Workshop on Nano Security

April 21, 2026, 14:00-18:00, Verona (co-located with DATE conference)

Final Technical Program

14:00 Keynote

Session chair: Ilia Polian(University of Stuttgart)

Intelligent & Perceptive Attack Counteraction for Next-Generation Secure Chips – From Sensing to Learning
Massimo Alioto (ECE – National University of Singapore)

14:45 Session 1: Modeling and Simulation of Hardware Security Threats

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

Integrating Optical Probing Security Evaluation Framework Into ASIC Design Flow
Sajjad Parvin (U Bremen), Frank Sill Torres (DLR), Rolf Drechsler (U Bremen an DFKI)

Limitations of Architectural Simulation for Security: Why Transient-Execution Countermeasures Must Be Designed and Evaluated on the RTL
Tobias Jauch, Philipp Schmitz, Alex Wezel, Simón Blanko Ortiz, Mohammad Rahmani Fadiheh, Dominik Stoffel, Wolfgang Kunz (RPTU Kaiserslautern-Landau)

Modeling of Tamper Resistance to Correlative Electromagnetic Analysis for Voltage-scaled Circuits
Yusuke Matsubayashi, Kazuki Minamiguchi, Hiroki Nishikawa, Yoshihiro Midoh, Noriyuki Miura and Jun Shiomi (U Osaka)

15:30 Coffee Break and Posters

EMBOSOM: Embedded Software Security into Modern Emerging Hardware Paradigms
Rolf Drechsler (U Bremen), Tim Güneysu and Pascal Sasdrich (RU Bochum), Christoph Lüth (U Bremen)

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

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

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

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)

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

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

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

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

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)

16:05 Special Session on Secure Compute-in-Memory Architectures

Session chair: Mahdi Fazeli, Halmstad University

Security Aspects of Computing-in-Memory Architectures in AI Era
Ahmad Patooghy (North Caroline A&T U), Mahdi Fazeli (Halmstad University)

A Case Study: Secure Reconfigurable FET-Based SRAM Architecture for In-Memory Computing
Farah Naz Syed (RU Bochum), Peng Chong, Juan Martinez, Stefan Slesazeck, Jens Trommer, Thomas Mikolajick (NamLab gGmbH), Akash Kumar (RU Bochum)

16:30 Session 2: Physical Attack Protections

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

Preventing Distinguishability between Multiplication and Squaring Operations
Alkistis Aikaterini Sigourou (Leibniz IHP), Zoya Dyka (Leibniz IHP and BTU Cottbus-Senftenberg), Peter Langendoerfer (BTU Cottbus-Senftenberg), Ievgen Kabin (Leibniz IHP)

Logic Locking with Lightweight Cryptography
Levent Aksoy (TU Tallinn), Muhammad Sohaib Munir (TU Tallinn), Sedat Akleylek (U Tartu)

Lifecycle Protecting Integrated Circuits Using Physical Unclonable Functions
Michael Pehl, Carl Riehm, Tim Music (TU Munich), Valentin Huber, Matthias Hiller (FhG AISEC), Ralf Brederlow (TU Munich)

17:15 Session 3: Emerging Technologies and Security

Session chair: Paolo Palmieri, University College Cork

Exploiting Ultra-Low Voltage RFETs for Dynamic Circuit Obfuscation in Embedded Security
Giulio Galderisi, Yuxuan He (NaMLab gGmbH), Aniruddh Holemadlu (RU Bochum), Juan Martinez, Thomas Mikolajick (NaMLab gGmbH), Akash Kumar (RU Bochum), Jens Trommer NaMLab gGmbH

Dynamic Key Change Scheme for Protecting Arbitrary Data Communication in a Multi-Die IC
Zheng-Hao Wang, Shi-Yu Huang (NTHU Taiwan), Chi-Kang Chen (TESDA)

Evaluation of Carbon Nanotube-based Integrated Crossbar PUFs
Martin Schmid (U Passau), Simon Böttger, Martin Ernst, Martin Hartmann, Sascha Hermann (TU Chemnitz), Elif Bilge Kavun (TU Dresden) Stefan Katzenbeisser (U Passau)

18:00 Workshop end

Talk abstracts see next page.

Abstracts

Keynote

Intelligent & Perceptive Attack Counteraction for Next-Generation Secure Chips – From Sensing to Learning

Massimo Alioto, ECE – National University of Singapore

Abstract: Physical security of next-generation silicon systems mandates major advances at their physical boundary, and hence in both on-chip sensing for attack detection and on-chip actuation for attack counteraction. This has recently motivated the investigation of a new class of on-chip always-on sensor interfaces and actuators that inexpensively monitor the chip environment, gaining physical context awareness and capturing physical anomalies. This trend is progressively fusing with relentless advances in inexpensive on-chip (AI) intelligence, which can oversee physical signals and events to orchestrate the on-chip security ecosystem.

In this keynote, the road towards ubiquitous intelligent & perceptive hardware security countermeasures is illustrated through a wide range of recent silicon demonstrations with unprecedented capabilities to perceive security events inexpensively, and react to them intelligently, all the time. The new concept of hardware patching and self-learned security is also discussed where circuit flexibility is introduced to make silicon chips able to evolve over time and counteract newly discovered vulnerabilities through (machine) learning-based physical protection mechanisms. Ultimately, this leads to a new exciting trend with hardware security improving over time, extending traditional software-level security to silicon systems chips.

Bio: Massimo Alioto is Provost's Chair Professor at the ECE Department of the National University of Singapore, where he leads the Green IC group and the Integrated Circuits and Embedded Systems area, among the others. Previously, he held positions at the University of Siena, Intel Labs – CRL (2013), University of Michigan - Ann Arbor (2011-2012), University of California – Berkeley (2009-2011), EPFL - Lausanne. He is (co)author of >400 publications on journals and conference proceedings, and four books with Springer (with two more coming). His primary research interests include ultra-low power and self-powered systems, green computing, circuits for machine intelligence, hardware security, and emerging technologies.

He was the Editor in Chief of the IEEE Transactions on VLSI Systems and Deputy Editor in Chief of the IEEE Journal on Emerging and Selected Topics in Circuits and Systems. He was the Chair of the Distinguished Lecturer Program for the IEEE CAS Society, and was a Distinguished Lecturer for the SSC and CAS Society. Previously, Prof. Alioto was the Chair of the "VLSI Systems and Applications" Technical Committee of the IEEE Circuits and Systems Society (2010-2012). He served as Guest Editor of numerous journal special issues (JSSC, TCAS-I, JETCAS…), Technical Program Chair of several IEEE conferences (ISCAS, SOCC, PRIME, ICECS), and TPC member (ISSCC, ASSCC), and is currently Associate Editor of the IEEE Journal on Solid-State Circuits and in the AdCom of SSCS. His research group contribution has been recognized through various best paper awards (e.g., ISSCC), and in the ten technological highlights of the TSMC annual report, among the others. Prof. Alioto is an IEEE Fellow.

Session 1: Modeling and Simulation of Hardware Security Threats

Integrating Optical Probing Security Evaluation Framework Into ASIC Design Flow

Sajjad Parvin (U Bremen), Frank Sill Torres (DLR), Rolf Drechsler (U Bremen an DFKI)

Abstract: Recently, a non-invasive laser-based Side-Channel Analysis (SCA) attack, namely Optical Probing (OP) attack, has been shown to pose an immense threat to the security of sensitive information on chips. Many published countermeasures mitigate OP by modifying the chip fabrication process, making them costly and often impractical for widespread adoption. In this work, we present an OP security evaluation framework that allows designers to assess and explore OP countermeasures directly at the circuit and layout-level, without relying on foundry-level process changes. The framework automates pre-silicon leakage analysis, enabling designers to quantify a design's robustness against OP attacks early in the development flow. By integrating security evaluation into the design phase, our approach supports informed trade-offs among power, area, performance, and security, and facilitates iterative circuit-level hardening before tape-out.

Limitations of Architectural Simulation for Security: Why Transient-Execution Countermeasures Must Be Designed and Evaluated on the RTL

Tobias Jauch, Philipp Schmitz, Alex Wezel, Simón Blanko Ortiz, Mohammad Rahmani Fadiheh, Dominik Stoffel, Wolfgang Kunz (RPTU Kaiserslautern-Landau)

Abstract: Transient execution side channels (TES) exploit the speculative mechanisms of modern CPUs to leak sensitive information through the microarchitectural state, as evidenced by Spectre-type vulnerabilities and continuing real-world exploits. While most research publications evaluate proposed secure-speculation countermeasures using architectural simulators, such as gem5, we argue that simulator-only evaluation is insufficient. Simulation lacks detail necessary to establish robust security guarantees, assess accurate overheads, or ensure feasibility of implementation. Based on case studies and RTL evaluation, we identify three recurring gaps between high-level simulation and hardware reality:

(i) a security gap, where microarchitectural transmitters and subtle timing behaviors may not be detectable in architectural simulation,
(ii) a performance evaluation gap, where freely chosen simulator parameters and simplified memory-system timing can significantly skew results, and
(iii) a hardware cost and feasibility gap, where critical paths, wiring complexity, and comparison-heavy logic can dominate both achievable frequency and practicality.

We motivate an RTL-focused evaluation in which architectural simulation remains essential for early exploration, but security sign-off, evaluation of timing and area overheads, and feasibility assessment are performed on RTL implementations, ideally augmented with systematic analysis under a formally defined threat model.

Modeling of Tamper Resistance to Correlative Electromagnetic Analysis for Voltage-scaled Circuits

Yusuke Matsubayashi, Kazuki Minamiguchi, Hiroki Nishikawa, Yoshihiro Midoh, Noriyuki Miura and Jun Shiomi (U Osaka)

Abstract: This paper proposes a voltage dependence model of tamper resistance to Correlative ElectroMagnetic Analysis (CEMA). ElectroMagnetic (EM) side-channel analysis is a critical threat to embedded crypto circuits in our information society. Attackers can noninvasively steal the secret key information by analyzing data-dependent EM leakage from the crypto circuits. It is well known that the attackers need more EM traces to disclose the secret key information if the supply voltage of the crypto circuits is downscaled. Therefore, the low-voltage operation has the potential to reduce the number of time-consuming rekeying operations which update the secret key information before the key information is disclosed. Motivated by this tradeoff relationship, this paper firstly presents a concept of a tamper-resistance-aware voltage scaling problem. The voltage-dependent tamper resistance model of CEMA is then proposed. The proposed model is then validated by using the measurement results of an Advanced Encryption Standard (AES) processors fabricated with a 180-nm process technology.

Special Session on Secure Compute-in-Memory Architectures

A Case Study: Secure Reconfigurable FET-Based SRAM Architecture for In-Memory Computing
Farah Naz Syed (RU Bochum), Peng Chong, Juan Martinez, Stefan Slesazeck, Jens Trommer, Thomas Mikolajick (NamLab gGmbH), Akash Kumar (RU Bochum)

Abstract: The article presents the study of a reconfigurable field effect transistor (RFET) based in-memory computing (IMC) architecture that combines logic and memory primitive circuit blocks within a unified device-circuit model. This architecture is based on a fundamental set of RFET-based primitive circuit blocks, such as NOT, NAND gates, an SRAM cell, and a sense amplifier, which facilitate binary computations within the memory array. By leveraging the inherent polarity reconfigurability of RFET devices, this IMC architecture eliminates the need for peripheral logic to switch between memory and computing modes. Unlike CMOS circuits that show asymmetrical I-V characteristics for p- and n-type transistors, RFET devices show symmetrical characteristics, which reduces power variation and improves security against power side-channel attacks. This RFET-based secure SRAM architecture demonstrates a higher read noise margin compared to a traditional CMOS-based SRAM approach, as verified through simulation results, which is a result of enhanced control of channel conduction with reduced bit-line voltage contention, thus reducing charge-sharing effects under process variations. In addition, this secure SRAM architecture demonstrates a lower leakage power consumption, which is a result of suppressed sub-threshold and junction leakages using electrostatically created source/drain junctions in the non-conducting state of RFET devices.

Session 2: Physical Attack Protections

Preventing Distinguishability between Multiplication and Squaring Operations
Alkistis Aikaterini Sigourou (Leibniz IHP), Zoya Dyka (Leibniz IHP and BTU Cottbus-Senftenberg), Peter Langendoerfer (BTU Cottbus-Senftenberg), Ievgen Kabin (Leibniz IHP)

Abstract: Scalar multiplication kP is a critical operation in Elliptic Curve Cryptosystems (ECC), often targeted by Side-Channel Analysis (SCA). Despite strategies based on atomic patterns to enhance security, the binary kP algorithms remain susceptible to simple SCA due to energy consumption variations in field multipliers during passing two different or two identical operands. This vulnerability arises independent of the multiplication method used. We implemented and analysed two mitigation techniques: one involving data redirection and another focusing on bus reloading.

Logic Locking with Lightweight Cryptography
Levent Aksoy (TU Tallinn), Muhammad Sohaib Munir (TU Tallinn), Sedat Akleylek (U Tartu)

Abstract: In the globalized integrated circuit (IC) manufacturing supply chain era, the hardware security threats, such as overproduction and piracy, have been causing serious damage to the IC design industry. Many techniques proposed to mitigate these threats have been broken since they do not rely on provably secure algorithms, and the ones using cryptography algorithms increase the hardware complexity significantly and have been vulnerable to removal and power analysis attacks. In this paper, we integrate a lightweight cryptography algorithm into a prominent logic locking technique and introduce a computer-aided design tool called LINDA, which automates the logic encryption process. Experimental results show that the secure designs generated by LINDA have significantly less hardware complexity when compared to those generated by previously proposed techniques using cryptography algorithms and are resilient to existing removal, algebraic, and logic locking attacks.

Lifecycle Protecting Integrated Circuits Using Physical Unclonable Functions
Michael Pehl, Carl Riehm, Tim Music (TU Munich), Valentin Huber, Matthias Hiller (FhG AISEC), Ralf Brederlow (TU Munich)

Abstract: In globalized markets, protecting chips throughout the supply chain and their entire lifecycles becomes increasingly difficult. In this extended abstract, we propose a novel concept to protect chips along the supply chain and over their entire lifetime. The key to protection is a strain-

based Physical Unclonable Function (PUF) and a cryptography-based authentication scheme. Both together protect the particularly critical chip transport. This work also discusses the security properties of the scheme.

Session 3: Emerging Technologies and Security

Exploiting Ultra-Low Voltage RFETs for Dynamic Circuit Obfuscation in Embedded Security
Giulio Galderisi, Yuxuan He (NaMLab gGmbH), Aniruddh Holemadlu (RU Bochum), Juan Martinez, Thomas Mikolajick (NaMLab gGmbH), Akash Kumar (RU Bochum), Jens Trommer NaMLab gGmbH

Abstract: Reconfigurable Field Effect Transistors are fully CMOS-compatible emerging devices able to switch between n-type and p-type operation modes at runtime. Their inherent polymorphism can be extended to the logic gate level enabling circuit obfuscation beyond traditional CMOS solutions. In this abstract we present the Three-Independent-Gate version of Reconfigurable Field Effect Transistors operating at 0.8 V fabricated on an industrial 22nm FDSOI platform from GlobalFoundries. We exploit the inherent self-dual nature of the logic gates built upon them to implement a circuit obfuscation scheme with the aim of merging two different circuits into a single one, illustrating a method that can be scaled towards larger cryptographic engines to mask their functionality to outside attackers. The method is validated by simulating a merged adder/half-subtract reconfigurable circuit in Cadence Virtuoso, using a developed Verilog-A model of the scaled version of the devices.

Dynamic Key Change Scheme for Protecting Arbitrary Data Communication in a Multi-Die IC
Zheng-Hao Wang, Shi-Yu Huang (NTHU Taiwan), Chi-Kang Chen (TESDA)

Abstract: In a multi-die IC, each die can come from different manufacturers and be assembled together. However, during assembly, these ICs face critical security threats in which unauthorized dies can be inserted and fully exposed die-to-die interconnects allow sensitive data to be eaves-dropped by unauthorized dies. To address this, we propose a low-cost dynamic key change scheme to protect arbitrary data communication among functional dies with minimal overhead. Experiments on FPGA demonstrate the effectiveness of our scheme integrated into a multi-die SoC design.

Evaluation of Carbon Nanotube-based Integrated Crossbar PUFs
Martin Schmid (U Passau), Simon Böttger, Martin Ernst, Martin Hartmann, Sascha Hermann (TU Chemnitz), Elif Bilge Kavun (TU Dresden) Stefan Katzenbeisser (U Passau)

Abstract: Physical unclonable functions (PUFs) based on carbon nanotube field-effect transistors (CNTFETs) offer promising characteristics for hardware security applications. This work presents the fabrication and comprehensive evaluation of CNT-PUFs implemented in 12x12 crossbar structures, assessed through measurements on real hardware. We demonstrate that CNTFETs retain their PUF-suitable properties when embedded in crossbar structures, yielding serially addressable ternary PUF responses comprising 144 trits. Based on 10 fabricated instances with four repeated measurements each, we evaluate uniformity, spatial correlation, uniqueness, and robustness. Despite non-ideal uniformity attributed to CNT reduction during fabrication, the devices achieve nearly ideal uniqueness (31.6% of theoretical 32.0% inter-device Hamming distance) and high robustness (maximum 3 unstable cells out of 144 per device), enabling practical deployment with low-cost error correction methods.