Call for Papers

12th International Workshop on
Constructive Side-Channel Analysis and Secure Design

COSADE 2021

Hybrid event - Lugano, Switzerland, 25 - 27 October 2021
https://www.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 efficient and secure implementations. 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 including methods based on machine learning
- **Efficient and secure HW/SW implementations:**
  Efficient and secure cryptographic implementations of cryptographic blocks including post-quantum cryptography, lightweight cryptography, random number generators, physical unclonable functions, symmetric cryptography, hash functions, leakage-resilient cryptography, fault-resistant and tamper-detection designs, white-box cryptography
- **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, …
- **Special Topics:**
  COSADE 2021 encourages special submissions related to:
  - Optimized measurement setups for side-channel and fault,
  - Implementation security of machine learning,
  - Efficient implementation and security evaluation of NIST PQC/LWC competition candidates.
  - Security of physical primitives like sensors and PUFs

Authors are invited to submit papers (PDF format) electronically by the submission link:
https://www.easychair.org/conferences/?conf=cosade2021

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:	4th April 2021
Notification of acceptance:	15th June 2021
Final version of papers:	2nd July 2021
Workshop date:	25th - 27th October 2021