Workshop on Nano Security

April 18, 2023, 8:30-12:30, Antwerp (co-located with DATE conference)

Technical Program

8:30 Keynote

Session chair: Ilia Polian, University of Stuttgart

Securing the Internet of Bodies using Human Body as a 'Wire'
Shreyas Sen, Purdue University

9:15 Session 1: PUFs and RNGs

Session chair: Nan Du, University of Jena and Leibniz IPHT

Carbon-Nanotube-Based Physical Unclonable Functions and True Random Number Generators
Nikolaos Athanasios Anagnostopoulos[1], Tolga Arul[1,2], Simon Böttger[3], Florian Frank[1], Ali Mohamed[3], Martin Hartmann[3], Sascha Hermann[3,4] and Stefan Katzenbeisser[1],
[1]University of Passau, [2]TU Darmstadt, [3]TU Chemnitz, [4]Fraunhofer ENAS, Chemnitz

Towards a PVT-Variation Resistant Resistor-Based PUF
Carl Riehm[1], Christoph Frisch[1], Florin Burcea[1], Matthias Hiller[2], Michael Pehl[1] and Ralf Brederlow[1],
[1]TU Munich [2]Fraunhofer AISEC, Garching

9:45 Session 2: Side-channel Attacks

Session chair: Ingrid Verbauwhede, KU Leuven

Practical Considerations for Optical Side-Channel Analysis: A Case Study on Reconfigurable FETs
Thilo Krachenfels[1], Giulio Galderisi[2], Thomas Mikolajick[2,3], Jens Trommer[2] and Jean-Pierre Seifert[1,4],
[1]TU Berlin, [2]NaMLab gGmbH, Dresden, [3]TU Dresden, [4]Fraunhofer SIT, Darmstadt

Side-Channel Leakage Evaluation of Multi-Chip Cryptographic Modules
Kazuki Monta[1], Takumi Matsumaru[1], Takaaki Okidono[2], Takuji Miki[1] and Makoto Nagata[1],
[1]Kobe U [2]SCU Co. Ltd, Tokyo

10:15-11:00 Poster session: Projects of Priority Program Nano Security

Session Chair: Shahar Kvatinsky, Technion

PUFMem: Intrinsic Physical Unclonable Functions from Emerging Non-Volatile Memories
Tolga Arul, Stefan Katzenbeisser, Florian Frank, University of Passau

nanoEBeam: E Beam Probing for backside attacks against nanoscale ICs
Frank Altmann, Jörg Jatzkowski, FhG IMWS Halle, Elham Amini, Jean-Pierre Seifert, Christian Boit
Thilo Krachenfels, TU Berlin

STAMPS: From Strain to Trust: tAMper aware silicon PufS
Ralf Brederlow, TU Munich, Matthias Hiller, FhG AISEC

RAINCOAT: Randomization in Secure Nano-Scale Microarchitectures
Christian Niesler[1], Jan Thoma[2], Lucas Davi[1], Tim Güneysu[2]
[1]University of Duisburg-Essen, [2]Ruhr University Bochum

OptiSecure: Securing Nano-Circuits against Optical Probing
Sajjad Parvin[1], Thilo Krachenfels[2], Frank Sill Torres[3], Jean-Pierre Seifert[2,4], Rolf Drechsler[1,5]
[1]University of Bremen, [2]TU Berlin, [3]DLR, Bremerhaven, [4]Fraunhofer SIT, Darmstadt, [5]DFKI, Bremen

MemCrypto: Towards Secure Electroforming-free Memristive Cryptographic Implementations
Nan Du (University of Jena and Leibniz IPHT), Ilia Polian (University of Stuttgart)

HaSPro: Verifiable Hardware Security for Out-of-Order Processors
Thomas Eisenbarth, University of Lübeck, Wolfgang Kunz, Tobias Jauch, TU Kaiserslautern

NANOSEC: Tamper-Evident PUFs based on Nanostructures for Secure and Robust Hardware Security Primitives
Sascha Hermann, TU Chemnitz, Stefan Katzenbeisser, Nikolaos Athanasios Anagnostopoulos, University of Passau

SecuReFET: Secure Circuits through inherent Reconfigurable FET
Shubham Rai, Akash Kumar, TU Dresden
Giulio Galderisi, Thomas Mikolajick, Jens Trommer, NaMLab gGmbH, Dresden

BioNanoLock: Bio-Nanoelectronic based Logic Locking for Secure Systems
Farhad Amirali Merchant, Vivek Pachauri, Rainer Leupers, Elmira Moussavi, RWTH Aachen

RRAMPUFTRNG: CMOS-compatible RRAM-based structures for the implementation of Physical Unclonable Functions (PUF) and True Random Number Generators (TRNG)
Sahitya Yarragolla, Torben Hemke, Thomas Mussenbrock, Ruhr University Bochum

11:00 Session 3: Trustworthy Electronics

Session chair: Jean-Pierre Seifert, TU Berlin

Quantifying Trust in Hardware through Physical Inspection
Bernhard Lippmann[1], Matthias Ludwig[1] and Horst Gieser[2],
[1]Infineon Technologies AG, Munich [2]Fraunhofer EMFT, Munich

(Un)Attractiveness for State Machine Obfuscation
Michaela Brunner[1], Hye Hyun Lee[1], Alexander Hepp[1], Johanna Baehr[1] and Georg Sigl[1,2],
[1]TU Munich [2]Fraunhofer AISEC, Garching

Thwarting Structural Attacks on Logic Locking with Reconfigurable Nanotechnologies
Armin Darjani, Nima Kavand and Akash Kumar,
TU Dresden

11:45 Panel

Moderator: Ilia Polian, University of Stuttgart

Security Issues in Heterogeneous Systems

Panelists:
Farimah Farahmandi, University of Florida
Sandip Kundu, University of Massachusetts, Amherst
Shahar Kvatinsky, Technion
Johanna Sepulveda, Airbus Defence and Space

12:30 Lunch