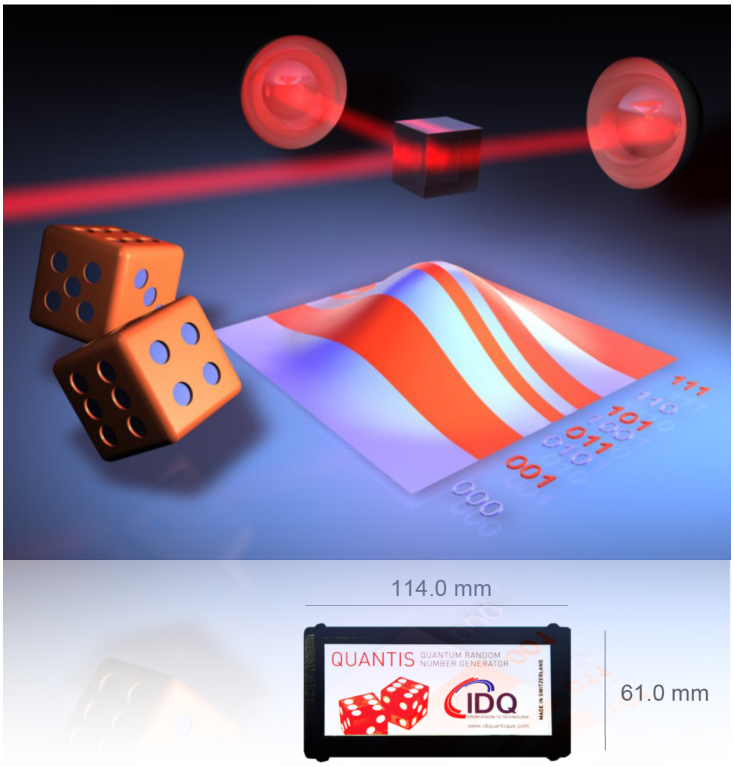
Proposta di Tesi di Laurea Triennale o Magistrale

Quantum Random Number Generator



Quantis-USB-4M

Supervisor:
Prof. Filippo Caruso
filippo.caruso@unifi.it
www.qdab.org

Physical random number generators based on a chaotic process
Macroscopic processes described by classical physics can be used to generate random numbers. Typical chaotic processes include the monitoring of some electric noise current in a resistor or in a diode. This current is not random, but just very complex to describe. Determinism is hidden behind complexity. Although their random numbers are likely to pass randomness tests, these generators are difficult to model. This implies that it is impossible to verify if they are operating properly while acquiring numbers. In addition, it is difficult to ensure that the system is not interacting with environment parameters like temperature or an electromagnetic field.

Physical random number generators based on a quantum process
Quantum physics is the only theory within the fabric of modern physics that integrates randomness.This fact was very disturbing to physicists like Einstein who invented quantum physics. However, its intrinsic randomness has been confirmed over and over again by theoretical and experimental research. Truly random numbers can be generated by monitoring radioactive decay of heavy elements. Although they produce numbers of excellent quality, such generators are not suitable for commercial applications.
A Quantum Random Number Generator (QRNG) is the first commercial physical random number generator based on quantum physics (id Quantique, 2001). The randomness is guaranteed by the random behaviour of single ‘light particles’ - called photons - hitting a semi-transparent mirror. The process by which photons incident on such a component is either reflected or transmitted is intrinsically random and cannot be influenced by external parameters. The quantum process used to generate the random bits, its immunity to external factors, plus the fact that this device performs live verifications of its internal functions, guarantees a high level of trust in the random numbers that are generated.
By really using this device in your hands, the candidate will first model this process, then analyse correlation properties of the produced data, and will also perform the list of tests (as NIST and DIEHARD tests) evaluating the randomness of the bit stream generated by QRNG, hence demonstrating that QRNG is the only device successfully passing all randomness tests. A possible application to the numerical simulation of a quantum dynamics will be also taken into account by investigate the role of true randomness on it.