THE 14TH INTERNATIONAL WORKSHOP ON "CONSTRUCTIVE SIDE-CHANNEL ANALYSIS AND SECURE DESIGN"

CALL FOR PAPERS

April 3-4, 2023
Munich, Germany

Side-channel analysis (SCA) and implementation attacks have become an important field of research and a 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 14th International Workshop on Constructive Side-Channel Analysis and Secure Design will be organized by the Technical University of Munich and the Fraunhofer Institute for Applied and Integrated Security and will be held at the Fraunhofer Institute in Garching near Munich.

The program committee is seeking original papers on all aspects of the side-channel analysis and other implementation attacks as well as efficient and secure implementations. You are invited to participate and submit your contributions to COSADE'23. The workshop's submission topics include, but are not limited to:

- **Implementation attacks & countermeasures:** Side-channel analysis, fault-injection attacks, probing and read-out, hardware trojans, cloning and counterfeiting, side-channel or fault-injection based reverse engineering, attacks or countermeasures based on machine learning methods
- **Efficient and secure HW/SW implementations:** Efficient and secure implementations of cryptographic blocks including post-quantum cryptography, lightweight cryptography, random number generators, physical unclonable functions (PUFs), symmetric cryptography, hash functions, leakage-resilient cryptography, fault-resistant and tamper-detection designs, white-box cryptography
- **Hardware-intrinsic security:** Foundations and practical aspects of hardware-intrinsic security, use of instance-specific and process-induced variations in electronic devices for cryptography, novel PUF designs, hardware-intrinsic security threats, supply-chain protection
- **Measurement setups, evaluation platforms, and open benchmarks:** Practical implementation and comparison of physical attacks including description of measurement setups, test platforms for evaluation of physical attacks, open benchmarks for physical attacks and countermeasures
- **Formal analysis and automated tools:** 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, 5G, ...

Workshop website for more information:
https://www.cosade.org/cosade23/

Submissions Instructions

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 18 pages, excluding only 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: https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines

Important Dates:

All deadlines are 23:59:59 Anywhere on Earth (AoE).

Paper submission deadline:	~~November 28, 2022~~ December 12, 2022
Rebuttal phase:	January 9-13, 2023
Notification of acceptance:	January 23, 2023
Camera-ready version:	February 5, 2023

Submission Website

Authors are invited to submit papers (PDF format) electronically using the submission form available on

https://easychair.org/conferences/?conf=cosade2023