Quantum random number generation from vacuum state fluctuations

Nuno A. Silva[1], Maurício Ferreira[1,2], Nelson J. Muga[1], Ana Rita Bastos[1], and Armando N. Pinto[1,3]

Random numbers are a prime requisite in many areas of science and information technologies. Standard (classical) random number generators (RNGs) only generate numbers that are statistically random. On the other hand, the output of a quantum random number generator (QRNG) is statistically random and unpredictable. This unpredictable is essential in applications such as cryptography.

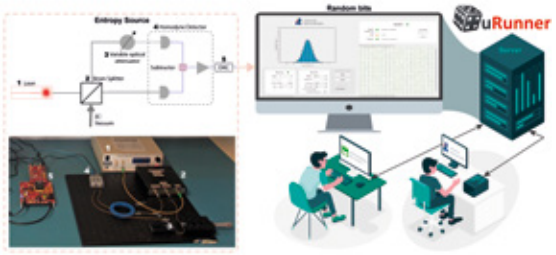
The performance of a RNG is directly dependent on the quality of its entropy source. In that sense, quantum technologies offer an ideal solution to implement those devices as they exploit the inherent randomness of quantum mechanics, leading to high values of entropy. Consequently, we can explore such high-value entropy sources to implement QRNGs operating at very high bit rates. Vacuum fluctuations are an example of a quantum physical process that can be explored as an entropy source for the generation of information-theoretical randomness. Additionally, it is possible to establish a minimum value for the quantum entropy source that is not susceptible to a decrease. This is in clear opposition to the standard (classical) random number generators, where the entropy source used cannot be theoretically provable, and its value is potentially manipulated by an attacker.

The QuRUNNER (http://qurunner.av.it.pt/) and the QuantumPrime (http://quantumprime.av.it.pt) projects, running at Instituto de Telecomunicações – Aveiro, are exploiting quantum photonic effects as a source of entropy to implement a QRNG. Those projects aims to provide a practical and reliable solution to distribute random numbers and prime random numbers to the scientific community. Our implementation provides, in real-time, strings of random numbers at high bit rates (150 Mb/s), with the quality of the random numbers being complemented by performing on-demand statistical tests.

Description of figures

A hardware-based random number generator, such as the one depicted in Fig. 1, can be divided into two main blocks: (1) the entropy source; and (2) the post-processing block. The entropy source imposes limits to the performance of the random number generator since it is associated with the uncertainty of the source. In particular, we are focusing on the quadrature fluctuations of optical quantum vacuum states, which can be measured using a laser and a homodyne detector, see Fig. 1. Note that each measurement performed in the quantum state returns a random value. The post-processing block is used for randomness extraction and eliminates the contributions of the different classical noise sources, as the hardware is intrinsically imperfect.

In 2020, the research team performed a first demonstration of the random number generator at Aveiro Techdays event, see Fig.2. To the best of our knowledge, this was the first demonstration in Portugal of a true random number generator exploiting the intrinsic probabilistic nature of the quantum physics.



1 – Institute of Telecommunications, University of Aveiro
2 – Department of Physics & Institute of Telecommunications, University of Aveiro
3 – Department of Electronics, Telecommunications and Informatics & Institute of Telecommunications, University of Aveiro

FIGURE 1
Schematics of the random number generator demonstrator.

FIGURE 2
Photograph of the demonstration of a random number generator at Aveiro Techdays.