Workshop on Nano Security

April 2, 2025, 14:00-18:00, Lyon (co-located with DATE conference)

Final Technical Program

14:00 Keynote

Session chair: Ilia Polian, University of Stuttgart

MemComputing and Implications for Security
Massimiliano Di Ventra, University of California San Diego

15:00 Session 1: Secure Emerging Architectures and Technologies

Session chair: Francesco Regazzoni, UVA, The Netherlands and USI/ALARI, Switzerland

An Obfuscated 2-bit Adder/Half-Subtract Circuit with Reconfigurable Field Effect Transistors
Giulio Galderisi[1], Niladri Bhattacharjee[1], Marc Wijvliet[2], Shubham Rai[2], Akash Kumar[3], Thomas Mikolajick[1,4], Jens Trommer[1]
[1]*NaMLab gGmbH, Dresden, Germany*
[2]*Chair of Processor Design, TU Dresden, Germany*
[3]*Chair of Embedded Systems, Ruhr University Bochum, Germany*
[4]*Chair of Nanoelectronics, TU Dresden, Germany*

Designing Memory Protection for a RISC-V Nano-VP
Spandan Das, Christoph Lüth, Rolf Drechsler
Dept. Mathematics and Informatics, University of Bremen, Bremen, Germany

In-and-Beyond Boundaries: GPIO Signaling Research and Use-Cases with TrustZone
Christian Niesler[1], Markus Ströhnisch[1], Moritz Peters[2], Tim Güneysu[2], Lucas Davi[1]
[1]*University of Duisburg-Essen, Essen, Germany*
[2]*Ruhr University Bochum, Germany*

16:00 Coffee Break and Posters

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), Pascal Sasdrich (RU Bochum), Christoph Lüth (U Bremen)

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 Katzenbeisser (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)

17:00 Invited Talk

Session chair: Jens Trommer, NaMLab gGmbH, Dresden, Germany

A shallow view on hardware locking systems beyond digital. From research perspective to methods and practical tools.
Damian Dudek, Information Technology Society in the Association for Electrical, Electronic & Information Technologies (VDE)

17:20 Session 2: Physical Attacks

Session chair: Nan Du, University of Jena, Germany

Distinguishability between Multiplication and Squaring Operations: a New Marker
Alkistis Aikaterini Sigourou[1], Zoya Dyka[1,2], Peter Langendoerfer[1,2], Ievgen Kabin[1]
[1]IHP – Leibniz-Institut für innovative Mikroelektronik, Frankfurt (Oder), Germany
[2]BTU Cottbus-Senftenberg, Cottbus, Germany

SCA Test Results Depend on the Measurement Equipment: Riscure vs. Teledyne LeCroy
Dmytro Petryk[1], Zoya Dyka[1,2], Peter Langendoerfer[1,2], Ievgen Kabin[1]
[1]IHP – Leibniz-Institut für innovative Mikroelektronik, Frankfurt (Oder), Germany
[2]BTU Cottbus-Senftenberg, Cottbus, Germany

18:00 Workshop end