Contribution ID: **5** Type: **not specified**

Quantum Random Number Generators

Thursday 23 January 2025 14:00 (45 minutes)

Unpredictability is usually perceived with a sense of discomfort. However, when it comes to protecting our digital life, it is essential since all the procedures for authentication, privacy preservation and encryption relies on keys, generated starting by random numbers. Whether algorithmic generation can be practical, it is irreducibly limited to pseudo-randomness by the very same deterministic nature of any software coded algorithm. "True"randomness can be a solution, as long as it is based on the observation of unpredictable natural phenomena. Random Power (RaP!) is a project turned into a start-up company where virtually endless streams of random bits can be generated by the analysis of the time series of self-amplified pulses seeded by quantum tunneling in dedicated silicon structures. By now, RaP! developed three embodiments of this patent protected principle, including an ASIC integrating advanced functionalities.

During the talk, needs, principle, state of development and issues related to starting up a company will be presented and discussed.

Presenter: CACCIA, Massimo (Universita & INFN, Milano-Bicocca (IT))