

# **2008 IEEE International Workshop on Hardware- Oriented Security and Trust**

**Anaheim, CA  
9 June 2008**



**IEEE Catalog Number:**  
**ISBN 13:**

**CFP08HOA-PRT**  
**978-1-4244-2401-6**

# IEEE International Workshop on Hardware-Oriented Security and Trust (HOST)

## Keynote:

- Dean Collins, Deputy Director, Microsystems Technology Office, DARPA  
“TRUST in Integrated Circuits and 3rd Party IP” ..... 1

## SESSION 1: Trojan Detection Methods

- Reza Rad, Jim Plusquellic and Mohammad Tehranipoor  
“Sensitivity Analysis to Hardware Trojans using Power Supply Transient Signals” 3  
Jie Li and John Lach,  
“At-Speed Delay Characterization for IC Authentication and Trojan Horse Detection” ..... 8  
Xiaoxiao Wang, Mohammad Tehranipoor and Jim Plusquellic,  
“Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions” . 15

## SESSION 2: Side-channel Attacks and Countermeasures

- Zhimin Chen and Patrick Schaumont,  
“Slicing Up a Perfect Hardware Masking Scheme” ..... 21  
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”..... 26  
Eric Menedez and Ken Mai,  
“A High-Performance, Low-Overhead, Power-Analysis-Resistant, Single-Rail Logic Style” ..... 33

## SESSION 3: Invited presentation

- Kevin Schutz, Atmel (invited paper),  
“The Role of Platform Integrity in Trustworthy Systems“ ..... 38

## SESSION 4: Trojan Detection Methods

- Mainak Banga and Michael S. Hsiao,  
“A Region Based Approach for the Identification of Hardware Trojans“ ..... 40  
Rajat Subhra Chakraborty, Somnath Paul and Swarup Bhunia,  
“On-Demand Transparency for Improving Hardware Trojan Detectability”..... 48  
Yier Jin and Yiorgos Makris,  
“Hardware Trojan Detection Using Path Delay Fingerprint” ..... 51

## Session 5: IC Piracy Protection, CAD Tool Security and PUFs

- Tom Kean, David McLaren and Carol Marsh,  
“Verifying the Authenticity of Chip Designs with the DesignTag System” ..... 59  
Jarrod A. Roy, Farinaz Koushanfar and Igor L. Markov,  
“Circuit CAD Tools as a Security Threat”..... 65  
S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen and P. Tuyls,

**“The Butterfly PUF: Protecting IP on every FPGA“ ..... 67**

**SESSION 6: Cryptography and Securing Hardware**

**Junfeng Fan and Ingrid Verbauwhede,**

**“Unified Digit-Serial Multiplier and Inverter in Finite Field  $GF(2^m)$ ” ..... 72**

**Jiawei Huang and John Lach,**

**“IC Activation and User Authentication for Security-Sensitive Systems” ..... 76**

**POSTERS**

**Yousra Alkabani and Farinaz Koushanfar,**

**”Designer’s Hardware Trojan Horse” ..... 82**

**Johann Großschädl, Tobias Vejda and Dan Page,**

**”Reassessing the TCG Specifications for Trusted Computing in Mobile and Embedded Systems” ..... 84**

**Ted Huffmire, Jonathan Valamehr, Timothy Sherwood, Ryan Kastner, Timothy**

**Levin, Thuy D. Dguyen and Cynthia Irvine,**

**“Trustworthy System Security through 3-D Integrated Hardware”..... 91**

**Malcolm Taylor, Chi-En Yin, Min Wu and Gang Qu,**

**”A Hardware-Assisted Data Hiding Based Approach in Building High-Performance Trusted Computing Systems” ..... 93**

**Francis Wolff and Chris Papachristou,**

**”An Embedded Flash Memory Vault for Software Trojan Protection” ..... 97**