Proposal for a post-doctoral contract in digital electronics and embedded systems for security

from September 2020
Laboratoire Hubert Curien Saint-Etienne, France

Title

Design, characterization and modelling of a random number generator based on oscillating structures.

Information

Project manager:
Viktor Fischer
fischer@univ-st-etienne.fr
04 77 91 57 92

Contract length:
First one-year contract ideally from September 2020 (possibility of shifting slightly). Possible extension of the contract up to 30 months.

Place:
Hubert Curien Laboratory, CNRS,
18 rue B. Lauras, 42000 SAINT ETIENNE
France
SESAM Team

Funding:
PSPC-regions program funded by the Auvergne Rhône Alpes region

Specific conditions:
Permission to access the premises depends on a preliminary security investigation.

Context:

Project outline:
The PSPC-regions project "SECURE-RISC-V" includes 3 partners: two small French companies Tiempo and GreenWaves-Technologies, and the Hubert Curien laboratory in Saint-Etienne.
The objective of the project is to secure microcontrollers targeting IoT applications and based on a RISC-V architecture with an adapted hardware security element.
GreenWaves-Technologies provides a high-performance, low-power multi-core architecture that is secured by the TIEMPO's secure element certifiable CC EAL5+ IP (intellectual property). The Hubert Curien laboratory provides support for the design and stochastic modelling of the random number generator based on asynchronous rings - STR (for Self-timed rings), for the design and verification of stochastic tests dedicated to the generator, as well as for the verification of the generator's security and the efficiency of its dedicated tests.
**Research team:**
SESAM (Systèmes Embarqués Sécurisés et Architectures Matérielles = secured embedded system and hardware architectures) is a research team from Hubert Curien Laboratory (UMR CNRS 5516) in St-Etienne, France.

SESAM is one of the French leaders in the field of physical security. It is internationally recognized for its work on random numbers generation in integrated circuits (ASICs and FPGAs). It collaborates with many companies and university laboratories.

The SESAM team has been involved for more than 3 years in the HECTOR European project. The objective of this project was to develop cryptographic primitives, including random number generators (TRNG) and their integration into complete cryptographic systems. Several generators were realized in reconfigurable circuits (FPGAs) and application-specific circuits (ASICs) and tested in evaluation boards specially designed for this type of testing.

The role of the SESAM team in this new project is to extend the results of its work on the random number generators certifiable according to the AIS 20/31 standard to the new technology used by the TIEMPO Company, as well as to verify the portability of the new secure generator to different technologies.

The use of the HECTOR project evaluation boards will facilitate the evaluation of the new generator and its comparison with other generators designed for the HECTOR project.

**Missions:**

- Study and modelling of asynchronous rings (STR) as a source of randomness in digital circuits.
- Implementation of random number generators (TRNG) based on these asynchronous rings in FPGA and ASIC circuits.
- Analysis of the statistical properties of the generated numbers.
- Stochastic modelling of the proposed generators.
- Proposal of embedded tests dedicated to the generators, based on their stochastic models.

**Desired profile:**

- Ph.D. degree required

**Required skills:**

- Good knowledge of digital electronics and embedded systems.
- Knowledge of CAD tools and FPGA design (Intel, Xilinx or Microsemi) as well as simulation tools (Modelsim).
- ASIC design using Cadence tools (design, simulation, verification)
- Good level of English

**Desired skills:**

- Data acquisition chain and data analysis (use of tcl and python languages in particular).
- Knowledge in signal processing, mathematical modelling, statistics.
- Basic knowledge in information security.

**To apply:**

Send Cover letter and CV by e-mail to fischer@univ-st-etienne.fr