ATTRACT

Random Power

In-silico quantum generation of random bit streams

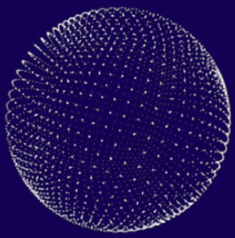
PUBLIC SUMMARY

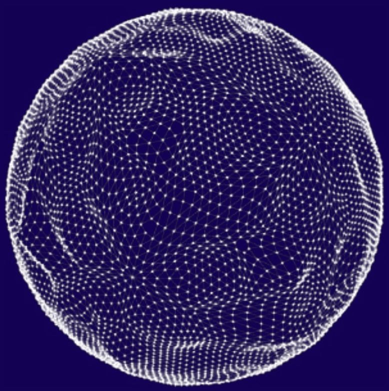
Unpredictability is usually perceived with a sense of uneasiness and discomfort. However, when it comes to secure our data, information, posts, pictures and whatever flows to (or from) the internet about us, protection relies on unpredictability. The impossibility for an eavesdropper or a hacker to break the walls protecting our digital life depends on secret keys, protocols and cyphering algorithms, namely the art & science of cryptography. Keys, essential to lock&unlock the doors, must be randomly generated. And true randomness implies unpredictability.

Random Power harnesses the quantum properties of semiconductors to generate a virtually endless stream of random bits feeding cyber-security systems. The principle is embodied in a Silicon device and benefits from micro-electronics advances; the source of randomness is endogenous and this is a genuine paradigm shift with respect to existing devices, providing simplification and robustness of the system; quantum properties of matter make unpredictability irreducibly unbreakable.

During the ATTRACT phase I project the consortium, comprising two research institutions and two companies, designed, produced, commissioned and fully qualified a small form factor board integrating a single bit generator. In a device about half the size of a credit card, bits were shown to flow to a host computer and assessed according to the test suites by the U.S. Nation Institute of Standard and Technology, proving the validity of the principle and the possibility to embed it off the labs, in an operational environment, and at low cost.

Now, the consortium includes RaP! a company spun-off by the original partners, and it has been enlarged to integrate teams with complementary knowledge and expertise from other ATTRACT projects and beyond, with the goal of developing a platform of True Random Bit Generators. Infrastructural applications will be targeted offering a Randomness Farm; IoT, mobile and automotive markets will be within reach integrating all the functionalities in a dedicated silicon chip. Technology will be complemented by high level services for exploiting the value of quantum secured unpredictability in a Root of Trust and numerical simulations.





Legal Disclaimer

The European Commission's support does not constitute an endorsement of the contents, which only reflect the views of the author. The Commission is not responsible for any use of the information contained therein.

This project has received funding from the European Union's Horizon 2020 research and innovative programme under grant agreement No. 101004462