Evariste III: A new multi-FPGA system for fair benchmarking of hardware dependent cryptographic primitives

Nathalie Bochard, Cédric Marchand, Oto Petura, Lilian Bossuet, Viktor Fischer

To cite this version:

HAL Id: ujm-01219840
https://hal-ujm.archives-ouvertes.fr/ujm-01219840
Submitted on 26 Oct 2015
**Evariste III**: A new multi-FPGA system for fair benchmarking of hardware dependent cryptographic primitives

Nathalie Bochard, Cédric Marchand, Oto Petura, Lilian Bossuet, Viktor Fischer
Laboratoire Hubert Curien, UMR 5516 CNRS - Université Jean Monnet, Saint-Etienne, France

### What’s new?
- 3 new FPGA modules, one with an embedded ARM processor
- New motherboard
  - ZIF connectors
  - JTAG chain I/O
- Serial connection of up to 6 modules via JTAG
- Box with 6 motherboards interconnected and chained
- 30 modules of each new FPGA family for PUF evaluation available
- SMA connectors in all modules for side channel analysis added

### Inherited from Evariste II
- Both scripting and fast acquisition data programs
- Open source system
- Remotely available via Internet
- Fast USB interface

### TRNGs
**System dedicated to True Random Number Generators**

First historical application, fair TRNG comparison thanks to:
- Unified hardware platform for different FPGA and ASIC technologies
- Linear power supply
- High quality low pass filters

![TRNG Diagram](image)

**Extended security approach**

- Randomness source
- Digital noise source
- Digitalized
- Alg. & Crypto post-processing
- Embedded tests
- Monitoring of the source of randomness
- Alarm 1
- Alarm 2

**TRNG output**

- Raw binary signal output

**Monitoring of the source of randomness**

1. FISCHER V., HADDAD P., BERNARD F. (2013) : 
An open-source multi-FPGA modular system for fair benchmarking of true random number generators», 23rd international conference on field programmable logic and applications (FPL2013), pp. FS3_8, Porto, Portugal

### 3 new modules:
1. Xilinx Spartan 6
2. Altera Cyclone V
3. Microsemi SmartFusion2 with ARM Cortex-M3

### Compatible with old modules:
1. Xilinx Spartan 3
2. Xilinx Virtex V
3. Altera Cyclone III (3 versions)
4. Altera Aria II
5. Microsemi Fusion (2 versions)
6. ASIC controlled with Fusion FPGA

### PUFs
**System dedicated to Physical Unclonable Functions**

- Evaluation of up to 6 modules in parallel with 6 motherboards placed in a box
- JTAG chain for reconfiguration in situ
- Zero insertion force connectors to facilitate exchange of modules

![PUF Diagram](image)

**Sources of funding:** European Union’s Horizon 2020 research and innovation program: HECTOR - Hardware Enabled Crypto and Randomness - grant agreement No 644052.

ANR 2013 call: SAIWARE - Salutary hardware design to fight against integrated circuit counterfeiting and theft - ANR-13-JS03-0003.

NATO SFP (Science for Peace) 2013: SFP13-084520 “Secure implementation of post-quantum cryptography”.