2015 IEEE International Symposium on Hardware Oriented Security and Trust

(HOST 2015)

Washington, DC, USA
5-7 May 2015

IEEE Catalog Number: CFP15HOA-POD
ISBN: 978-1-4673-7422-4

Session 1	**Keynote I**
Date/Time	Tuesday, 5 May 2015 / 09:00 – 10:00
Chair	Mark Tehranipoor, *U. of Connecticut*

Keynote Talk: IOT Security: Challenges and Solutions N/A
Dr. RAMESH SEPEHRRAD
Vice President, National Governance, Risk and Compliance Comcast

Session 2	**Invited Industrial Session**
Date/Time	Tuesday, 5 May 2015 / 10:20 – 11:35
Chair	Mark Tehranipoor, *U. of Connecticut*

Mentor Graphics' view of Security N/A
Serge Leef, *Mentor Graphics*

Comcast's view of Security N/A
Jim Fahrny, *Senior Fellow, Comcast*

Honeywell's view of Security N/A
Ken Heffner, *Fellow, Honeywell*

Session 3	**Efficient Implementation of Secure Systems**
Date/Time	Tuesday, 5 May 2015 / 01:00 – 02:15
Chair	Qiaoyan Yu, *University of New Hampshire*

Silent SIMON: A Threshold Implementation under 100 Slices 1
Aria Shahverdi, Mostafa Taha and Thomas Eisenbarth

Robust True Random Number Generator Using Hot-Carrier Injection Balanced Metastable Sense Amplifiers 7
Mudit Bhargava, Kaship Sheikh and Ken Mai

Efficient and Secure Split Manufacturing via Obfuscated Built-In Self-Authentication 14
Kan Xiao, Domenic Forte and Mark (Mohammed) Tehranipoor

Session 4	**PUF**
Date/Time	Tuesday, 5 May 2015 / 02:35 – 03:50
Chair	Ioannis Savidis, *Drexel University*

Security Analysis of Index-Based Syndrome Coding for PUF-Based KeGeneration 20
Georg T. Becker, Alexander Wild and Tim Güuneysu

Exploiting Resistive Cross-point Array for Compact Design of Physical Unclonable Function 26
Pai-Yu Chen, Runchen Fang, Rui Liu, Chaitali Chakrabarti, Yu Cao and Shimeng Yu

A Family of Schmitt-Trigger-based Arbiter-PUFs and Selective Challenge-Pruning for Robustness and Quality 32
Cheng Wei Lin and Swaroop Ghosh

Session 5	**Poster Session**
Date/Time	Tuesday, 5 May 2015 / 04:00 – 05:50
Chair	Garrett S. Rose, *University of Tennessee*

Maximum-Likelihood Decoding of Device-Specific Multi-Bit Symbols for Reliable Key Generation 38
Meng-Day (Mandel) Yu, Matthias Hiller and Srinivas Devadas

A Practical DPA on Grain v1 using LS-SVM 44
Abhishek Chakraborty, Bodhisatwa Mazumdar and Debdeep Mukhopadhyay

FPGA SoC Architecture and Runtime to Prevent Hardware Trojans from Leaking Secrets 48
Gedare Bloom, Bhagirath Narahari, Rahul Simha, Ali Namazi and Renato Levy

A Security-aware Design Scheme for Better Hardware Trojan Detection Sensitivity 52
Chongxi Bao, Yang Xie and Ankur Srivastava

Automatic Obfuscated Cell Layout for Trusted Split-Foundry Design 56
Carlos Tadeo Ortega Otero, Jonathan Tse, Robert Karmazin, Benjamin Hill and Rajit Manohar

High Precision Fault Injections on the Instruction Cache of ARMv7-M Architectures 62
Lionel Rivière, Zakaria Najm, Pablo Rauzy, Jean-Luc Danger, Julien Bringer and Laurent Sauvage

Power Analysis of the t-Private Logic Style for FPGAs 68
Zachary N. Goddard, Nicholas LaJeunesse and Thomas Eisenbarth

TVVF: Estimating the Vulnerability of Hardware Cryptosystems against Timing Violation Attacks 72
Bilgiday Yuce, Nahid Farhady Ghalaty and Patrick Schaumont

Validation of RTL Laser Fault Injection Model with respect to Layout Information 78
Athanasios Papadimitriou, Marios Tampas, David Hély, Vincent Beroulle, Paolo Maistri and Regis Leveugle

Linear Complementary Dual Code Improvement to Strengthen Encoded Circuit Against Hardware Trojan Horses 82
Xuan Thuy Ngo, Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley and Zakaria Najm

Preventing Fault Attack on Stream Cipher using Randomization 88
Shamit Ghosh and Dipanwita Roy Chowdhury

Post-Layout Estimation of Side-Channel Power Supply Signatures 92
Sushmita Kadiyala Rao, Deepak Krishnankutty, Ryan Robucci, Nilanjan Banerjee and Chintan Patel

Template Attack on Masking AES Based on Fault Sensitivity Analysis 96
Qian Wang, An Wang, Liji Wu, Gang Qu and Guoshuang Zhang

Session 6	**Keynote II**
Date/Time	Wednesday, 6 May 2015 / 09:00 – 10:00
Chair	Saverio Fazzari, *Booz Allen Hamilton*

Keynote Talk: **Is it safe? N/A**
Mr. W. ERIC HERR
Director, Technology Integration Office (TIO)
Office of the Under Secretary of Defense (AT&L)

Session 7	**Panel**
Date/Time	Wednesday, 6 May 2015 / 10:15 – 11:45
Moderators	Saverio Fazzari, *Booz Allen Hamilton* and Mark Tehranipoor, *U. of Connecticut*

- **Kerry Bernstein**, *DARPA*
- **Serge Leef**, *Mentor Graphics*
- **TBA**, *Northrup Grumman*
- **Nina Amla**, *NSF*
- **Celia Merzbacher**, *SRC*

Session 8	**Invited Government Session**
Date/Time	Wednesday, 6 May 2015 / 01:00 – 02:15
Chair	Saverio Fazzari, *Booz Allen Hamilton*

- **DARPA SHIELD Program** N/A
  Arnett Brown, *Booz Allen Hamilton*
- **AFRL Trusted Initiative** N/A
  Matt Casto, *AFRL, Dayton OH*
- **OSD Harward Assurance Initiative** N/A
  Brett Hamilton, *NAVSEA-CRANE*

Session 9	**Side Channel and Fault Attacks Analysis I**
Date/Time	Wednesday, 6 May 2015 / 02:30 – 03:45
Chair	Yier Jin, *U. of Central Florida*

- **Diagonal Fault Analysis of Grøstl in Dedicated MAC Mode** **100**
  Dhiman Saha and Dipanwita Roy Chowdhury
- **Neural Network Based Attack on a Masked Implementation of AES** **106**
  Richard Gilmore, Neil Hanley and Maire O'Neill
- **A DPA-Resistant Self-Timed Three-Phase Dual-Rail Pre-Charge Logic Family** **112**
  Nail Etkin Can Akkaya, Burak Erbagci, Raymond Carley and Ken Mai

Session 10	**Side Channel and Fault Attacks Analysis II**
Date/Time	Wednesday, 6 May 2015 / 04:00 – 05:15
Chair	Domenic Forte, *U. of Connecticut*

- **Efficient 2nd-order Power Analysis on Masked Devices Utilizing Multiple Leakage** **118**
  Liwei Zhang, A. Adam Ding, Yunsi Fei and Pei Luo
- **Simulation and Analysis of Negative-Bias Temperature Instability Aging on Power Analysis Attacks** **124**
  Xiaofei Guo, Naghmeh Karimi, Francesco Regazzoni, Chenglu Jin and Ramesh Karri
- **Achieving Side-Channel Protection with Dynamic Logic Reconfiguration on Modern FPGAs** **130**
  Pascal Sasdrich, Amir Moradi, Oliver Mischkey and Tim Güuneysu

Session 11	**Keynote III**
Date/Time	Thursday, 7 May 2015 / 09:00 – 10:00
Chair	James Plusquellic, *University of New Mexico*

Keynote Talk: **SoC Security Objectives: What Does Your Market Say?** N/A
Dr. DHINESH MANOHARAN
Director, Product Security Research, Security Center of Excellence
Intel

Session 12	**Hardware Trojan Horses, Security Analysis, Evaluations, and Metrics**
Date/Time	Thursday, 7 May 2015 / 10:20 – 11:35
Chair	Houman Homayoun, *George Mason University*

Evaluating the Security of Logic Encryption Algorithms 137
Pramod Subramanyan, Sayak Ray and Sharad Malik

GDS-II Trojan Detection using Multiple Supply Pad V_{DD} and GND I_{DDQ}s in ASIC Functional Units 144
I. Wilcox, F. Saqib and J. Plusquellic

Resilient Hardware Trojans Detection based on Path Delay Measurements 151
Ingrid Exurville, Loic Zussay, Jean-Baptiste Rigaudz and Bruno Robisson

Session 13	**Secure and Trusted Synthesis and Design**
Date/Time	Thursday, 7 May 2015 / 11:35 – 12:25
Chair	Gregory L. Creech, *ElectroScience Laboratory, Ohio State University*

Physically Secure and Fully Reconfigurable Data Dtorage Using Optical Scattering 157
Roarke Horstmeyer , Sid Assawaworrarit, Ulrich Rührmairy and Changhuei Yang

Toward Automatic Proof Generation for Information Flow Policies in Third-Party Hardware IP 163
Mohammad-Mahdi Bidmeshki and Yiorgos Makris