2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2020)

San Jose, California, USA
7 – 11 December 2020

IEEE

IEEE Catalog Number: CFP20HOA-POD
ISBN: 978-1-7281-7406-8

****** 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: CFP20HOA-POD
ISBN (Print-On-Demand): 978-1-7281-7406-8
ISBN (Online): 978-1-7281-7405-1

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 Programme

Session 1	**Side Channel Attack and Mitigation 1**
Date/Time	December 8, 2020 (Tuesday) / 14:30 – 14:50 hrs
Session Co-Chairs	**Aydin Aysu and Jim Plusquellic**

Session 2	**SoC Security**
Date/Time	December 8, 2020 (Tuesday) / 14:30 - 14:50 hrs
Session Co-Chairs	**William Diehl and Dmitry Ponomarev**

Session 3	**Anti-counterfeit, Anti-tamper and Side-Channel**
Date/Time	December 9, 2020 (Wednesday) / 15:30 - 15:45 hrs
Session Co-Chairs	**Ujjwal Guin and Fareena Saqib**

Towards the Avoidance of Counterfeit Memory: Identifying the DRAM Origin...111
B. M. S. Bahar Talukder, Vineetha Menon, Biswajit Ray, Tempestt Neal and Md Tauhidur Rahman

Hardware/Software Obfuscation against Timing Side-channel Attack on a GPU...122
Elmira Karimi, Yunsi Fei and David Kaeli

Latch-Based Logic Locking...132**
Joseph Sweeney, Mohammed Zackriya V, Samuel Pagliarini and Lawrence Pileggi

Session 4	**CAD Tools and Privacy**
Date/Time	December 9, 2020 (Wednesday) / 15:30 - 15:45 hrs
Session Co-Chairs	**Ioannis Savidis and JV Rajendran**

CPU and GPU Accelerated Fully Homomorphic Encryption...142
Toufique Morshed, Md Momin Al Aziz and Noman Mohammed

ReGDS: A Reverse Engineering Framework from GDSII to Gate-level Netlist...154
Rachel Selina Rajarathnam, Yibo Lin, Yier Jin and David Z. Pan

Evaluating Security Specification Mining for a CISC Architecture...164
Calvin Deutschbein and Cynthia Sturton

Session 5	**Side Channel Attack and Mitigation 2**
Date/Time	December 10, 2020 (Thursday) / 12:45 - 13:00 hrs
Session Co-Chairs	**Robert Karam and Lang Lin**

RS-Mask: Random Space Masking as an Integrated Countermeasure against Power and Fault Analysis...176
Keyvan Ramezanpour, Paul Ampadu and William Diehl

Architecture Correlation Analysis (ACA): Identifying the Source of Side-channel Leakage at Gate-level...188
Yuan Yao, Tarun Kathuria, Baris Ege and Patrick Schaumont

MaskedNet: The First Hardware Inference Engine Aiming Power Side-Channel Protection...197
Anuj Dubey, Rosario Cammarota and Aydin Aysu

DeepEM: Deep Neural Networks Model Recovery through EM Side-Channel Information Leakage...209
Honggang Yu, Haocheng Ma, Kaichen Yang, Yiqiang Zhao and Yier Jin

Session 6	**Fault Injection**
Date/Time	December 10, 2020 (Thursday) / 12:45 - 13:00 hrs
Session Co-Chairs	**Svetla Nikova and Shahin Tajik**

High Precision Laser Fault Injection using Low-cost Components...219
Martin S. Kelly and Keith Mayes

Cryptographic Fault Diagnosis using VerFI...229
Victor Arribas, Felix Wegener, Amir Moradi and Svetla Nikova

DESIV: Differential Fault Analysis of SIV-Rijndael256 with a Single Fault...241
Aikata, Banashri Karmakar and Dhiman Saha

Statistical Ineffective Fault Analysis of GIMLI...252
Michael Gruber, Matthias Probst and Michael Tempelmeier

Session 7	**Reverse Engineering and Physical Attacks**
Date/Time	December 11, 2020 (Friday) / 12:30 - 12:45 hrs
Session Co-Chairs	**Naghmeh Karimi and Ryan Helinski**

The Key is Left under the Mat: On the Inappropriate Security Assumption of Logic Locking Schemes...262
M Tanjidur Rahman, Shahin Tajik, M Sazadur Rahman, Mark Tehranipoor and Navid Asadizanjani

Lattice PUF: A Strong Physical Unclonable Function Provably Secure against Machine Learning Attacks...273
Ye Wang, Xiaodan Xi and Michael Orshansky

Attack of the Genes: Finding Keys and Parameters of Locked Analog ICs Using Genetic Algorithm...284
Rabin Yu Acharya, Sreeja Chowdhury, Fatemeh Ganji and Domenic Forte

Session 8	**IoT Security and HW Security Primitives**
Date/Time	December 11, 2020 (Friday) / 12:30 - 12:45 hrs
Session Co-Chairs	**Jiafeng Xie and Chengmo Yang**

A Post-Quantum Secure Discrete Gaussian Noise Sampler...295
Rashmi Agrawal, Lake Bu and Michel A. Kinsy

LAHEL: Lightweight Attestation Hardening Embedded Devices using Macrocells...305
Orlando Arias, Dean Sullivan, Haoqi Shan and Yier Jin

Protecting RESTful IoT Devices from Battery Exhaustion DoS Attacks...316
Stefan Hristozov, Manuel Huber and Georg Sigl