ANNOUNCEMENT AND CALL FOR PAPERS

COSADE 2011

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

Darmstadt, Germany, February 24-25, 2011

http://cosade2011.cased.de

Side-channel analysis (SCA) and implementation attacks have 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 resistance of cryptographic 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 contributing talks. COSADE 2011 also appreciates work in progress.

The topics of COSADE 2011 include, but are not limited to:

Cryptography and side-channel analysis:

- Constructive side-channel analysis and implementation attacks in general
- Stochastic approach in power analysis
- Interaction between side-channel analysis and design
- Advanced stochastic methods in side-channel analysis, especially in power- and electromagnetic analysis
- Leakage models and security models for side-channel analysis in the presence and absence of countermeasures
- Side-channel analysis under black-box assumption
- Design-oriented implementation attacks and fault analysis techniques
- Algebraic side-channel analysis and combination of implementation attacks with algebraic cryptanalysis
- Side-channel leakage assessment methodologies, models, and metrics
- Application of constructive side-channel analysis apart from attacks and design

Secure Design and Architectures:

- SCA-aware design criteria and design techniques
- Verification methods and models for side-channel leakages within the design phase
- Evaluation methodologies for side-channel resistant designs, acquisition and analysis
- Methods, tools, and platforms for evaluation of side-channel characteristics of a design
- Criteria for the design flow of countermeasures
- HW/SW acceleration and support tools for constructive SCA
- Leakage-resilient and fault-tolerant design
- Countermeasures against implementation attacks at algorithmic-, logic-, register transfer- and physical level
- Countermeasures against side-channel and implementation attacks on FPGAs, HW/SW-Co-design architectures, and SoC

Contributions:
Prospective authors are invited to submit extended abstracts (4-6 pages) but full papers with max. 15 pages are also welcome. All submitted contributions will be peer reviewed by experts in the field. The manuscript should be single-spaced with at least eleven-point fonts and reasonable margins. All manuscripts must be submitted electronically at following the link: http://cosade2011.cased.de/submissions.html

Workshop Proceedings:
Accepted contributions will appear in the workshop proceedings published by CASED. COSADE 2011 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 deadline:	November 15, 2010
Notification to authors:	January 05, 2011
Final version due:	January 31, 2011
COSADE workshop:	February 24-25, 2011

Location:

Fraunhofer Institute for Secure Information Technology SIT, Rheinstraße 75, 64295 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:

Stanislav Bulygin, Technische Universität Darmstadt, Germany
Jean Luc Danger, Telecom ParisTech, France
Markus Dichtl, Siemens AG, Germany
Wolfgang Effing, Giesecke & Devrient, Germany
Viktor Fischer, Université de Saint-Etienne, France
Ernst-Günter Giessmann, T-Systems International GmbH, Germany
Josh Jaffe, Cryptography Research, USA
Marc Joye, Technicolor, France
Çetin Kaya Koç, University of California Santa Barbara, USA
Ralf Laue, KOBIL Systems, Germany
Stefan Mangard, Infineon Technlogies AG, Germany
Sandra Marcello, Thales, France
David Naccache, ENS Paris, France
Reinhard Posch, IAIK, Austria
Christof Paar, Ruhr-Universität Bochum, Germany
Akashi Satoh, RCIS, Japan
Georg Sigl, Technische Universität München, Germany
Francois-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
Annelie Heuser, TU Darmstadt, Germany

Further Information:

For more information about the COSADE 2011 workshop please visit our website at http://cosade2011.cased.de or alternatively send an email with your request to: cosade2011@cased.de.