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
- Motherboard with ZIF (zero insertion force) connectors
- 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[1]

- Both scripting and fast acquisition data programs
- Open source system
- Remotely available via Internet
- Fast USB interface

Laboratoire Hubert Curien
evariste.univ-st-etienne.fr
Log in
LABORATOIRE Hubert CURIEN UMR • CNRS • 5516 • ST-ETIENNE
TRNG Benchmarking
Home page | Aims of the portal | Access to cards | Contact

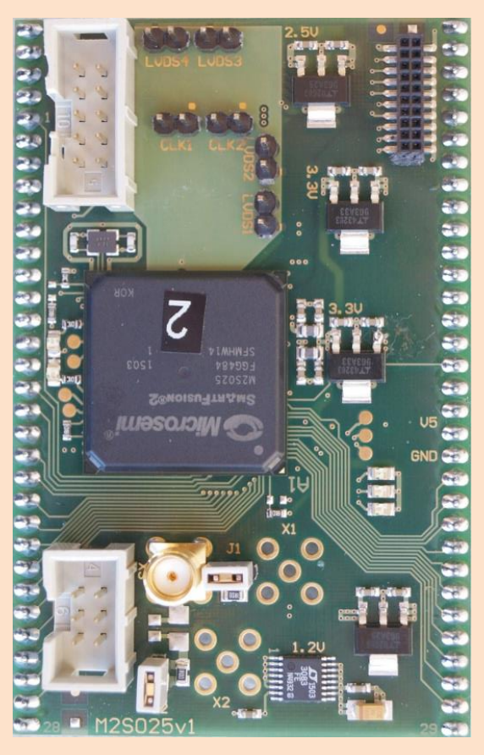
Presentation of the research group SES TRNG test

In the framework of its research, the group SES (Secured Embedded System) c
implements True Random Number Generators (TRNGs) dedicated for cryptogra
of basic cryptographic primitives. The issue of random number generation is c
systems. Random numbers are often used in key generation processes, auth
padding, in many digital signature and encryption schemes, and even in sor
applications, security depends to a great extent on the quality of the sourc
exploited. Besides quality and unpredictability requirements, the generato

3 new modules:

I.

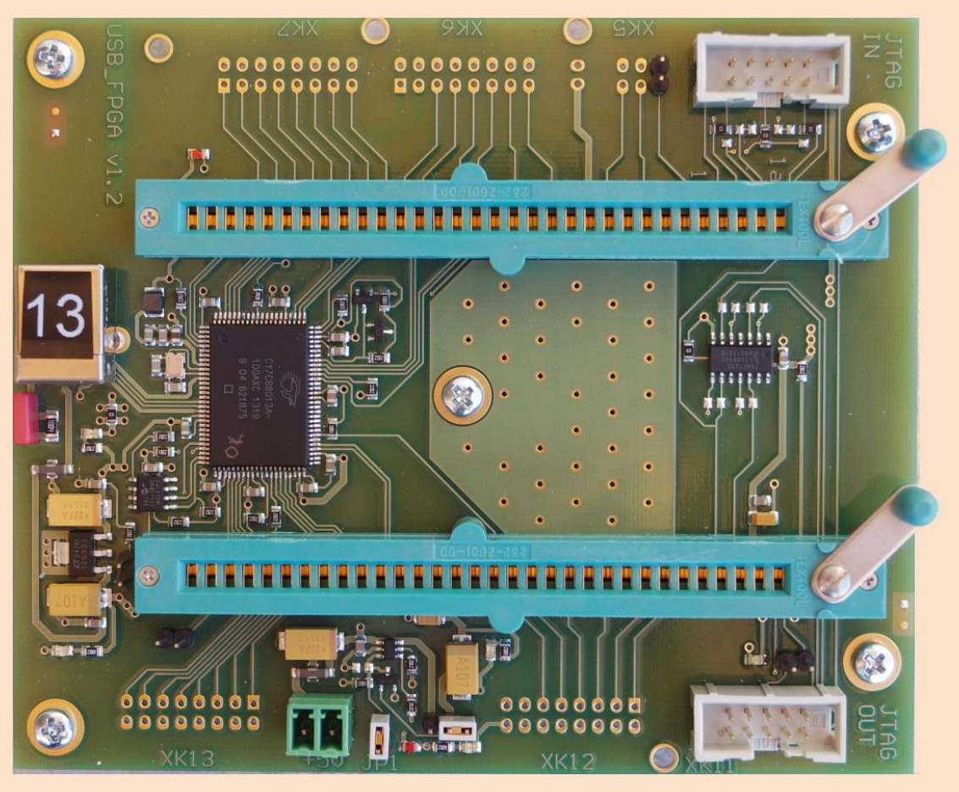
II.



III.

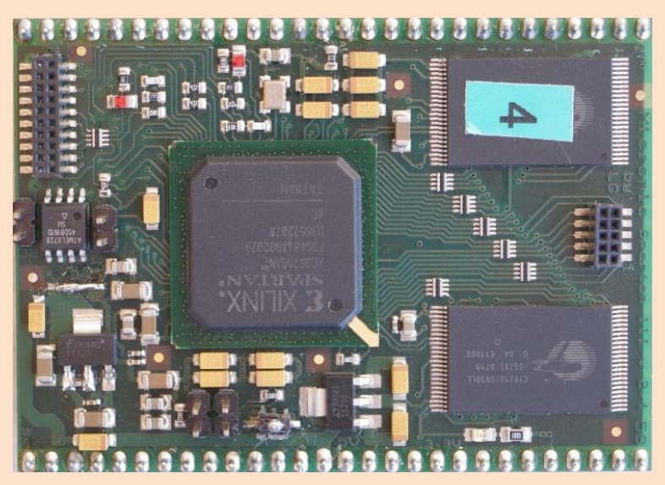
I. Xillinx Spartan 6
II. Altera Cyclone V
III. Microsemi SmartFusion2 with ARM Cortex-M3

- New motherboard
  - ZIF connectors
  - JTAG chain I/O



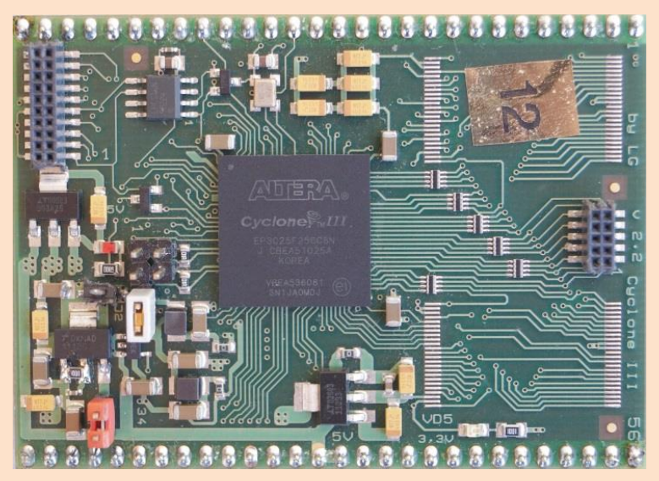
Compatible with old modules:

1. Xillinx 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



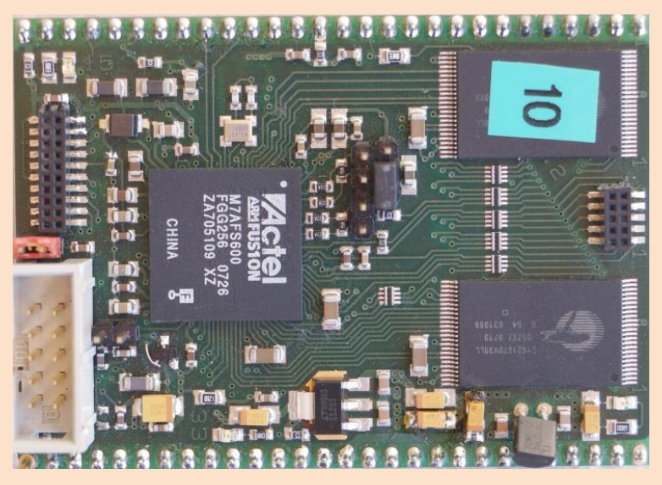
1.

2.

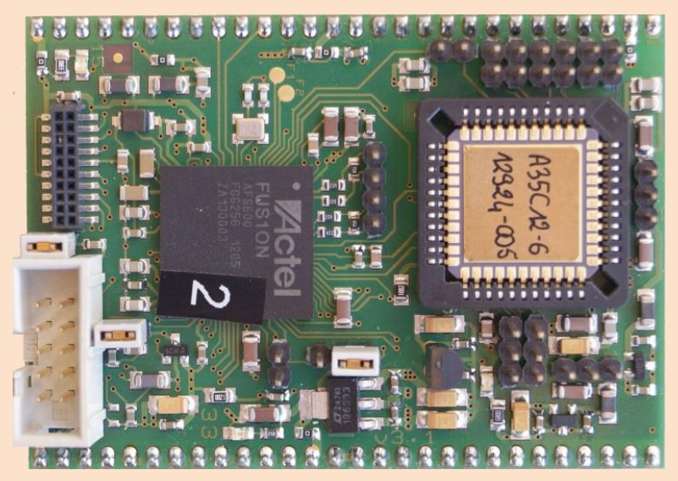


3.

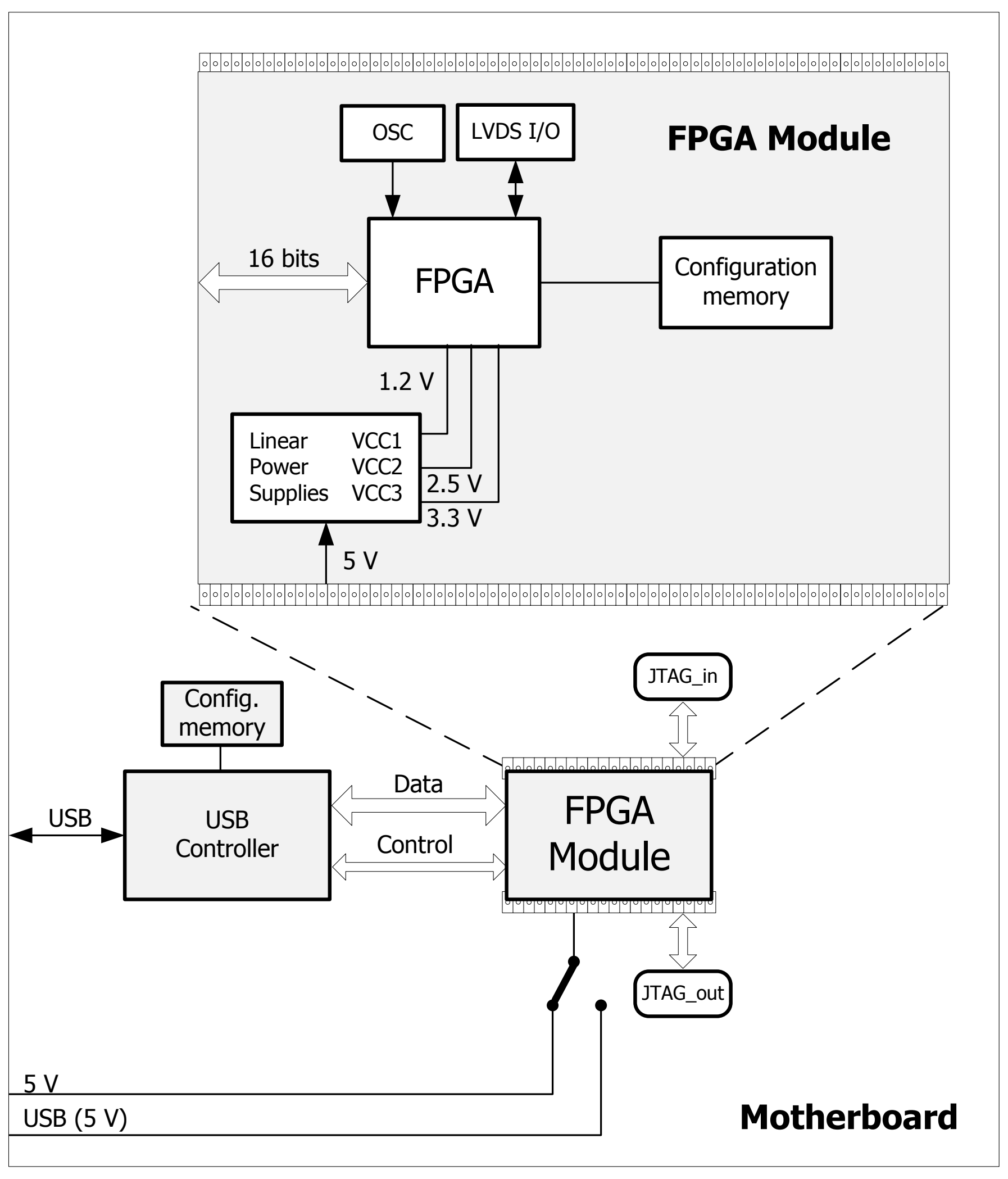
4.



5.

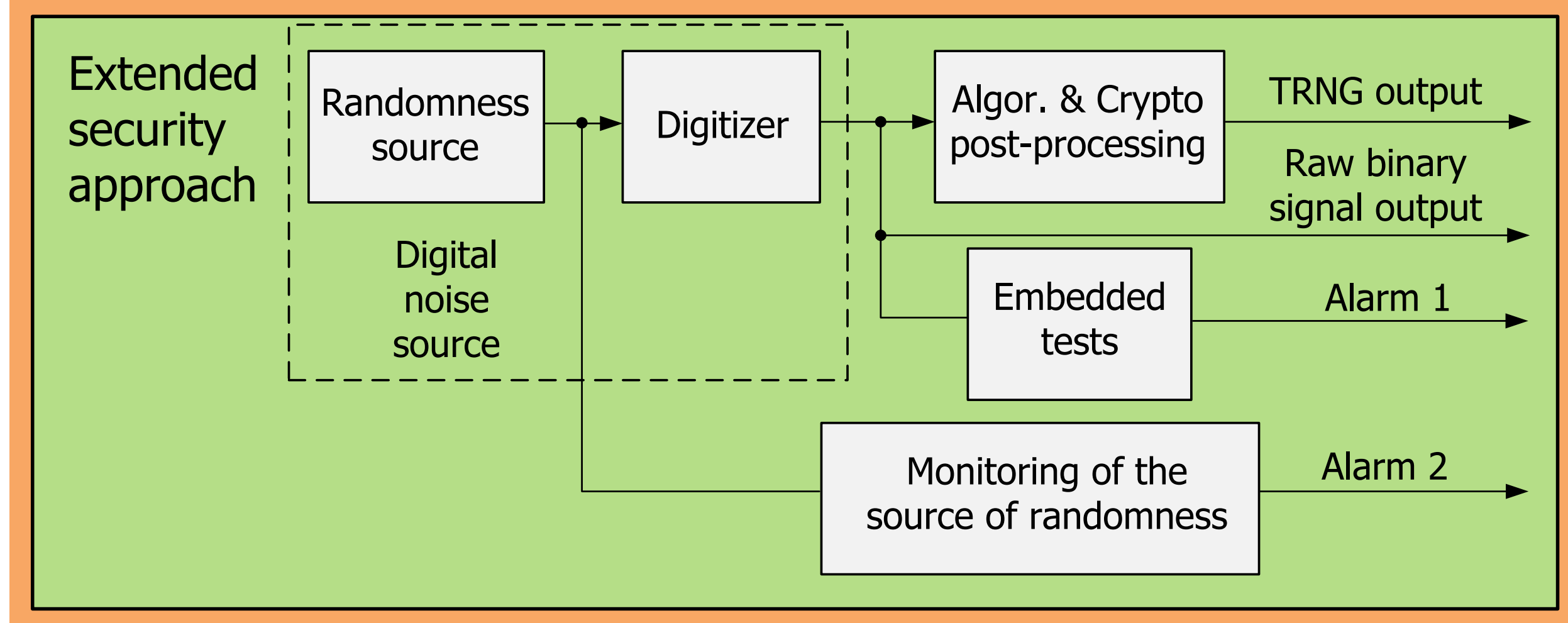


6.



TRNGs

System dedicated to True Random Number Generators

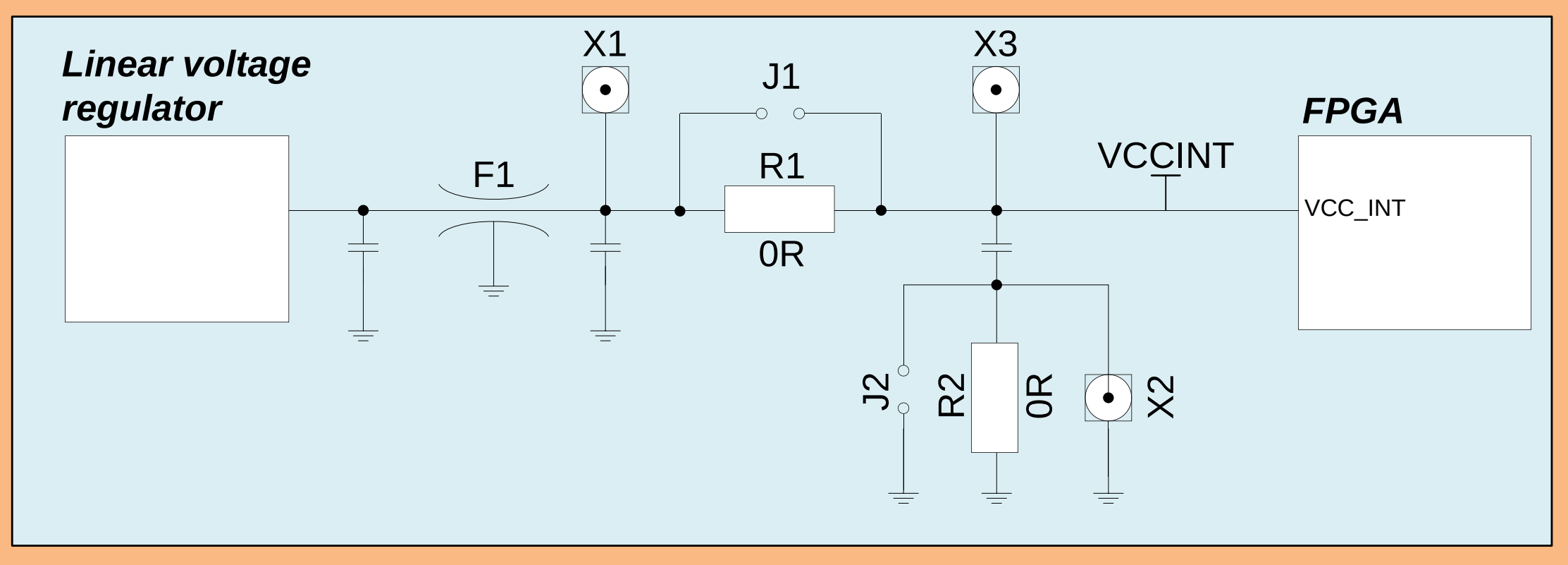


First historical application, fair TRNG comparison thanks to:

- Unified hardware platform for different FPGA and ASIC technologies
- Linear power supply
- High quality low pass filters

SCAs

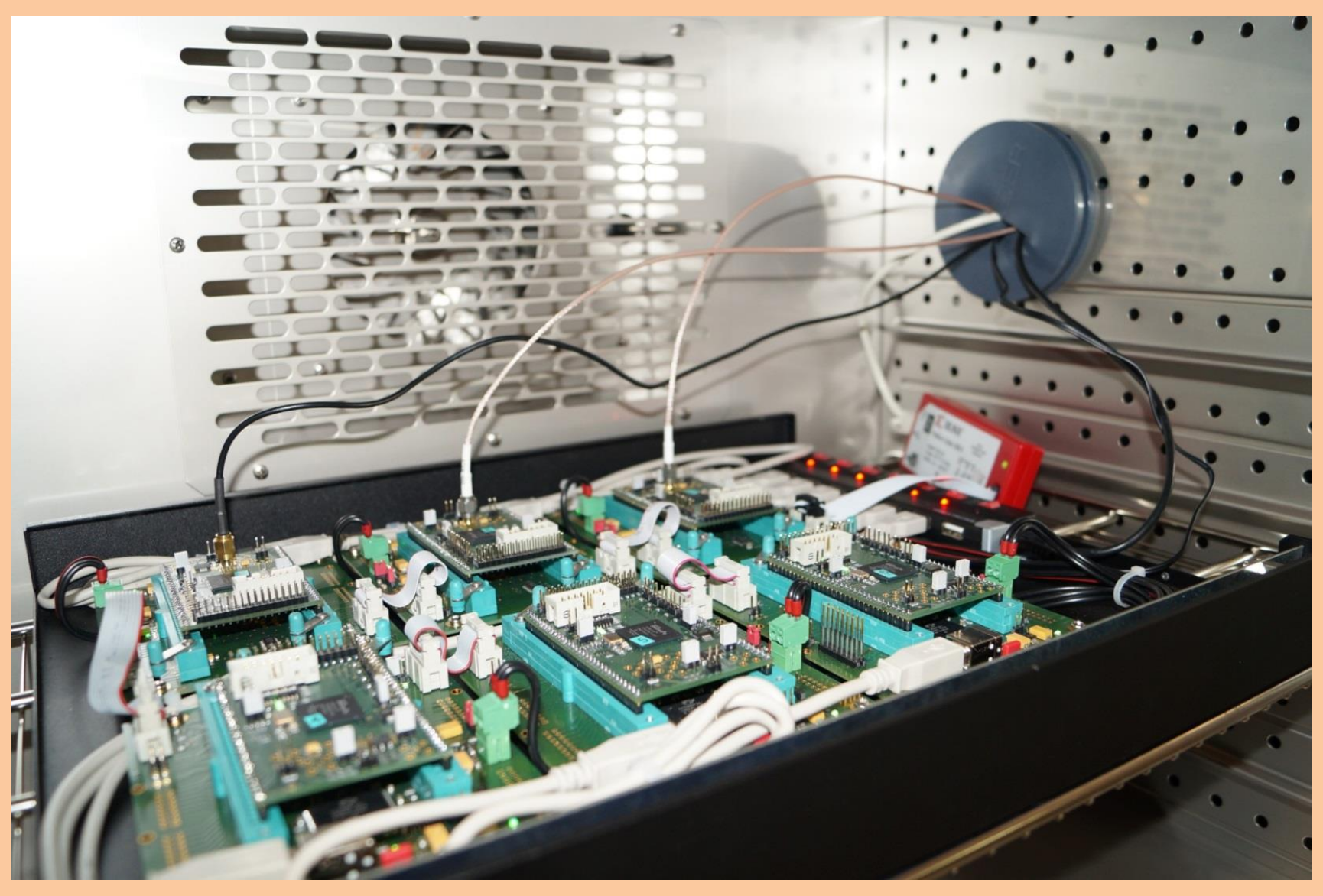
System dedicated to Side Channel Analyses



- Access to power supply lines in different places of the design
- SMA connectors for easier access and performance
- Embedded ARM processor in new modules to study software primitives

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

[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. PS3_8, Porto, Portugal

http://labh-curien.univ-st-etienne.fr/wiki-evariste-ii/

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: SALWARE - Salutary hardware design to fight against integrated circuit counterfeiting and theft - ANR-13-JS03-0003.
NATO SfP (Science for Peace) 2013: SFPP 984520 "Secure implementation of post-quantum cryptography".