COMPACT FPGA HARDWARE PLATFORM FOR POWER ANALYSIS ATTACKS ON CRYPTOGRAPHIC ALGORITHMS IMPLEMENTATIONS

Martin PETRVALSKY*, Milos DRUTAROVSKY*, Michal VARCHOLA*,**
*Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics, Technical University of Košice, Letna 9, 042 00 Košice, Slovak Republic, E-mail: martin.petrvalsky@tuke.sk, milos.drutarovsky@tuke.sk
**ELIT SYSTEMS, s. r. o. Košice, Slovak Republic, E-mail: michal@varchola.sk

ABSTRACT

In this paper, we present a compact hardware platform for power analysis attacks such as a differential power analysis attack. The board is equipped with FPGA chip (namely Altera Cyclone III) and four different measurement points. We provide hardware details of the presented platform and we thoroughly present each of the points dedicated for power consumption measurements. They are used for an extraction of vulnerable information through the power counsumption measured during cryptographic operations. In addition, we provide an example of the power analysis attack based on the differential power analysis. We show properties of the board using attacks on straightforward AES S-box operations and on scalable multiplications in the elliptic curve digital signature algorithm.

Keywords: *Altera Cyclone III, cryptography, differential power analysis, FPGA evaluation board, measurement points*

1. INTRODUCTION

Embedded devices running implementations of cryptographic algorithms such as Field-Programmable Gate Arrays (FPGAs) or MicroController Units (MCUs) are often targets for Side-Channel Attacks (SCAs) [1]. Power consumption [2], electromagnetic [3] or acoustic waves [4], temperature [5] and running time [6] of cryptographic algorithms can leak secret information to an adversary. If we aim for a secure system, the vulnerable algorithms have to be protected from aforementioned attacks by using countermeasures.

We focus on attacks based power consumption analysis and their countermeasures, especially on a Correlation Based Differential Power Analysis (CBDPA) [7]. Other power analysis attacks are for example Simple Power Analysis (SPA) [8] which can extract secret information from a shape of a single power consumption trace or other Differential Power Analyses (DPA) [9] which uses statistical tools to recover vulnerable data.

We choose Advanced Encryption Standard (AES) [10] as attacked algorithm so we can easily test our new platform. AES is a standard which is often a target of attacks in research of SCAs so results can be compared with other attack implementations. Our team is focused on research of Elliptic Curve Cryptography (ECC) [11], especially Digital Signature Algorithm based on ECC (ECDSA) [12, 13]. Thus, the second demonstrated attack on an algorithm, the multi-precision multiplication that is a part of the ECDSA.

In order to develop new attacks and especially new countermeasures, researchers need to have reference platforms where experiments with reproducible conditions can be performed. The development of countermeasures requires highest possible signal to noise ratio to detect most of the leakage.

One of the most widespread boards for SCA based on FPGA is Side-channel Attack Standard Evaluation BOard (SASEBO) [14]. Examples of boards based on MCU are INSTAC-8 and INSTAC-32 used in [15] developed by Tamper-Resistance Standardization research Committee (TRSC). Our research team uses a custom evaluation board based on MCU (e.g. in [16]) with which we detect new attacks and develop new countermeasures for cryptographic algorithms implementations implemented on MCUs.

2. PLATFORM AND MEASUREMENT SETUP

We present a special DIgital SIgnature Power Analysis (DISIPA) platform (Fig. 1) which is designed especially for the purpose of side channel power analyses attack of the Altera Cyclone III FPGA. Our system provides the following features:

- classic (**2**) and new measurement points (**1, 3, 4**) (Fig. 2, Fig. 3):
  1. current flow from the power supply to a linear regulator measured as voltage drop on resistor **R1** (typically, a value of resistors is 1 Ω) using connectors **A** and **B** (a differential probe or two oscilloscope channels are needed),
  2. current flow from a linear regulator to the FPGA measured as voltage drop on resistor **R2** using connectors **C** and **D** (a differential probe or two oscilloscope channels are needed),
  3. voltage on a decoupling capacitor **C3** using connector **E** (can be measured by a single-ended probe),
  4. current flow from a decoupling capacitor **C4** to the FPGA measured as voltage drop on resistor **R4** using connector **F** (can be measured by a single-ended probe),
- an Electro-Magnetic Interference (EMI) shield which protects the entire DISIPA board against an external electromagnetic pollution,
- strong analog Murata filters are assembled on a power line in order to minimize noise from the power supply (as well as leaks from the board),
- the FPGA device and measurement points circuitry have their own chambers in the EMI shield. Lin-

ear regulators, filters, configuration circuitry, input/output circuitry, and the main Murata filter have separate chambers as well.

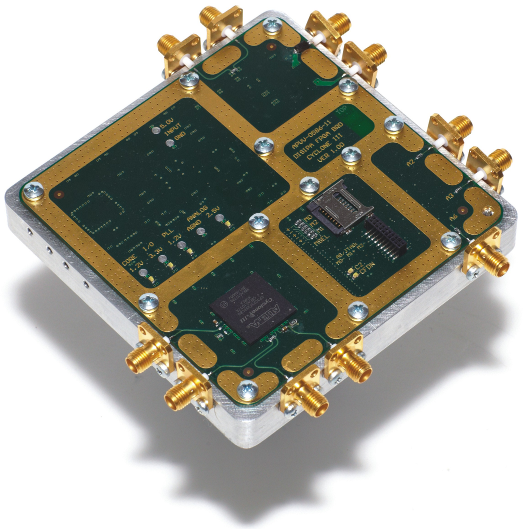

Fig. 1 Structure of the new DISIPA platform based on Altera Cyclone III FPGA. The platform includes the EMI shield (upper lid is not shown) and 11 SMA connectors.

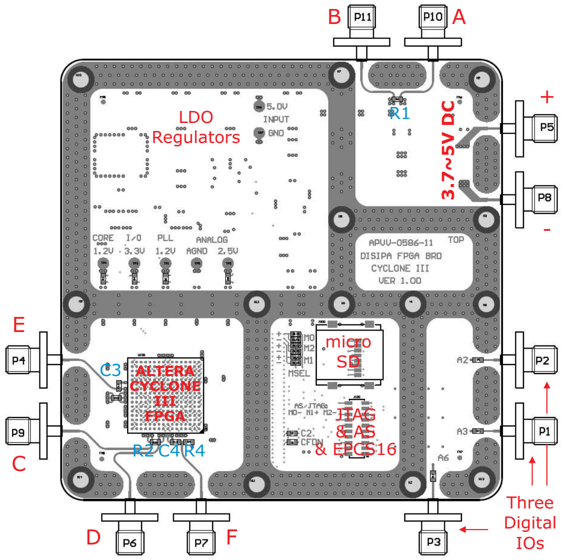

Fig. 2 The DISIPA side channel analysis platform drawing with description. The board includes three digital input-output connectors (IOs), six measurement connectors (**A–F**) and two connectors for power supply (**+, -**). The platform is divided into several "chambers" containing different components. These components are shielded not only against external electromagnetic pollution but also against mutual EMI between various parts of the platform.

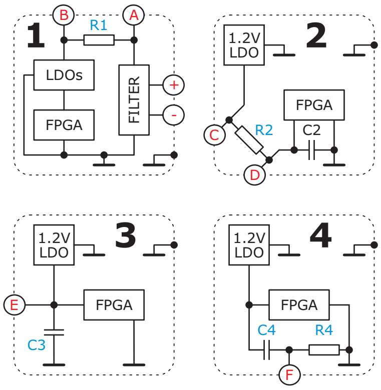

Fig. 3 Four measurement points with different electronic topology are implemented in DISIPA platform in order to compare their properties for the CBDPA. These measurement points provides clean view on a current flow from the power supply to a linear regulator (**1**), current flow from a linear regulator to the FPGA (**2**), voltage on the decoupling capacitor **C3** (**3**) and current flow from the decoupling capacitor **C4** (**4**).

Described improvements enhance signal-to-noise ratio of the leakage. In other words, they reduce the number of traces needed for a successful CBDPA attack. We intend to get as clean leakage signal as possible with this platform in order to assess the strength of particular countermeasures. It can turn out that simple (but efficient) EMI shielding, or the usage of another measurement point causes otherwise secure CBDPA countermeasure to be inadequate. The main advantage in comparison to SASEBO board [14] is possibility of EMI/EMC shielding by the aluminum box which protects the board against an external electromagnetic pollution.

According to our experience, all measurement points (new and old) can be used for CBDPA. The best CBDPA attack results (in the meaning of higher success rate and lower complexity of the attack) are achieved using the measuring point given in Fig. 4, which is modified measuring point 3 in Fig. 3. In order to enhance signal-to-noise ratio, low-noise wide-band amplifier with +35 dB gain is used. DC part of the signal is removed by DC-blocking capacitor. We use the Agilent DSO9404A digital oscilloscope for power consumption measurements (Fig. 5).

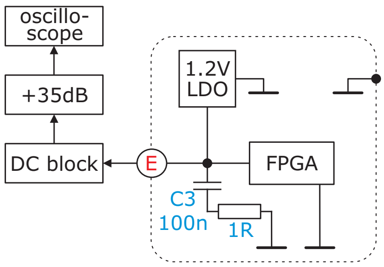

Fig. 4 The modified measuring point **3** used for power traces acquisition with its own measurement setup. The modification gives us the best results (leakage-noise ratio) among the measurement points.

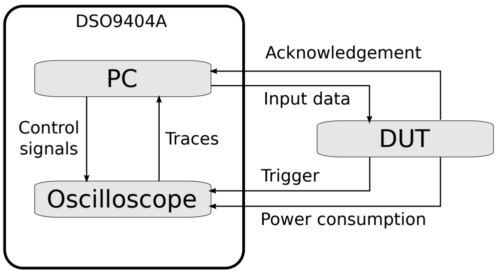

Fig. 5 Workflow of the power traces acquisition – the whole process is controlled by a software running on oscilloscope's PC. Firstly, the PC sets up the oscilloscope (channels, number of samples, sample rate, ranges, trigger, etc.). Afterwards, PC sends the data to a Device Under Test (DUT). The device rises a trigger, starts an algorithm and after it finishes, it clears the trigger. The oscilloscope measures power consumption while DUT executes the cryptographic algorithm. Finally, the PC saves the power consumption traces to a hard-disk drive. In next step, PC sends new data and the process is repeated until the desired number of traces is reached.

3. EXPERIMENTAL RESULTS

For the new DISIPA platform testing, we perform attacks for two types of operations. Firstly, we deploy a CBDPA on the AES algorithm. We target byte substitution operation S-box. We used this attack to calibrate the platform since we know what results should be obtained from our previous research. Secondly, we attack a multiplication operation of the ECDSA algorithm using the CBDPA as well.

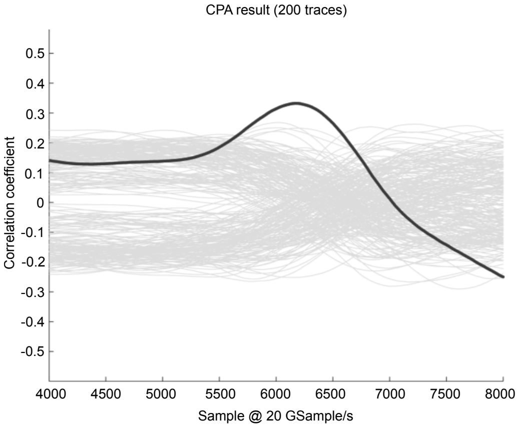

Fig. 6 Detail of correlation analysis results for the AES substitution byte operation using 200 power consumption traces. The bold line represents a correlation vector for the correct hypothesis. Gray lines represent false hypotheses. The attack is successful if the correct hypothesis correlation coefficient significantly and repeatedly differs from other hypotheses coefficients. Location of this difference points at the moment when a vulnerable intermediate value is processed (around sample 6,200 in this figure).

We use measuring point **4** for attacking the unprotected implementation AES. Attack on the ECDSA was performed using modified measuring point **3** with modification depicted in Fig. 4. We apply (1) in order to evaluate the coefficients for CBDPA attacks. Coefficients with higher values represents a higher similarity of measured traces with the currently tested hypothesis.

$$r_{H,X}(\eta) = \frac{\sum_{i=1}^{N}[(X_i(\eta) - \bar{X}(\eta))(H_i - \bar{H})]}{\sqrt{\sum_{i=1}^{N}[X_i(\eta) - \bar{X}(\eta)]^2 \sum_{i=1}^{N}(H_i - \bar{H})^2}} \qquad (1)$$

where $r_{H,X}(\eta)$ is Pearson's correlation coefficient for η-th sample (measured during the cryptographic algorithm evaluation), N is a number of traces, $X_i(\eta)$ is a value of η-th sample measured during i-th measurement (i-th trace), $\bar{X}(\eta)$ is a mean value of corresponding η-th samples (from all traces), H_i is a hypothesis of power consumption for one value of input data corresponding with i-th measurement (i-th trace) and $\bar{H}$ is a mean value of all hypotheses H_i.

3.1. Attack on the Byte Substitution in the AES Algorithm

We attack the byte substitution operation in the first round of the unprotected AES algorithm [10]. The first step of AES (after receiving 128-bit input data c represented as 16 bytes $c_1, c_2, ..., c_{16}$) is addition in $GF(2^8)$ with 128-bit secret key k. The addition is done byte by byte using bitwise exclusive or ($\oplus$) operation: $s_i = k_i \oplus c_i$. Afterwards, the attacked operation follows - byte substitution $S_i = SBOX(s_i)$. Byte substitution is often done by a lookup table.

We can reliably recover correct key byte using 200 power consumption traces. The results of attacking the S-box operation of the AES algorithm are depicted in Fig. 6, Fig. 7 and Fig. 8. Excellent results are achieved when traces with the same inputs are averaged together (Fig. 8).

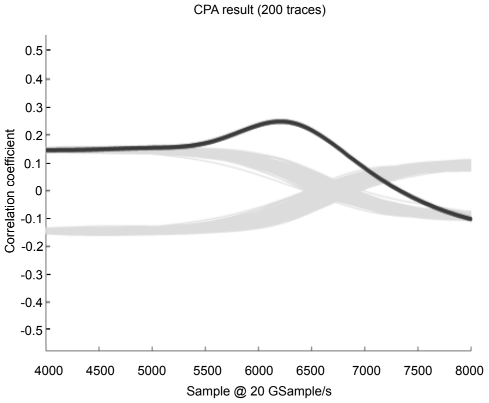

Fig. 7 Detail of correlation analysis results for the AES substitution byte operation using 16,000 power consumption traces. The bold line represents a correlation vector of the correct hypothesis. Gray lines represent false hypotheses. Compared to Fig. 6, the noise in correlation analysis is reduced with increasing number of traces.

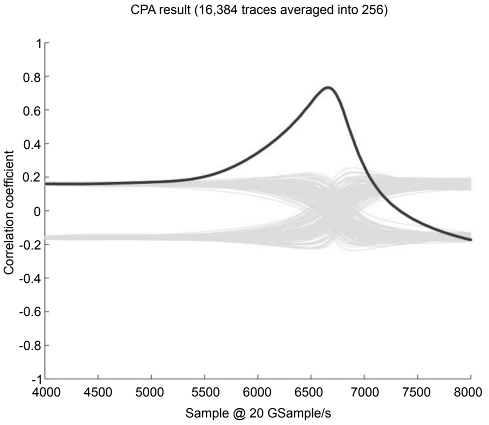

Fig. 8 Detail of correlation analysis results for the AES substitution byte operation where we measure 16,386 power consumption traces with 256 different bytes inputs and then we average traces with the same input resulting 256 averaged traces on which we perform the attack. Compared to Fig. 7 we obtain better results (higher ratio between correct hypothesis and false hypotheses correlation coefficients) by applying averaging of the traces.

Moreover, despite the strong filtration of the power line, we were able to perform a successful CBDPA attack by acquiring traces on the external power cord (before **+** and **-** connectors in Fig. 2). The distance between the board and a measurement point was approximately 50 cm. We used a cascade of two 35 dB amplifiers (70 dB in total) and enhanced pre-processing of acquired traces based on an investigation of clock-frequency harmonics. Thus, we needed 500,000 traces to perform a successful attack on a single byte substitution operation. An interesting fact is that the otherwise narrow correlation peak (only few clock cycles when measured directly on the FPGA measurement points) was spread out in time for at least 100 clock cycles. This effect is caused by the strong filtration which stretches a signature of the side-channel leakage in the time domain. The amplitude of clock-frequency harmonics was just several tens of nanovolts.

3.2. Attack on the Scalable Multiplication in a Protected ECDSA

Another example of an application of the platform is an attack on a scalable multi-precision multiplication used in the ECDSA. A successful collision power analysis is performed attacking final signature computation of the ECDSA (where the private key d_A is combined with ephemeral private key k_{priv}, hash of the message e and the ephemeral public key k_{pub}). Results of the attack is shown in Fig. 9. More details can be found in [12].

4. CONCLUSION

In this paper, we described a novel compact hardware platform based on FPGA which is dedicated for delicate power consumption measurement and thus for side-channel attacks research. The Altera Cyclone III FPGA board was used as a reference platform in the DISIPA project. Our board allows 4 different topologies for measurements and high resistance against noise (EMI shield, strong Murata filters, special design of the FPGA and measurement points).

We proved that all measurement points are usable in terms of CBDPA attacks. Furthermore, we performed a successful attack measured on an external power cord. In this work, we demonstrated main features of the board on two example attacks. Firstly, we successfully attacked AES byte substitution operation using CBDPA. Secondly, we deploy the attack on scalable multiplication operations of the ECDSA algorithm which was successful as well.

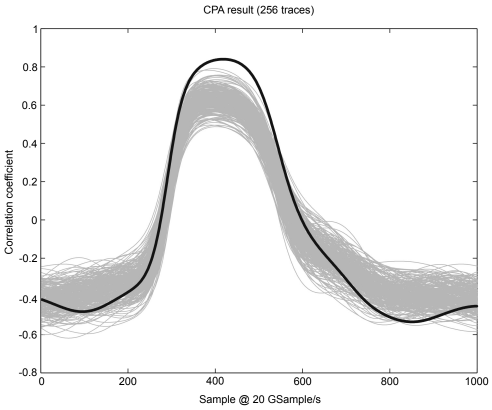

Fig. 9 Detail of correlation analysis result for the second multiplication for $d_A(i) = 0x49$. The low pass filtering with cutoff frequency of $4.5\times$ clock frequency is used. The bold line represents a correlation vector for the both multiplications identical intermediate value.

In the future research, we will closely test each of the measurement points and evaluate their effectiveness. Furthermore, we will develop similar platform for MCUs and other embedded cryptographic devices which will be similarly tested as FPGAs.

ACKNOWLEDGEMENT

This work was performed in the framework of the COST Action IC1204 (Trustworthy Manufacturing and Utilization of Secure Devices). The Altera Cyclone III FPGA board was developed and sponsored by the DISIPA project. This work was supported by the Slovak Research and Development Agency, project number APVV-0586-11.

REFERENCES

[1] ZHOU, Y. – FENG, D.: Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing, 2005. http://eprint.iacr.org/2005/388.

[2] MANGARD, S. – OSWALD, E. – POPP, T.: *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[3] HOMMA, N. – AOKI, T. – SATOH, A.: Electromagnetic information leakage for side-channel analysis of cryptographic modules. In *Electromagnetic Compatibility (EMC), 2010 IEEE International Symposium on* (2010), pp. 97–102.

[4] SIMON, L. – ANDERSON, R.: Pin skimmer: Inferring pins through the camera and microphone. In *Proceedings of the Third ACM Workshop on Security and Privacy in Smartphones & Mobile Devices* (2013), SPSM '13, pp. 67–78.

[5] BROUCHIER, J. – KEAN, T. – MARSH, C. – NACCACHE, D.: Temperature attacks. *Security Privacy, IEEE 7*, 2 (2009), 79–82.

[6] BRUMLEY, B. B. – TUVERI, N.: Remote Timing Attacks Are Still Practical. *Computer Security – ESORICS 2011: 16th European Symposium on Research in Computer Security, Leuven, Belgium, September 12-14, 2011. Proceedings.* Springer Berlin Heidelberg, Berlin, Heidelberg, 2011, pp. 355–371.

[7] BRIER, E. – CLAVIER, C. – OLIVIER, F.: Correlation Power Analysis with a Leakage Model. *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings.* Springer Berlin Heidelberg, Berlin, Heidelberg, 2004, pp. 16–29.

[8] WU, K. – LI, H. – CHEN, T. – YU, F.: Simple power analysis on elliptic curve cryptosystems and countermeasures: Practical work. In *Electronic Commerce and Security, 2009. ISECS '09. Second International Symposium on* (2009), vol. 1, pp. 21–24.

[9] KOCHER, P. C. – JAFFE, J. – JUN, B. – ROHATGI, P.: Introduction to differential power analysis. *J. Cryptographic Engineering 1*, 1 (2011), 5–27.

[10] DAEMEN, J. – RIJMEN, V.: *The Design of Rijndael: AES - The Advanced Encryption Standard.* Information Security and Cryptography. Springer Berlin Heidelberg, 2002.

[11] HANKERSON, D. – MENEZES, A. J. – VANSTONE, S.: *Guide to Elliptic Curve Cryptography.* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.

[12] VARCHOLA, M. – DRUTAROVSKY, M. – REPKA, M. – ZAJAC, P.: Side channel attack on multiprecision multiplier used in protected ecdsa implementation. In *2015 International Conference on ReConFigurable Computing and FPGAs (ReConFig)* (Dec. 2015), pp. 1–6.

[13] GLAS, B. – SANDER, O. – STUCKERT, V. – MÜLLER-GLASER, K. D. – BECKER, J.: Prime field ECDSA signature processing for reconfigurable embedded systems. *Int. J. Reconfig. Comp. 2011* (2011), 1–12.

[14] Side-channel Attack Standard Evaluation Board (SASEBO). http://satoh.cs.uec.ac.jp/SASEBO/en/index.html

[15] HUTTER, M. – KIRSCHBAUM, M. – PLOS, T. – SCHMIDT, J.-M. – MANGARD, S.: Exploiting the difference of side-channel leakages. In *Constructive Side-Channel Analysis and Secure Design - COSADE 2012, 3rd International Workshop, Darmstadt, Germany, May 3-4, 2012, Proceedings.* (2012), vol. 7275 of *Lecture Notes in Computer Science*, Springer, pp. 1 – 16.

[16] PETRVALSKY, M. – DRUTAROVSKY, M. – VARCHOLA, M.: Differential power analysis attack on ARM based AES implementation without explicit synchronization. In *Radioelektronika (RADIOELEKTRONIKA), 2014 24th International Conference* (April 2014), pp. 1–4.

Received April 21, 2016, accepted June 1, 2016

BIOGRAPHIES

Martin Petrvalsky was born on the 16th of September, 1988 in Pribram. He received his Bachelor's degree in 2010 and Master's degree in 2012 in Technical University of Košice. He graduated from Department of Electronics and Multimedia Communications from Faculty of Electrical Engineering and Informatics. He is a Ph.D. student in Department of Electronics and Multimedia Communications. His current research focuses on side channel attacks on embedded devices and its countermeasures.

Milos Drutarovsky was born in Prešov in Slovak Republic, in 1965. He received his Ing. (M.Sc.) degree and Ph.D. degree in Radioelectronics from the Faculty of Electrical Engineering, Technical University of Košice, in 1988 and 1995, respectively. He defended his habilitation work - Digital Signal Processors in Digital Signal Processing in 2000. He is currently working as an associate professor at the Department of Electronics and Multimedia Communications of the Faculty of Electrical Engineering and Informatics, Technical University of Košice. His current research focuses on embedded electronics, applied cryptography, algorithms and architectures for embedded cryptographic architectures, digital signal processing, digital signal processors, field programmable devices and soft microcontrollers embedded into FPGA circuits.

Michal Varchola was born in Košice in Slovak Republic, in 1984. He finished Secondary Electrotechnical School in Košice in the field of Automation Technology, in 2002. He received his Ing. (M.Sc.) degree in Electronics and Communication Technologies from Faculty of Electrical Engineering and Informatics, Technical University of Košice, in 2007. He successfuly defended his Philosophiae Doctor (Ph.D.) degree in Infoelectronics from Faculty of Electrical Engineering, Technical University of Košice on August 27, 2010 under supervision of Assoc. Prof. Milos Drutarovsky, Ph.D. His main research area is Cryptography for Embedded Systems and particularly Cryptographic True Random Number Generators (TRNGs) for Field Programmable Gate Arrays (FPGAs).