HOST-2008
IEEE International Workshop on Hardware-Oriented Security and Trust

June 9, 2008, Anaheim Convention Center, Room 204A, Anaheim, CA
Co-located event at the Design Automation Conference

Theme
“Hardware Trojan Detection and Isolation”

Program:
======
7:30-8:30 Registration

8:30-8:45 Welcome and Program Introduction: Mohammad Tehranipoor

8:45-9:30 Keynote:
   Dean Collins, Deputy Director, Microsystems Technology Office, DARPA
   “TRUST in Integrated Circuits and 3rd Party IP”

9:30-9:45 break

SESSION 1: Trojan Detection Methods
Session chair: Miron Abramovici (DAFCA)
9:45 - 10:05
   Reza Rad, Jim Plusquellic and Mohammad Tehranipoor
   “Sensitivity Analysis to Hardware Trojans using Power Supply Transient Signals”
10:05 - 10:25
   Jie Li and John Lach,
   "At-Speed Delay Characterization for IC Authentication and Trojan Horse Detection”
10:25 - 10:45
   Xiaoxiao Wang, Mohammad Tehranipoord and Jim Plusquellic,
   “Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions”

10:45 - 11:00 coffee

SESSION 2: Side-channel Attacks and Countermeasures
Session chair: Ryan Kastner (UCSD)
11:00 - 11:20
   Zhimin Chen and Patrick Schaumont,
"Slicing Up a Perfect Hardware Masking Scheme"
11:20 - 11:40
Sylvain Guilley, Sumanta Chaudhuri, Jean-Luc Danger, Laurent Sauvage, Philippe
Hoogvorst, Maxime Nassar, Tarik Graba and Vinh-Nga Vong,
"Place-and-Route Impact on the Security of DPL Designs in FPGAs"
11:40 - 12:00
Eric Menedez and Ken Mai,
“A High-Performance, Low-Overhead, Power-Analysis-Resistant, Single-Rail Logic
Style”

12:00-1:15 lunch

SESSION 3: Invited presentation
Session chair: Patrick Schaumont (Virginia Tech)
1:15 - 1:45
Kevin Schutz, Atmel (invited paper),
“The Role of Platform Integrity in Trustworthy Systems“

SESSION 4: Trojan Detection Methods
Session chair: Ian Harris (UC-Irvine)
1:45 - 2:05
Mainak Banga and Michael S. Hsiao,
“A Region Based Approach for the Identification of Hardware Trojans“
2:05 - 2:25
Rajat Subhra Chakraborty, Somnath Paul and Swarup Bhunia,
"On-Demand Transparency for Improving Hardware Trojan Detectability”
2:25 - 2:45
Yier Jin and Yiorgos Makris,
“Hardware Trojan Detection Using Path Delay Fingerprint”

2:45 - 3:00 coffee

SESSION 5: IC Piracy Protection, CAD Tool Security and PUFs
3:00 - 3:20
Tom Kean, David McLaren and Carol Marsh,
“Verifying the Authenticity of Chip Designs with the DesignTag System”
3:20 - 3:40
Jarrod A. Roy, Farinaz Koushanfar and Igor L. Markov,
“Circuit CAD Tools as a Security Threat”
3:40 - 4:00
S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen and P. Tuyls,
“The Butterfly PUF: Protecting IP on every FPGA“

4:00 - 4:15 break
SESSION 6: Cryptography and Securing Hardware
4:15 - 4:35
Junfeng Fan and Ingrid Verbauwhede,
“Unified Digit-Serial Multiplier and Inverter in Finite Field GF(2^m)”
4:35 - 4:55
Jiawei Huang and John Lach,
“IC Activation and User Authentication for Security-Sensitive Systems”

POSTER SESSION
5:00 - 5:45
Miron Abramovic, “A Solution for On-Line TRUST Validation”
Yousra Alkabani and Farinaz Koushanfar, ”Designer’s Hardware Trojan Horse”
Johann Groszschaedl, Tobias Vejda and Dan Page, ”Reassessing the TCG Specifications for Trusted Computing in Mobile and Embedded Systems”
Malcolm Taylor, Chi-En Yin, Min Wu and Gang Qu, ”A Hardware-Assisted Data Hiding Based Approach in Building High-Performance Trusted Computing Systems”
Francis Wolff and Chris Papachristou, ”An Embedded Flash Memory Vault for Software Trojan Protection”