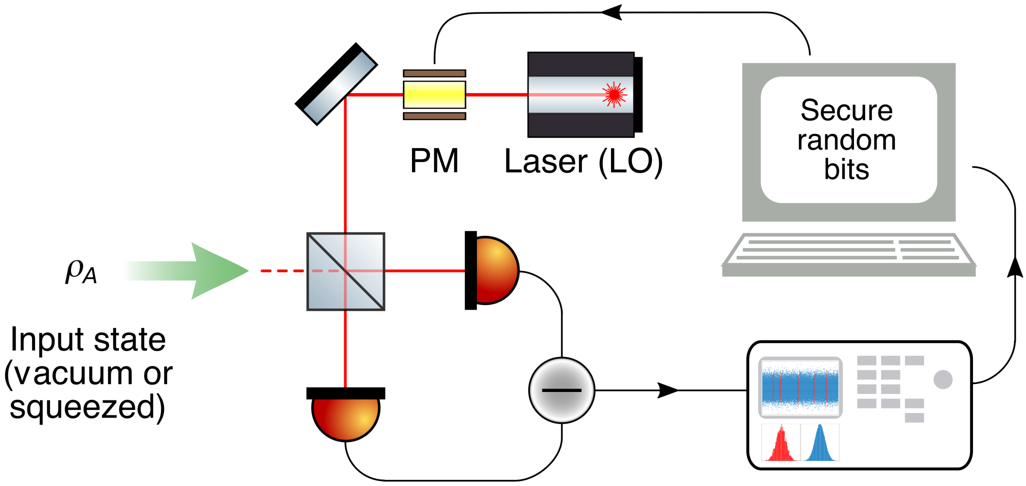
Metodo e apparato per generare numeri casuali



Description of the invention

Random numbers are used in countless applications of everyday life (cryptography, Monte Carlo methods, gambling games). The only way to produce trustworthy random numbers is by means of sampling natural random processes with devices called True Random Number Generators (TRNGs). At present time, the state of art of hardware random number generation can be grouped into two main categories: TRGNs based on Classical Physics and TRGNs based on Quantum Physics processes. The present invention belong to the latter type, exploiting the intrinsic randomness of quantum measurements. It consists of a method and an apparatus to generate random numbers by means of measurements of the quantum fluctuations of the electromagnetic vacuum in two complementary bases. With our method not only the random sequence is derived from measurements that are known to give unpredictable outputs, but the validity of the procedure is intrinsically verified by exploiting the quantum uncertainty principle. The apparatus includes: a laser, a phase modulator, a modulator controller, a balanced beam splitter, a pair of balanced photodetectors, an electronic unit which performs the subtraction of the photodetectors current signals emitting a signal proportional to the amplitude fluctuation of the quadrature selected by the phase modulator, a device which samples the signal difference and a unit which ensures the random selection.

Fields of Application

This random number generator finds applications in cryptography, gambling, statistical sampling, computer simulation, completely randomized design and other areas where producing an unpredictable result is desirable.

Advantages of the invention

The main advantage of the present invention with respect the prior art is that it lets to generate random numbers with the high rate allowed by the continuous variables framework but in a provably secure way according the Quantum Information principles. Thus, the main distinctive features are:

- Security: this method allows to quantify and eliminate the amount of information an eavesdropper, exploiting classical or quantum correlations, can have on the quantum system employed for random number generation. There is no other method which guarantees such a level of security.
- High rate: the rate random number can be generated is faster than QRNGs which exploit measurements of discrete variables or every other present method.

Commercialization Advancement Status

Proof of concept and experimental validation: Phys. Rev. Lett. 118, 060503 (2017).
The Italian patent was released on 28/03/2017.

Titolarità del brevetto: Università di Padova.

Inventori Proponenti: Dott. Marangon Davide Giacomo, dott. Vallone Giuseppe, prof. Villoresi Paolo- Dipartimento di Ingegneria dell'Informazione (DEI).

Status del brevetto: Numero brevetto italiano 0001427912 rilasciato in data 28/03/2017.
Futura domanda di estensione europea.
Disponibilità alla licenza: Italia.

Interessato a scoprire di più su questo brevetto o sui progetti innovativi sviluppati dall'Università di Padova? Contatta Unismart Padova Enterprise.

www.unismart.it/contatti