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

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

Cryptographic primitives such as True Random Number Generator (TRNG), Physical Unclonable Function (PUF) but also cryptographic algorithms need to be tested and evaluated in different technologies, but with identical system architecture and operating conditions in order to be fairly compared. The random data generated by a TRNG or responses of a PUF are strongly linked to the underlying technology, but also to the environment conditions (EMI, temperature, power supply voltage…). Similarly, success of the side channel attacks on cryptographic algorithms depends strongly on technology, system architecture and operating conditions.

Most of FPGA families have their own evaluation boards developed by their constructors and they are not adapted to fair benchmarking and side channel analysis (SCA). Indeed, all these boards are built in a completely different ways and have different architectures, communication protocols and peripherals. Consequently, fair comparison of TRNGs, PUFs or side channel attacks using standard evaluation boards is clearly impossible.

The proposed multi-FPGA modular system Evariste III that is derived from the older Evariste II modular system [1], which was aimed at testing TRNGs, is now extended to be suitable for testing all hardware dependent cryptographic primitives: TRNGs, PUFs, but also for performing side channel attacks on cryptographic algorithms in different FPGA technologies with a unified hardware platform.

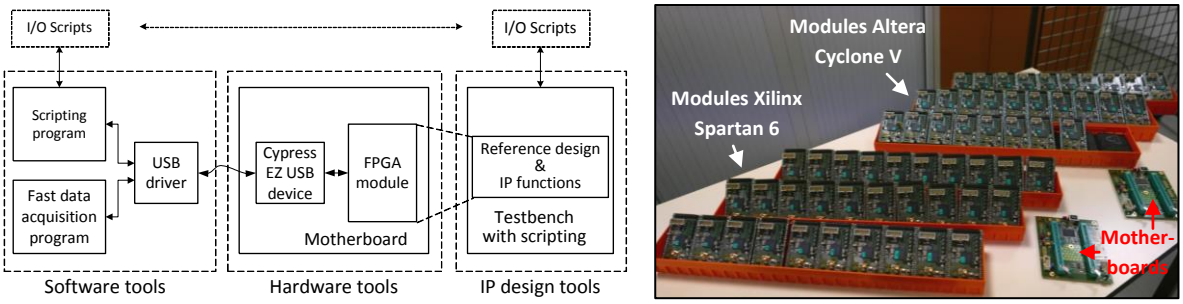

Figure 1: Evariste III system (left), Evariste III hardware (right): motherboards and application modules

The hardware system of Evariste III is composed of a set of motherboards with ZIF (zero insertion force) connectors and application modules (see Figure 1). A base of six motherboards placed in a box interconnected by a JTAG chain makes a parallel evaluation of up to six modules possible. This is very helpful in PUF characterization that needs numerous data acquisitions to be performed in different operating conditions [2]. Besides the ZIF connectors for application modules, the Evariste III motherboards contain a USB interface controller, linear power supplies, high quality low pass filters and all necessary connectors.

Three types of application modules have been designed for this new modular system. Each module is built around different FPGA family: Altera Cyclone V, Xilinx Spartan 6 and Microsemi Smart Fusion 2 with an embedded SoC based on an ARM processor. All daughter modules contain SMA connectors making SCA easier.

The Evariste III motherboards are compatible with old modules of Evariste II (9 types of modules are available). The software tools and IP functions are open source. Reference designs can be freely downloaded. For academic institutions, the hardware can be made available remotely. Researchers can download related tools from the website and can upload their configuration bitstream to the remote FPGA. They can then download random data or PUF responses that were generated in the same hardware and in the same working conditions, in order to compare fairly different state-of-the-art TRNGs or PUFs.

[1] http://labh-curien.univ-st-etienne.fr/wiki-evariste/index.php/Main_Page
[2] http://www.univ-st-etienne.fr/salware/