Call for Papers

10th International Workshop on
Constructive Side-Channel Analysis and Secure Design

COSADE 2019

Darmstadt, Germany, 3. - 5. April 2019

http://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.
In 2019, the International Workshop on Constructive Side-Channel Analysis and Secure Design celebrates its 10th anniversary and is held by TU Darmstadt, Darmstadt, Germany. The program committee is seeking original papers on all aspects of the side-channel analysis and other implementation attacks as well as secures design. Submission topics of interest 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

Authors are invited to submit papers (PDF format) electronically by the submission link: https://www.easychair.org/conferences/?conf=cosade19.

Submitted papers must be original, unpublished, anonymous and not submitted to journals or other conferences/workshops that have proceedings.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 15 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:	1st December 2018
Notification of acceptance:	25th January 2019
Final version of papers:	15th February 2019
Workshop date:	3rd - 5th April 2019

Springer Lecture Notes in Computer Science
LNCS LNAI LNBI

Organized by:
Technical University of Darmstadt
TECHNISCHE UNIVERSITÄT DARMSTADT

Organized in collaboration with:
SFB 1119 CROSSING
CROSSING

Sponsored by:

Gold Sponsor
riscure
Challenge your security

Silver Sponsor
Rambus
Cryptography Research