Sunday June 2, 2013

8:45-9:00am: Opening Remarks
Ramesh Karri (NYU-Poly) and Farinaz Koushanfar (Rice U)

9:00-10:00am: Opening Keynote
Session Chair: Michael Hsiao (Virginia Tech)

Title: The Reincarnation and Untapped Potential of Trusted Computing
Prof. Dr. Ing. Ahmad-Reza Sadeghi; Professor at TU Darmstadt and Scientific Director of Fraunhofer Inst. for Secure Information Systems (SIT), Director of Intel-TU Darmstadt Security Inst.

10:00-10:20am: Break

10:20-11:35am Physically Unclonable Functions I
Session Chair: Ingrid Verbauwhede (KU Leuven)

Cloning Physically Unclonable Functions
Clemens Helfmeier, Dmitry Nedospasov, Christian Boit and Jean-Pierre Seifert (Semiconductor Devices, TU Berlin)

Intellectual Property Protection for FPGA Designs with Soft Physical Hash Functions: First Experimental Results
Stéphanie Kerckhof, François Durvaux, François-Xavier Standaert and Benoit Gérard (UCL Crypto Group)

Novel Strong PUF based on Nonlinearity of MOSFET Subthreshold Operation
Mukund Kalyanaraman and Michael Orshansky (University of Texas at Austin)

11:45am-1:00pm: Lunch

1:00-2:00pm: Poster Session and Industrial Demo

Microsemi Product Demo: Using a Microsemi SmartFusion®2 SoC FPGA as the Root-of-Trust to Securely Boot a Target Processor
Presenter: Richard Newell, Senior Principal Product Architect, SoC Products Group, Microsemi Corp.

Poster: Information Leakage behind the Curtain: Abusing Anti-EMI Features for Covert Communication
Johannes Bauer, Sebastian Schinzel and Felix Freiling (Friedrich-Alexander Universität Erlangen)

Poster: Localized Electromagnetic Analysis of RO PUFs
Dominik Merli, Johann Heyszl, Benedikt Heinz, Dieter Schuster, Frederic Stumpf and Georg Sigl (Fraunhofer Research Institution AISEC)

Poster: Enhancing Fault Sensitivity Analysis Through Templates
Filippo Melzani and Andrea Palomba (ST Microelectronics)

Poster: Hardware Implementations of the WG-5 Cipher for Passive RFID Tags
Mark Aagaard, Guang Gong and Rajesh Mota (U of Waterloo)

Poster: Adapting Voltage Ramp-up Time for Temperature Noise Reduction on Memory-based PUFs
6th Annual IEEE International Symposium on Hardware-Oriented Security and Trust (HOST’13)

Mafalda Cortez, Vincent van der Leest, Roel Maes, Geert-Jan Schrijen and Said Hamdioui (Delft U)

Poster: Model Building attacks on Physically Unclonable Functions using Genetic Programming
Indrasish Saha, Ratan Rahul Jeldi and Rajat Subhra Chakraborty (IIT-Kharagpur)

Poster: BISA: Built-In Self-Authentication for Preventing Hardware Trojan Insertion
Kan Xiao and Mohammad Tehranipoor (University of Connecticut)

Poster: A Bulk Built-in Sensor for Detection of Fault Attacks
Rodrigo Possamai Bastos, Frank Sill Torres, Jean-Max Dutertre, Marie-Lise Flottes, Giorgio Di Natale and Bruno Rouzeyre (TIMA Lab (CNRS - Grenoble INP - UJF))

2:00-2:20pm: Break

2:20-3:35pm: Obfuscation and Identification
Session Chair: William Robinson (Vanderbilt U)

Structural Transformation for Best-Possible Obfuscation of Sequential Circuits
Li Li and Hai Zhou (Northwestern University)

An Efficient Algorithm for Identifying Security Relevant Logic and Vulnerabilities in RTL Designs
David W. Palmer and Parbati Kumar Manna (Intel)

WordRev: Finding Word-Level Structures in a Sea of Bit-Level Gates
Wenchao Li, Adria Gascon, Pramod Subramanyan, Wei Yang Tan, Ashish Tiwari, Sharad Malik, Natarajan Shankar and Sanjit A. Seshia (UC Berkeley)

3:35-4:00pm: Break

4:00-5:40pm: Novel Implementations
Session Chair: Francesco Regazzoni (TU Delft)

On Implementing Trusted Boot for Embedded Systems
Muhammad Khalid, Carsten Rolfes and Andreas Ibing (Fraunhofer AISEC)

Low-Cost and Area-Efficient FPGA Implementations of Lattice Based Cryptography
Aydin Aysu, Cameron Patterson and Patrick Schaumont (Virginia Tech)

Design and Implementation of Rotation Symmetric S-boxes with High Nonlinearity and High DPA Resilience
Bodhisatwa Mazumdar, Debdeep Mukhopadhyay and Indranil Sengupta (IIT Kharagpur)

On-chip Lightweight Implementation of Reduced NIST Randomness Test Suite
Vikram Suresh, Daniele Antonioli and Wayne Burleson (University of Massachusetts, Amherst)

5:40-6:30pm: Reception
Monday June 3, 2013

9:00-10:00am: Monday Keynote
Session Chair: Ted Huffmire (Naval Postgraduate School)
Title: Achieving Trust in design and manufacturing through the application of Circuit Camouflage
Dr. Ron Cocchi, Ph.D., Vice President and Chief Technology Officer, Syphermedia International.

10:00-10:15am: Break

10:15-11:30am: Hardware Trojan
Session Chair: Swarup Bhunia (Case Western U)
Cycle-Accurate Information Assurance by Proof-Carrying Based Signal Sensitivity Tracing
Yier Jin, Bo Yang and Yiorgos Makris (University of Central Florida)
On Hardware Trojan Design and Implementation at RTL
Jie Zhang and Qiang Xu (The Chinese University of Hong Kong)
Malicious Circuitry Detection Using Fast Timing Characterization via Test Points
Sheng Wei and Miodrag Potkonjak (University of California, Los Angeles)

11:30-12:45pm: Lunch and Lunch Keynote
Session Chair: Mohammad Tehranipoor (U Connecticut)
Title: “Counterfeit IC’s – What’s Done and What Must be Done?”
Dan Dimase, Honeywell

12:45-2:00pm Panel
Panel: “Trust me, my chip is more secure than his!”
Organized by Dr. Vivek Vedula, Freescale,
Moderator Dr. Celia Merzbacher, SRC
Panelists: Chen-Yong Cher, IBM, Rob Aitken, ARM, Flemming L. Andersen, Soja Richard Freescale, Winhtrop Wu, AMD

2:00-3:15pm: Side Channel
Session Chair: Yiorgos Makris (UT Dallas)
Frontside Laser Fault Injection on Cryptosystems - Application to the AES last round -
Cyril Roscian, Jean-Max Dutertre and Assia Tria (Ecole Nationale Supérieur des Mines de Saint Etienne (ENSMSE)
Side-Channel Analysis of MAC-Keccak
Mostafa Taha and Patrick Schaumont (Virginia Tech)
Pre-Processing Power Traces with a Phase-Sensitive Detector
Philip Hodgers, Neil Hanley and Maire O’Neill (Queens University Belfast)

3:15-3:30pm: Break

3:30-4:45pm: Physically Unclonable Functions II
Session Chair: Jean-Pierre Seifert (TU Berlin)
Austin Convention Center, Austin, TX, USA
Side Channel Modeling Attacks on 65nm Arbiter PUFs Exploiting CMOS Device Noise
Jeroen Delvaux and Ingrid Verbauwhede (KU Leuven)

Stability Analysis of a Physical Unclonable Function based on Metal Resistance Variations
Jing Ju, Raj Chakraborty, Charles Lamech and Jim Plusquellic (University of New Mexico)

An Error-Tolerant Bit Generation Technique For Use With A Hardware-Entangled Path Delay PUF
James Aarestad, Dhruva Acharyya and Jim Plusquellic (University of New Mexico)

4:45-5:00pm: Closing Remarks & Best Student Paper Award