Modular Evaluation Platform for Evaluation and Testing of Physically Unclonable Functions

Marek Laban*†, Milos Drutarovsky*, Viktor Fischer‡, and Michal Varchola†
*Department of Electronics and Multimedia Communications
Technical University of Kosice Park Komenskeho 13, 04120 Kosice, Slovak Republic
†MICRONIC, Sliacska 2/C, 83102, Bratislava, Slovak Republic
‡Univ. Lyon, UJM-Saint-Etienne, CNRS, Laboratoire Hubert Curien
UMR 5516, F-42023, Saint-Etienne, France
Email: laban@micronic.sk, milos.drutarovsky@tuke.sk, fischer@univ-st-etienne.fr, varchola@micronic.sk

***Abstract*—Physical unclonable functions in field programmable arrays are always linked to the used hardware. Therefore, it is necessary to have high amount of simple devices for evaluation purposes. One of the suitable platform for such evaluation is HECTOR Evaluation Platform. The following paper describes this platform, compares it with existing solutions, and shows several examples of its using. The proposed platform consists of a motherboard and exchangeable daughter board modules. These are designed to be as simple as possible to allow cheap and independent evaluation across many devices. In comparison to similar existing solutions, proposed platform excels in its simple architecture, which allows remote using of module. The platform is also suitable for evaluation of other cryptographic primitives like true random number generators, encryption systems, and etc. Platform's components are adjusted for side channel attacks measurements.**

HECTOR evaluation platform was designed and optimized to fulfil the European HECTOR project (H2020) requirements.

I. Introduction

These days information appears mostly in a digital form. An electronic mail is used more often than a traditional mail, documents are stored in a digital form more than on a paper and information is often very expensive. Therefore, cryptography has become increasingly important to ensure data security.

Cryptography applies mathematical methods to ensure information security requirements such as data confidentiality, integrity, and authentication, but also authentication of devices and subjects [1]. It uses cryptographic primitives to build cryptographic protocols. Cryptographic primitives like Physical Unclonable Functions (PUFs) and Random Number Generators (RNGs) extract randomness from the underlying hardware [2]. Although other cryptographic primitives like symmetric- or asymmetric-key ciphers, and one way functions are deterministic, their implementation in hardware can leak confidential information and it is therefore hardware dependent, too.

A. Physically Unclonable Functions and Their Evaluation

There are many human attributes like fingerprint, DNA or human's dentition for unique and unpredictable person identification. Similarly, electronic device can be identified using a PUF. Its principle is based on an exploitation of Manufacturing Process Variation (MPV), in order to generate a binary number specific for various devices. The definition given in [3] defines PUF as *a physical entity which produces an output value at least in dependence of physical structures which are hard to clone.* PUFs can be used to authenticate hardware or to generate hardware dependent confidential keys [4], [5].

As with the other cryptographic primitives, PUF should meet the recommendations and criteria defined in a standard. However, such standard is just arisen. Its name is *Security Requirements and Test Methods for Physically Unclonable Functions for Generating Non-Stored Security Parameters*, marked as ISO/IEC NP 20897 [6]. The standardization process began in 2015.

Since every PUF is based on MPV, its output should differ from device to device. In order to properly evaluate PUF, it is necessary to test given PUF on many devices. In addition, temperature or voltage deviations have a big influence to the PUF's output and they need to be evaluated too.

B. HECTOR Project

In the framework of the information security politics of the European Union, a project called HECTOR (Hardware Enabled Crypto and Randomness) was recently accepted for funding [7]. HECTOR is a European cooperative research project. The project emerged from the scientific cooperation of several partners. The main objective of this project is to close the gap between basic algorithmic approaches and hardware-level security implementations. The project task is to study, design and implement RNGs and PUFs with demonstrable entropy guarantees and quality metrics. This includes on-the-fly entropy estimation and evaluation of robustness against physical attacks, which is needed in the security evaluation and certification process.

It requires to evaluate in a fair way many hardware dependent cryptographic primitives (RNGs, PUFs, authenticated encryption algorithms), in many different technologies. A flexible platform for testing and evaluation of primitives implemented on various Field Programmable Gate Array (FPGA) and Application-Specific Integrated Circuit (ASIC) devices was therefore needed. According to minimal production costs

and influence of environmental conditions, such platform should be very simple and carefully designed.

II. HECTOR Evaluation Platform

In the framework of the HECTOR project, HECTOR Evaluation Platform was arisen. The main motivation for designing of the platform was to design the modular hardware, which would be optimized for a thorough, but still easy evaluation of cryptographic primitives implemented in FPGA and ASIC devices. The platform consists of a *motherboard* and several types of interchangeable *daughter boards*. Evaluated cryptographic primitives are implemented in daughter board with hardware resources significantly reduced. Data are stored, processed, and transmitted to a PC using the motherboard featuring large choice of peripherals and interfaces. The daughter board can be connected to the motherboard remotely and can be thus placed in a hostile environment during attacks.

A. Daughter Board

The HECTOR daughter board modules are designed to allow evaluation of primitives across different FPGA families and ASICs. The selected architecture has two main advantages. First, the daughter modules contain only the necessary hardware components, which minimize their impact on the behaviour of the target primitive. Second, the module is simple and thus cheaper, i.e. a huge number of modules can be manufactured to test PUFs.

In the framework of the project four types of daughter modules were designed featuring Altera Cyclone V, Xilinx Spartan-6, Microsemi SmartFusion2 FPGA (see Fig. 1), and another one featuring a custom ASIC. Selected devices represent recent FPGA families of main FPGA vendors.

The daughter modules are connected to the motherboard using a SATA connector. It is used to power the board and to transfer data between the daughter board and the motherboard. The SATA connector is used mainly for its good signal integrity and mechanical features. The SATA interface protocol is not supported by the hardware. Instead, four LVDS (Low Voltage Differential Signaling) signal couples, three single ended wires and power supply voltages are present on the connector. The daughter boards contain high quality power filters. To reduce the cost and the electric noise, and to increase board's reliability, all power regulators are placed on the motherboard.

B. Motherboard

The main task of the motherboard is to control daughter modules, to read and eventually to process data from the modules and to ensure data transfers to the PC. The board uses USB interface to communicate with the PC and a variety of connectors for plugging in different daughter modules (see Fig. 2).

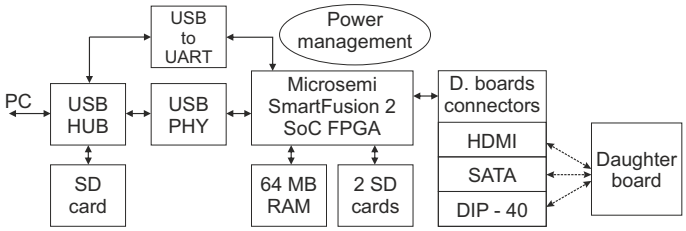

Fig. 2: Motherboard hardware block diagram.

The motherboard is based on the Microsemi SmartFusion2 – system on chip FPGA device. It integrates a flash-based FPGA fabric and an ARM Cortex-M3 processor. The time-critical parts of the system can be processed by the fabric and the communication protocol can be implemented in the Microcontroller Sub-System (MSS).

The HECTOR motherboard features synchronous external 512 Mb (64 MB) DDR SDRAM memory. It runs at 166 MHz, for a total theoretical bandwidth over 5.3 Gbps. It is provided as a flexible volatile memory for user applications.

The communication between the motherboard and the host PC is ensured via USB by two data channels. The first one, the virtual COM port, is designed to exchange the control and status packets using a simple UART protocol. It utilizes FTDI device supported by many operating systems. The second channel is designed to provide reliable high-speed data transfers using the USB mass storage class interface, which is natively supported by operation systems.

The motherboard is powered by an external power supply. In order to reduce the cost of daughter boards, the boards are powered from dedicated voltage regulators, which are placed

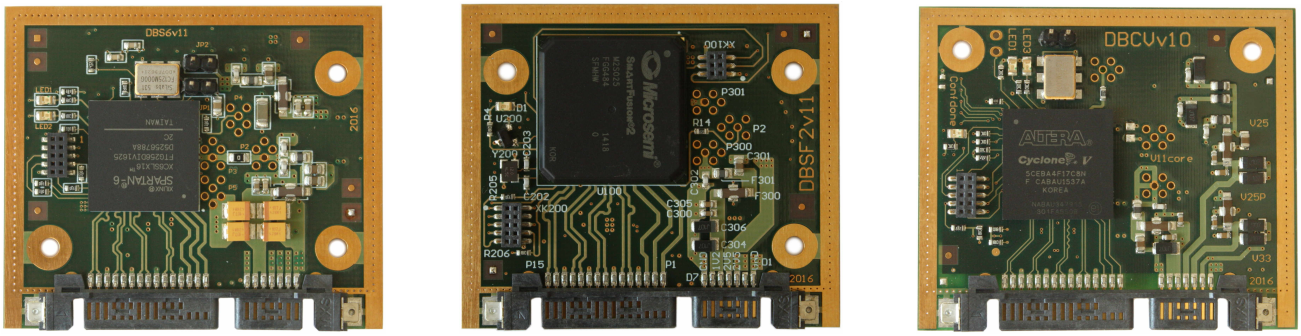

Fig. 1: HECTOR daughter boards featuring Xilinx Spartan 6, Microsemi SmartFusion2, and Altera Cyclone V.

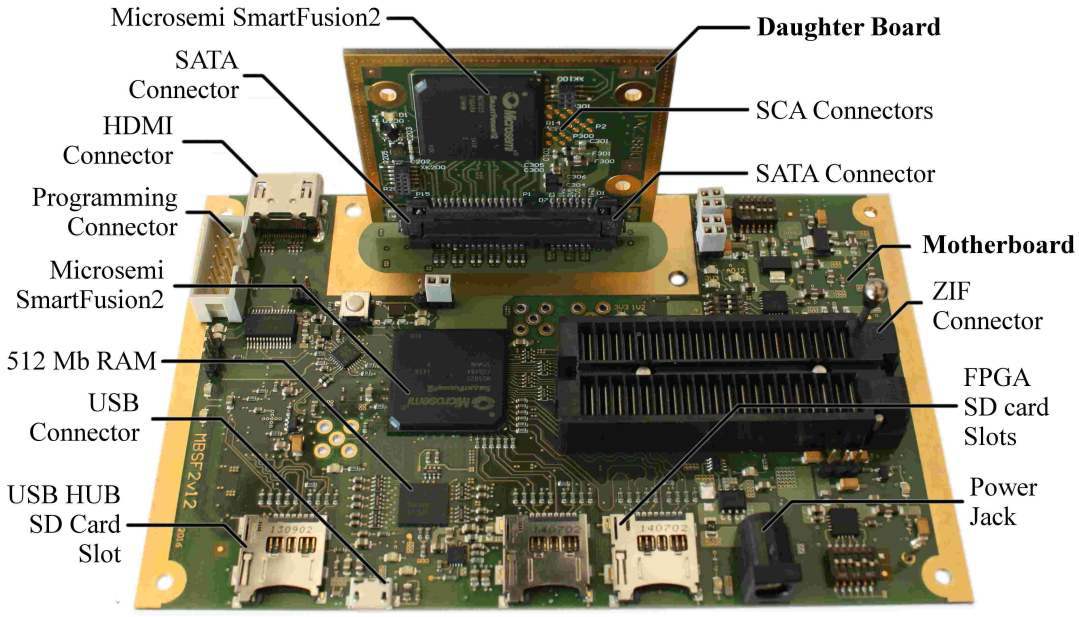

Fig. 3: Layout of the HECTOR motherboard featuring the SmartFusion2 FPGA device.

on the motherboard. Three of them are user-configurable by micro switches. The configurable regulators ensure compatibility across various daughter boards, which usually require different power supplies (e.g. the power voltage of the FPGA core may be different). The whole set of power supplies is properly filtered to minimize interference and noise. Only linear regulators are used on the board due to their low noise compared to noisy switching regulators. This low noise feature is very important for fair TRNG and PUF evaluation, as well as for evaluation of robustness against side channel attacks.

The motherboard provides three connectors for connecting of modules:

- High-Definition Multimedia Interface (HDMI) connector,
- Serial-ATA (SATA) connector,
- Zero Insertion Force (ZIF) connector.

The daughter boards can be plugged directly into the motherboard using the SATA connector or remotely using a common HDMI cable with a custom HDMI to SATA adapter.

The SATA connector ensures easy, reliable, low cost and low noise connection. An optional aluminium lid can be used to protect the daughter board from surrounding electro-magnetic fields, if necessary.

Connection of the daughter board via the HDMI cable can be useful when the tested device should be placed in a temperature controlled chamber or a Faraday cage. To make the connection easier, the same data signals are presented on the both SATA and HDMI connectors. However, in the case of a remote use of daughter boards, the power must be provided from an external power source connected to the available HDMI to SATA adapter.

ZIF connector, which is available on the motherboard is dedicated to expansion boards, e.g. boards with switches and LEDs.

III. Configuration of the System and Reference Designs

A set of tools is provided in several reference designs: the user applications running on the PC, and the motherboard hardware and firmware adapted to various user applications placed in daughter boards [8].

The proposed software tools and configuration of the system vary depending on the application. For the sake of place, we will briefly present only the one example of a PUF implementation in Section III-C. However the platform is also suitable for evaluation of any other cryptographic primitives like TRNG, symmetric or asymmetric key cryptography, as well as Side Channel Attacks (SCAs) on some primitives.

A. PC Application Software

The main task of the PC application software is to provide the user API to the motherboard via USB interface. It uses a virtual COM port to transfer the commands and the state words and a USB mass storage interface to transfer data. Created data files can be accessed directly from the host PC.

To ensure flexibility and system independence, the software running on the PC is developed in a TCL language. Only a TCL interpreter is needed to read user scripts. The TCL interpreter is usually installed during the FPGA design software installation (e.g. Quartus or Libero). The script can be very easily edited and adapted to user requirements.

B. Motherboard Firmware and Hardware

The motherboard firmware runs on the microcontroller subsystem inside the FPGA device. The components of the platform are depicted in Fig. 4. The microcrontroller sybsystem part has the following roles:

- Communication with the host PC,

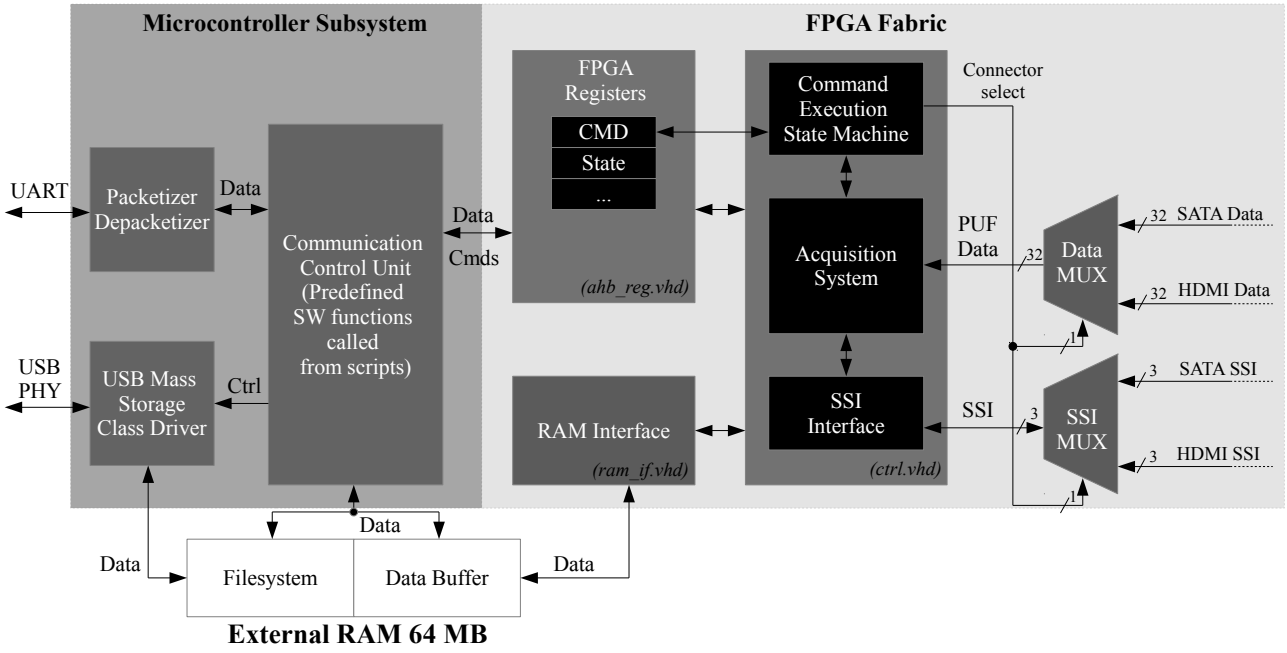

Fig. 4: Block diagram of SmartFusion2 internal system.

- Control of the device under test by sending commands to the FPGA fabric,
- Maintenance of the file-system for data transfers (files can have up to 30 MB).

The main role of the *Packetizer-Depacketizer* block is to maintain a communication protocol based on transferring small packets via UART.

The *USB mass storage class disk drive* provides access to file-system located in the the first half of the external RAM. It behaves like a common USB flash drive connected to the PC, if it is activated. The second half of the RAM is used as a cache reserved for data acquisitions.

A *Communication Control* block contains several predefined functions, which manage operations in the FPGA and reply to received packets. These functions (instructions) are called by packets received from the PC.

Microcontroller communicates with FPGA using a several registers. These registers are used for controlling of the input/output pins, exchanging of the device state, and entering of some commands.

One of the registers is command register. It controls *Command Execution State Machine* implemented in the FPGA fabric. There are defined commands for selecting of the daughter board's connector, starting of the data acquisition, and etc.

Serial Synchronous Interface (*SSI*) utilizes three signal wires for an easy data exchange between the host PC and the daughter board. It can be used for transferring of daughter board's state, or for controlling of the daughter board.

C. PUF Reference Design

We use Ring Oscillator (RO) PUF proposed by Kodytek et al. in [9] as an example of HECTOR Evaluation Platform using. Proposed principle selects two ROs and counts theirs oscillations using two 16-bit counters. When one of the counters overflows value of the second one is recorded. Several selected bits from the recorded counter are extracted and used as response of the PUF function.

In our example, Kodytek PUF function is located in the daughter board, where the function is controlled by *PUF Control Unit* (see Fig. 5). *PUF Control Unit* selects RO pairs, sets the number of measurement repetitions, starts the PUF response generation and reports a daughter board status. Daughter board's statuses and commands are transferred to/from daughter board using SSI.

If one of the counters overflows, then the 16-bit value of the second one is always serialized and transferred to the motherboard via a fast serial interface. The interface uses three signals: *Data*, *Strb*, *Sync*. Serial data are shifted into the motherboard, where the 16-bit word is reconstructed and recorded to the external RAM. At the end of the data acquisition, recorded 16-bit words are available for the host PC as the file in the mass storage class device.

Multiplexers in the motherboard allow to connect the board either directly to the SATA connector, or via HDMI cable and an SATA to HDMI adapter.

The data acquisition is initialized and controlled by the host PC, which executes the TCL scripts. The scripts consist of the instructions, which reset the daughter board, create file-system on motherboard, start the acquisition, configure *PUF Control Unit* and etc.

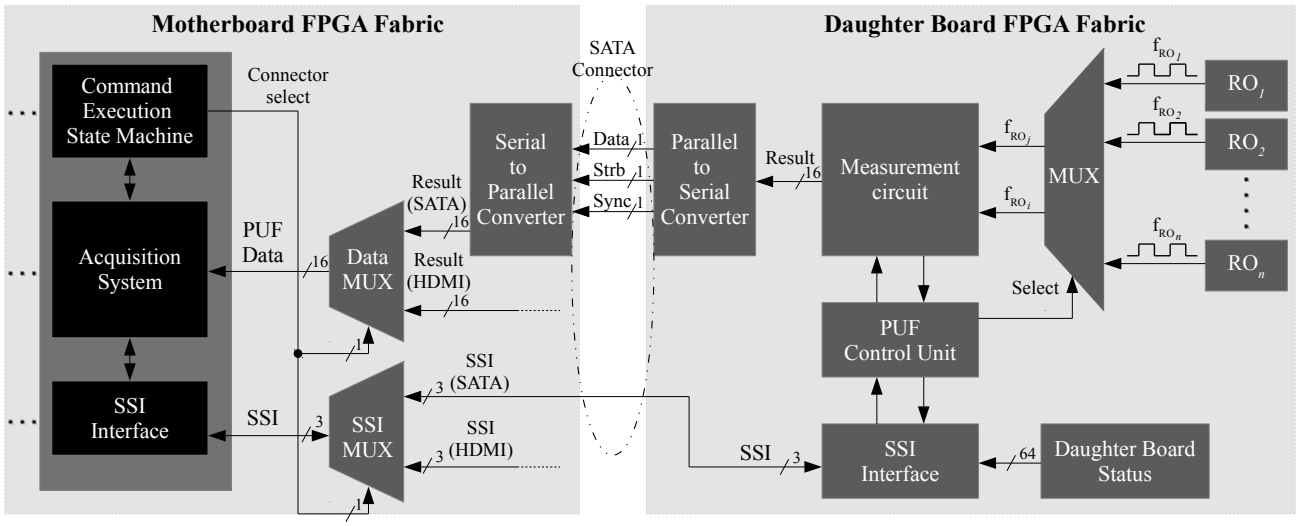

Fig. 5: Example of PUF implementation in Hector Evaluation Platform.

The proposed example simplifies the evaluation of the bit selection. The interface for acquisition is very fast and allows to record the data stream up to 30 MB. The PUF can be easily controlled and adjusted via SSI interface.

D. PUF Measurement Example

The main advantage of HECTOR Evaluation Platform is its independent measurement methods. It was mentioned earlier, that PUF functions are very sensitive to environmental changes like temperature or voltage. Therefore, it is necessary to test these changes. At the same time, the evaluator must be sure, that the environmental changes (e.g. high temperature) affect just the target device and not any devices which process data. Thanks to HECTOR Evaluation Platform, the target device – daughter board, and processing device – motherboard can be independently connected using a HDMI cable.

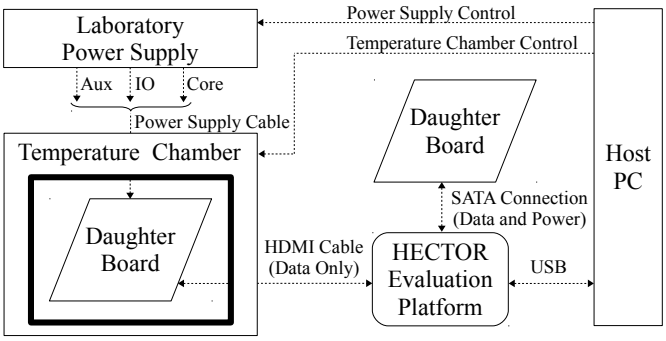

Fig. 6: Example of laboratory measurement configuration.

Fig. 6 shows an example of the laboratory measurement. Daughter board is placed into the temperature chamber. Data are transferred to the motherboard via the HDMI cable. Daughter board is powered from an independent laboratory power supply, where several power lanes are connected (core power, input/output pins power, and etc.). Since there are no voltage regulators on the daughter board, every FPGA power lane can be easily changed. Thanks to the control of laboratory power supply and temperature chamber from the host PC, measurement process can be automatized.

If it is necessary to test response of many devices, several daughter boards can be placed into the chamber. They would be connected by several HDMI cables, but just one cable could be connected to the motherboard at one time. Alternatively they can be easily interchanged and tested via SATA connector (outside the chamber).

IV. State of the Art

The hardware dedicated to the evaluation of cryptographic primitives must fulfill special requirements, especially from the point of view of electric noises, electro-magnetic interference, and robustness of the design. Several solutions are currently available.

The Research Center for Information Security (RCIS) of AIST and Tohoku University developed the Side-channel Attack Standard Evaluation BOard (SASEBO) [10] as a research project funded by METI (Ministry of Economy, Trade and Industry, Japan). Several SASEBO boards aimed at evaluation of cryptographic functions implemented in FPGAs, ASICs, and Smartcards are available. The boards were designed essentially as platforms for evaluation of the SCAs. They contain mostly two FPGAs: one as a Target of Evaluation (ToE), and the second one, which controls the target. Unfortunately, the platform is not modular, because both devices are located on the same board. Therefore the ToE cannot be separated and placed remotely in a hostile environment. The second disadvantage of the SASEBO boards in the context of the HECTOR project is, that only a limited choice of FPGA devices is available. This argument is valid also for SAKURA boards,

which are successors of the SASEBO boards. Last but not least, the SASEBO (and SAKURA) boards are complex and thus expensive and consequently, not suitable for evaluation of PUFs, where a large amount of devices must be tested.

Another platform, a Flexible Open-source BOard for Side-channel analysis (FOBOS) [11] was designed by the George Mason University for conducting side-channel attacks on FPGAs. The platform consists of two different boards, one is used as a control board and another one as a Device Under Test (DUT). Both cards are connected together by a module, which is called a bridge connector. The advantage of this platform is that it uses commercially available boards – it is therefore cheaper. But the use of the commercially available general purpose evaluation boards is also the main disadvantage of this solution. These boards are not intended for SCA evaluation purposes, they contain many redundant components and switching power supplies generating significant electronic noise. In addition, various bridge connectors and communication interfaces are needed for different types of DUTs.

Evariste III [12] is a platform aimed at development and evaluation of cryptographic functions and primitives in reconfigurable hardware. The platform was developed by the Jean Monnet University in cooperation with the MICRONIC company. It is a modular platform containing daughter boards (featuring target FPGAs or ASICs) and a motherboard containing USB data interface device. Three daughter boards designed for Evariste III and several other daughter boards designed for older platform Evariste II are available. The Evariste III modules contain connectors for SCA measurements. The main disadvantage of the Evariste III (and the Evariste II) system is that the modules cannot be used remotely, and that they are relatively expensive since they contain power supplies. Last but not least, a large high-speed external RAM memory, which is needed for high-speed data acquisition, is available only on few daughter boards (which are thus more expensive).

V. Conclusion

HECTOR evaluation platform was designed following the project requirements and it reflects the needs of all HECTOR partners. It is a little bit difficult to compare modularity or performance of the existing similar platforms, because every platform has a slightly different architecture. SASEBO and FOBOS boards are aimed mainly at SCAs. Evariste III is the successful predecessor of HECTOR evaluation platform. Nevertheless, the new proposed platform differs and excels from SASEBO, FOBOS, and Evariste III platforms in the following points:

- **Motherboard features large 64 MB RAM memory,** which is necessary for acquisition of long continuous data streams (e.g. data from TRNG).
- **The number of components on the daughter board module is limited to a strict minimum.** It reduces price of the modules. This is particularly useful, if huge number of devices are needed for PUF evaluation. At the same time it minimizes undesirable effects on the ToE.
- **The daughter board can be placed remotely in a hostile environment.** Thanks to the HDMI cable connection daughter board can be placed into some chamber. The separation minimizes undesirable influence to the measurement equipment and some active attacks can be performed.
- **Every daughter board have the same communication interface and connector.** Just like Evariste III, different types of daughter boards with the same implemented primitive do not require change of the motherboard implementation or its hardware.

HECTOR Evaluation Platform is a unique and powerful tool set particularly suitable for testing and evaluation of cryptographic primitives as well as SCAs. However, the platform is sufficiently flexible to be adapted to a variety of the other applications.

Proposed hardware and software means will be used for development and testing of new PUFs. All the IP functions and software tools from the example are open-source. According to the HECTOR consortium agreement, the HECTOR evaluation boards can be used by third parties for an educational dissemination purposes.

Acknowledgment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644052. This work was also supported by the Slovak Research and Development Agency under the contract No. APVV-15-0692.

References

[1] Menezes, Oorschot, Vanstone, *Handbook of Applied Cryptography*, CRC Press, October 1996

[2] M. Laban, M. Drutarovsky: Low-cost ARM Cortex-M0 Based TRNG for IoT Applications, Acta Electrotechnica et Informatica, Vol. 18, No. 1, 2018, p. 52-56, DOI: 10.15546/aeei-2018-0008

[3] Ch. Bohm, M. Hofer 2013. *Physical Unclonable Functions in Theory and Practice.* Springer New York Heidelberg Dordrecht London, ISBN 978-1-4614-5039-9, p. 4

[4] B. Colombier, U. Mureddu, M. Laban, O. Petura, L. Bossuet, V. Fischer, *Complete activation scheme for FPGA-oriented IP cores design protection*, 27th International Conference on Field Programmable Logic and Applications (FPL), Ghent, Belgium, 2017

[5] Z. Paral, S. Devadas, *Reliable and Efficient PUF-Based Key Generation Using Pattern Matching*, 2011 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), San Diego CA, USA, 2011

[6] International Organization for Standardization *Security requirements, test and evaluation methods for physically unclonable functions for generating nonstored security parameters*, ISO/IEC NP 20897, Available online: https://www.iso.org/standard/69403.html

[7] *HECTOR project* web page, available: https://hector-project.eu/

[8] Laban, M., *Development tools for evaluation of cryptographic primitives implemented in reconfigurable hardware*, Master thesis, Technical University of Kosice, Kosice, May 2016, p. 1-91

[9] F. Kodytek, R. Lorencz, *A design of ring oscillator based PUF on FPGA*, IEEE 18th International Symposium on Design and Diagnostics of Electronic Circuits & Systems, Belgrade, Serbia, 2015

[10] Nartional institute of AIST, *Side-Channel Attack Standard Evaluation Board SASEBO*, available online: http://satoh.cs.uec.ac.jp/SASEBO/en/

[11] Velegalati, Kaps *Towards a Flexible, Opensource BOard for Side-channel analysis (FOBOS)*, available online: https://cryptography.gmu.edu/fobos/

[12] Laboratoire Hubert Curien, *Evariste wiki page*, available online: http://labh-curien.univ-st-etienne.fr/wiki-evariste/index.php/Main_Page