

# Hardware Security

Edited by

Osnat Keren<sup>1</sup>, Ilia Polian<sup>2</sup>, and Mark M. Tehranipoor<sup>3</sup>

1 Bar-Ilan University, IL, [osnat.keren@biu.ac.il](mailto:osnat.keren@biu.ac.il)

2 Universität Passau, DE, [ilia.polian@uni-passau.de](mailto:ilia.polian@uni-passau.de)

3 University of Florida – Gainesville, US, [tehranipoor@ece.ufl.edu](mailto:tehranipoor@ece.ufl.edu)

---

## Abstract

This report documents the program and outcomes of Dagstuhl Seminar 16202 “Hardware Security”, which was held in Schloss Dagstuhl – Leibniz Center for Informatics from May 16–20, 2016. This seminar aims to bring together a group of researchers, who are actively involved in the design and the security assessment of hardware primitives. The seminar was organized around presentations given by several participants on their current research, and ongoing work. In addition to these presentations, the program also included three discussion sessions, and two special sessions on curriculum development and funding programs. The seminar was indeed successful in familiarizing the researchers with recent developments in hardware security field of study, providing better understanding of still unsolved problems, and pointing out future research directions.

The paper is further organized as follows. Section 1 summarizes the most important goals of the seminar. Section 3 is devoted to the abstracts of the presentations given in the seminar, whereas in Section 4 the abstracts of the discussion sessions are provided.

**Seminar** May 16–20, 2016 – <http://www.dagstuhl.de/16202>

**1998 ACM Subject Classification** B.7.m [Integrated Circuits] Miscellaneous, C.3 [Special-Purpose and Application-Based Systems] Smartcards and Real-time and Embedded Systems, E.3 [Data Encryption] Code Breaking and Standards, E.4 [Coding and Information Theory] Error Control Codes, I.2.6 [Learning] Concept Learning, K.6.5 [Security and Protection] Authentication and Unauthorized Access

**Keywords and phrases** Hardware security; Passive and active side-channel analysis; Machine learning; Cryptographic blocks; True random number generators; Physically unclonable functions; Hardware Trojan

**Digital Object Identifier** 10.4230/DagRep.6.5.72

**Edited in cooperation with** Fatemeh Ganji

## 1 Executive Summary

*Osnat Keren*

*Ilia Polian*

*Mark M. Tehranipoor*

**License**  Creative Commons BY 3.0 Unported license  
© Osnat Keren, Ilia Polian, and Mark M. Tehranipoor

The convergence of IT systems, data networks (including but not limited to the Internet) and ubiquitous embedded devices within the cyberphysical system paradigm has led to the emergence of new security threats associated with the system hardware. Manipulating the hardware components that implement security functions can compromise system integrity,



Except where otherwise noted, content of this report is licensed under a Creative Commons BY 3.0 Unported license

Hardware Security, *Dagstuhl Reports*, Vol. 6, Issue 5, pp. 72–93

Editors: Osnat Keren, Ilia Polian, and Mark M. Tehranipoor



DAGSTUHL  
REPORTS

Dagstuhl Reports  
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

provide unauthorized access to protected data, and endanger intellectual property. Additionally, secure hardware is required to protect software in a proper manner tampering. Addressing these vulnerabilities is essential in order to prevent the hardware from becoming the Achilles heel of today's systems. Current technology trends point towards massive utilization of hardware circuits in larger cyberphysical systems that are interacting with the physical environment via sensors and actuators. At the same time cyberphysical systems are more and more integrated via open networks, most notably the Internet. Moreover, they interact with each other, forming systems of systems that exhibit highly complex, emergent behavior and constantly change their boundaries, with new sub-systems continuously entering and leaving. As a consequence, hardware-related threats must be addressed by appropriate countermeasures at realistic costs.

The seminar will focus on security threats where hardware components play the main role, and on countermeasures to address these threats. The emphasis is on generic algorithmic advances on the boundary between computer science and other disciplines. While Hardware Security is a very diverse scientific field, the seminar will specifically focus on its three main areas: passive and active side-channel analysis of security-relevant hardware components (cryptographic blocks, true random number generators) which goes beyond classical cryptanalysis; physical unclonable functions (PUFs) and authentication solutions on their basis; and new threats through hardware Trojans and counterfeit ICs as well as techniques for their detection and neutralization.

## 2 Table of Contents

### Executive Summary

|  |    |
|--|----|
| <i>Osnat Keren, Ilia Polian, and Mark M. Tehranipoor</i> . . . . . | 72 |
|--|----|

### Overview of Talks

|  |    |
|--|----|
| Dismantling real-world ECC with Horizontal and Vertical Template Attacks<br><i>Lejla Batina</i> . . . . .  | 76 |
| Machine Learning Attacks on Delay Based PUFs and Protocols<br><i>Georg T. Becker</i> . . . . .   | 76 |
| Hardware Security in Advanced CMOS Technologies<br><i>Wayne P. Burlison</i> . . . . .  | 77 |
| Metastable Latches: a Boon for Combined PUF/TRNG Designs<br><i>Jean-Luc Danger</i> . . . . .   | 78 |
| Security and Privacy of Non-Volatile Memories<br><i>Swaroop Ghosh</i> . . . . .  | 78 |
| Protecting Cryptographic Components in Hardware against Side-Channel and Fault-Injection Attacks<br><i>Tim Erhan Güneysu, Amir Moradi, and Tobias Schneider</i> . . . . .  | 79 |
| On the Synthesis of Side-Channel resistant Cryptographic Modules<br><i>Sorin A. Huss</i> . . . . .   | 79 |
| Hardware Security – Industrial Experiences<br><i>Michael Hutter</i> . . . . .  | 80 |
| Security Oriented Codes<br><i>Osnat Keren</i> . . . . .  | 80 |
| Practical Aspects of Integrating PUFs in Industrial Applications<br><i>Roel Maes</i> . . . . .   | 82 |
| Side-Channel Security through Dynamic Reconfiguration: a Trade-off between Granularity and Side-Channel Resistance?<br><i>Nele Mentens</i> . . . . .   | 82 |
| Fault Space Transformation: A Generic Approach to Counter Differential Fault Analysis and Differential Fault Intensity Analysis on AES-like Block Ciphers<br><i>DebdEEP Mukhopadhyay and Sikhar Patranabis</i> . . . . . | 83 |
| PUFs in AMD64 CPUs and GPUs<br><i>Ruben Niederhagen, Daniel J. Bernstein, and Pol Van Aubel</i> . . . . .  | 83 |
| Practical HW Security Attacks That Require Minimal Reverse Engineering<br><i>Elad Peer</i> . . . . .   | 84 |
| Trojans in Early Design Steps – An Emerging threat<br><i>Ilia Polian</i> . . . . .   | 84 |
| Virtual Proofs of Reality and Their Physical Implementation<br><i>Ulrich Rührmair</i> . . . . .  | 85 |
| Constructive Side-Channel Analysis<br><i>Werner Schindler</i> . . . . .  | 85 |

|  |    |
|--|----|
| Error Correction Schemes for Physical Unclonable Functions<br><i>Georg Sigl</i> . . . . .      | 86 |
| No Place to Hide: Contactless Probing of Secret Data on FPGAs<br><i>Shahin Tajik</i> . . . . . | 87 |
| Unlocking the Potential of Hardware Security<br><i>Mark M. Tehranipoor</i> . . . . .           | 88 |
| <b>Discussion Sessions</b>   |    |
| PUFs and Security Components<br><i>Domenic Forte</i> . . . . .                                 | 88 |
| Design for Security<br><i>Wayne P. Burleson and Ilia Polian</i> . . . . .                      | 89 |
| Side Channel Analysis<br><i>Debdeep Mukhopadhyay and Ilia Polian</i> . . . . .                 | 91 |
| <b>Participants</b> . . . . .  | 93 |

### 3 Overview of Talks

#### 3.1 Dismantling real-world ECC with Horizontal and Vertical Template Attacks

*Lejla Batina (Radboud University Nijmegen, NL)*

**License** © Creative Commons BY 3.0 Unported license  
© Lejla Batina

**Joint work of** Margaux Dugardin, Louiza Papachristodoulou, Zakaria Najm, Lejla Batina, Jean-Luc Danger, Sylvain Guilley, Jean-Christophe Courrege, and Carine Therond

**Main reference** M. Dugardin, L. Papachristodoulou, Z. Najm, L. Batina, J.-L. Danger, S. Guilley, J.-C. Courrege, C. Therond, “Dismantling real-world ECC with Horizontal and Vertical Template Attacks”, in Proc. of the 7th Int’l Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE’16), LNCS, Vol. 9689, pp. 88–108, Springer, 2016; pre-print available from IACR.

**URL** [http://dx.doi.org/10.1007/978-3-319-43283-0\\_6](http://dx.doi.org/10.1007/978-3-319-43283-0_6)

**URL** <http://eprint.iacr.org/2015/1001>

Recent side-channel attacks on elliptic curve algorithms have shown that the security of these cryptosystems is a matter of serious concern. The development of techniques in the area of Template Attacks makes it feasible to extract a 256-bit secret key with only 257 traces. This paper enhances the applicability of this attack by exploiting both the horizontal leakage of the carry propagation during the finite field multiplication, and the vertical leakage of the input data. As a further contribution, our method provides detection and auto-correction of possible errors that may occur during the key recovery. These enhancements come at the cost of extra traces, while still providing a practical attack. Finally, we show that the elliptic curve technology developed in PolarSSL running on a ARM STM32F4 platform is completely vulnerable, when used without any modifications or countermeasures.

#### 3.2 Machine Learning Attacks on Delay Based PUFs and Protocols

*Georg T. Becker (Ruhr-Universität Bochum, DE)*

**License** © Creative Commons BY 3.0 Unported license  
© Georg T. Becker

**Main reference** G. T. Becker, “The gap between promise and reality: on the insecurity of XOR arbiter PUFs”, in Proc. of the 17th Int’l. Workshop on Cryptographic Hardware and Embedded Systems (CHES’15), LNCS, Vol. 9293, pp. 535–555, Springer, 2015.

**URL** [http://dx.doi.org/10.1007/978-3-662-48324-4\\_27](http://dx.doi.org/10.1007/978-3-662-48324-4_27)

In this talk I give an overview of the current state-of-the-art in machine learning attacks on XOR Arbiter PUFs and argue why we are far away from building secure Strong PUFs. In particular, I present the Reliability-based Machine Learning attack I introduced last year at CHES.

##### References

- 1 G. T. Becker. On the Pitfalls of Using Arbiter-PUFs as Building Blocks. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 34(8), 2015.

### 3.3 Hardware Security in Advanced CMOS Technologies

Wayne P. Burleson (*University of Massachusetts – Amherst, US*)

License © Creative Commons BY 3.0 Unported license  
© Wayne P. Burleson

Joint work of See References

CMOS technology trends pose challenges and opportunities for Hardware Security design, applications and threats. VLSI research has evolved over the last decades, solving design problems related to area, timing, power, testing, and others, but most recently, security and privacy have moved to the forefront. Driving applications have also advanced to smaller and more autonomous systems, culminating in the Internet of Things which requires rethinking of security and privacy requirements and solutions at both the thing and cloud level. Implantable medical devices in particular present unique design constraints and threat models. Variations in advanced CMOS technology and operating environment present challenges and opportunities related to security, illustrated in three recent research projects : 1) Hardware Trojans present a real vulnerability during untrusted design/manufacturing especially in random number generation where functional validation is difficult. 2) Variations in the data retention time of memory cells can be used as a static entropy source, also known as physical unclonable functions (PUF), however reliably extracting this entropy across temperature variation requires novel processing based on ranking and hashing functions. 3) Environmental variations that impact PUFs can be used for virtual proofs of physical reality, a powerful new concept and capability in hardware security. Finally, on-chip sensor networks to monitor behavior and variations can be used to detect vulnerabilities, however can introduce their own vulnerabilities if not secured across untrusted processes in multi-core processors. Many open problems remain in all of these areas, from specific application and implementation issues, to novel attacks and countermeasures.

#### References

- 1 S. Ghoreishizadeh, T. Yalçin, A. Pullini, G. De Micheli, W. Burleson, S. Carrara, A Light-weight Cryptographic System for Implantable Biosensors. In IEEE Biomedical Circuits and Systems Conf. (BioCAS), 2014.
- 2 G.T. Becker, F. Regazzoni, C. Paar and W. Burleson, Stealthy Dopant-Level Hardware Trojans. In Workshop on Cryptographic Hardware and Embedded Systems (CHES), 2013.
- 3 X. Xu, A. Rahmati, D. Holcomb, K. Fu, W. Burleson, Reliable Physical Unclonable Functions Using Data Retention Voltage of SRAM Cells, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015.
- 4 U. Ruhrmair, J. Martinez-Hurtado, X. Xu, C. Kraeh, C. Hilgers, D. Kononchuk, J. J. Finley, and W. P. Burleson. Virtual Proofs of Reality and their Physical Implementation. In IEEE Symp. on Security and Privacy, 2015.
- 5 S. Madduri, R. Vadlamani, W. Burleson and R. Tessier, A Monitor Interconnect and Support Subsystem for Multicore Processors, In Design, Automation and Test in Europe (DATE), 2009.

### 3.4 Metastable Latches: a Boon for Combined PUF/TRNG Designs

*Jean-Luc Danger (ENST – Paris, FR)*

License  Creative Commons BY 3.0 Unported license  
© Jean-Luc Danger

This talk presents a way to take advantage of simple latches to generate both a TRNG and a PUF. The main idea is to place the latch very close to its metastable state. Hence a small noise will make the latch converge towards a stable state either ‘0’ or ‘1’. This corresponds to the TRNG application. This concept can work only if many latches are placed in parallel as it is not possible to get a metastable state for most of the latches. At this point it is possible to use these former latches as a PUF as they are always in a stable state ‘0’ and ‘1’ which depends only on the process variation. This talk gives methods on how to obtain the set of  $N$  latches to have good TRNG (given an expected entropy) and a good PUF (in term of Bit error rate).

### 3.5 Security and Privacy of Non-Volatile Memories

*Swaroop Ghosh (University of South Florida, US)*

License  Creative Commons BY 3.0 Unported license  
© Swaroop Ghosh

Non-volatile memories (NVM) such as Spin-Transfer Torque RAM (STTRAM), Resistive RAM and Domain Wall Memory have drawn significant attention due to complete elimination of bitcell leakage. In addition to plethora of benefits such as density, non-volatility, low-power and high-speed, majority of NVMs are also compatible with CMOS technology enabling easy integration. Although promising, I will show that NVMs bring new security and privacy challenges that were absent in their conventional volatile memory counterparts. Assuring data integrity and privacy against malicious attacks is particularly critical on deployed systems that are hard to maintain and enforce physical security. I will present two aspects to NVM security in Last Level Cache (LLC) using STTRAM as test case: (i) Data integrity which pertains to data corruption by malicious attack with the intention to launch denial-of-service. Such attacks exploit the fact that NVMs are fundamentally susceptible to ambient parameters such as magnetic field and temperature. I will describe these vulnerabilities and attack models, and, propose two micro-architectural techniques to assure data integrity under attack namely, cache bypassing and checkpointing. These techniques allow seamless computation in presence of attack at minimal design overhead. (ii) Data privacy which pertains to sensitive data such as keys and passwords being compromised. Storage such as Hard Disk Drive (HDD) has been the non-volatile part of memory system traditionally protected by encryption. Although effective, the latency associated with encryption makes it non-trivial for application in higher levels of memory stack such as LLC. I will present the vulnerabilities and attack models, and, propose two low-overhead techniques to maintain data privacy namely, Semi Non-Volatile Memory which is similar to NVM but with very low retention time so that the data vanishes after power is turned OFF, and, irreversible erasure of data at power down using residual charge from power rail.

### 3.6 Protecting Cryptographic Components in Hardware against Side-Channel and Fault-Injection Attacks

*Tim Erhan Güneysu (Universität Bremen, DE), Amir Moradi, and Tobias Schneider*

**License** © Creative Commons BY 3.0 Unported license  
 © Tim Erhan Güneysu, Amir Moradi, and Tobias Schneider  
**Joint work of** Tobias Schneider, Amir Moradi, and Tim Güneysu  
**Main reference** T. Schneider, A. Moradi, T. Güneysu, “ParTI – Towards Combined Hardware Countermeasures against Side-Channel and Fault-Injection Attacks”, in Proc. of the 36th Annual Int’l Cryptology Conference – Advances in Cryptology (CRYPTO’16), LNCS, Vol. 9815, pp. 302–332, Springer, 2016.  
**URL** [http://dx.doi.org/10.1007/978-3-662-53008-5\\_11](http://dx.doi.org/10.1007/978-3-662-53008-5_11)

Side-channel analysis and fault-injection attacks are known as major threats to any cryptographic implementation. Hardening cryptographic implementations with appropriate countermeasures is thus essential before they are deployed in the wild. However, countermeasures for both threats are of completely different nature: Side-channel analysis is mitigated by techniques that hide or mask key-dependent information while resistance against fault-injection attacks can be achieved by redundancy in the computation for immediate error detection. Since already the integration of any single countermeasure in cryptographic hardware often comes with significant costs with respect to performance and area, a combination of multiple countermeasures is expensive and often even associated with undesired side effects.

In this talk, we introduce a countermeasure for cryptographic hardware implementations that combines the concept of a provably-secure masking scheme based on threshold implementation with an error detecting approach for fault detection. As a case study, we apply our generic construction to the lightweight LED cipher. Our LED instance achieves first-order resistance against side-channel attacks combined with a fault detection capability that is superior to that of simple duplication for most error distributions at an increased area demand of 12%.

### 3.7 On the Synthesis of Side-Channel resistant Cryptographic Modules

*Sorin A. Huss (TU Darmstadt, DE)*

**License** © Creative Commons BY 3.0 Unported license  
 © Sorin A. Huss

Over the last decades computer aided engineering (CAE) tools have been developed and improved in order to ensure a short time-to-market in the chip design business. Up to now, these design tools do not yet support an integrated design strategy for the development of side-channel resistant hardware implementations. In order to close this gap, a novel framework named AMASIVE (Adaptable Modular Autonomous Side-Channel Vulnerability Evaluator) was developed. It supports the designer in implementing devices hardened against power attacks by exploiting novel security-driven synthesis methods. This talk explains how a design can be hardened in an automatic way by means of appropriate countermeasures which are tailored to the previously identified weaknesses. In addition to the theoretical introduction of the fundamental concepts, we demonstrate an application to the hardening of a complete hardware implementation of the block cipher PRESENT.



### 3.8 Hardware Security – Industrial Experiences

*Michael Hutter (Cryptography Research Inc. – San Francisco, US)*

**License** © Creative Commons BY 3.0 Unported license  
© Michael Hutter

**Joint work of** Elke de Mulder, Mark Marson, Peter Pearson, Andrew J. Leiserson, Megan A. Wachs, Gilbert Goodwill, Benjamin Jun, Josh Jaffe, Pankaj Rohatgi, Michael Hutter

**Main reference** G. Goodwill, B. Jun, J. Jaffe, P. Rohatgi, “A Testing Methodology for Side Channel Resistance Validation”, in Proc. of the 2011 NIST Non-Invasive Attack Testing Workshop, Nara, Japan, 2011.

**URL** [http://csrc.nist.gov/news\\_events/non-invasive-attack-testing-workshop/papers/08\\_Goodwill.pdf](http://csrc.nist.gov/news_events/non-invasive-attack-testing-workshop/papers/08_Goodwill.pdf)

In this talk, I give an overview on the Test Vector Leakage Assessment Methodology (TVLA) as an efficient way to evaluate side-channel resistance. TVLA includes a set of specific and non-specific tests to determine leakage of intermediates of cryptographic algorithms. After that I highlight state of the art methodologies in secure hardware design and will provide details on a secure logic style called Look-up Table based Masked Dual-Rail with Pre-charge Logic (LMDPL).

#### References

- 1 E. De Mulder, M. Hutter, M. E. Marson, P. Pearson. Using Bleichenbacher’s Solution to the Hidden Number Problem to Attack Nonce Leaks in 384-bit ECDSA: extended version. *Journal of Cryptographic Engineering* 4(1), 2014.
- 2 G. Goodwill, B. Jun, J. Jaffe, P. Rohatgi. A Testing Methodology for Side Channel Resistance Validation. NIST Non-Invasive Attack Testing Workshop, Nara, Japan, 2011.
- 3 A. J. Leiserson, M. E. Marson, M. A. Wachs. Gate-Level Masking under a Path-Based Leakage Metric. In *Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2014.

### 3.9 Security Oriented Codes

*Osnat Keren (Bar-Ilan University, IL)*

**License** © Creative Commons BY 3.0 Unported license  
© Osnat Keren

The cryptographic components as well as the on-chip memories are threatened by fault injection attacks. The faults induce errors that modify the behavior of the device. An attacker can use the information obtained from the incorrectly-functioning hardware to retrieve classified information, or, substitute correct information by a wrong one.

Fault injection attacks can be detected with relatively high probability by security oriented codes. Security oriented codes substantially differ from reliability oriented codes for which the error is assumed to be random and hence is of low multiplicity.

In this talk, we’ll discuss the differences between reliability- and security-oriented codes in terms of the channel and error models, design requirements and efficiency criteria. We’ll briefly review existing security oriented codes that aim to detect weak and strong fault injection attacks, and introduce open problems and design challenges.

#### References


- 1 N. Admaty, S. Litsyn and O. Keren., Punctuating, Expurgating and Expanding the  $q$ -ary BCH Based Robust Codes In *IEEE Convention of Electrical and Electronics Engineers in Israel*, 2012.

- 2 K. D. Akdemir, G. Hammouri, B. Sunar. Non-linear Error Detection for Finite State Machines. *Computer Science, Information Security Applications (5932)*, 2009.
- 3 K. D. Akdemir, Z. Wang, M. G. Karpovsky, B. Sunar. Design of Cryptographic Devices Resilient to Fault Injection Attacks Using Nonlinear Robust Codes. *Fault Analysis in Cryptography*, 2012.
- 4 R. Cramer, Y. Dodis, S. Fehr, C. Padró, and D. Wichs. Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors. In *Advances in Cryptology, Eurocrypt*, 2008.
- 5 S. Engelberg, O. Keren. A Comment on the Karpovsky-Taubin Code. In *IEEE Trans. Info. Theory* 57(12), 2011.
- 6 G. Gaubatz, B. Sunar, and M. G. Karpovsky. Non-linear Residue Codes for Robust Public-Key Arithmetic. In *Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2006.
- 7 M. G. Karpovsky and A. Taubin. A New Class of Nonlinear Systematic Error Detecting Codes. *IEEE Trans. Info. Theory* 50(8), 2004.
- 8 M. G. Karpovsky, K. Kulikowski, Z. Wang. Robust Error Detection in Communication and Computation Channels. In *Int. Workshop on Spectral Techniques (Keynote paper)*, 2007.
- 9 M. G. Karpovsky and Z. Wang. Design of Strongly Secure Communication and Computation Channels by Nonlinear Error Detecting Codes. *IEEE Trans Computers*, 2014.
- 10 O. Keren and M. Karpovsky. Relations between the Entropy of a Source and the Error Masking Probability for Security Oriented Codes. *IEEE Transactions on Communications* 63(1), 2015.
- 11 K. J. Kulikowski, M. G. Karpovsky, A. Taubin. Robust Codes and Robust, Fault Tolerant Architectures of the Advanced Encryption Standard. *Journal of System Architecture* (53), 2007.
- 12 Y. Neumeier, O. Keren. Robust Generalized Punctured Cubic Codes. In *IEEE Trans. on Information theory* 60(5), 2014.
- 13 Y. Neumeier, O. Keren. A New Efficiency Criterion for Security Oriented Error Correcting Codes. In *IEEE European Test Symp.*, 2014.
- 14 K. T. Phelps. A Combinatorial Construction of Perfect Codes. *SIAM Journal Alg. disc Meth.*, 1983
- 15 I. Shumsky and O. Keren. Security-Oriented State Assignment. In *Workshop on Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE)*, 2013.
- 16 I. Shumsky and O. Keren. Enhancement of Hardware Security by Hamming Ball Based State Assignment. *Information Security Journal: A Global Perspective. Special issue on Trustworthy Manufacturing and Utilization* 22, 5(6), 2013.
- 17 I. Shumsky, O. Keren and M. Karpovsky. Robustness of Security-Oriented Codes Under Non-Uniform Distribution of Codewords. *Dependable Computing and Communications Symp. at the Intl. Conf. on Dependable Systems and Networks (DSN-DCCS)*, 2013.
- 18 B. Sunar, G. Gaubatz, E. Savas. Sequential Circuit Design for Embedded Cryptographic Applications Resilient to Adversarial Faults. In *IEEE Trans. Computers* 57(1), 2008.
- 19 V. Tomashevich, S. Srinivasan, F. Foerg, and I. Polian. Cross-level Protection of Circuits Against Faults and Malicious Attacks. In *IEEE Intl. On-Line Testing Symp. (IOLTS)*, 2012.
- 20 V. Tomashevich, Y. Neumeier, R. Kumar, O. Keren and I. Polian. Protecting Cryptographic Hardware against Malicious Attacks by Nonlinear Robust Codes. In *IEEE Intl. Symp. on Defect and Fault Tolerance in VLSI Systems (DFT'14)*, 2014.
- 21 J. L. Vasil'ev. On Nongroup Close-Packed Codes. *Probl. Kibernet* (8), 1962.
- 22 Z. Wang and M. G. Karpovsky. Algebraic Manipulation Detection Codes and Their Application for Design of Secure Cryptographic Devices. In *Intl. Symp. on On-Line Testing*, 2011.

- 23 Z.Wang and M.G.Karpovsky. Reliable and Secure Memories Based on Algebraic Manipulation Correction Codes. In Intl. Symp. on On-line Testing, 2012.
- 24 Z. Wang, Mark G. Karpovsky, Konrad J. Kulikowski. Replacing Linear Hamming Codes by Robust Nonlinear Codes Results in a Reliability Improvement of Memories. In Intl. Symp. Dependable Computing, 2009.
- 25 Z. Wang, M.G. Karpovsky, K. Kulikowski. Design of Memories with Concurrent Error Detection and Correction by Non-Linear SEC-DED Codes. Journal of Electronic Testing 26(5), 2010.

### 3.10 Practical Aspects of Integrating PUFs in Industrial Applications

*Roel Maes (Intrinsic-ID – Eindhoven, NL)*

License  Creative Commons BY 3.0 Unported license  
© Roel Maes

Joint work of Roel Maes, Vincent van der Leest, Erik van der Sluis, Frans Willems, Geert-Jan Schrijen

Physically unclonable functions (PUFs) have been studied in an academic research context for more than a decade. The last couple of years, industrial applications of PUFs have also started to appear, driven by the availability of commercial PUF IP and PUF-supported implementations, among others from Intrinsic-ID (Eindhoven, NL). The industrial application domains of PUFs are diverse, ranging from very-high security government and defense applications to extremely lightweight Internet-of-Things (IoT) platforms, and from end-point in-the-field sensors and controllers to cloud-based servers and (virtual) machines.

While instigated by academic research, the practical challenges of integrating PUFs in an industrial context do not run entirely parallel with academic research tracks, and are to some extent still unresolved or at least candidate for improvement. In this talk, a number of the more important practical aspects are aligned, and presented to the academic community. These highlighted points are collected from real-life experiences with industrial partners (aspiring to) integrating PUFs in their products, and include among others:

- the quest for more efficient error-correction techniques
- solutions for dealing with low-entropy PUFs
- insight and solutions for aging effects of PUFs
- design-for-test for PUF-based solutions
- appropriate use of PUFs in case of reset, zeroization, ...
- health testing of PUFs
- ...

### 3.11 Side-Channel Security through Dynamic Reconfiguration: a Trade-off between Granularity and Side-Channel Resistance?

*Nele Mentens (KU Leuven, BE)*

License  Creative Commons BY 3.0 Unported license  
© Nele Mentens

Countermeasures against implementation attacks include hiding data and masking data. A class of countermeasures that has been proposed in the past decade are those that are based on dynamically reconfigurable architectures. This presentation gives an overview of the architectures and the technology that can be used as well as the options for generating new configuration data.

### 3.12 Fault Space Transformation: A Generic Approach to Counter Differential Fault Analysis and Differential Fault Intensity Analysis on AES-like Block Ciphers

*Debdeep Mukhopadhyay (Indian Institute of Technology – Kharagpur, IN) and Sikhar Patranabis (Indian Institute of Technology – Kharagpur, IN)*

**License** © Creative Commons BY 3.0 Unported license  
 © Debdeep Mukhopadhyay and Sikhar Patranabis  
**Joint work of** Sikhar Patranabis, Abhishek Chakraborty, Debdeep Mukhopadhyay, Partha Pratim Chakrabarti (Department of Computer Science and Engineering IIT Kharagpur, India)  
**Main reference** S. Patranabis, A. Chakraborty, D. Mukhopadhyay, P. P. Chakrabarti, “Using State Space Encoding To Counter Biased Fault Attacks on AES Countermeasures”, in IACR Cryptology ePrint Archive, Vol. 2015, pp. 806, 2015.  
**URL** <http://eprint.iacr.org/2015/806>

Classical fault attacks such as Differential Fault Analysis (DFA) as well as biased fault attacks such as the Differential Fault Intensity Analysis (DFIA) have been a major threat to cryptosystems in recent times. DFIA combines principles of side channel analysis and fault attacks to try and extract the key using faulty ciphertexts only. Till date, no effective countermeasure that can thwart both classical DFA as well as DFIA based attacks has been reported in the literature to the best of our knowledge. In particular, traditional redundancy based countermeasures that assume uniform fault distribution are found to be vulnerable against DFIA due to its use of biased fault models. In this talk, we discuss our proposition of a novel generic countermeasure strategy that combines the principles of redundancy with that of fault space transformation to achieve security against both DFA and DFIA based attacks on AES-like block ciphers. As a case study, we have applied our proposed technique to obtain temporal and spatial redundancy based countermeasures for AES-128, and have evaluated their security against both DFA and DFIA via practical experiments on a SASEBO-GII board. Results show that our proposed countermeasure makes it practically infeasible to obtain a single instance of successful fault injection, even in the presence of biased fault models.

### 3.13 PUFs in AMD64 CPUs and GPUs

*Ruben Niederhagen (TU Eindhoven, NL), Daniel J. Bernstein, and Pol Van Aubel*

**License** © Creative Commons BY 3.0 Unported license  
 © Ruben Niederhagen, Daniel J. Bernstein, and Pol Van Aubel  
**Joint work of** Pol Van Aubel, Daniel J. Bernstein, Tanja Lange, Ruben Niederhagen  
**Main reference** P. Van Aubel, D. J. Bernstein, R. Niederhagen, “Investigating SRAM PUFs in Large CPUs and GPUs”, in Proc. of the 5th Int’l Conf. on Security, Privacy, and Applied Cryptography Engineering (SPACE’15), LNCS, Vol. 9354, pp. 228–247, Springer, 2015; pre-print available at IACR.  
**URL** [http://dx.doi.org/10.1007/978-3-319-24126-5\\_14](http://dx.doi.org/10.1007/978-3-319-24126-5_14)  
**URL** <http://eprint.iacr.org/2015/760>


Physically unclonable functions (PUFs) provide data that can be used for cryptographic purposes: on the one hand randomness for the initialization of random-number generators; on the other hand individual fingerprints for unique identification of specific hardware components. However, today’s off-the-shelf personal computers advertise randomness and individual fingerprints only in the form of additional or dedicated hardware.

This research introduces a new set of tools to investigate whether intrinsic PUFs can be found in PC components that are not advertised as containing PUFs. In particular, we investigate AMD64 CPU registers as potential PUF sources in the operating-system kernel,

the bootloader, and the system BIOS; the CPU cache in the early boot stages; and shared memory on Nvidia GPUs. We found non-random non-fingerprinting behavior in several components but revealed usable PUFs in Nvidia GPUs.

### 3.14 Practical HW Security Attacks That Require Minimal Reverse Engineering

*Elad Peer (CISCO Systems – Haifa, IL)*

License  Creative Commons BY 3.0 Unported license  
© Elad Peer

Practical attacks against secure hardware can roughly be divided into two cases: cloning, which usually requires extensive physical reverse engineering, and security breach attacks, which usually requires only little physical reverse engineering effort.

In this talk I demonstrate the validity of the above claim by showing two case studies that deal with security breach attacks. First, an attack that was issued against a complex SoC is described. In this attack a secure boot over the design was obtained. Careful analysis of the documentation reveals vulnerabilities both in the security standard which was the basis for this SoC, and in the implementation itself. Using those vulnerabilities an attack was developed and demonstrated using a laser fault injection or, alternatively, using an electromagnetic fault injection. A second case study briefly describes some straightforward low cost physical methods that enable retrieval of information from non volatile memories. Here, methods ranging from microscopy imaging to electric force microscopy are mentioned, and the usability of simple physical tools to overcome complex channels is demonstrated.

### 3.15 Trojans in Early Design Steps – An Emerging threat

*Ilia Polian (Universität Passau, DE)*

License  Creative Commons BY 3.0 Unported license  
© Ilia Polian

Historically, IT security concentrated on attack scenarios targeting software and communication networks, but more recently, the system hardware moved into the focus of attackers. Hardware-related threats are relevant even for extremely software-dominated systems, which still contain some amount of hardware on which the software runs; compromising this hardware makes the entire system vulnerable. Even worse, many software-centric security solutions rely on a hardware-based root of trust which stores secret keys and provides essential security functions; successful attacks on such root-of-trust blocks renders the entire security concept ineffective. With the emergence of paradigms like cyberphysical systems, internet of things, or Industrie 4.0 that connect the physical world, IT systems and global connectivity, hardware blocks are at risk to become the Achille's heel of entire infrastructures.

The presentation focuses on one emerging attack scenario: Hardware Trojans. These are malicious modification of system hardware with the purpose to gain control over its functionality and, e.g., be able to deactivate the affected block at the attacker's will ("kill switch"), or establish a side-channel to access confidential data processed by the device ("backdoor"). The term "hardware Trojans" was traditionally associated with threats stemming from external, untrusted foundries. However, the presentation is specifically

concerned with Trojans that are introduced into the system during early design steps by a rogue in-house designer, by an external provider of intellectual property blocks integrated into the design, or even by an electronic design automation tool. The devastating damage potential of such attacks, the applicable countermeasures against them and their deficiencies are discussed. An under-investigated attack surface is the system specification which is created in a lengthy and complex process. If an attacker succeeds in planting a Trojan during the specification phase, such a Trojan is extremely hard to uncover and to detect, because any trusted reference is completely lacking.

### 3.16 Virtual Proofs of Reality and Their Physical Implementation

*Ulrich Rührmair (Ruhr-Universität Bochum, DE)*

License  Creative Commons BY 3.0 Unported license  
© Ulrich Rührmair

We discuss the question of how physical statements can be proven over digital communication channels between two parties (a “prover” and a “verifier”) residing in two separate local systems. Examples include: (i) “a certain object in the prover’s system has temperature  $X$  °C”, (ii) “two certain objects in the prover’s system are positioned at distance  $X$ ”, or (iii) “a certain object in the prover’s system has been irreversibly altered or destroyed”. As illustrated by these examples, our treatment goes beyond classical security sensors in considering more general physical statements. Another distinctive aspect is the underlying security model: We neither assume secret keys in the prover’s system, nor do we suppose classical sensor hardware in his system which is tamperresistant and trusted by the verifier. Without an established name, we call this new type of security protocol a “virtual proof of reality” or simply a “virtual proof” (VP).

In order to illustrate our novel concept, we discuss example VPs based on temperature sensitive integrated circuits, disordered optical scattering media, and quantum systems. The corresponding protocols prove the temperature, relative position, or destruction/modification of certain physical objects in the prover’s system to the verifier. These objects (so-called “witness objects”) are prepared by the verifier and handed over to the prover prior to the VP. Furthermore, we illustrate the practical validity of our method for all our optical and circuit-based VPs in detailed proof-of-concept experiments.

Our work touches upon, and partly extends, several established concepts in cryptography and security, including physical unclonable functions, quantum cryptography, interactive proof systems, and, most recently, physical zero-knowledge proofs.

### 3.17 Constructive Side-Channel Analysis

*Werner Schindler (BSI – Bonn, DE)*

License  Creative Commons BY 3.0 Unported license  
© Werner Schindler

**Joint work of** Kerstin Lemke-Rust, Christof Paar, Annelie Heuser, Michael Kasper, Marc Stöttinger, Werner Schindler, c.f. the bibliography

Power analysis is an essential part of evaluations of security implementations on smart cards and FPGAs etc. A successful attack shows that the implementation is vulnerable but usually does not give advice how to fix the problem.

In this talk we treat the stochastic approach, which combines the expertise of an engineer with methods from multivariate statistics. The stochastic approach is an effective attack method, which provides the leakage with regard to a vector space basis. This feature can also be used to identify the significant contributions of the leakage, which in turn supports target-oriented redesign. Moreover, apart from further benefits the stochastic approach allows to verify (within the limits of statistics) or to falsify leakage model assumptions.

### References

- 1 W. Schindler, K. Lemke, C. Paar. A Stochastic Model for Differential Side Channel Analysis. In Cryptographic Hardware and Embedded Systems (CHES), 2005.
- 2 K. Lemke-Rust and C. Paar. Analyzing Side Channel Leakage of Masked Implementations with Stochastic Methods. In European Symp. on Research in Computer Security, 2007.
- 3 W. Schindler. Advanced Stochastic Methods in Side Channel Analysis on Block Ciphers in the Presence of Masking. *Journal of Math. Crypt.* (2), 2008.
- 4 M. Kasper, W. Schindler, M. Stöttinger. A Stochastic Method for Security Evaluation of Cryptographic FPGA Implementations. In Intl. Conf. on Field-Programmable Technology, 2010.
- 5 J. Doget, E. Prouff, M. Rivain, F.-X. Standaert. Univariate Side Channel Attacks and Leakage Modeling. *Journal of Cryptographic Engineering* (1), 2011.
- 6 A. Heuser, M. Kasper, W. Schindler, M. Stöttinger. How a Symmetry Metric Assists Side-Channel Evaluation – A Novel Model Verification Method for Power Analysis. In EUR-OMICRO Conf. on Digital System Design, 2011.
- 7 A. Heuser, W. Schindler, M. Stöttinger. Revealing Side-Channel Issues of Complex Circuits by High-Dimensional Leakage Models. In Design, Automation and Test in Europe (DATE), 2012.
- 8 A. Heuser, M. Kasper, W. Schindler, M. Stöttinger. A Difference Method for Side-Channel Analysis Exploiting High-Dimensional Leakage Models. In Topics in Cryptology – CT-RSA 2012.
- 9 W. Schindler. Understanding the Reasons for the Side-Channel Leakage is Indispensable for Secure Design (extended abstract). In PROOFS: Security Proofs for Embedded Systems, 2012.

## 3.18 Error Correction Schemes for Physical Unclonable Functions

*Georg Sigl (TU München, DE)*

License © Creative Commons BY 3.0 Unported license

© Georg Sigl

Joint work of Michael Pehl, Matthias Hiller, Meng-Day Yu, Michael Weiner, Leandro Rodrigues Lima, Maximilian Birkner

Physical Unclonable Functions (PUFs) derive unique properties from manufacturing variations in integrated circuits. This can be used as a fingerprint for device identification as well as for secret key generation. This talk first shows the analogy between PUF key generation and the information theoretical model of deriving a secret key from a compound source. This model can be used to derive properties for syndrome coding and the generation of error correction information, i.e. the helper data. From recent theoretical results we can conclude that it is possible to generate an information theoretically secure error correction scheme. We have developed such a scheme which we call Systematic Low Leakage Coding (SLLC). It splits the PUF response in a key related part and in a masking part. Helper data are generated by XORing the masking part of the PUF response with the syndrome generated with a

systematic code. This scheme provides inherent information theoretic security without the need of a hash function or strong extractor, and optimal asymptotic performance concerning maximum key size and minimum helper data size. The secrecy leakage is bounded by a small epsilon that goes to zero for PUFs with independent well distributed bits. The reference implementation for an ASIC application scenario shows that our scheme does not require the 47% hardware overhead for the hash function that is mandatory for the state-of-the-art approaches.

Another scheme, which is not optimal under the above assumptions, is called Differential Sequence Coding. With this scheme we can generate very efficient error correction for PUFs with low input bit reliability. The scheme picks reliable bits using pointers which measure the distance between reliable bits. After compression these pointers can be stored very efficiently, i.e. denser than a bit mask selecting the reliable bits from all bits. Combined with a Viterbi decoder and a lightweight hash function to counteract helper data manipulation attacks, this scheme outperforms other schemes considering helper data size, number of PUF bits, and slice count.

In order to perform analysis of PUF structures a FPGA cluster is presented offering 234 FPGAs which could be put in a temperature chamber. This setup is available at Fraunhofer AISEC and is offered to the community for generation of reliability data for FPGA PUF structures. With those data the quality of the PUF can be assessed a lot better than with simulation or testing on a few FPGAs. These data are needed further to generate models of PUFs and for proper dimensioning of error correction codes. With this setup we want to support the community in developing new PUFs and enable design of even more optimized key generation schemes.

## References

- 1 M. Hiller, M.-D. (Mandel) Yu, M. Pehl. Systematic Low Leakage Coding for Physical Unclonable Functions. In ACM Asia Conf. on Computer and Communications Security, 2015.
- 2 M. Hiller, Georg Sigl: Increasing the Efficiency of Syndrome Coding for PUFs with Helper Data Compression. Design, Automation and Test in Europe (DATE), 2014.
- 3 M. Hiller, L. Rodrigues Lima, G. Sigl. Seesaw: An Area-Optimized FPGA Viterbi Decoder for PUFs. Digital System Design (DSD), 2014.
- 4 M. Hiller, M. Weiner, L. Rodrigues Lima, M. Birkner, G. Sigl. Breaking through Fixed PUF block Limitations with Differential Sequence Coding and Convolutional Codes. Intl. workshop on Trustworthy Embedded Devices, 2013.

## 3.19 No Place to Hide: Contactless Probing of Secret Data on FPGAs

*Shahin Tajik (TU Berlin, DE)*

License © Creative Commons BY 3.0 Unported license  
© Shahin Tajik

Joint work of Heiko Lohrke, Jean-Pierre Seifert, Christian Boit, Shahin Tajik

Field Programmable Gate Arrays (FPGAs) have been the target of different physical attacks in recent years. Many different countermeasures have already been integrated into these devices to mitigate the existing vulnerabilities. However, there has not been enough attention paid to semi-invasive attacks from the IC backside due to the following reasons. First, the conventional semi-invasive attacks from the IC backside – such as laser fault injection and photonic emission analysis – cannot be scaled down without further effort to the very



latest nanoscale technologies of modern FPGAs and programmable SoCs. Second, the more advanced solutions for secure storage, such as controlled Physically Unclonable Functions (PUFs), make the conventional memory-readout techniques almost impossible. In this paper, however, novel approaches have been explored: Attacks based on Laser Voltage Probing (LVP) and its derivatives, as commonly used in Integrated Circuit (IC) debug for nanoscale low voltage technologies, are successfully launched against a 60 nanometer technology FPGA. We discuss how these attacks can be used to break modern bitstream encryption implementations. Our attacks were carried out on a Proof-of-Concept PUF-based key generation implementation. To the best of our knowledge this is the first time that LVP is used to perform an attack on secure ICs.

### 3.20 Unlocking the Potential of Hardware Security

*Mark M. Tehranipoor (University of Florida – Gainesville, US)*

License  Creative Commons BY 3.0 Unported license  
© Mark M. Tehranipoor

Hardware security has seen major growth over past decade. Significant amount of attention has been given to development of new security primitives, protection against malicious inclusion, secure architecture, hardware metering, etc. In this talk we present new applications to hardware security engineers. Some discussed topics are nano-enabled security, electronics clones, security rule checks for integrated circuits and non-electronics supply chain security.

## 4 Discussion Sessions

### 4.1 PUFs and Security Components

*Domenic Forte (University of Florida – Gainesville, US)*

License  Creative Commons BY 3.0 Unported license  
© Domenic Forte

Over the past 15 years, research in physical unclonable functions (PUFs) has been driven by the need for low-cost cryptographic key generation/storage and authentication. Yet, there still exist many challenges and unanswered questions regarding the practical limitations of PUFs, the future of PUF research, and the use of PUFs in emerging applications. More recently, the Internet of Things (IoT) has become another hot topic. While experts are excited about the applications enabled by IoT, there is skepticism surrounding our ability to maintain security and privacy at the resource constrained endpoint devices in IoT infrastructure.

The purpose of this session was to discuss these topics from the following three perspectives:

1. *Sources of Variability Impacting PUFs*– There are three categories of variability, each of which presents distinct challenges and opportunities. Process variation is responsible for the existence of PUFs. Although accurate knowledge of process variations (including their statistics) is needed to truly improve the overall quality of PUFs, such information is commonly withheld by foundries (with good reason) and varies with technology. Similarly, current design-for-manufacturability (DfM) techniques, which are geared towards suppression of process variation, are also left in the hands of the foundry. With respect to environmental variability, DC and AC sources need to be considered separately. DC

sources have been demonstrated as useful in executing attacks, but might be partially mitigated with sensors that monitor the PUF's environment. DC and AC sources both lead to PUF reliability problems. In the case of process and environmental variations, simulations are limited for PUF evaluation. Aging is the last major source of variability. On the one hand, accelerated aging has been shown as a way to reinforce PUF values for better reliability. On the other, burn-in is time consuming, costly, and could negatively impact non-PUF portions of ICs. An alternative strategy to deal with aging-induced reliability issues is error correction, but it requires accurate estimation of errors. One of the more promising concepts is anti-aging design, such as incorporation of sleep modes into PUFs.

2. *Emerging Applications of PUFs*– There are many practical challenges limiting the scope of PUFs, such as the lack of benchmarking capabilities and suitable metrics to fairly compare PUFs, vulnerability of strong PUFs to machine learning attacks, and the needs to erase and certify PUF challenge-response pairs. If ever realized, public PUFs based on the simulation-execution time gap might overcome some of these issues. However, a more promising opportunity is presented by expanding the PUF concept and rebranding PUFs as “unique objects”. Unique objects are similar to silicon PUFs in that they harvest statistics for unique identification. However, they are based on optical, biological, and quantum phenomena, and harvest even more information. The most interesting applications for unique objects include monitoring the surrounding environment/conditions, virtual proofs of destruction, and tamper evidence. Unique objects might also be integrated into ICs through additive manufacturing/printing and/or investigation of novel materials. Realization of unique objects shall require interdisciplinary research.
3. *Design of Public Key Cryptography for IoT*– Cryptography in IoT is application-specific and should be governed by threat models, resource constraints, and semiconductor economics. Although IoT devices might contain complex processors, the needs of the application often outweigh those of security leaving little time, area, etc. left for crypto modules and protocols. While PUFs might seem like an excellent fit for IoT, they are still too fragile to replace conventional cryptography. Approaches that balance the trade-offs between latency, device power, and hardware might be even more promising.

## 4.2 Design for Security

Wayne P. Burlleson (*University of Massachusetts – Amherst, US*) and Ilia Polian (*Universität Passau, DE*)

License © Creative Commons BY 3.0 Unported license  
© Wayne P. Burlleson and Ilia Polian

Security is emerging as a new target during design of circuits and systems. During the session, four research questions related to “design for security” were discussed. Below is the summary of the discussions.

### (1) How to balance between security, quality, yield, cost and reliability of an integrated circuit?

The key difference of security from other design objectives is the presence of a human attacker and, as a consequence, a large diversity of attacks. As a consequence, any countermeasures have to be considered risk management under cost constraints, rather than bullet-proof

protections. Prerequisites for designing systematic countermeasures are models of threats (resources at an attacker's disposal), security requirements and available assets. Based on them, certification procedures (including but not limited to formal proofs) can be developed in compliance with existing (legal or technical) regulations. However, all models and abstractions have limitations, and better models of channels to be protected and of attack vectors would be useful. Lessons from safety engineering, debug and reliability should be considered, yet these fields lack some aspects that are essential for secure design. An area which is particularly hard to model is insider attacks, because the techniques employed for such attacks and the consequences of these attacks largely depend on the specific attacker's creativity and malicious intent; it is extremely difficult to create models that are valid for all or most environments.

### **(2) Can Hardware Trojans be detected by low-cost approaches with sufficient confidence?**

Security against hardware Trojans stemming from various sources is difficult to achieve, and it requires a secure design chain, root-of-trust modules and authenticated CAD tools. Anti-Trojan approaches can be categorized into prevention of their effects and detection of their operation; the latter is much easier if a golden (Trojan-free) model is available (which is often not the case). In general, measures that provide resilience against Trojans and other threats (e.g., power-grid instabilities) are desired. A Trojan that protects itself against detection can be compared with "kleptography" (stealing information without being noticed) in context of public-key cryptography. A particularly hard class of Trojans includes those inserted above HDL level; their detection perhaps requires a partition of the system functionality into trusted domains (or trusted IP). Regarding the economic dimension of Trojans (and other security threats) it was discussed whether market forces are sufficient to motivate companies to integrate security features, or whether regulation or specific incentives from the lawmaker are needed. It is possible that market forces are only sufficient to cover very simple, easy-to-understand threats.

### **(3) HW security threat models in context of larger-scale threats (e.g., network, software, social)**

Hardware is the foundation of and "the ultimate insider" in electronic systems. Hardware protects software, and a hardware-related attack can have a very broad impact. The expectations on hardware obsolescence are not always met, and we may be facing attacks on decades-old hardware blocks designed without security considerations. The perceived threat may not always correspond to the actual level of risk; in particular, improved security does not imply larger customer demand. Therefore, security measures might be difficult to justify economically (but this may change as soon as first large-scale real-world attacks will be reported). Hardware vulnerabilities are difficult to study, and one reason is that meaningful investigations require knowledge of internal industry items and procedures that are considered proprietary or secret. In any case, it is important to understand the application under attack and the (real or perceived) threats; one example is unauthorized vehicle tuning, which can compromise safety and can lead to increased warranty costs.

#### (4) How to build automated verification tools for security-critical hardware components that check functional and security aspects?

The construction of such tools requires collaboration with other communities. The basic techniques are, in general, known; these include certification, debug and formal verification. Both a sound theory and efficient implementations are needed to make such approaches practical. This requires expressive and reliable metrics that quantify security threats like side-channel vulnerabilities. It would be ultimately desirable to have “security by design” circuits which do not need separate verification.

### 4.3 Side Channel Analysis

*Debdeep Mukhopadhyay (Indian Institute of Technology – Kharagpur, IN) and Ilia Polian (Universität Passau, DE)*

License © Creative Commons BY 3.0 Unported license  
© Debdeep Mukhopadhyay and Ilia Polian

It is an open area of research as to how to model side-channel attacks such as to balance between accuracy and simplicity. It was discussed that the starting test to detect leakage should be unspecific tests like Test Vector Leakage Assessment (TVLA) tests. These tests which are based on the statistical T-test, are generic and independent of the underlying leakage as it provides an estimate of the fact whether a given circuit leaks information. In cases where the T-test as originally defined does not estimate a leakage, as it estimates the first order leakage (which should be enough for most applications), further tests for higher order leakage may be performed.

For specific tests the underlying leakage model plays a crucial role, and it was discussed on what should be ideal leakage models. On one hand there could be simple linear leakage models, like Hamming weight or linear combination of the values of the bits of a target register; while on the other hand the leakage models could be non-linear to better estimate the electrical models of the device under test.

It was stressed that sometimes our designs of countermeasures are over-designed, as they are based on very strong assumptions of the adversarial power. Like we often consider insider attackers with access to several internals of a circuit, which may not be true in practice. Further effect of side channels on larger designs were deliberated upon. The source of the leakage depending on the attack model should be identified and accordingly countermeasures should be designed. It was emphasized that the overheads of the countermeasures should be estimated with the overall System-on-Chip (SOC) in perspective, as since the crypto-core is a small part of the entire design, the overhead on the crypto-core is a small percentage of the entire SOC. For larger designs we should be more precise on the source of leakage and then design suitable countermeasures. For proper understanding on leakage due to the underlying electrical phenomenon, it was suggested there should be active collaborations with device physics experts.

The next issue which was discussed was modelling methods for fault analysis. It was felt that there should be extensive study on understanding of fault injection techniques, considering a wide variety of fault injection methods, with accompanying validation with silicon results. The models will estimate the precision of faults for various injection methods. Also for modelling of fault attacks, definition of exploitable faults and corresponding leakage thereof wrt. different attack methods like Differential Fault Analysis (DFA), Differential

Fault Intensity Analysis (DFIA) needs to be defined. Further, while analyzing the attacks the effect of the fault cone which leads to an error need to be observed too.

The importance of development of CAD tools for automating the fault attack procedure for given ciphers was stressed to analyze new ciphers. Information theoretic tools were emphasized for discovering the attacks, along with development of algebraic analysis and SAT solvers. These tools require defining suitable metrics for fault analysis, defining exploitable faults in the pursuit of detecting weaknesses of design architectures and synthesizing them into stronger architectures. The fault simulation tools in the reliability community could be used to study the propagation of faults.

The next topic that was discussed was the extent of reverse engineering required for developing practical attacks. Often attacks, like Differential Power Analysis (DPA) or DFA use information which can be obtained by simple, low effort reverse engineering. These could include ascertaining timing by glitches, power analysis, physical inspection, even social engineering. While many of these techniques may be costly, the use of expensive reverse engineering methods for developing practical attacks could be a topic of future research .

The discussions were concluded with the topic of application of coding theory, both linear and non-linear codes, against side channel attacks, fault attacks, and Trojans. The use of linear codes with complementary duals (LCD) could be a useful technique. However, the contradiction between various attack vectors should be studied: for example, error detection techniques used for fault analysis could open side channel leakage sources. Thus it is important to develop holistic countermeasures, and the effectivity of the countermeasures against these threats also should be modelled to increase confidence in them.

## Participants

- Lejla Batina  
Radboud Univ. Nijmegen, NL
- Georg T. Becker  
Ruhr-Universität Bochum, DE
- Christian Boit  
TU Berlin, DE
- Jan Burchard  
Universität Freiburg, DE
- Wayne P. Burleson  
University of Massachusetts –  
Amherst, US
- Jean-Luc Danger  
ENST – Paris, FR
- Linus Feiten  
Universität Freiburg, DE
- Domenic Forte  
University of Florida –  
Gainesville, US
- Fatemeh Ganji  
TU Berlin, DE
- Swaroop Ghosh  
University of South Florida, US
- Jorge Guajardo Merchan  
Robert Bosch LLC –  
Pittsburgh, US
- Tim Erhan Güneysu  
Universität Bremen, DE
- Sorin A. Huss  
TU Darmstadt, DE
- Michael Hutter  
Cryptography Research Inc. –  
San Francisco, US
- Ramesh Karri  
New York University, US
- Osnat Keren  
Bar-Ilan University, IL
- Tanja Lange  
TU Eindhoven, NL
- Roel Maes  
Intrinsic-ID – Eindhoven, NL
- Nele Mentens  
KU Leuven, BE
- Debdeep Mukhopadhyay  
Indian Institute of Technology –  
Kharagpur, IN
- Ruben Niederhagen  
TU Eindhoven, NL
- Sikhar Patranabis  
Indian Institute of Technology –  
Kharagpur, IN
- Elad Peer  
CISCO Systems – Haifa, IL
- Ilia Polian  
Universität Passau, DE
- Wenjing Rao  
Univ. of Illinois – Chicago, US
- Francesco Regazzoni  
University of Lugano, CH
- Ulrich Rührmair  
Ruhr-Universität Bochum, DE
- Kazuo Sakiyama  
The Univ. of  
Electro-Communications –  
Tokyo, JP
- Werner Schindler  
BSI – Bonn, DE
- Georg Sigl  
TU München, DE
- Shahin Tajik  
TU Berlin, DE
- Mark M. Tehranipoor  
University of Florida –  
Gainesville, US

