Paper ID: 63980
oral

IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Space Communications and Navigation Global Technical Session (8-GTS.3)

Author: Mr. Balazs Solymos
Budapest University of Technology and Economics, Hungary

Dr. Laszlo Bacsardi
Budapest University of Technology and Economics, Hungary

STATISTICAL TESTING TOOLS FOR QUANTUM RANDOM NUMBER GENERATORS ONBOARD CUBESATS.

Abstract

There are need for good random numbers in several space communication and navigation applications and random numbers need to be generated onboard a satellite as well. Quantum random number generators already present a provably secure entropy source for cryptographic applications with many existing physical realizations. Advances in quantum optics are also making these devices ever more accessible. Many possible realizations of these share the required underlying technology with other quantum communication use cases and experiments, which is advantageous since it makes experimental data for the various building blocks of a given generator architecture more available. This and the easy applicability of the output (entropy for cryptography) of these devices makes them a good candidate for quantum communication satellite missions as they often can be investigated alongside other applications utilizing similar hardware (e.g. quantum key distribution experiments), a particularly fortunate possibility for CubeSat missions where efficiently utilizing available payload is especially important.

Due to the inherent nature of randomness, verifying an entropy source as truly random cannot be done with absolute certainty. In practice, however, statistical tools exist to still test for types of unwanted regularity and predictability in a sequence and are routinely used for verifying proper functioning of generators. These, often batteries of multiple tests, are computationally expensive to run, which can make their applicability in space applications limited, since computational capacity on satellites is still expensive.

To explore the question and possibility of using statistical tools with quantum random number generators in a space environments, we used our already existing processing system made for a traditional optical quantum random number generator, for the examination and evaluation of the most widely used statistical tools. Our main goal was to find out the exact cost and applicability of these, especially in cases where the tried and tested way of running curated test suites is no longer an option due to limited resources.