L2 CMI : generation of pseudo-random numbers on micro-devices

Supervisor : J.-F. Couchot
FEMTO-ST Institute, UMR 6174 CNRS,
Département d'Informatique des Systèmes Complexes (DISC),
Université de Franche-Comté, Belfort, France.
couchot@femto-st.fr

A pseudo-random number generator is an algorithm that can produce a sequence of numbers whose properties are close to those of randomly generated numbers (e. g. rolling a dice). For example, the numbers must be independent of each other, their observation must not make it possible to guess what the composition of a later sequence will be. PRNGs are used in many applications such as numerical simulation, cryptography, etc.

The DISC/AND department of the FEMTO-ST laboratory has extensive experience in PRNG research [CCBH19, BGCO18] The objective of this project is to study PRNG implementations on micro-devices:

- the first task will be to study some PRNG, like the Mersenne Twister's one, which the gold standard[MN98] for instance in Python language,
- it will next be a matter of evaluating the existing implementations embedded in the micropython library. The statistical quality of the generated numbers will evaluated by using existing statistical tests such as TestU01 [LS07], NIST test suite [BIRS+10].
- It will continue by deploying generators that usually run on conventional CPUs on these supports. Micro-devices will be provided to students.

References

[BGCO18] Mohammed Bakiri, Christophe Guyeux, Jean-François Couchot, and Abdelkrim Kamel Oudjida. Survey on hardware implementation of random number generators on FPGA: theory and experimental analyses. *Comput. Sci. Rev.*, 27:135–153, 2018.

[BIRS+10] Lawrence E Bassham III, Andrew L Rukhin, Juan Soto, James R Nechvatal, Miles E Smid, Elaine B Barker, Stefan D Leigh, Mark Levenson, Mark Vangel, David L Banks, et al. Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications, 2010.

[CCBH19] Sylvain Contassot-Vivier, Jean-François Couchot, Mohammed Bakiri, and Pierre-Cyrille Héam. Fast and robust prngs based on jumps in n-cubes for simulation, but not exclusively for that. In *17th International Conference on High Performance Computing & Simulation, HPCS 2019, Dublin, Ireland, July 15-19, 2019*, pages 650–657. IEEE, 2019.

[LS07] Pierre L'ecuyer and Richard Simard. Testu01: Ac library for empirical testing of random number generators. *ACM Transactions on Mathematical Software (TOMS)*, 33(4):1–40, 2007.

[MN98] Makoto Matsumoto and Takuji Nishimura. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, 8(1):3–30, 1998.