Technology Offer

METHOD FOR PRODUCING RANDOM NUMBERS ON THE BASIS OF QUANTUM NOISE

Ref.-No.: 1629-5565-WT

The invention relates to a new method for an improved production of random numbers and verification of their randomness. In order to do so, it uses the quantum mechanical properties of microscopic particles and structures. A number sequence is generated by means of a repetitive quantum mechanical random process. The measurement of this process is performed by a homodyndetection of an optical input signal, where the signal interferes with a local oscillator, e.g. a laser, at a central beam splitter so that the signal gets detectable and measurable. Due to the beam splitter one obtains two signals which can be detected e.g. by a photodiode and will be subtracted later. Finally, this leads to an output signal basically corresponding to a quadrature of phase space, built of amplitude and optical phase of the electro-magnetic field of the optical input signal.

If one now chooses a vacuum state as an optical input signal, meaning that the entrance of the beam splitter is blocked in such a way that no photon can pass, one gets a non-zero amplitude quadrature resulting from the quantum mechanical uncertainty principle. This measured “quantum noise“ is per definition random and can therefore be used for the generation of the desired number sequence.

What distinguishes the present invention from earlier applications is the review of the outcome, which is done by entropy calculations. In this way one can ensure that the resulting numbers satisfy the requirements concerning range and randomness.

Advantages

- Verified and reliable results
- Simple experimental set-up
- Miniaturisation possible
- Implementation on chip possible
- Many applications

Applications

- Cryptography
- Numerical simulations
- Monte-Carlo simulations
- Solving differential equations
- Complex functions

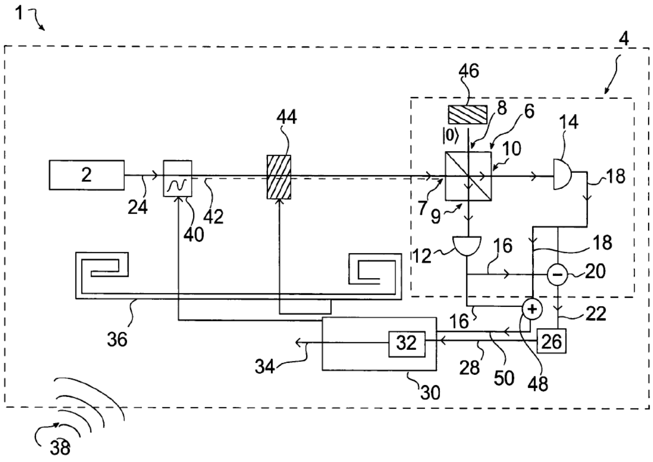

Fig. 1

Background

The production of random numbers and particularly the grade of randomness is an important issue in many sectors. In cryptography, random numbers are needed to create keys with highest safety standards. The more randomly a sign sequence of a key was chosen, the harder it will be to predict unknown parts of the key when knowing only a few fragments. In technical applications, numerical simulations often are the only method to solve certain problems such as scoring the results of differential equations. There are cases in which the quality of a simulation’s result mainly depends on the grade randomness of the used input numbers.

Unfortunately, for some techniques such as Monte-Carlo simulations having many significant applications in e.g. meteorology, nuclear medicine, risk management etc., the algorithm itself may be even more advanced and progressed than the generation of the numbers needed to run the simulation, accordingly restricting the whole technique.

The present invention aims to solve this problem by providing a reliable manner to generate numbers using the randomness of quantum mechanics.

Technology

In order to achieve a quantum noise limitation, meaning that all the statistical fluctuations in the output signal are caused by the quantum mechanical uncertainty principle, one has to clean the output signal of technical noise coming from the laser or the measurement mechanism. Due to the subtraction of the signals as outlined above, the technical noise cannot be recognized in the output signal, which can be circumvented by a suitable linear combination or rather a sum of the signals. This sum is compared to the ascertained test signal in order to be able to estimate the amount of noise. The technical noise can then be minimized by e.g. adjusting the division ratio of the beam splitter.

For the verification of the final quantum noise results, the randomness or rather the entropy of the first number sequence is enhanced by checking whether the underlying physical model is correct or rather how high the quantitative deviations are. For this purpose, e.g. the radiant power being radiated onto the laser and the measurement mechanism is estimated by an antenna apparatus and the quantum noise in the output signal is determined at random instants of time. If the radiant power exceeds a critical value, the laser and the measurement mechanism can probably not work undisturbed and do not reflect the quantum mechanical random process in a proper way. In such a case, the generation of random numbers may be paused temporarily.

The generation of a random number by means of a certain algorithm enables quantifying the noise fractions, which are not of a quantum mechanical origin and therefore potentially problematic, since the algorithm reacts to fractions whose intrinsic entropy is too small. The determination of the fraction of quantum noise at random instants of time for regulating the algorithm increases the safety in addition.

Patent Information

EP 3814886 B1 (validated in Austria, France, Germany, Italy, Great Britain, Spain and Switzerland)

PD Dr. Wolfgang Tröger
Senior Patent- & License Manager
Physicist
Phone: +49 (0)89 / 29 09 19 - 27
eMail: troeger@max-planck-innovation.de