Third International Workshop on Constructive Side-Channel Analysis and Secure Design
May 03-04 2012, Darmstadt, Germany

COSADE 2012

Side-channel analysis (SCA) and implementation attacks have become an important field of research at universities and in the industry. In order to enhance the resistance of cryptographic and security critical implementations within the design phase, constructive attacks and analyzing techniques may serve as a quality metric to optimize the design- and development process. This workshop provides an international platform for researchers, academics, and industry participants to present their work and their current research topics. It is an excellent opportunity to meet experts and to initiate new collaborations and information exchange at a professional level. The workshop will feature both invited presentations and contributed talks. The topics of COSADE 2012 include, but are not limited to:

Side-Channel Analysis and Implementation Attacks:

- Constructive side-channel analysis and implementation attacks in general
- Profiled and non-profiled methods for constructive side-channel analysis
- Non-invasive, semi-invasive and invasive implementation attacks
- Power attacks and electromagnetic analysis
- Advanced stochastic methods in SCA, especially in power- and electromagnetic analysis
- Stochastic approach in power analysis
- Leakage models and security models for side-channel analysis in the presence and absence of countermeasures
- Advanced methods for Differential Power Analysis and Mutual Information Analysis
- Algebraic side-channel analysis and combination of implementation attacks with algebraic cryptanalysis
- Side-channel analysis under black-box assumptions
- Side-channel analysis and implementation attacks on cyber physical systems and embedded devices
- Timing-analysis, cache-attacks and micro-architectural analysis
- Decapsulation and preparation techniques
- Side-channel based reverse engineering
- Side-channel analysis in cloud and virtualization contexts

Cryptographic Engineering, Secure Design and Side-channel Evaluation:

- Cryptographic engineering and secure design methods in general
- Leakage resilience, tamper resistance and fault tolerance by design
- Interaction between side-channel analysis and secure design
- Evaluation methodologies for side-channel resistant designs, acquisition and analysis
- Advanced techniques for physical side-channel measurement, side-channel acquisition and preprocessing
- Verification methods for side-channel analysis and fault analysis
- Side-channel aware and tamper-resistant design criteria and design techniques
- Countermeasures against implementation attacks at algorithmic-, logic-, register transfer- and physical level
- Secure designs and countermeasures for FPGAs, HW/SW Codesign-architectures and SoC
- Fault injection and fault tolerance tools for reconfigurable hardware and SoC
- Evaluation platforms and tools for testing of side-channel characteristics
- New and emerging methods and applications for constructive side channel analysis and secure design

Workshop Proceedings:

The proceedings will be published in the Springer CCIS or LNCS series (final confirmation pending). In order to be included in the proceedings, the authors of accepted papers must guarantee that their paper will be presented at the conference. In addition, the Journal of Cryptographic Engineering will be publishing selected papers.

Springer

Lecture Notes in Computer Science
LNCS LNAI LNBI

Contributions:
Prospective authors are invited to submit full papers with max. 15 pages. Submissions must be anonymous and must not identify the submitting authors, directly or indirectly, anywhere in the manuscript. The manuscripts must follow the LNCS default author instructions at URL http://www.springer.de/comp/lncs/authors.html.

All manuscripts must be submitted electronically at following the link: http://cosade2012.cased.de/submission.html

Work in Progress Session:
COSADE 2012 also comprises a special session "Work in progress" (WiP session). The WiP session will be dedicated to new, on-going research in constructive side channel analysis and secure design. Applicants should submit extended abstracts (4-6 pages) by March 13, 2012. The manuscript should also follow the LNCS default author instructions.

Important Dates:

~~Submission deadline:~~	~~December 12, 2011~~
Submission extented:	December 16, 2011
Notification to authors:	February 14, 2012
Final version due:	February 28, 2012
Submission deadline "WiP":	March 13, 2012
Notification to authors "WiP":	April 1, 2012
COSADE workshop:	May 03-04, 2012

Location:
Darmstadtium – science & congress center
Schlossgraben 1, 64283 Darmstadt
http://www.darmstadtium.de/

General Chair and Program Chair:
Werner Schindler (co-chair)
Bundesamt für Sicherheit in der Informationstechnik (BSI), Germany

Sorin A. Huss (co-chair)
Integrated Circuits and Systems Labs (ISS)
TU Darmstadt, Germany

Program Committee:

Onur Aciiçmez, 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, Telecom ParisTech, France
Markus Dichtl, Siemens AG, Germany
Viktor Fischer, Université de Saint-Etienne, France
Tim Güneysu, Ruhr-Universität Bochum, Germany
Ernst-Günter Giessmann, T-Systems GmbH, 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, UCSB, USA & Istanbul Sehir University
Arjen Lenstra, EPFL, Switzerland
Pierre-Yvan Liardet, ST Microelectronics, France
Stefan Mangard, Infineon Technlogies AG, Germany
Sandra Marcello, Thales, France
David Naccache, ENS Paris, France
Elisabeth Oswald, Universitiy of Bristol, UK
Emmanuel Prouff, Oberthur, 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, TU München, Germany
Francois-Xavier Standaert, UC Louvain, Belgium
Lionel Torres, University Montpellier, France
Ingrid Verbauwhede, K.U. Leuven, Belgium
Marc Witteman, Riscure, Netherlands
Michael Waidner, Fraunhofer SIT, Germany

Further Information:
For more information about the COSADE 2012 workshop please visit our website at http://cosade2012.cased.de or alternatively send an email with your request to: cosade2012@cased.de.

Local Organisation:
Michael Kasper, Fraunhofer SIT, Germany
Marc Stöttinger, TU Darmstadt, Germany
Annelie Heuser, TU Darmstadt, Germany
Michael Zohner, TU Darmstadt, Germany