



**Steering Committee:**

Jean-Luc Danger  
Télécom ParisTech, FR  
Werner Schindler  
Bundesamt für Sicherheit in der  
Informationstechnik (BSI), DE

**General Chair:**

Alberto Ferrante  
ALaRI - USI, CH  
Banik Subhadeep  
EPFL, CH

**Program Chairs:**

Guido Bertoni  
Security Pattern, IT  
Francesco Regazzoni  
Alari - USI, CH

**Program Committee:**

Divya Arora  
Intel, US  
Reza Azarderakhsh  
Florida Atlantic University, US  
Josep Balasch  
KU Leuven, BE  
Georg T. Becker  
EMST, DE  
Davide Bellizia  
UCL Crypto Group, BE  
Sonia Belaïd  
CryptoExperts, FR  
Shivam Bhasin  
Nanyang Technological  
University, SG  
Elke De Mulder  
Cryptography Research, US  
Fabrizio De Santis  
Siemens AG, DE  
Baris Ege  
Riscure, NL  
Wieland Fischer  
Infineon Technologies, DE  
Samaneh Ghandali  
Google, US  
Sylvain Guilley  
Secure-IC, FR  
Tim Güneysu  
Ruhr-Universität Bochum, DE  
Annelie Heuser  
CNRS, IRISA, FR  
Naofumi Homma  
Tohoku University, JP  
James Howe  
PQShield, UK  
Jens-Peter Kaps  
George Mason University, US  
Elif Bilge Kavun  
The University of Sheffield, UK  
Osnat Keren  
Bar-Ilan University, IL  
Roel Maes  
Intrinsic-ID, NL  
Pedro Massolino  
Radboud University, NL  
Marcel Medwed  
NXP Semiconductors, AT  
Debdepp Mukhopadhyay  
IIT Kharagpur, IN  
Makoto Nagata  
Kobe University, JP  
Paolo Palmieri  
University College Cork, IE  
Collin O'Flynn  
NewAE Technology Inc., CA  
Gerardo Pelosi  
Politecnico di Milano, IT  
Ilia Polian  
Universität Stuttgart, DE  
Kazuo Sakiyama  
The University of Electro-  
Communications, JP  
Johanna Sepulveda  
Airbus, DE  
Patrick Schaumont  
Virginia Tech, US  
Georg Sigl  
TU Munich, DE  
Marc Stöttinger  
Continental AG, DE  
Ruggero Susella  
STMicroelectronics, IT

# Call for Papers

11<sup>th</sup> International Workshop on  
Constructive Side-Channel Analysis and Secure Design

## COSADE 2020

Lugano, Switzerland, 1. - 3. April 2020

<http://cosade.org>

Side-channel analysis (SCA) and implementation attacks have become an important field of research and real threat. 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.

The program committee is seeking original papers on all aspects of the side-channel analysis and other implementation attacks as well as secure design. Submission presenting practical attacks, test platforms, and open benchmarks are particularly encouraged. Submission topics include, but are not limited to:

- **Implementation attacks and exploitations:**  
Side-channel analysis, fault-injection attacks, probing and read-out, hardware Trojans, cloning and counterfeiting, side-channel or fault-injection based reverse engineering
- **Secure implementation:**  
Cryptographic blocks (including post-quantum and lightweight ciphers), random number generators, physical unclonable functions, leakage-resilient cryptography, fault-injection tolerant design, and tamper-detection
- **Implementation attack-resilient architectures and schemes:**  
Trusted environment (Secure boot, execution, storage, isolation, virtualization, firmware update), protections against micro-architectural side-channels and covert channels, cache attacks, software-enabled implementation attacks, white-box cryptography
- **Secure design and evaluation:**  
Security and leakage models, formal analysis of secure implementations, design automation and tools, evaluation tooling, domain-specific security analysis of e.g., IoT, medical, automotive, industrial-control systems, mobile, security analysis based on artificial intelligence
- **Practical attacks, test platforms and open benchmarks:**  
Practical implementation of physical attacks, practical demonstrators of Trojan insertion, test platforms for evaluation of physical attacks, open benchmarks for hardware Trojans, physical attacks and countermeasures.

Authors are invited to submit papers (PDF format) electronically by the submission link: <https://www.easychair.org/conferences/?conf=cosade20>

Submitted papers must be original, unpublished, anonymous and not submitted to journals or other conferences/workshops that have proceedings. Submissions must be written in English, strictly follow Springer LNCS format (with default margins, font size, etc.) and should be at most 20 pages, excluding references. Papers not meeting these guidelines risk rejection without consideration. All submissions will be blind-refereed. Submission implies the willingness of at least one of the authors to register and present the paper. The proceedings will be published in the Springer Lecture Notes in Computer Science (LNCS) series. Accepted papers must follow the LNCS author instructions at: <http://www.springer.de/comp/lncs/authors.html>

### Important Dates

Submission of papers:	<del>7<sup>th</sup> December 2019</del> 17 <sup>th</sup> December 2019
Notification of acceptance:	30 <sup>th</sup> January 2020
Final version of papers:	15 <sup>th</sup> February 2020
Workshop date:	1 <sup>st</sup> - 3 <sup>rd</sup> April 2020