Session 36 Overview: *Hardware Security*

DIGITAL ARCHITECTURES AND SYSTEMS SUBCOMMITTEE

2021 IEEE International Solid- State Circuits Conference (ISSCC) | 978-1-7281-9549-0/20/$31.00 ©2021 IEEE | DOI: 10.1109/ISSCC42613.2021.9365930

Session Chair:
Hirofumi Shinohara
Waseda University, Kitakyushu, Japan

Session Co-Chair:
Massimo Alioto
National University of Singapore, Singapore

Session Moderator:
Ingrid Verbauwhede
KU Leuven, Leuven, Belgium

With the proliferation of electronics in intelligent and connected devices, the need for hardware security continues to grow. Security primitives require increasing levels of protection against physical manipulation and passive side-channel attacks. The first paper describes a unified in-memory TRNG/PUF, followed by techniques for power and EM side-channel attack resistance. A strong PUF based on an SPN network and hot-carrier injection is presented. The next two papers cover additional PUFs, which are respectively based on oscillator collapse and a self-checking and self-healing technique.

9:15 AM

36.1 Unified In-Memory Dynamic TRNG and Multi-Bit Static PUF Entropy Generation for Ubiquitous Hardware Security

Sachin Taneja, National University of Singapore, Singapore, Singapore

In Paper 36.1, the National University of Singapore uses a single 16Kb SRAM for unified dynamic/static entropy generation, achieving 3.6Mbps TRNG throughput and 1.78-to-3.84% PUF BER in 28nm CMOS.

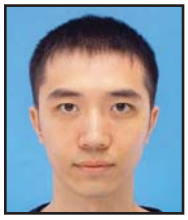
9:23 AM

36.2 An EM/Power SCA-Resilient AES-256 with Synthesizable Signature Attenuation Using Digital-Friendly Current Source and RO-Bleed-Based Integrated Local Feedback and Global Switched-Mode Control

Archisman Ghosh, Purdue University, West Lafayette, IN

In Paper 36.2, Purdue in collaboration with Intel, evaluates the resistance against power and EM side-channel attacks of an AES256 implemented in 65nm CMOS with two countermeasures: a digital signal attenuation circuit with a synthesizable current source and digital RO-bleed, and a time-varying transfer function, improving security by 25% over existing work.

9:31 AM



36.3 A Modeling Attack Resilient Strong PUF with Feedback-SPN Structure Having <0.73% Bit Error Rate Through In-Cell Hot-Carrier Injection Burn-In

Kunyang Liu, Waseda University, Kitakyushu, Japan

In Paper 36.3, Waseda University shows a modeling-attack-resilient strong PUF robust against 20M training CRPs, featuring less than 0.73% BER through in-cell hot-carrier injection burn-in in 130nm CMOS.

9:39 AM

36.4 A Physically Unclonable Function Combining a Process Mismatch Amplifier in an Oscillator Collapse Topology

Jaehan Park, Pohang University of Science and Technology, Pohang, Korea

In Paper 36.4, Pohang University of Science and Technology presents a hybrid PUF combining a process-mismatch amplifier in an oscillator-collapse topology fabricated in 40nm CMOS. The proposed scheme achieves a worst case BER of 0.0019% across a supply voltage of 0.7 to 1.4V and a temperature of -40 to 125°C after stabilizations.

9:43 AM

36.5 An Automatic Self-Checking and Healing Physically Unclonable Function (PUF) with $<3\times10^{-8}$ Bit Error Rate

Yan He, Rice University, Houston, TX

In Paper 36.5, Rice University presents a self-checking and healing technique to improve the reliability of PUF cells, requiring only 27% masking ratio to achieve BER of 3.34E-8 across -40-125°C and 0.7-1.4V supply in 65nm CMOS.