HERVA

A FPGA-Based Post-Processing and Validation Platform for Random Number Generators

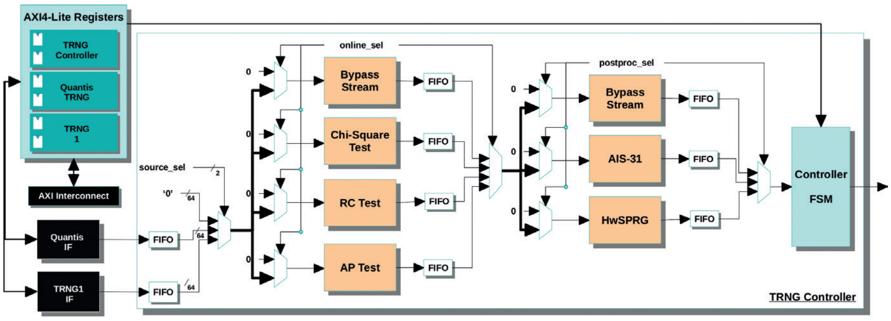
Florent Glück, Laurent Gantel, Fabien Vannel,
Andres Upegui, Alexandre Duc, Lucie Steiner

Brief description

HERVA is a FPGA-based hardware platform to validate and post-process multiple true random number generators sources. We devised a hardware implementation of a provably secure post-processing algorithm which improves random number quality while maintaining high data throughput. A platform providing hardware acceleration was implemented to validate the generated numbers through statistical tests and to improve randomness. The platform is modular and targets both IoT devices and back-end servers.

Key points

- The FPGA-based hardware platform can validate an entropy source (generated numbers) through x^2 and SP800-90B online statistical tests.
- The platform is able to improve the entropy source's randomness by using AIS-31 or SPRG post-processing hardware cores.
- Any entropy source can be added to the post-processing and validation platform.
- The platform is modular and can be adapted to both IoT edge devices and back-end servers.



Block diagram of the TRNG Validation Platform.

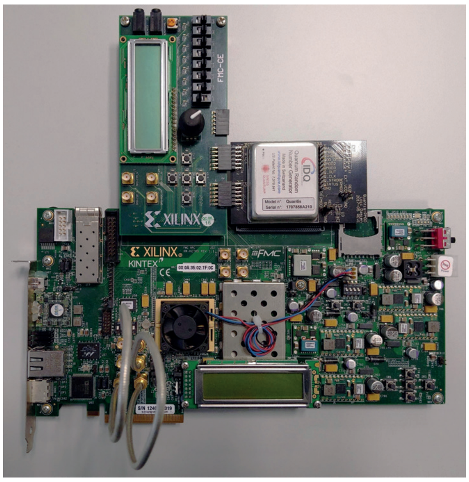


Photo of the hardware platform with an IDQ Quantis source.

HERVA is a fully functional and configurable, FPGA-based, validation platform for true random number generators. This hardware platform offers both online tests to validate random numbers on-the-fly, and post-processing cores to enhance the entropy of the final output.

Moreover, a novel hardware implementation of SPRG, an efficient and proven safe post-processing algorithm is implemented. This hardware module has the benefit of improving the output randomness while providing high throughput. The use of a seed ensures higher security for the generated numbers and the throughput of the module allows to regularly renew this seed to keep high quality numbers.

We tested our platform using the Dieharder software suite which offers a wide range of statistical tests. We showed that after performing the SPRG post-processing on the IDQ Quantis source, the generated bits successfully pass most Dieharder statistical tests.

The proposed platform allows users to continuously test the entropy source's generated bits and remove the bias to improve their quality. In addition, the modularity of the architecture eases the process of tailoring the hardware to system constraints and desired entropy. Consequently, it allows designers to find the best trade-off between available resources and random numbers quality.