ANNOUNCEMENT AND CALL FOR PAPERS

COSADE 2010

First International Workshop on
Constructive Side-Channel Analysis and Secure Design

Darmstadt, Germany, February 4-5, 2010

http://cosade2010.cased.de

Side-channel analysis (SCA) has become an important field of research at universities and in the industry. Of particular interest is constructive side-channel analysis, as successful attacks support a target-oriented associated design process. In order to enhance the side-channel resistance of cryptographic implementations within the design phase, constructive SCA 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 contributing talks. COSADE 2010 also appreciates work in progress.

The topics of COSADE 2010 include, but are not limited to:

Cryptography and side-channel analysis:

- Constructive side-channel analysis in general
- Stochastic approach in power analysis
- Interaction between side-channel analysis and design
- Advanced stochastic methods in side-channel analysis, especially in power analysis and EM analysis
- Leakage models and security models for side-channel analysis in the presence and absence of countermeasures
- Side-channel analysis under black-box assumptions
- Evaluation methodologies for side-channel resistant designs, data acquisition, and analysis
- Side-channel leakage assessment methodologies, models, and metrics

Secure Design and Architectures:

- SCA-aware design criteria, design techniques, and tools
- Verification methods and models for side-channel leakages within the design process
- Methods, tools, and platforms for the evaluation of the side-channel characteristics of a design
- Criteria for the design flow of countermeasures
- HW / SW-acceleration for constructive SCA
- Leakage-resilient designs
- Countermeasures against side-channel attacks on
  - FPGAs
  - HW/SW Co-design architectures
  - System on a Chip
- Countermeasures against attacks at algorithmic-, logic-, register transfer-, and physical levels

Contributions:
Prospective authors are invited to submit extended abstracts. All submitted contributions will be peer reviewed by experts in the field. The submissions should not exceed four pages. Manuscripts should be single-spaced with at least twelve-point fonts and reasonable margins. All manuscripts must be submitted electronically at following the link: http://cosade2010.cased.de/submission.html

Workshop Proceedings:
Accepted contributions will appear in the workshop proceedings published by CASED. Expected are extended abstracts but full papers are also welcome. COSADE 2010 does not claim an exclusive copyright on the presented work. This approach shall prevent submissions from conflicting with proceedings of forthcoming conferences and workshops. The participants will receive the proceedings as handouts and in electronic form.

Important Dates:
Submission of abstracts: December 06, 2009
Notification to authors: January 03, 2010
Final version due: January 25, 2010

Location:
Center for Advanced Security Research Darmstadt (CASED), Mornewegstrasse 32, 64293 Darmstadt, Germany

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:

Markus Dichtl, Siemens AG, Germany
Wolfgang Effing, Giesecke & Devrient, Germany
Victor Fischer, Université de Saint-Etienne, France
Marc Joye, Thomson R&D, France
Çetin Kaya Koç, University of California Santa Barbara, USA
Ralf Laue, KOBIL Systems, Germany
Stefan Mangard, Infineon Technologies AG, Germany
David Naccache, ENS Paris, France
Reinhard Posch, IAIK TU Graz, Austria
Christof Paar, Ruhr-Universität Bochum, Germany
Akashi Satoh, RCIS, Japan
Jean-Pierre Seifert, TU Berlin, Germany
Fracois-Xavier Standaert, Université Catholique de Louvain, Belgium
Ingrid Verbauwhede, Katholieke Universiteit Leuven, Belgium

Local Organisation:

Michael Kasper, Fraunhofer SIT, Germany
Marc Stöttinger, TU Darmstadt, Germany

Further Information:

For more information about the COSADE 2010 workshop please visit our website at http://cosade2010.cased.de or alternatively send an email with your request to: cosade2010@cased.de.