A Low-Cost Unified Experimental FPGA Board for Cryptography Applications

Matěj Bartík, Jiří Buček

Czech Technical University in Prague, Faculty of Information Technology
{matej.bartik; jiri.bucek}@fit.cvut.cz

***Abstract*—This paper describes the evaluation of available experimental boards, the comparison of their supported set of experiments and other aspects. The second part of this evaluation is focused on the design process of the PCB (Printed Circuit Board) for an FPGA (Field Programmable Gate Array) based cryptography environment suitable for evaluating the latest trends in the IC (Integrated Circuit) security like Side–Channel Attacks (SCA) or Physically Unclonable Function (PUF). It leads to many criteria affecting the design process and also the suitability for evaluating and measuring results of the attacks and their countermeasures. The developed system should be open, versatile and unrestricted by the U.S. law [1].**

I. Introduction

Security issues (cryptanalysis and side-channel attacks) are getting more and more important during last years. Nowadays, current research on hardware security is focused on two methods: how to decrease vulnerability of integrated circuits to leak their secrets and how to devise methods of secure authentication. For example, the Differential Power Analysis (DPA) is probably the most efficient way to retrieve secrets from ICs, and practically all security devices must include some form of countermeasures. The representative example of authentication (and also key generation) is PUF, the security of which is widely discussed and attacks and countermeasures are developed.

The progress of these technologies requires to teach future hardware security engineers how to evaluate attacks and countermeasures against attacks. Laboratory courses require [2] huge amount of (expensive) experimental boards like SASEBO [4] or Evariste [5] project. PUF related research requires the same or higher number of experimental boards. Both of the goals require to design and create a low cost development board equipped with a state of the art FPGA. The board design process should reflect the needs of cryptographic experiments and applications.

II. Supported Experiments

In the following subsections, we will summarize the intended experimental application fields of the development board.

A. Power Analysis Attacks

Every digital circuit leaks some internal information via its power consumption. Paul Kocher et al. [6] showed that by power consumption measuring during cryptographic operations and by analyzing these measurements, the secret key can be discovered, even though the cipher is otherwise (mathematically) secure. In order to experiment with power analysis attacks, a current measuring device (usually a resistor) is added to a supply rail in order to measure the current consumption.

The power consumption is measured as a sequence of samples in time (a power trace) using a digital oscilloscope (see Fig. 1), and the power traces are then transferred to a computer for analysis. There are several methods for analyzing the power traces. Simple power analysis (SPA) use a single power trace to directly discover the secret key.

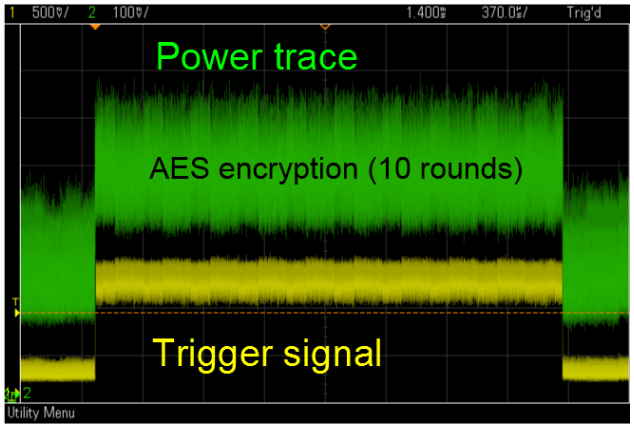

Fig. 1. The power trace example of the AES cipher [2].

Differential power analysis (DPA) uses multiple power traces, each is measured for the encryption with different (known) data [7]. The secret key is then derived part by part using statistical methods (testing of hypotheses about the values of the sub-keys). For each sub-key, all possible values are analyzed, a hypothetical power consumption is computed using the known data and a power model, and the correct one is found by correlating the hypothetical consumption with the measured consumption across all traces for some point in time.

B. Physically Unclonable Function (PUF)

The PUF [8] [9] is a challenge–response mechanism that uses physical properties of integrated circuits (deviations in the manufacturing process like unique delay of the logic circuits paths in the each IC) to create a unique response that identifies the IC conclusively. The fundamental principle of PUF is shown in Fig. 2. The response can be used as a secret key for the cryptography or memoryless key storage.

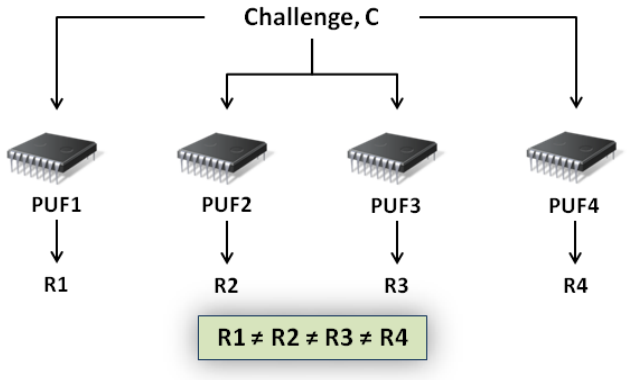

Fig. 2. The principle of the PUF with different responses (Rx) [9].

C. Cipher Implementation

An FPGA is a perfect tool for implementing of any cipher, for example the AES (Advanced Encryption Standard) cipher (that can be attacked by the DPA method). Modern FPGAs are using a hardcoded AES cipher block as a protection against copying the FPGA bitstream [20]. We can also apply the DPA [11] technique to attack the FPGA configuration and bitstream loading block to retrieve the secret key for the bitstream decryption.

D. FPGA Configuration and AES Decryption of the Bitstream

A modern FPGAs can use an AES cipher as a protection against copying the FPGA bitstream [20]. We can also apply the DPA [11] technique to attack the FPGA configuration and bitstream loading block to retrieve the secret key for the bitstream decryption.

E. SHA-1 Challenge – Response Authentication

The SHA–1 EEPROMs like Maxim Integrated DS2432 is predecessor (see Fig. 3) of the PUF technology used for a bitstream authentication [21]. This SHA–1 EEPROM can be also attacked like the PUF.

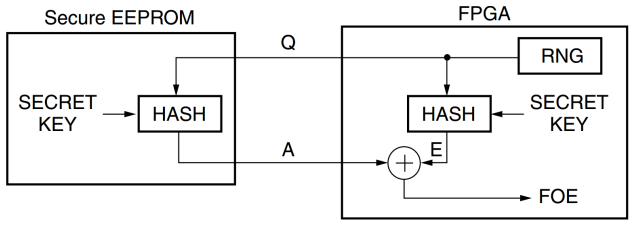

Fig. 3. The principle of the SHA-1 challenge – response authentication. [21]

F. Evaluating Quality of the TRNG

Random number generation is of critical importance for many cryptographic methods and applications, such as key generation, digital signature computation, and challenge-response authentication. True random number generators (TRNGs) rely on physical noise sources such as thermal noise, phase jitter or metastability, from which they extract entropy to produce a random bitstream. Some methods are suitable for implementation in FPGAs, such as ring-oscillator based TRNG [3].

III. Available Competing Platforms

In this section a brief comparison will be presented between three similar projects (SASEBO [4], Evariste [5] and FOBOS [15]) focused on the creation of the unified environment for testing, evaluating a measuring systems implementing cryptographic hardware.

A. SASEBO

SASEBO [4] is the most complex project focused on the cryptography providing a complete toolset of boards (see Table I.), software and measuring equipment. There are seven different SASEBO boards differing by the used chip (ASIC or FPGA). The most of SASEBO boards (see Fig. 5) contains one FPGA for interfacing PC over the USB port (trough a dedicated chip) and control the dedicated ASIC/FPGA (up to Xilinx Kintex-7) for cryptography purpose (a control – victim schema is used, see Fig. 4).

TABLE I. Comparison of the SASEBO boards [22]

Board	Vendor	Control	Victim	Year
SASEBO	Xilinx	XC2VP30	XC2VP7	2007
SASEBO–G	Xilinx	XC2VP30	XC2VP7	2008
SASEBO–GII	Xilinx	XC3S400A	XC5VLX30 or LX50	2009
SASEBO–GIII	Xilinx	XC6SLX45	XC7K325T	2013
SASEBO–B	Altera	EP2S30F672C5N	EP2S15F484C5N	2008
SASEBO–R	ASIC	XC2VP30	LSI 130nm process	2008
SASEBO–W	Xilinx	XC6SLX150	Smart Card socket	2012

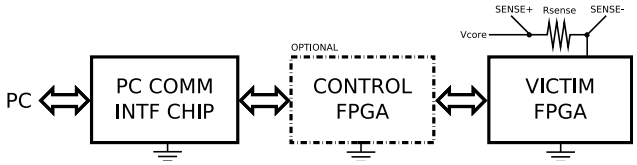

Fig. 4. The control – victim block diagram

Control & cryptographic parts have separate power supplies to limit the interference between them, but interference can spread over the common ground. The cryptographic chip usually has no decoupling capacitors (or a few positions for mounting capacitors, but the number of positions is significantly lower than the amount recommended by the chip vendor) reducing the average number of required measurements for the DPA [12]. The biggest disadvantage of the SASEBO boards are their price (approximately 1500$–2000$) that prevent to equip each student with his own board. Further disadvantages are lack of decoupling capacitors that are mounted on commercial FPGA boards according to FPGA vendor datasheet (we can't simulate the real operating conditions for the PUF).

B. Evariste II and Evariste III

The Evariste II project [5] is focused primarily on fair benchmarking of true random number generators, but can also be used for other purposes (see Fig. 6). There are 9 different boards with different FPGA chips using the motherboard for acquiring measured data. These boards have the same general features like using linear low–noise power regulators to supply voltage for the FPGA (Core, Auxiliary, I/O). Like in the

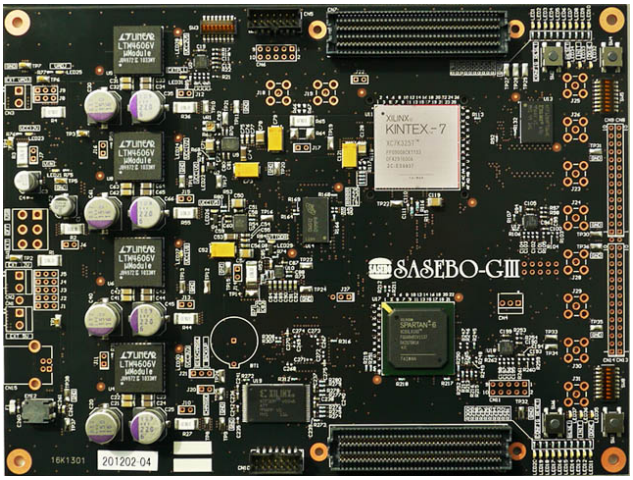

Fig. 5. The SASEBO–GIII board. [13].

SASEBO, the communication and data acquisition is provided by the USB interface (Cypress FX2 – CY7C68013A), but there is no control FPGA. The control and the interface part is implemented in the measured FPGA. There is no isolation from the communication IC (FX2) to prevent the interference. Currently supported boards are in Table II.

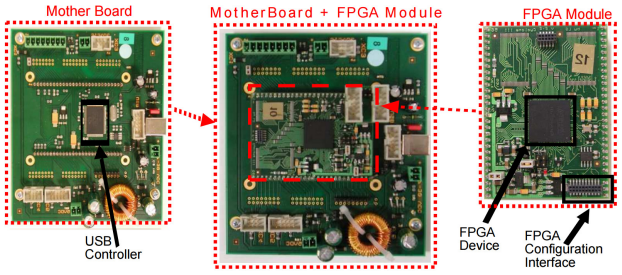

Fig. 6. Setup of the Evariste II project. [14]

TABLE II. COMPARISON OF THE EVARISTE II AND III BOARDS [14]

Evariste II Modules		
Board	**Vendor**	**Chip**
Cyclone III FPGA module v2.2	Altera	EP3C25F256-C8
Cyclone III FPGA module v2.4	Altera	EP3C25F256-C8
Arria II FPGA module v 1.0	Altera	EP2AGX45CU17C6
Spartan 3 FPGA module v 2.1	Xilinx	XC3S700AN
Virtex 5 FPGA module v 1.0b	Xilinx	XC5VLX30T
Fusion FPGA module v 2.0	Microsemi	M7AFS600 FGG256X2
Evariste III Modules		
Board	**Vendor**	**Chip**
Spartan 6 FPGA module v 1.0	Xilinx	XC6FLX16
Cyclone V FPGA module v.CyV2	Altera	5CEBA4F17C8N
SmartFusion2 FPGA module v.1	Microsemi	M2S025FGG484

C. FOBOS

The idea of FOBOS project [15] is an attempt to create a unified environment for cryptographic purposes using ordinary FPGA development boards widely used for teaching. All twelve supported boards are in the university program of both major FPGA vendors, Xilinx and Altera.

FOBOS shares the same idea of SASEBO (dual FPGA system control–victim), but each part is created from an individual development board. The effort is focused on saving money by using ordinary boards to create a low–cost system. In case that the university/laboratory doesn't already have these boards (see Table III.), the price for equipping students is high (cheaper half of these boards are discontinued, second half is expensive). There is no isolation to prevent noise from the control system.

TABLE III. COMPARISON OF THE FOBOS BOARDS. [15]

FOBOS Control Boards		
Board	**Chip**	**Price**
Nexys–2	XC3S500E	149 $ (Discontinued)
Nexys–3	XC6LX16	270 $
FOBOS Victim Board — Xilinx FPGA based		
Board	**Vendor**	**Chip**
Spartan–3E Starter Kit	XC3S500E	299 $ (Legacy)
Spartan–3E - 1600 DB	XC3S1600E	225 $ (Discontinued)
Atlys	XC6LX45	419 $ (Legacy)
Genesys	XC5VLX50T	899 $ (Legacy)
ML605	XC6VLX240T	1995 $
KC705	XC7K325T	1695 $
FOBOS Victim Board — Altera FPGA based		
Altera DE1	Cyclone II 2C20	150 $
Altera DE2-115	Cyclone IV EP4CE115	495 $
Cyclone III Starter	Cyclone III EP3C25F324	200 $
Altera DE4	Stratix IV GX EP4SGX230	2995 $

IV. EXPERIMENTAL BOARD REQUIREMENTS

In this section we will discuss some requirements for the PCB to support all mentioned goals [16]. Requirements for one goal can be opposite for the another goal.

A. Simple / Differential Power Analysis (SPA/DPA)

The secret key is obtained by measuring the FPGA core power consumption. From these measurements a power trace waveform (representing voltage in the time) we will created, from which the secret key can be determined. Two main SPA/DPA requirements must be met: ability to measure the current for the FPGA core (using a shunt resistor) and remove decoupling capacitors for increasing current surges (voltage peaks) that made the key recovery much easier (but not impossible [17]). Additional requirements for attacking FPGA configuration block are: presence of a (Quad) SPI Flash chip as a bitstream storage and V_{BATT} pin have to be connected out onto a pin header (FPGA key storage is a volatile memory).

B. Physically Unclonable Function (PUF)

The result of PUF circuit prototype can vary due to different operational conditions and other influences from the environment surrounding the measured board. Parameters that affect measurements outside the board are the change of the operating temperature and EMI (Electro Magnetic Interference) in the power supply source.

The most important parameter is the FPGA core voltage, that can not be simply modified on an ordinary board and should meet the requirements of the FPGA chip vendor (tolerance is typically 3%–5%). The core voltage of modern FPGAs is usually 1 V, so the variance can be maximally 100 mV peak–to–peak using a proper decoupling technique. A precise power solution with a voltage control in the order of millivolts and ability to change output voltage on–the–fly from the control system is required. The solution should support a standardized

interconnection bus like an I^2C or an SPI to support automated measurements. The current required by a typical mid–range FPGA core is 3–4 amperes, thus limits the choice.

C. Cipher Implementation in the FPGA

Asymmetric ciphers and methods need mostly more FPGA resources than symmetric ones. The board (and FPGA footprint and pinout) should be the same for all chips across the FPGA family. This allows to use smaller or bigger chips on demand and modify the board price to reach expected budget.

D. General Requirement – EMC and Measurement Process

The general requirements also affect the final design of the board. The most common one is to comply with the EMC (Electro Magnetic Compatibility) requirements [18]. The measured values can be jammed by other circuits placed on the board. For example, Cypress FX2 (CY7C68013A) is widely used for communication between PC and FPGA via USB. The inner architecture of FX2 includes the 8051 microcontroller. There is no way to be sure that the measured consumption (for SPA/DPA) is from the FPGA only. Even FX2 is not sharing power supplies with the FPGA, a noise from I/O pins can cause a small interference in measured voltages.

This is an example based on our research [2] with Evariste boards where the Cypress FX2 circuit is used. We are able to retrieve the AES secret key no matter how the AES were calculated because the power activity of the FX2 is higher than the power activity of the measured FPGA. To lower the system noise, optocouplers circuits should be used to divide the board to an FPGA part and the interface part. The control will be provided by a control application on PC.

V. Characteristics of the Experimental Board

A. System Partitioning

The cost of the designed system can be reduced in different ways. The first idea is not to use the control–victim schema like SASEBO or FOBOS. The price goes down by removing one FPGA chip (one development board), so we got inspired by the Evariste project. The save of one FPGA will reduce the board size and might allow to use a lower count of PCB layers.

B. FPGA

The majority of the mentioned boards from all projects are based on the Xilinx Spartan-3E technology. On the other hand, there are only two boards equipped with a state of the art FPGA like Xilinx Kintex-7. The final board should contain a modern FPGA. Xilinx provides a cheaper alternative to Kintex-7 called Artix-7, based on same technology with similar features. Artix-7 FPGAs are available in many packages, but the FT256 package is the only one that met the requirements (4 layer PCB, variety of available chips).

C. FPGA Core Voltage Power Solution

We have selected an Artix-7 FPGA (model XC7A100T) as a maximum configuration. This requires a power supply that can deliver up to 3 A. We got our attention by the Texas Instrument TPS62360 chip [19]. The TPS62360 key features are programmable output voltage (0.77 V–1.4 V via I^2C interface in 10 mV steps) and differential load sensing for precise output voltage accuracy (less than 0.5%). The functional diagram is depicted in Fig. 7.

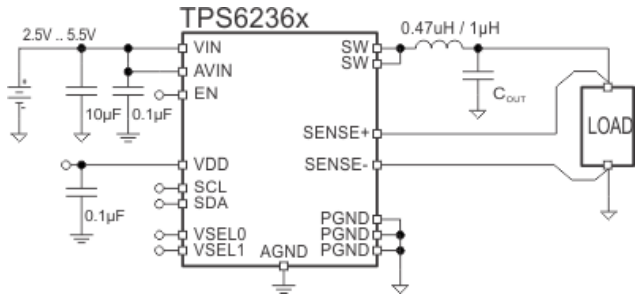

Fig. 7. The functional diagram of the Texas Instrument TPS62360 [19].

D. Interface Part

The interface part should support the I^2C bus (due to the selected power supply) and one usual communication protocol for interacting the board by the PC. An UART interface was chosen for its simplicity to reduce the number of the optocouplers (thus the board complexity). The FTDI FT2232H chip supports both interfaces using only one chip. The interface part and the FPGA part are isolated by the bi-directional optocouplers for an I^2C and an UART and isolation can be increased by removing thin stripes of the soldermask from both sides to decrease capacitive binding and leakage currents.

E. Measurement of the FPGA Core Voltage

This requirement can be solved by adding a high accuracy shunt resistor with two SMA connectors (before and after the shunt resistor). SMA connectors were chosen for an easy connection between the board and an oscilloscope (or an ADC card). Traces between the shunt resistor and SMAs are routed to 50 ohm impedance to match oscilloscope probes. Using both SMA connectors makes possible to add a differential operational amplifier and we also provided a pin header for this feature.

F. Customization Options for Specific Needs

The board is designed to use SMD (Surface Mount Devices) with reasonable dimensions for hand soldering. All discrete parts are in 0603 (or larger) package with exception of the decoupling capacitors under the FPGA (0402 package) and can be easily added/removed by hot air gun and tweezers according to measured experiments. Unused FPGA pins can be connected to pin headers. A differential pairs are more universal for the future board extension. We can use a cheap motherboard like the Evariste project that provides LEDs, buttons, switches, displays, etc. for educational purposes for teaching digital design in a general way.

VI. Price Calculation of the Experimental Board

The experimental board is designed (see Fig. 8 and Fig. 9) for small batch production of 30 boards. The board outline is the same as the smart card dimensions thus the area of the board is 7.17 square inch (46.25 cm^2). The BGA (Ball Grid Array) packages require an ENIG (Electroless Nickel Immersion Gold) surface finishing. The board price is 11$ including a stencil.

The components price depends on the used FPGA. For our needs the Artix-7 35T (XC7A35T-1FTG256C) is sufficient and the cost is 25$ only. The price for all remaining components is 95$ and the cost of the assembly process is 34$ per board. The cost of the assembled board is approximately 165$ (respectively 200$ including VAT and other charges) that is significantly below the price of competitor boards (SASEBO 1500$, Evariste 500$, FOBOS 1000$) with the same or more features supported. The total price will be even lower thanks to discounts (25%) for chips applied from 10–25 chips.

VII. Conclusion

We evaluated three different projects (SASEBO, Evariste, FOBOS) focused on measuring and evaluating cryptographic applications in hardware (FPGA). We described their advantages and disadvantages (the spread of the EMI to the measured part because of no isolation between the control part and measured part) and we summarized a state of the art (requirements) for a new low–cost FPGA board (and effects of these requirements).

The board has been designed to be versatile and universal for evaluating various cryptographic techniques (PUF, SPA, DPA, cipher implementation and others attacks/countermeasures) and is the only board supporting the SPA/DPA and the PUF evaluation at the same board. The board is fully operational and we delivered a state of the art FPGA (Xilinx Artix-7) equipped board to researchers, teachers and student regardless of low cost demands. The board is further easily customizable to extend the range of possible experiments with a basic soldering equipment.

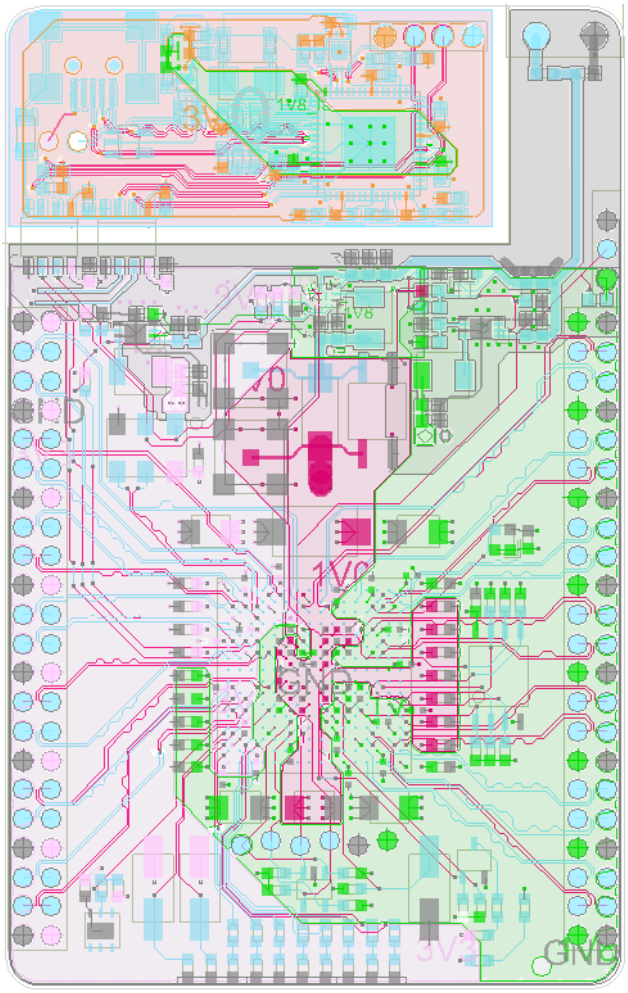

Fig. 8. The developed PCB of new experimental board with an Artix–7 FPGA and isolated communication interface part with only 4 layers.

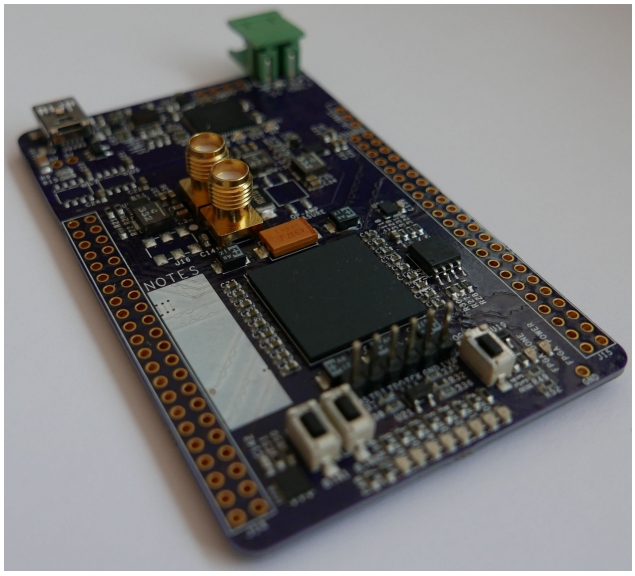

Fig. 9. The developed and operational board with assembled components.

Acknowledgment

This research has been partially supported by the project SGS16/121/OHK3/1T/18 and by the grant GA16-05179S of the Czech Grant Agency, Fault-Tolerant and Attack-Resistant Architectures Based on Programmable Devices: Research of Interplay and Common Features (2016–2018).

References

[1] SASEBO-G-II-32 Side-channel Attack Standard Evaluation Board, Digilent Inc. [Online]. Available: http://store.digilentinc.com/sasebo-g-ii-32-side-channel-attack-standard-evaluation-board-by-inrevium-retired/

[2] Stepanek, F.; Bucek, J.; Novotny, M., "Differential Power Analysis under Constrained Budget: Low Cost Education of Hackers," in Digital System Design (DSD), 2013 Euromicro Conference on, pp.645-648, 4-6 Sept. 2013 doi: 10.1109/DSD.2013.130

[3] Buchovecká, S.; Lórencz, R.; Kodýtek, F.; Buček, J., "True Random Number Generator based on ROPUF circuit", in Digital System Design (DSD), 2016 Euromicro Conference on, pp.519-523, Aug. 31-Sept. 2, 2016

[4] Simion, E.; Burciu, P., "A view to SASEBO project," in Electronics, Computers and Artificial Intelligence (ECAI), 2013 International Conference on , vol., no., pp.1-6, 27-29 June 2013 doi: 10.1109/ECAI.2013.6636186

[5] Fischer, V.; Bernard, F.; Haddad, P., "An open-source multi-FPGA modular system for fair benchmarking of True Random Number Generators," in Field Programmable Logic and Applications (FPL), 2013 23rd International Conference on , vol., no., pp.1-4, 2-4 Sept. 2013 doi: 10.1109/FPL.2013.6645570

[6] Kocher, P., Jaffe, J., Jun, B. Differential power analysis, In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388397. Springer, Heidelberg (1999)

[7] Benhadjyoussef, N.; Mestiri, H.; Machhout, M.; Tourki, R., "Implementation of CPA analysis against AES design on FPGA," in Communications and Information Technology (ICCIT), 2012 International Conference on , vol., no., pp.124-128, 26-28 June 2012 doi: 10.1109/ICCITechnol.2012.6285774

[8] PUF Physical Unclonable Functions, NXP [Online]. Available: www.nxp.com/documents/other/75017366.pdf

[9] Background on Physical Unclonable Functions (PUFs), Virginia Tech [Online]. Available: http://rijndael.ece.vt.edu/puf/background.html

[10] Developing Tamper Resistant Designs with Xilinx Virtex-6 and 7 Series FPGAs (XAPP1084), Xilinx [Online]. Available: http://tinyurl.com/p32ez9f

[11] Sugawara, T.; Homma, N.; Aoki, T.; Satoh, A., "Differential power analysis of AES ASIC implementations with various S-box circuits," in Circuit Theory and Design, 2009. ECCTD 2009. European Conference on , vol., no., pp.395-398, 23-27 Aug. 2009 doi: 10.1109/ECCTD.2009.5275004

[12] DPA Characteristic Evaluation of SASEBO for Board Level Simulations, Toshihiro Katashita, Akashi Satoh, Katsuya Kikuchi, Hiroshi Nakagawa and Masahiro Aoyagi, First International Workshop on Constructive Side-Channel Analysis and Secure Design 2010 (COSADE 2010), Proceedings of COSEADE 2010, pp.36-39, February 2010.

[13] Hori, Y.; Katashita, T.; Sasaki, A.; Satoh, A., "SASEBO-GIII: A hardware security evaluation board equipped with a 28-nm FPGA," in Consumer Electronics (GCCE), 2012 IEEE 1st Global Conference on , vol., no., pp.657-660, 2-5 Oct. 2012 doi: 10.1109/GCCE.2012.6379944

[14] Hardware, Laboratoire Hubert Curien [Online]. Available: https://labh-curien.univ-st-etienne.fr/wiki-evariste/index.php/Hardware

[15] R. Velegalati and J.-P. Kaps, Towards a Flexible, Opensource BOard for Side-channel analysis (FOBOS), June, 2013, Cryptographic architectures embedded in reconfigurable devices, CRYPTARCHI 2013

[16] Katashita, T.; Satoh, A.; Sugawara, T.; Homma, N.; Aoki, T., "Development of side-channel attack standard evaluation environment," in Circuit Theory and Design, 2009. ECCTD 2009. European Conference on , vol., no., pp.403-408, 23-27 Aug. 2009 doi: 10.1109/ECCTD.2009.5275001

[17] Iokibe, K.; Amano, T.; Toyota, Y., "On-board decoupling of cryptographic FPGA to improve tolerance to side-channel attacks," in Electromagnetic Compatibility (EMC), 2011 IEEE International Symposium on , vol., no., pp.925-930, 14-19 Aug. 2011 doi: 10.1109/ISEMC.2011.6038441

[18] Hubing, T., "PCB EMC design guidelines: a brief annotated list," in Electromagnetic Compatibility, 2003 IEEE International Symposium on , vol.1, no., pp.34-36 vol.1, 18-22 Aug. 2003 doi: 10.1109/ISEMC.2003.1236559

[19] TPS62360 Datasheet, Texas Instruments [Online]. Available: http://www.ti.com/lit/gpn/tps62360

[20] Developing Tamper Resistant Designs with Xilinx Virtex-6 and 7 Series FPGAs (XAPP1084), Xilinx [Online]. Available: http://tinyurl.com/p32ez9f

[21] FPGA IFF Copy Protection Using Dallas Semiconductor/Maxim DS2432 Secure EEPROMs (XAPP780), Xilinx [Online]. Available: http://tinyurl.com/nglv9mf

[22] Side-channel attack standard evaluation board (SASEBO), http://www.morita-tech.co.jp/SASEBO/en/index.html, Morita Tech. Co., Ltd. SASEBO Web Site.