Important Dates

Paper submission 29 October
Notification 02 January
Pre-proceedings version 15 January
Workshop 7–8 March
Final version 01 April

Steering Committee

Soen Huss
Technische Universität Darmstadt

Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik

Conference Chair

Jean-luc Danger, Télécom ParisTech

Program Chair

Emmanuel Prouff, ANSSI

Program Committee

Guido Bertoni
ST Microelectronics, Italy

Ray Cheung
City University of Hong Kong, Hong Kong

Jean-Sébastien Coron
Université de Paris Diderot, France

Hermann Drexler
Giesecke & Devrient, Germany

Cécile Dumas
CEA LETI, France

Benoît Felt
HRSC, France

Catherine Gheoty
University of Waterloo, Canada

Benedikt Gierlichs
KU Leuven, Belgium

Christophe Giraud
Ceribis Technologies, France

Sylvain Guilley
Télécom ParisTech, France

Helena Handschuh
CRI, USA

Naofumi Homma
Tohoku University, Japan

Ilya Iyinov
Technical University, The Netherlands

Markus Kuhn
University of Cambridge, UK

Thi-Lai Le
Thympo, France

Víctor Lomné
ANSSI, France

Stefan Mangard
Infineon, Germany

Amir Moradi
Bilkent University, Turkey

Dheepak Mukhopadhyay
Indian Institute of Technology Kharagpur, India

Elisabeth Oswald
University of Bristol, UK

Axel Poschmann
Diemex Technologies, Singapore

Ananda Rajan
Diatel Corporation, USA

Denis Real
DGA-MI/CELAR, France

Mathieu Rivain
CryptoExperts, France

Kazuo Sakurai
The University of Electro-Communications Tokyo, Japan

Akihito Sakai
NICT, Japan

Patrick Schaumont
Virginia Tech, Blacksburg, USA

Jorn-Marc Schmidt
LAI, Graz, Austria

François-Xavier Standaert
UCL, Belgium

Hugo Theheault
Université Toulouse, France

Camille Vuillaume
Renesas Electronics, Japan

Mathias Wagner
NXP, Germany

Call For Papers

COSADE 2013

Paris, France, 7–8 March 2013

http://www.cosade.org/

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. Since 2010, COSADE 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 exchange on new results with international experts and to initiate new collaborations and information exchange at a professional level. The workshop will feature both invited presentations and contributed talks.

The fourth International Workshop on Constructive Side-Channel Analysis and Secure Design will be organized and held by Telecom ParisTech, Paris, France.

The topics of COSADE 2013 include, but are not limited to:

- **Constructive side-channel analysis and implementation attacks**
- Semi-invasive, invasive and fault attacks
- Leakage models and security models for side-channel analysis
- Cache-attacks and micro-architectural analysis
- Decapsulation and preparation techniques
- Side-channel based reverse engineering
- Leakage Resilient Implementations
- Evaluation methodologies for side-channel resistant designs
- Secure designs and countermeasures
- Evaluation platforms and tools for testing side-channel characteristics

Submitted papers should present novel contributions related to the topics listed above. They must be original, unpublished, anonymous and not submitted to another conference or journal for consideration of publication. Papers must be written in English and they should not exceed 15 pages. Submissions not meeting these guidelines risk rejection without consideration of their merits. All submissions will be blind-refereed. Authors are invited to submit their manuscripts (PDF or PS format) by filling in the submission form available on the following web site: http://www.easychair.org/conferences/?conf=cosade2013.

Submission implies the willingness of at least one of the authors to register and present the paper. The proceedings will be published as a Springer Lecture Notes in Computer Science volume.