

2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2018)

**Washington, DC, USA
30 April – 4 May 2018**



**IEEE Catalog Number: CFP18HOA-POD
ISBN: 978-1-5386-4732-5**

**Copyright © 2018 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:	CFP18HOA-POD
ISBN (Print-On-Demand):	978-1-5386-4732-5
ISBN (Online):	978-1-5386-4731-8

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	IoT Security
Date / Time	Tuesday, May 1, 2018 / 11:00 - 12:20
Session Chair	TBA

- 1 **Syndrome: Spectral Analysis for Anomaly Detection on Medical IoT and Embedded Devices**
Nader Sehatbakhsh, Monjur Alam, Alireza Nazari, Alenka Zajic and Milos Prvulovic
- 9 **Remote Attestation of IoT Devices via SMARM: Shuffled Measurements Against Roving Malware**
Xavier Carpent, Norrathep Rattanavipanon and Gene Tsudik
- 17 **TZSlicer: Security-Aware Dynamic Program Slicing for Hardware Isolation**
Mengmei Ye, Jonathan Sherman, Witawas Srisa-an and Sheng Wei
- 25 **Zero-Permission Acoustic Cross-Device Tracking**
Nikolay Matyunin, Jakub Szefer and Stefan Katzenbeisser

Session 2	Physical Attacks and Tamper Resistance
Date / Time	Tuesday, May 1, 2018 / 15:15 - 16:15
Session Chair	TBA

- 33 **Dividing the Threshold: Multi-Probe Localized EM Analysis on Threshold Implementations**
Robert Specht, Vincent Immler, Florian Unterstein, Johann Heyszl and Georg Sigl
- 41 **Direct Read of Idle Block RAM from FPGAs Utilizing Photon Emission Microscopy**
Jacob Couch, Nicole Whewell, Andrew Monica and Stergios Papadakis
- 49 **B-TREPID: Batteryless Tamper-Resistant Envelope with a PUF and Integrity Detection**
Vincent Immler, Johannes Obermaier, Martin König, Matthias Hiller and Georg Sigl

Session 3	Cryptanalysis and Side Channel Attacks
Date / Time	Wednesday, May 2, 2018 / 11:00 - 12:20
Session Chair	TBA

- 57 **Fault-Assisted Side-Channel Analysis of Masked Implementations**
Yuan Yao, Mo Yang, Conor Patrick, Bilgiday Yuce and Patrick Schaumont
- 65 **An Efficient SAT-Based Algorithm for Finding Short Cycles in Cryptographic Algorithms**
Elena Dubrova and Maxim Teslenko
- 73 **The CAESAR-API in the Real World - Towards a Fair Evaluation of Hardware CAESAR Candidates**
Michael Tempelmeier, Fabrizio De Santis, Georg Sigl and Jens-Peter Kaps
- 81 **Horizontal Side-Channel Vulnerabilities of Post-Quantum Key Exchange Protocols**
Aydin Aysu, Youssef Tobah, Mohit Tiwari, Andreas Gerstlauer and Michael Orshansky

Session 4	Anti-counterfeit and Anti-Reverse Engineering
Date / Time	Wednesday, May 2, 2018 / 13:30 - 14:30
Session Chair	TBA

- 89 **Independent Detection of Recycled Flash Memory: Challenges and Solutions**
Preeti Kumari, B. M. S. Bahar Talukder, Sadman Sakib, Biswajit Ray and Md Tauhidur Rahman
- 96 **A Compact Energy-Efficient Pseudo-Static Camouflaged Logic Family**
Prashanth Mohan, NEC Akkaya, Burak Erbagichi and Ken Mai
- 103 **CTCG: Charge-Trap Based Camouflaged Gates for Reverse Engineering Prevention**
Asmit De, Anirudh Iyengar, Mohammad Nasim I. Khan, Sung-Hao Lin, Sandeep Thirumala, Swaroop Ghosh and Sumeet Gupta

Session 5	Physical Unclonable Functions (PUFs) and Chip Odometers
Date / Time	Thursday, May 3, 2018 / 10:00 - 11:00
Session Chair	TBA

- 111 **Secure Chip Odometers Using Intentional Controlled Aging**
Nail Etkin Can Akkaya, Burak Erbagci and Ken Mai
- 118 **Fresh Re-Keying with Strong PUFs: a New Approach to Side-Channel Security**
Xiaodan Xi, Aydin Aysu and Michael Orshansky
- 126 **Large Scale RO PUF Analysis over Slice Type, Evaluation Time and Temperature on 28nm Xilinx FPGAs**
Robert Hesselbarth, Florian Wilde, Chongyan Gu and Neil Hanley

Poster Session 1	Physical Unclonable Functions
Date / Time	Tuesday, May 1, 2018 / 16:15 - 17:45
Session Chair	TBA

- 134 **Abnormal Vehicle Behavior Induced Using Only Fabricated Informative CAN Messages**
Junko Takahashi, Masashi Tanaka, Hitoshi Fuji, Toshio Narita, Shunsuke Matsumoto and Hiroki Sato
- 138 **A Flexible Leakage Trace Collection Setup for Arbitrary Cryptographic IP Cores**
Athanassios Moschos, Apostolos P. Fournaris and Odysseas Koufopavlou
- 143 **Chaos Computing for Mitigating Side Channel Attack**
Md. Badruddoja Majumder, Md Sakib Hasan, Mesbah Uddin and Garrett S. Rose
- 147 **Comparison of Cost of Protection Against Differential Power Analysis of Selected Authenticated Ciphers**
William Diehl, Abubakr Abdulgadir, Farnoud Farahmand, Jens-Peter Kaps and Kris Gaj
- 153 **Delay Model and Machine Learning Exploration of a Hardware-Embedded Delay PUF**
Wenjie Che, Manel Martinez-Ramon, Fareena Saqib and Jim Plusquellic Enthentica
- 159 **Energy Efficient and Side-Channel Secure Hardware Architecture for Lightweight Cipher SIMON**
Arvind Singh, Nikhil Chawla, Monodeep Kar and Saibal Mukhopadhyay
- 163 **FPGA-Oriented Moving Target Defense against Security Threats from Malicious FPGA Tools**
Zhiming Zhang, Qiaoyan Yu, Laurent Njilla and Charles Kamhou
- 167 **Hardware Virtualization for Protection Against Power Analysis Attack**
Kai Yang, Jungmin Park, Mark Tehranipoor and Swarup Bhunia

- 173 **Inverse Gating for Low Energy Encryption**
Subhadeep Banik , Andrey Bogdanov, Francesco Regazzoni, Takanori Isobe, Harunaga Hiwatari and Toru Akishita
- 177 **Lowering the Barrier to Online Malware Detection Through Low Frequency Sampling of HPCs**
Patrick Cronin and Chengmo Yang
- 181 **On State Encoding Against Power Analysis Attacks for Finite State Controllers**
Richa Agrawal and Ranga Vemuri

Poster Session 2	Poster Session
Date / Time	Wednesday, May 2, 2018 / 14:30 - 15:30
Session Chair	TBA

- 187 **Prefetch-guard: Leveraging hardware prefetchers to defend against cache timing channels**
Hongyu Fang, Sai Santosh Dayapule, Fan Yao, Miloš Doroslovački and Guru Venkataramani
- 191 **Protecting Block Ciphers against Differential Fault Attacks without Re-keying**
Anubhab Baksi, Shivam Bhasin, Jakub Breier, Mustafa Khairallah and Thomas Peyrin
- 195 **R2D2: Runtime Reassurance and Detection of A2 Trojan**
Yumin Hou, Hu He, Kaveh Shamsi, Yier Jin, Dong Wu and Huaqiang Wu
- 201 **Repurposing SoC Analog Circuitry For Additional COTS Hardware Security**
Adam Duncan, Lei Jiang and Martin Swamy
- 205 **RF-PUF: IoT Security Enhancement through Authentication of Wireless Nodes using In-situ Machine Learning**
Baibhab Chatterjee, Debayan Das and Shreyas Sen
- 209 **Robust, Low-Cost and Accurate Detection of Recycled ICs using Digital Signatures**
Mahabubul Alam, Sreeja Chowdhury, Mark M. Tehranipoor and Ujjwal Guin
- 215 **SAT-based Reverse Engineering of Gate-Level Schematics using Fault Injection and Probing**
Shahzad Keshavarz, Falk Schellenberg, Bastian Richter, Christof Paar and Daniel Holcomb
- 221 **Self-Authenticating Secure Boot for FPGAs**
G. Pocklassery, W. Che, F. Saqib, M. Areno and J. Plusquellic Enthentica
- 227 **SIN² : Stealth Infection on Neural Network – A Low-cost Agile Neural Trojan Attack Methodology**
Tao Liu , Wujie Wen and Yier Jin
- 231 **Securing Interconnected PUF Network with Reconfigurability**
Hongxiang Gu and Miodrag Potkonjak
- 235 **Value Prediction for Security (VPsec): Countering Fault Attacks in Modern Microprocessors**
Rami Sheikh, Ro Cammarota and Wenjia Ruan