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.