Tuesday, May 6

8:45 - 9:00 Opening Remarks
HOST 2014 General and Program Chairs

9:00 - 10:00 SESSION 1: KEYNOTE
Kerry Bernstein, DARPA
"Insuring the Integrity of Our Electronic Component Supply Chain" 10:00 - 10:20 BREAK

10:20 - 11:35 SESSION 2: SPLIT FABRICATION
Session Chair: Jim Plusquellic

- Kaushik Vaidyanathan, Bishnu P Das, Ekin Sumbul, Renzhi Liu and Larry Pileggi. Building Trusted ICs using Split Fabrication
- Meenatchi Jagasivamani, Peter Gadfort, Michel Sika, Michael Bajura and Michael Fritze. Split Fabrication Obfuscation: Metrics and Techniques

11:45 - 1:00 LUNCH

Industrial Talk (MicroSemi): Securing Reconfigurable Devices and Designs Against > Insiders and Other Supply Chain Threats

1:00 - 2:15 SESSION 3: HARDWARE TRUST & CHARACTERIZATION
Session Chair: Hassan Salmani

- Franco Stellari, Peilin Song, Alan Weger, James Culp, Alyssa Herbert and Dirk Pfeiffer. Verification of Untrusted Chips using Trusted Layout and Emission Measurements
- Jean-Michel Cioranesco, Jean-Luc Danger, Tarik Graba, Sylvain Guilley, Yves Mathieu, David Naccache and Xuan Thuy Ngo. Cryptographically Secure Shields
Daisuke Fujimoto, Daichi Tanaka, Noriyuki Miura, Makoto Nagata, Yu-Ichi Hayashi, Naofumi Homma, Shivam Bhasin and Jean-Luc Danger. Side-Channel Leakage on Silicon Substrate of CMOS Cryptographic Chip

2:15 - 2:35 BREAK

2:35 - 3:50 SESSION 4: PUFS I
Session Chair: Gang Qu

- Raghavan Kumar and Wayne Burleson. On Design of a Highly Secure PUF based on Non-Linear Current Mirrors
- Patrick Koeberl, Jiangtao Li, Anand Rajan and Wei Wu. Entropy Loss in PUF-based Key Generation Schemes: The Repetition Code Pitfall
- Durga Prasad Sahoo, Sayandeep Saha, Debdeep Mukhopadhyay, Rajat Subhra Chakraborty and Hitesh Kapoor. Composite PUF: A New Design Paradigm for Physically Unclonable Functions on FPGA

3:50 - 5:30 SESSION 5: POSTER SESSION

5:30 RECEPTION

Wednesday May 7

8:45 - 10:00 SESSION 6: COUNTERMEASURES
Session Chair: Yier Jin

- Nicolas Moro, Karine Heydemann, Amine Dehbaoui, Bruno Robisson and Emmanuelle Encrenaz. Experimental evaluation of two software countermeasures against fault attacks
- Xiaofei Guo, Debdeep Mukhopadhyay, Chenglu Jin and Ramesh Karri. NREPO: Normal Basis Recomputing with Permuted Operands
- Meng-Day (Mandel) Yu, David M'Raihi, Ingrid Verbauwhede and Srinivas Devadas. A Noise Bifurcation Architecture for Linear Additive Physical Functions

10:00 - 10:20 BREAK

10:20 - 11:50 SESSION 7: PANEL
"Teaching Cyber-Security in STEM Curriculums: K through PhD"
Organizer: Ken Mai / Moderator: Jim Plusquellic
Swarup Bhunia, Case Western Reserve University
Jeremy Epstein, National Science Foundation  
Jim Plusquellic, University of New Mexico  
William Zortman, Sandia National Laboratories

11:50 - 1:40 LUNCH
Keynote by Jerome Roddy, Intelligent Decisions, Inc.

"GUNMAN, We Can Learn from Anyone, Especially from Our Enemies"

1:45 - 3:00 SESSION 8: SECURITY ATTACKS  
Session Chair: Youngok Pino

- Loic Zussa, Jean-Max Dutertre, Jessy Clediere and Bruno Robisson. Analysis of the fault injection mechanism related to negative and positive power supply glitches using an on-chip voltmeter
- Kamil Gomina, Jean-Baptiste Rigaud, Philippe Gendrier, Philippe Candelier and Assia Tria. Power supply glitch attacks: design and evaluation of detection circuits
- Sk Subidh Ali, Samah Mohamed Saeed, Ozgur Sinanoglu and Ramesh Karri. New Scan Attacks Against State-of-the-art Countermeasures and DFT

3:00 - 3:20 BREAK

3:20 - 4:45 SESSION 9: PUFS II  
Session Chair: Domenic Forte

- Roel Maes and Vincent Van Der Leest. Countering the Effects of Silicon Aging on SRAM PUFs
- Anirudh Iyengar, Kenneth Ramclam and Swaroop Ghosh. DWM-PUF: Novel low-power security primitives using spintronic domain wall memories
- Siva Nishok Dhanuskodi, Arunkumar Vijayakumar and Sandip Kundu. A Chaotic Ring Oscillator based Random Number Generator

Posters:
- Shivam Bhasin, Tarik Graba, Zakaria Najm and Jean-Luc Danger A Look into SIMON from a Side-Channel Perspective
- Franck Courbon, Jacques Fournier, Philippe Loubet-Moundi and Assia Tria Increasing the efficiency of laser fault injections using fast low cost gate level reverse engineering
- Dylan Ismari and Jim Plusquellic IP-Level Implementation of a Resistance-Based Physical Unclonable Function
- Sava Krstic, David Palmer, Randy Osborne, Eran Talmor and Jin Yang Security of SoC Firmware Load Protocols
• Kotaro Okamoto, Naofumi Homma, Takafumi Aoki and Sumio Morioka Hierarchical Formal Design of Side-channel Resistant Cryptographic Processors Using a Combination
• Stjepan Picek, Baris Ege, Lejla Batina, Domagoj Jakobovic and Kostas Papagiannopoulos Optimality and Beyond: The Case of 4x4 S-boxes
• Oliver Soell, Thomas Korak, Michael Muehlberghuber and Michael Hutter EM-Based Detection of Hardware Trojans on FPGAs
• Merrielle Spain, Benjamin Fuller, Kyle Ingols and Robert Cunningham Robust Keys from Physical Unclonable Functions
• Mostafa Taha and Patrick Schaumont Side-Channel Countermeasure for SHA-3 at Almost-Zero Area Overhead
• Sebastien Tiran, Sebastien Ordas, Yannick Teglia, Michel Agoyan and Philippe Maurine A Frequency Leakage Model for SCA
• Kan Xiao, Md. Tauhidur Rahman, Domenic Forte, Mohammad Tehranipoor, Mei Su and Yu Huang Bit Selection Algorithm Suitable for High-Volume Production of SRAM-PUF
• Norimasa Yoshimizu Hardware Trojan Detection by Symmetry Breaking in Path Delays