IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Advances in Space-based Communication Systems and Services, Part 1 (2)

Author: Mr. Norbert M.K. Lemke
OHB System AG - Oberpfaffenhofen, Germany

Dr. Rainer Rathje
OHB System AG-Bremen, Germany
Dr. Christoph Pacher
Austrian Institute of Technology GmbH (AIT), Austria
Dr. Christoph Marquardt
Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany

SPACEBORNE QUANTUM RANDOM NUMBER GENERATORS (QRNG) – DEVELOPMENTS TOWARDS A PRODUCT

Abstract

Random numbers play an increasing role in many applications in science, technology, and communication, especially for data encryption. For standard applications Deterministic Random Number Generators (DRNG) generate random numbers, e.g. from the computation of cryptographic functions on the basis of a true random number as seed. These can be generated at high rates, but each output is deterministically generated from a previous output. In contrast, True Random Number Generators (TRNGs) rely on unpredictable physical effects, i.e. with no correlation to past events. In particular, quantum key distribution (QKD) for tap-proof communications require the combination with TRNG at high output rate. To overcome long distances with QKD, it is indispensable to use a satellite relay in Earth orbit in the medium term according to the state of the art.

The European Commission ordered several studies to prepare for a European Quantum Communication Infrastructure (EuroQCI). It tasked ESA to provide a solution for the space component of this infrastructure with the Secure And cryptoGrAphic (SAGA) project studies. One contributing mission to this project is Eagle-1 that aims to fly a demonstrator mission for QKD. In order to ensure the highest possible security of the cryptographic key exchange, a high-quality TRNG needs to be part of its payload. For TRNGs it is essential to model the underlying internal dynamical processes and to prove that the random numbers have the desired property of a nearly perfect entropy source and that the random sequence cannot be manipulated by an attacker in a way that would give him (partial) knowledge of the generated number sequence. Due to the difficulty of this modelling, classical TRNGs use sources that have a low output rate. QKD, however, requires an extremely high rate of randomness.

This is where QRNGs come into play: QRNGs exploit the pure randomness of the quantum measurement process, which is generally accepted in quantum mechanics, to generate true randomness. When implemented correctly, these measurements can be performed at very high rates. If one succeeds in producing a device that eliminates all (high-order) correlations due to macroscopic operating parameters in its measurement result and prevents state manipulation of the measured quantum mechanical states, one obtains a TRNG that quantifiably generates private independent uniformly distributed randomness at a high data rate.

The paper describes the development steps toward a QRNG product for space applications with definition, modelling, environmental testing and the certification approach. This QRNG will be EU-27 based and is an ideal candidate for future EC funded missions like the upcoming connectivity satellite constellation.