2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2017)

Mclean, Virginia, USA
1 – 5 May 2017

IEEE Catalog Number: CFP17HOA-POD
ISBN: 978-1-5386-3930-6

Copyright © 2017 by the Institute of Electrical and Electronics Engineers, Inc
All Rights Reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

***** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP17HOA-POD
ISBN (Print-On-Demand):	978-1-5386-3930-6
ISBN (Online):	978-1-5386-3929-0

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings.com

Technical Program

Session 1	Architecture Level Security
Date / Time	Tuesday, May 2, 2017 / 11:00 - 12:20
Session Chair	**Aaron Cohen**, *US Naval Research Laboratory*

- **Intrinsic Rowhammer PUFs: Leveraging the Rowhammer Effect for Improved Security.....1**
  Andr'e Schaller, Wenjie Xiong, Nikolaos Athanasios Anagnostopoulos, Muhammad Umair Saleem, Sebastian Gabmeyer, Stefan Katzenbeisser and Jakub Szefer
- **When Good Protections Go Bad: Exploiting Anti-DoS Measures to Accelerate Rowhammer Attacks.....8**
  Misiker Tadesse Aga, Zelalem Birhanu Aweke and Todd Austin
- **Hermes: Secure Heterogeneous Multicore Architecture Design.....14**
  Michel A. Kinsy, Shreeya Khadka, Mihailo Isakov and Anam Farrukh
- **Reviving Instruction Set Randomization.....21**
  Kanad Sinha, Vasileios P. Kemerlis and Simha Sethumadhavan

Session 2	Primitives and Implementations
Date / Time	Tuesday, May 2, 2017 / 13:30 - 15:00
Session Chair	**Wayne A. Reed**, *KCNSC*

- **Creating Security Primitive by Nanoscale Manipulation of Carbon Nanotubes.....29**
  Zhaoying Hu and Shu-Jen Han
- **Automatic Generation of High-Performance Modular Multipliers for Arbitrary Mersenne Primes on FPGAs.....35**
  Philipp Koppermann, Fabrizio De Santis, Johann Heyszl and Georg Sigl
- **Efficient Configurations for Block Ciphers with Unified ENC/DEC Paths.....41**
  Subhadeep Banik, Andrey Bogdanov and Francesco Regazzoni
- **Memory-Constrained Implementation of Lattice-based Encryption Scheme on Standard Java Card.....47**
  Ye Yuan, Kazuhide Fukushima, Shinsaku Kiyomoto and Tsuyoshi Takagi
- **Towards a Memristive Hardware Secure Hash Function (MemHash).....51**
  Leonid Azriel and Shahar Kvatinsky

Session 3	Side-Channel Attack/Analysis
Date / Time	Wednesday, May 3, 2017 / 11:05 - 12:20
Session Chair	**Alpa Trivedi**, *Intel, USA*

- **Stateless Leakage Resiliency from NLFSRs.....56**
  Mostafa Taha, Arash Reyhani-Masoleh and Patrick Schaumont
- **High Efficiency Power Side-Channel Attack Immunity using Noise Injection in Attenuated Signature Domain.....62**
  Debayan Das, Shovan Maity, Saad Bin Nasir, Santosh Ghosh, Arijit Raychowdhury and Shreyas Sen
- **Exploring Timing Side-channel Attacks on Path-ORAMs.....68**
  Chongxi Bao and Ankur Srivastava
- **Photonic Side Channel Attacks Against RSA.....74**
  Elad Carmon, Jean-Pierre Seifert and Avishai Wool

Session 4	New Attacks
Date / Time	Wednesday, May 3, 2017 / 13:30 - 14:50
Session Chair	**Fareena Saqib**, *Florida Institute of Technology*

- **Characterising a CPU Fault Attack Model via Run-Time Data Analysis.....79**
  Martin S. Kelly, Keith Mayes and John F. Walker
- **Breaking Active-Set Backward-Edge CFI.....85**
  Michael Theodorides and David Wagner
- **INFECT: INconspicuous FEC-based Trojan: a Hardware Attack on an 802.11a/g Wireless Network.....90**
  Kiruba Sankaran Subramani, Angelos Antonopoulos, Ahmed Attia Abotabl, Aria Nosratinia and Yiorgos Makris
- **AppSAT: Approximately Deobfuscating Integrated Circuits.....95**
  Kaveh Shamsi, Meng Li, Travis Meade, Zheng Zhao, David Z. Pan and Yier Jin
- **Challenging On-Chip SRAM Security with Boot-State Statistics.....101**
  Joseph McMahan, Weilong Cui, Liang Xia, Jeff Heckey, Frederic T. Chong and Timothy Sherwood

Session 5	Enhanced Hardware Security
Date / Time	Thursday, May 4, 2017 / 10:20 - 12:00
Session Chair	**Greg Creech**, *GLC Consulting*

- **A Novel Physiological Features-Assisted Architecture for Rapidly Distinguishing Health Problems from Hardware Trojan Attacks and Errors in Medical Devices.....106**
  Taimour Wehbe, Vincent J. Mooney, Abdul Qadir Javaid and Omer T. Inan,
- **Using Computational Game Theory to Guide Verification and Security in Hardware Designs.....110**
  Andrew M. Smith, Jackson R. Mayo, Vivian Kammler, Robert C. Armstrong and Yevgeniy Vorobeychik
- **Physical Unclonable Functions and Dynamic Partial Reconfiguration for Security in Resource-Constrained Embedded Systems.....116**
  G. Pocklassery, Venkata K Kajuruli, J. Plusquellic and F. Saqib
- **New Clone-Detection Approach for RFID-Based Supply Chains.....122**
  Hoda Maleki, Reza Rahaeimehr, Chenglu Jin and Marten van Dijk
- **Take a Moment and have some *t*: Hypothesis Testing on Raw PUF Data.....128**
  Vincent Immler, Matthias Hiller, Johannes Obermaier and Georg Sigl

Session 6	Physical Unclonable Functions
Date / Time	Thursday, May 4, 2017 / 13:00 - 14:00
Session Chair	**Sanghamitra Roy**, *Utah State University*

- **A New Maskless Debiasing Method for Lightweight Physical Unclonable Functions.....134**
  Aydin Aysu, Ye Wang, Patrick Schaumont and Michael Orshansky
- **A Stochastic All-Digital Weak Physically Unclonable Function for Analog/Mixed-Signal Applications.....140**
  Troy Bryant, Sreeja Chowdhury, Domenic Forte, Mark Tehranipoor and Nima Maghari
- **Improving Reliability of Weak PUFs via Circuit Techniques to Enhance Mismatch.....146**
  Vinay C. Patil, Arunkumar Vijayakumar, Daniel E. Holcomb and Sandip Kundu

Session 7	Poster Session
Date / Time	
Session Chair	**Wujie Wen**, *Florida International University*

- **Ag Conductive Bridge RAMs for Physical Unclonable Functions.....151**
  Bertrand Cambou, Fatemeh Afghah, Derek Sonderegge, Jennifer Taggart, Hugh Barnaby and Michael Kozicki
- **Fabrication Security and Trust of Domain-Specific ASIC Processors.....152**
  Michael Vai, Karen Gettings and Theodore Lyszczarz
- **Øzone: Efficient Execution with Zero Timing Leakage for Modern Microarchitectures.....153**
  Zelalem Birhanu Aweke and Todd Austin
- **LWE-Based Lossless Computational Fuzzy Extractor for the Internet of Things.....154**
  Christopher Huth, Daniela Becker, Jorge Guajardo, Paul Duplys and Tim Güneysu
- **Cache Timing Attacks on Recent Microarchitectures.....155**
  Alexandros Andreou, Andrey Bogdanov and Elmar Tischhauser
- **Analyzing Security Vulnerabilities of Three-Dimensional Integrated Circuits.....156**
  Jaya Dofe and Qiaoyan Yu
- **A Novel Offset Method for Improving Bitstring Quality of a Hardware-Embedded Delay PUF.....157**
  Wenjie Che, Jim Plusquellic and Fareena Saqib
- **Malicious CAN-message Attack against Advanced Driving Assistant System.....158**
  Mitsuru Shiozaki, Takaya Kubota, Masashi Nakano, Yuuki Nakazawa and Takeshi Fujino
- **Improving FPGA based SHA-3 Structures.....159**
  Magnus Sundal and Ricardo Chaves
- **On Secure Implementations of Quantum-Resistant Supersingular Isogeny Diffie-Hellman.....160**
  Brian Koziel, Reza Azarderakhsh and David Jao
- **Parameter Biasing Obfuscation for Analog IP Protection.....161**
  Vaibhav Venugopal Rao and Ioannis Savidis
- **Circuit Recognition with Deep Learning.....162**
  Yu-Yun Dai and Robert K. Brayton
- **Detection of Counterfeit ICs using Public Identification Sequences.....163**
  Peter Samarin and Kerstin Lemke-Rust
- **Threshold Voltage Defined Multi-Input Complex Gates.....164**
  Asmit De and Swaroop Ghosh
- **Platform Agnostic, Scalable, and Unobtrusive FPGA Network Processor Design of Moving Target Defense over IPv6 (MT6D) over IEEE 802.3 Ethernet.....165**
  Joseph Sagisi, Joseph Tront and Randy Marchany
- **TTLock: Tenacious and Traceless Logic Locking.....166**
  Muhammad Yasin, Bodhisatwa Mazumda, Jeyavijayan (JV) Rajendran and Ozgur Sinanoglu
- **Exploiting Safe Error based Leakage of RFID Authentication Protocol using Hardware Trojan Horse.....167**
  Krishna Bagadia, Urbi Chatterjee, Debapriya Basu Roy, Debdeep Mukhopadhyay and Rajat Subhra Chakraborty
- **Characterizing EEPROM for Usage as a Ubiquitous PUF Source.....168**
  Chris Pavlina Jacob Torrey and Kyle Temkin
- **On Designing Optimal Camouflaged Layouts.....169**
  Thomas Broadfoot, Carl Sechen and Jeyavijayan (JV) Rajendran
- **Connecting the Dots: Privacy Leakage via Write-Access Patterns to the Main Memory.....170**
  Tara John, Syed Kamran Haider, Hamza Omar and Marten van Dijk

- **Correlation Power Analysis Attack against STT-MRAM Based Cyptosystems.....171**
  Abhishek Chakraborty, Ankit Mondal and Ankur Srivastava
- **Synthesis of Hardware Sandboxes for Trojan Mitigation in Systems on Chip.....172**
  Christophe Bobda, Taylor J.L. Whitaker, Charles Kamhoua, Kevin Kwiat and Laurent Njilla

Program Overview

1 May 2017, Monday (Tutorials)	
13:00 - 15:30	**TUTORIAL 1 and TUTORIAL 2** Tutorial Chair: **Domenic Forte**, University of Florida **T1. Protecting Electronics Supply Chain from Design to Resign** **Prof. Mark Tehranipoor**, University of Florida **T2. Trusted Platform Modules and Their Applicability to Hardware and Software Security Mitigations** **Topher Timzen**, Intel Security Center of Excellence (SeCoE) **Chandni Bhowmik**, Intel Security Center of Excellence (SeCoE)
15:30 - 16:00	**Break**
14:00 - 18:30	**TUTORIAL 3 and TUTORIAL 4** **T3. Security and Trust in the Analog/Mixed-Signal/RF Domain: A Survey and a Perspective** **Prof. Yiorgos Makris**, The University of Texas at Dallas **T4. Hardware Security and Trust Challenges in Emerging IoT Systems and Applications** **Prof. Fareena Saqib**, Florida Institute of Technology **Prof. Jim Plusquellic**, University of New Mexico **Prof. Mohammad Al Faruque**, University of California--Irvine

2 May 2017, Tuesday	
07:30 - 08:30	Registration & Continental Breakfast
08:30 - 08:45	Opening Remarks: HOST 2017 General and Program Chairs
08:45 - 09:00	HOST 10th Anniversary Ceremony
09:00 - 09:45	Keynote I: Improbabilities of Security **Speaker:** Paul Kocher *Cryptography Research, Inc. / Rambus*
09:45 - 10:15	Visionary Talk I : The Role of Infrastructure IP in Securing SOCs **Speaker:** Yervant Zorian, *Synopsys Chief Architect and Fellow*
10:15 - 11:00	Hardware Demo Competition & Posters **Hardware Demo Chair:** *Jim Plusquellic, University of New Mexico* **Poster Session Chair:** *Wujie Wen, Florida International University*
11:00 - 12:20	Session 1: Architecture Level Security **Session Chair:** Aaron Cohen, *US Naval Research Laboratory*
12:20 - 13:30	**LUNCH**

12:30 - 12:50	**LUNCH TALK** Speaker: **Jim Plusquellic**, CTO, Enthentica; Professor, University of New Mexico Title: ***Hardware-Based Security and Trust For IoT and Supply Chain Authentication***
13:30 - 15:00	Session 2: Primitives and Implementations **Session Chair:** Wayne A. Reed, *KCNSC*
15:00 - 16:00	Hardware Demo Competition & Posters **Hardware Demo Chair:** *Jim Plusquellic, University of New Mexico* **Poster Session Chair:** *Wujie Wen, Florida International University*
16:00 - 16:30	Keynote II: Establishing Hardware Trust: Challenges, Opportunities and (Im)possibilities **Speaker:** Todd M. Austin *University of Michigan*
16:30 - 17:45	PANEL I: DoD and Hardware Security **Panel Moderator:** Saverio Fazzari, *Booz Allen* Panelists: • **Matthew Casto,** Air Force Research Lab • **Jeremy Muldavin,** OSD • **Brett Hamilton,** Navy • **Christine Rink,** Aerospace

3 May 2017, Wednesday	
07:45 - 08:45	Registration and Continental Breakfast
08:45 - 09:30	Keynote III: Long-Term Strategy for DoD Trusted and Assured Microelectronics Needs **Speaker:** Jeremy Muldavin *OSD*
09:30 - 10:00	Visionary Talk II : Hardware-assisted Security: So Close yet So Far **Speaker:** Ahmad-Reza Sadeghi, *Technische Universität Darmstadt, Germany*
10:00 - 11:00	Hardware Demo Competition & Posters **Hardware Demo Chair:** *Jim Plusquellic, University of New Mexico* **Poster Session Chair:** *Wujie Wen, Florida International University*
11:00 - 12:20	Session 3: Side-Channel Attack/Analysis **Session Chair:** Alpa Trivedi, *Intel USA*
12:20 - 13:30	**LUNCH**
12:30 - 12:50	**LUNCH TALK** Speaker: **Pim Tuyls**, CEO, Intrinsic-ID
13:30 - 14:50	Session 4: New Attacks **Session Chair:** Fareena Saqib, *Florida Institute of Technology*
14:50 - 16:00	Hardware Demo Competition & Posters **Hardware Demo Chair:** *Jim Plusquellic, University of New Mexico* **Poster Session Chair:** *Wujie Wen, Florida International University*

16:00 - 17:30	PANEL II: Security and Architecture **Panel Moderator:** Julien Carreño, *Security Architecture Lead, Intel* Panelists: • **Milos Prvulovic,** Georgia Tech • **Yan Solihin,** NC State University • **Sandip Ray,** NXP Semiconductor • **Serge Leef,** Mentor Graphics • **Yousef Iskander,** Cisco
18:00	RECEPTION and AWARD ANNOUNCEMENTS

4 May 2017, Thursday	
07:45 - 08:45	Continental Breakfast
08:45 - 09:30	Keynote IV: Cyber deception: An emerging cyber security research thrust **Speaker:**Cliff Wang, *Army Research Office*
09:30 - 10:00	Visionary Talk III : Hardware based Security and the Cloud **Speaker:** Carlos V. Rozas, *Intel, Portland, USA*
10:00 - 10:20	**Break**
10:20 - 12:00	Session 5: Enhanced Hardware Security **Session Chair:** Greg Creech, *GLC Consulting*
12:00 - 13:00	**LUNCH**
12:10 - 12:30	**LUNCH TALK** Speaker: **Jason Sanabia**, President & CEO, Raith America Title: ***Latest Developments in Large Area, High Resolution SEM and FIB for Semiconductor Reverse Engineering***
13:00 - 14:00	Session 6: Physical Unclonable Functions **Session Chair:** Sanghamitra Roy, *Utah State University*
14:00	CONCLUDING REMARKS: HOST 2017 and HOST 2018 General and Program Chairs
14:30 - 18:00	The 1st Workshop for Women in Hardware and Systems Security (WISE)

5 May 2017, Friday	
08:30 - 13:30	Internet of Things (IoT) and Automotive Security Workshop (IASW)

Hardware Demos

- **Supply Chain and IoT PUF-based Authentication.....N/A**
  Wenjie Che, Goutham Pocklassery, Venkata K. Kajuluri, Jim Plusquellic and Fareena Saqib
- **Why Do You Trust Sensors? Analog Cybersecurity Attack Demos.....N/A**
  Andrew Kwong, Connor Bolton, Timothy Trippel, Wenyuan Xu and Kevin Fu
- **Complete Activation Scheme for IP Design Protection.....N/A**
  Brice Colombier, Ugo Mureddu, Marek Laban, Oto Petura, Lilian Bossuet and Viktor Fischer
- **SPOILD: Side-channel Power-based Instruction-Level Disassembler.....N/A**
  Fahim Rahman, Jungmin Park, Xiaolin Xu, Domenic Forte and Mark Tehranipoor
- **Hardware Trojan Detection through Electromagnetic Side-Channel Statistical Analysis: A Gold Chip Free Approach.....N/A**
  Jiaji He and Xiaolong Guo
- **Automatic Data Extraction from CBRAM and ReRAM Arrays.....N/A**
  Raul Chipana, Bilal Habib, Bertrand Cambou and Jennifer Taggart
- **Leveraging Electromagnetic Emanations for IoT Security.....N/A**
  Nader Sehatbakhsh, Robert Callan, Monjur Alam, Milos Prvulovic and Alenka Zajic
- **IoTA: IoT Assurance.....N/A**
  John Clemens, Raj Pal and Branden Sherrell
- **A Processor + FPGA based Platform for Control Flow Integrity Enforcement.....N/A**
  Anirudh Iyengar, Advisor: Swaroop Ghosh & Trent Jaeger
- **Counterfeit IC Detection: A Defect Database and Test Procedure.....N/A**
  Md Mahbub Alam, Sreeja Chowdhury, Navid Asadizanjani, Mark Tehranipoor and Domenic Forte
- **Hardware Hacking Security Education Platform (HaHa SEP): Enabling Hands-On Applied Research of Hardware Security Theory \ Principles.....N/A**
  Jason Vosatka, Shuo Yang, Domenic Forte and Mark Tehranipoor
- **Enhancing Power-Side-Channel-Attack Resistance via a Security-Aware Integrated Voltage Regulator.....N/A**
  M. Kar, A. Singh, S. Mathew, A. Rajan, V. De and S. Mukhopadhyay
- **Data Exfiltration using Building Automation to Bridge Air Gapped System.....N/A**
  Marcial Tienteu, Asia Mason, Michael Talley, Tellrell White, Edmund Ahovi, Denzel Hamilton, Kevin Kornegay, Michel Reece and Willie Thompson
- **Spoofing, DOS, DDOS Attacks On a Z-Wave Home Automation System.....N/A**
  Latha Suryavanshi Mahadeva Rao, Khir Henderson, Tsion Yimer, Aaron Edmund, Kevin Kornegay and Jumoke Ladeji-Osias
- **Hardware Demo: Hacking Z-Wave using Insider Tools.....N/A**
  Aaron Edmond, Khir Henderson, Latha Suryavanshi and Tsion Yimer
- **UCR: An Unclonable Environmentally-Sensitive Chipless RFID Tag.....N/A**
  Kun Yang, Haoting Shen, Domenic Forte and Mark M. Tehranipoor
- **Demonstration of Built-in Secure Register Bank (BSRB) Protection Scheme for Embedded System Security.....N/A**
  Sean D. Kramer and Zhiming Zhang
- **Prevention & Detection of Hardware Trojans in Wireless Cryptographic ICs: Silicon Demonstration.....N/A**
  Georgios Volanis, C. Kapatsori, Yu Liu and Yiorgos Makris
- **Real-time Causal Internet Log Analytics by HW/SW/Projection Co-design.....N/A**
  Bita Darvish Rouhani, Mohammad Ghasemzadeh and Farinaz Koushanfar
- **Demonstration of Hardware Trojan Attacks & Defenses in an IEEE 802.11a/g Network.....N/A**
  Kiruba S. Subramani, Angelos Antonopoulos, Ahmed Attia Abotabl, Aria Nosratinia and Yiorgos Makris
- **FAME: Fault Aware Microprocessor Extension Demonstrator.....N/A**

Chinmay Deshpande, Marjan Ghodrati, Bilgiday Yuce, Abhishek Bendre, Conor Patrick, Nahid Farhady Ghalaty, Leyla Nazhandali and Patrick Schaumont

- **Demo: Practical Cryptographically-Secure PUFs based on Learning Parity with Noise.....N/A**
  Chenglu Jin, Charles Herder, Ling Ren, Phuong Ha Nguyen, Benjamin Fuller, Srinivas Devadas and Marten van Dijk
- **Synthesis of Hardware Sandboxes for Trojan Mitigation in Systems on Chip --- Hardware Demo Proposal.....N/A**
  Christophe Bobda, Taylor JL Whitaker, Charles Kamhoua, Kevin Kwiat and Laurent Njilla
- **Hardware Based Secure CAN Bus Communication.....N/A**
  Ali Shuja Siddiqui, Jim Plusquellic and Fareena Saqib
- **Implementation Diversity and Dynamic Partial Reconfiguration for Impeding Differential Power Analysis Attacks on FPGAs.....N/A**
  Nahome G. Bete, Meghanath Nakka, Jim Plusquellic, Fareena Saqib, Chintan Patel and Ryan Robucci
- **Ag Conductive Bridge RAMs for Physical Unclonable Functions.....N/A**
  Bertrand Cambou, Fatemeh Afghah Derek Sonderegger, Jennifer Taggart, Hugh Barnaby and Michael Kozicki