (2017)

Max-Planck-Innovation GmbH
Amalienstr. 33
80799 München
www.max-planck-innovation.de