**Workshop on Nano Security**

**March 25, 2024, 14:00-17:30, Valencia (co-located with DATE conference)**

**Technical Program**

**14:00 Keynote**

Session chair: Michael Hutter, PQShield, Vienna

The Impact of Logic Synthesis and Technology Mapping on Logic Locking Security
*Lilas Alrahis, NYU Abu Dhabi*

**14:45 Session 1: Secure Architectures**

Session chair: Giorgio Di Natale, TIMA, Grenoble

Okapi: A Lightweight Architecture for Secure Speculation Exploiting Locality of Memory Accesses
*Philipp Schmitz[1], Tobias Jauch[1], Alex Wezel[1], Mohammad R. Fadiheh[2], Thore Tiemann[3], Jonah Heller[3], Thomas Eisenbarth[3], Dominik Stoffel[1], Wolfgang Kunz[1]*
*[1]RPTU Kaiserslautern-Landau, [2]Stanford U, [3]U Lübeck*

Neuromorphic and In-Memory Computing Based on Memristive Circuits for Predictive Maintenance and Supply-Chain Management and Security
*Nikolaos Athanasios Anagnostopoulos, Nico Mexis, Stefan Katzenbeisser, Elif Bilge Kavun, Tolga Arul, U Passau*

**15:15-16:00 Poster session: Projects of Priority Program Nano Security**

OnE-Secure: Securing State-of-the-Art Chips Against High-Resolution Contactless Optical and Electron-Beam Probing Attacks
*Sebastian Brand (FhG IMWS), Rolf Drechsler (U Bremen), Jean-Pierre Seifert TU Berlin), Frank Sill Torres (DLR)*

STAMPS-PLUS: Exploration of an integrated Strain-based TAMPer Sensor for Puf and trng concepts with best-in-class Leakage resilience and robUStness
*Ralf Brederlow (TU Munich), Matthias Hiller (FhG AISEC), Michael Pehl (TU Munich)*

RAINCOAT: Randomization in Secure Nano-Scale Microarchitectures 2
*Lucas Davi (U Duisburg-Essen), Tim Güneysu (RU Bochum)*

EMBOSOM: Embedded Software Security into Modern Emerging Hardware Paradigms
*Rolf Drechsler (U Bremen), Tim Güneysu (RU Bochum)*

MemCrypto: Towards Secure Electroforming-free Memristive Cryptographic Implementations
*Nan Du (FSU Jena), Ilia Polian (U Stuttgart)*

HaSPro: Verifiable Hardware Security for Out-of-Order Processors
*Thomas Eisenbarth (U Lübeck), Wolfgang Kunz (TU Kaiserslautern)*

NanoSec2: Nanomaterial-based platform electronics for PUF circuits with extended entropy sources
*Sascha Herrmann (TU Chemnitz), Stefan Kat-zenbeisser (U Passau), Elif Kavun (U Passau)*

SecuReFET: Secure Circuits through Inherent Reconfigurable FET
*Akash Kumar (TU Dresden), Thomas Mikolajick (NaMLab GmbH)*

SSIMA: Scalable Side-Channel Immune Micro-Architecture
*Amir Moradi (TU Darmstadt)*

SeMSiNN: Secure Mixed-SIgnal Neural Networks
*Maurits Ortmanns (U Ulm), Ilia Polian (U Stuttgart)*

**16:30 Session 2: Physical Aspects of Secure Computing in the Nano Regime**

Session chair: Francesco Regazzoni, University of Amsterdam and ALARI, Lugano

Hardware Trojan Detection Using Optical Probing
*Sajjad Parvin[1], Frank Sill Torres[2], Rolf Drechsler[1], [1]U Bremen, [2]DLR Bremen*

A Cautionary Note about Bit Flips in ReRAM
*Felix Staudigl[1], Jan Philipp Thoma[2], Christian Niesler[3], Karl J. X. Sturm[1], Rebecca Pelke[1], Dominik Sisejkovic[1], Jan Moritz Joseph[1], Tim Güneysu[2], Lucas Davi[3], Rainer Leupers[1]*
*[1]RWTH Aachen, [2]RU Bochum, [3]U Duisburg Essen*

An Analysis of the Effects of Temperature on the Performance of ReRAM-Based TRNGs
*Nico Mexis, Nikolaos Athanasios Anagnostopoulos, Stefan Katzenbeisser, Tolga Arul, U Passau*

**17:15 Session 3: Emerging Technologies for Security**

Session Chair: Haralampos Stratigopoulos, Sorbonne University, CNRS, LIP6, Paris

A Guide to Assessing Emerging Reconfigurable Nanotechnologies for Robust IP Protection
*Armin Darjani, Nima Kavand, Akash Kumar, TU Dresden*

Fingerprinting and Identification of Hall Sensors
*Christoph Frisch[1], Tobias Chlan[1], Carl Riehm[1], Markus Sand[2], Markus Stahl-Offergeld[3], Michael Pehl[1], Ralf Brederlow[1,3]*
*[1]TU Munich, [2]LZE GmbH, [3]Fraunhofer Institute for Integrated Circuits IIS*

Memristors in the Context of Security and AI
*Alexander Tekles, Tolga Arul, Nico Mexis, Stefan Katzenbeisser, Nikolaos Athanasios Anagnostopoulos, U Passau*

**18:00 Workshop end**