Random Power: a platform of True Random Bit Generators based on quantum tunnelling

Massimo Caccia[1,2]

On behalf of the ATTRACT Consortium

1. *University of Insubria, Department of Science and High Technology, via Valleggioi 11, 22100 Como, Italy*
2. *Random Power, Via Macedonio Melloni 40, 20129, Milano - Italy*

Abstract: Random Power, a project supported by the European Commission and turned into a start-up company, designed a platform of high native entropy Random Bit Generators based on Quantum Tunnel in a Silicon Chip.

The use of massive amounts of random numbers is a critical issue in security-related techniques and tools for protecting and sharing data in open, distributed environments as well as their deployment in large statistical and numericalsimulations. The need for high-quality random numbers has driven the search for new, more reliable, and robust approaches for their generation. Current solutions are divided into two main categories: True Random Number Generators (TRNGs) and algorithm based Pseudo Random Number Generators (PRNGs). TRNGs are driven by observables connected to stochastic, chaotic, or quantum natural phenomena. The latter, where unpredictability is rooted in the laws of nature, guarantees the highest level of security and can be considered the root of every high level cryptographic process.
Random Power (RaP!), an international consortium supported by the European Commission, developped a platform of Quantum Random Bit Generators (QRBGs) based on self-amplified stochastic "dark" pulses seeded by quantum tunneling in arrays of customised Single Photon Avalanche Diodes (SPAD) integrated in a CMOS chip designed and produced in 180nm technology. CMOS compliancy is deemed to be essential to offer the possibility to integrate in a single die advanced functionalities required to make the generator compliant to the certification specifications by the U.S. National Institute of Standard and Technology. The major features embedded in the RaP! chip are shown in Fig. 1.

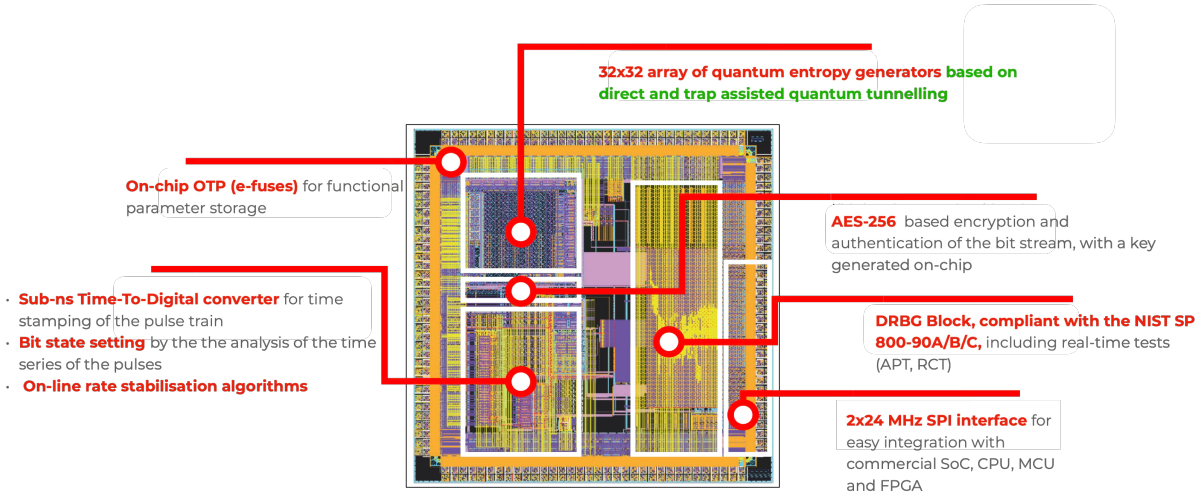

Fig. 1 Functional Blocks of the QRBG designed by the ATTRACT consortium

The main specifications of the RaP! chip will be presented, with a focus on the challenges faced during the design. Main results from the characterisation, including the measurement of the native entropy, will also be presented.