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.