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

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, the International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE) provides an international platform for researchers, academics, and industry participants to present their work and their current research topics. The Technical University of Munich and the Fraunhofer Institute for Applied and Integrated Security AISEC organize the 14th COSADE workshop at the Fraunhofer Institute in Garching near Munich. We would be happy to welcome you!

Program:

Sunday, April 2, 19:00-21:00: Welcome reception in a Bavarian restaurant in the center of Munich

Monday, April 3	
10:00	Registration
11:00	Opening/Welcome
11:15	**Keynote** **Lightweight Authenticated Encryption** Florian Mendel
12:15	Lunch
13:45	**Fault Injection Analyses and Countermeasures** • **SAMVA: Static Analysis for Multi-Fault Attack Paths Determination** A. Gicquel, D. Hardy, K. Heydemann, and E. Rohou • **Efficient Attack-Surface Exploration for Electromagnetic Fault Injection** D. A. E. Carta, V. Zaccaria, G. Quagliarella, and M. C. Molteni • **A CCFI Verification Scheme Based on the RISC-V Trace Encoder** A. Zgheib, O. Potin, J.-B. Rigaud, and J.-M. Dutertre
15:00	Coffee Break
15:45	**Side-Channel Analyses and Countermeasures** • **ASCA vs. SASCA - A Closer Look at the AES Key Schedule** E. Strieder, M. Ilg, J. Heyszl, F. Unterstein, and S. Streit • **Removing the Field Size Loss from Duc et al.'s Conjectured Bound for Masked Encodings** J. Béguinot, W. Cheng, S. Guilley, Y. Liu, L. Masure, O. Rioul, and F.-X. Standaert • **Improving Side-channel Leakage Assessment using Pre-silicon Leakage Models** D. Shanmugam and P. Schaumont
17:00	Bus Transfer to Social Event
18:00	Special Tour Nymphenburg Palace
19:30	Conference Dinner

Tuesday, April 4	
09:00	**Real-World Security – An Industrial Perspective** • **SOC: Spot the Odd Circuit** P.-Y. Liardet (eShard) • **Riscure Vision on Post Quantum Cryptography** M. Witteman (Riscure)
10:00	Coffee Break
10:45	**Attacks on PQC and Countermeasures** • **Fast First-Order Masked NTTRU** D. Heinz and G. Dreo Rodosek • **On the Feasibility of Single-Trace Attacks on the Gaussian Sampler Using a CDT** S. Marzougui, I. Kabin, J. Krämer, T. Aulbach, and J. P. Seifert • **Punctured Syndrome Decoding Problem: Efficient Side-Channel Attacks against Classic McEliece** V. Grosso, P.-L. Cayrel, B. Colombier, and V.-F. Dragoi
12:00	Lunch
13:30	**Keynote** **Recent Developments on Threshold Implementations** Siemen Dhooghe
14:30	Coffee Break
15:15	**Session 4: Analyses and Tools** • **Energy Consumption of Protected Cryptographic Hardware Cores - An Experimental Study** A. R. Shahmirzadi, T. Moos, and A. Moradi • **Whiteboxgrind - Automated Analysis of Whitebox Cryptography** T. Holl, K. Bogad, and M. Gruber • **White-Box Cryptography with Global Device Binding from Message-Recoverable Signatures and Token-Based Obfuscation** S. Agrawal, E. A. Bock, Y. Chen, and G. Watson
16:30	Farewell

Visit https://www.cosade.org for further information.

Venue:
Fraunhofer Institue for Applied and Integrated Security AISEC on the research campus in Garching (https://www.aisec.fraunhofer.de/)

Registration Fees:
Early Bird (until incl. Feb. 28, 2023): 250 EUR
Regular (Mar. 1 – Mar. 17, 2023): 300 EUR
Visit our website for further options

Registration Link: https://eveeno.com/cosade

www.cosade.org

Steering Committee
Jean-Luc Danger, Télécom ParisTech (FR)
Werner Schindler, BSI (DE)

General Chair
Georg Sigl, TUM & Fraunhofer AISEC (DE)

Program Chairs
Elif Bilge Kavun, Uni Passau (DE)
Michael Pehl, TUM (DE)