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

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

Technical Program

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

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

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

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

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