Constructive Side-Channel Analysis and Secure Design

Third International Workshop, COSADE 2012
Darmstadt, Germany, May 3-4, 2012
Proceedings
COSADE 2012, the Third Workshop on Constructive Side-Channel Analysis and Secure Design, was held in Darmstadt, Germany, during May 3–4, 2012. COSADE 2012 was supported by CASED and its partners TU Darmstadt and Fraunhofer SIT as well as by the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI).

For researchers and experts from academia, industry and government who are interested in attacks on cryptographic implementations and/or secure design, COSADE workshops present a great opportunity to meet and enjoy intensive discussions.

The program provides plenty of time for information exchange on the further development of existing and for the establishment of new scientific collaborations.

This year 49 papers from several areas such as side-channel analysis, fault analysis, secure design, and architectures were submitted. Each paper was assigned to three reviewers. The decision process was very challenging and resulted in the selection of 16 interesting papers. Their carefully revised versions are contained in the conference proceedings.

The Program Committee consisted of 33 members from 12 countries. The members were carefully selected to represent both academia and industry, as well as to include high-profile experts with research relevant to COSADE 2012. The Program Committee was supported by 48 external reviewers. We are deeply grateful to the members of the Program Committee as well as to the external reviewers for their dedication and hard work.

Besides 16 contributed presentations, two highly relevant invited talks were held. Mathias Wagner considered “700+ Attacks Published on Smart Cards: The Need for a Systematic Counter Strategy,” while Viktor Fischer gave “A Close Look at Security in Random Number Generators Design.” The workshop program included special sessions. The presentation “Using Multi-Area Diode Lasers and Developing EM FI Tools” considered fault injection attacks. Moreover, the outcome of DPA contest v3 was presented at COSADE 2012, and DPA contest v4 was announced.

COSADE 2012 also had a Work in Progress session where cutting-edge research results were presented. These contributions are not contained in this volume since the submission deadline expired after the editorial deadline of these proceedings.

We are also very grateful to Annelie Heuser, Michael Kasper, Marc Stöttinger and Michael Zohner for the local organization. Finally, we would like to profoundly thank and give our regards to all the authors who submitted their papers to this workshop, and entrusted us with a fair and objective evaluation of their work. We appreciate their creativity, hard work, and interesting results.

March 2012

Werner Schindler
Sorin A. Huss
General Chairs and Program Chairs

Werner Schindler  
Bundesamt für Sicherheit in der Informationstechnik (BSI), Germany

Sorin A. Huss  
Integrated Circuits and Systems Lab (ICS), Technische Universität Darmstadt, Germany

Local Organizers

Annelie Heuser  
Technische Universität Darmstadt, Germany

Michael Kasper  
Fraunhofer SIT, Germany

Marc Stöttinger  
Technische Universität Darmstadt, Germany

Michael Zohner  
Technische Universität Darmstadt, Germany

Program Committee

Onur Acimez  
Samsung Electronics, USA

Guido Bertoni  
ST Microelectronics, Italy

Stanislav Bulygin  
TU Darmstadt, Germany

Ray Cheung  
City University of Hong Kong, Hong Kong

Jean-Luc Danger  
 Télécom ParisTech, France

Markus Dichtl  
Siemens AG, Germany

Viktor Fischer  
Université de Saint-Etienne, France

Ernst-Günter Giessmann  
T-Systems International GmbH, Germany

Tim Güneysu  
Ruhr-Universität Bochum, Germany

Lars Hoffmann  
Giesecke & Devrient GmbH, Germany

Naofumi Homma  
Tohoku University, Japan

Marc Joye  
Technicolor, France

Jens-Peter Kaps  
George Mason University, USA

Çetin Kaya Koç  
University of California Santa Barbara, USA and Istanbul Şehir University, Turkey

Arjen Lenstra  
EPFL, Switzerland

Pierre-Yvan Liardet  
ST Microelectronics, France

Stefan Mangard  
Infineon Technologies AG, Germany

Sandra Marcello  
Thales, France

David Naccache  
ENS Paris, France
Elisabeth Oswald  University of Bristol, UK  
Emmanuel Prouff  Oberthur Technologies, France  
Anand Rajan  Intel Corporation, USA  
Steffen Reith  Hochschule RheinMain, Germany  
Akashi Satoh  RCIS, Japan  
Patrick Schaumont  Virginia Tech, Blacksburg, USA  
Abdulhadi Shoufan  Khalifa University Abu-Dhabi, UAE  
Sergei Skorobogatov  University of Cambridge, UK  
Georg Sigl  Technische Universität München, Germany  
Francois-Xavier Standaert  Université Catholique de Louvain, Belgium  
Lionel Torres  LIRMM, University of Montpellier 2, France  
Ingrid Verbauwhede  Katholieke Universiteit Leuven, Belgium  
Marc Witteman  Riscure, The Netherlands  
Michael Waidner  Fraunhofer SIT, Germany  

**External Reviewers**

Michel Agoyan  Bernhard Jungk  Mathieu Renaud  
Joppe Bos  Markus Kasper  Vladimir Rozic  
Lilian Boussuet  Michael Kasper  Fabrizio de Santis  
Pierre-Louis Cayrel  Toshihiro Katashita  Laurent Sauvage  
Guillaume Duc  Stéphanie Kerckhof  Hermann Seuscheck  
Junfeng Fan  Chong Hee Kim  Marc Stöttinger  
Lubos Gaspar  Jiangtao Li  Daehyun Strobel  
Benedikt Gierlichs  Marcel Medwed  Mostafa Taha  
Christophe Giraud  Filippo Melzani  Junko Takahashi  
Sylvain Guilley  Oliver Mischke  Michael Tunstall  
Yu-Ichi Hayashi  Amir Moradi  Rajesh Velegalati  
Stefan Heyse  Abdelaziz Moulay  Markus Wamser  
Matthias Hiller  Nadia El Mrabet  Michael Weiss  
Phillipe Hoogvorst  Jean Nicolai  Carolyn Withnall  
Gabriel Hospodar  David Oswald  Meiyuan Zhao  
Dimitar Jetchev  Gilles Piret  Michael Zohner
# Table of Contents

## Practical Side-Channel Analysis

Exploiting the Difference of Side-Channel Leakages .......................... 1  
*Michael Hutter, Mario Kirschbaum, Thomas Plos,  
Jörn-Marc Schmidt, and Stefan Mangard*

Attacking an AES-Enabled NFC Tag: Implications from Design to a Real-World Scenario ......................................................... 17  
*Thomas Korak, Thomas Plos, and Michael Hutter*

## Invited Talk I

700+ Attacks Published on Smart Cards: The Need for a Systematic Counter Strategy ................................................................. 33  
*Mathias Wagner*

## Secure Design

An Interleaved EPE-Immune PA-DPL Structure for Resisting Concentrated EM Side Channel Attacks on FPGA Implementation ...... 39  
*Wei He, Eduardo de la Torre, and Teresa Riesgo*

An Architectural Countermeasure against Power Analysis Attacks for FSR-Based Stream Ciphers .............................................. 54  
*Shohreh Sharif Mansouri and Elena Dubrova*

Conversion of Security Proofs from One Leakage Model to Another: A New Issue ................................................................. 69  
*Jean-Sébastien Coron, Christophe Giraud, Emmanuel Prouff,  
Soline Renner, Matthieu Rivain, and Praveen Kumar Vadnala*

## Side-Channel Attacks on RSA

Attacking Exponent Blinding in RSA without CRT .......................... 82  
*Sven Bauer*

A New Scan Attack on RSA in Presence of Industrial Countermeasures ................................................................. 89  
*Jean Da Rolt, Amitabh Das, Giorgio Di Natale, Marie-Lise Flottes,  
Bruno Rouzeyre, and Ingrid Verbauwhede*

RSA Key Generation: New Attacks .............................................. 105  
*Camille Vuillaume, Takashi Endo, and Paul Wooderson*
**Fault Attacks**

A Fault Attack on the LED Block Cipher .................................................. 120  
*Philipp Jovanovic, Martin Kreuzer, and Ilia Polian*

Differential Fault Analysis of Full LBlock ............................................... 135  
*Liang Zhao, Takashi Nishide, and Kouichi Sakurai*

Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator ................................................................. 151  
*Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer, François Poucheret, Bruno Robisson, and Philippe Maurine*

**Invited Talk II**

A Closer Look at Security in Random Number Generators Design ........... 167  
*Viktor Fischer*

**Side-Channel Attacks on ECC**

Same Values Power Analysis Using Special Points on Elliptic Curves .... 183  
*Cédric Murdica, Sylvain Guilley, Jean-Luc Danger, Philippe Hoogvorst, and David Naccache*

The Schindler-Itoh-attack in Case of Partial Information Leakage ........ 199  
*Alexander Krüger*

**Different Methods in Side-Channel Analysis**

Butterfly-Attack on Skein’s Modular Addition ....................................... 215  
*Michael Zohner, Michael Kasper, and Marc Stöttinger*

MDASCA: An Enhanced Algebraic Side-Channel Attack for Error Tolerance and New Leakage Model Exploitation .................................... 231  
*Xinjie Zhao, Fan Zhang, Shize Guo, Tao Wang, Zhijie Shi, Huiying Liu, and Keke Ji*

Intelligent Machine Homicide: Breaking Cryptographic Devices Using Support Vector Machines ................................................................. 249  
*Annelie Heuser and Michael Zohner*

**Author Index** ............................................................................................ 265