2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2019)

McLean, Virginia, USA
6-10 May 2019

IEEE

IEEE Catalog Number: CFP19HOA-POD
ISBN: 978-1-5386-8065-0

IEEE Catalog Number:	CFP19HOA-POD
ISBN (Print-On-Demand):	978-1-5386-8065-0
ISBN (Online):	978-1-5386-8064-3

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	Fault and Side Channel Technical Session
Date / Time	Tuesday, May 7, 2019 / 13:00 - 14:40
Session Chair	Aydin Aysu, *(NCSU, United States)*

Laser-induced Single-bit Faults in Flash Memory: Instructions Corruption on a 32-bit Microcontroller
Brice Colombier, Alexandre Menu, Jean-Max Dutertre, Pierre-Alain Moëllic, Jean-Baptiste Rigaud and Jean-Luc Danger

STELLAR: A Generic EM Side-Channel Attack Protection through Ground-Up Root-cause Analysis
Debayan Das, Mayukh Nath, Baibhab Chatterjee, Santosh Ghosh and Shreyas Sen

High Capability and Low-Complexity: Novel Fault Detection Scheme for Finite Field Multipliers over GF(2^m) based on MSPB
Chiou-Yng Lee and Jiafeng Xie

Extracting Side-Channel Leakage from Round Unrolled Implementations of Lightweight Ciphers
Nikhil Chawla, Arvind Singh, Nael Mizanur Rahman, Monodeep Kar and Saibal Mukhopadhyay

A Statistical Fault Analysis Methodology for the Ascon Authenticated Cipher
Keyvan Ramezanpour, Paul Ampadu and William Diehl

Session 2	IP Trust and Anti-Counterfeit Technical Session
Date / Time	Tuesday, May 7, 2019 / 15:00 - 16:40
Session Chair	Xiaolin Xu, *University of Illinois at Chicago, United States*

ENTT: A Family of Emerging NVM-based Trojan Triggers
Karthikeyan Nagarajan, Mohammad Nasim Imtiaz Khan and Swaroop Ghosh

Golden Gates: A New Hybrid Approach for Rapid Hardware Trojan Detection using Testing and Imaging
Qihang Shi, Nidish Vashistha, Hangwei Lu, Haoting Shen, Bahar Tehranipoor, Damon L Woodard and Navid Asadizanjani

Detecting Recycled SoCs by Exploiting Aging Induced Biases in Memory Cells
Ujjwal Guin, Wendong Wang, Charles Harper and Adit D. Singh

FLATS: Filling Logic and Testing Spatially for FPGA Authentication and Tamper Detection
Adam Duncan, Grant Skipper, Andrew Stern, Adib Nahiyan, Fahim Rahman, Andrew Lukefahr, Mark Tehranipoor and Martin Swany

QIF-Verilog: Quantitative Information-Flow based Hardware Description Languages for Pre-Silicon Security Assessment
Xiaolong Guo, Raj Gautam Dutta, Jiaji He, Mark M. Tehranipoor and Yier Jin

Session 3	Architecture Level Security Technical Session
Date / Time	Wednesday, May 8, 2019 / 10:20 - 12:00
Session Chair	Seyed-Abdollah Sohrab Aftabjahani, *Intel, United States*

A Fetching Tale: Covert Communication with the Hardware Prefetcher
Patrick Cronin and Chengmo Yang

Using Power-Anomalies to Counter Evasive Micro-Architectural Attacks in Embedded Systems
Shijia Wei, Aydin Aysu, Michael Orshansky, Andreas Gerstlauer and Mohit Tiwari

COTSknight: Practical Defense against Cache Timing Channel Attacks using Cache Monitoring and Partitioning Technologies
Fan Yao, Hongyu Fang, Miloš Doroslovački and Guru Venkataramani

CoPHEE: Co-processor for Partially Homomorphic Encrypted Execution
Mohammed Nabeel, Mohammed Ashraf, Eduardo Chielle, Nektarios G. Tsoutsos and Michail Maniatakos

Efficient and Flexible Low-Power NTT for Lattice-Based Cryptography
Tim Fritzmann and Johanna Sepúlveda

Session 4	(Anti)Reverse Engineering and Obfuscation Technical Session
Date / Time	Wednesday, May 8, 2019 / 13:00 - 14:40
Session Chair	Nektarios Georgios Tsoutsos, *University of Delaware, United States*

Improving on State Register Identification in Sequential Hardware Reverse Engineering
Michaela Brunner, Johanna Baehr and Georg Sigl

On the Impossibility of Approximation-Resilient Circuit Locking
Kaveh Shamsi, David Z. Pan and Yier Jin

Exploiting Proximity Information in a Satisfiability Based Attack Against Split Manufactured Circuits
Suyuan Chen and Ranga Vemuri

SURF: Joint Structural Functional Attack on Logic Locking
Prabuddha Chakraborty, Jonathan Cruz and Swarup Bhunia

Securing AES against Localized EM Attacks through Spatial Randomization of Dataflow
Ge Li, Vishnuvardhan Iyer and Michael Orshansky

Session 5	Assorted Technical Session
Date / Time	Thursday, May 9, 2019 / 10:00 - 11:40
Session Chair	Vivek Venugopalan, *USC ISI, United States*

MPCircuits: Optimized Circuit Generation for Secure Multi-Party Computation
M. Sadegh Riazi, Mojan Javaheripi, Siam U. Hussain and Farinaz Koushanfar

SIA: Secure Intermittent Architecture for Off-the-Shelf Resource-Constrained Microcontrollers
Daniel Dinu, Archanaa S. Khrishnan and Patrick Schaumont

RATAFIA: Ransomware Analysis using Time And Frequency Informed Autoencoders
Manaar Alam, Sarani Bhattacharya, Swastika Dutta, Sayan Sinha, Debdeep Mukhopadhyay and Anupam Chattopadhyay

Using Hardware Software Codesign for Optimised Implementations of High-Speed and Defence in Depth CAESAR Finalists
Michael Tempelmeier, Maximilian Werner and Georg Sigl

In-depth Analysis and Enhancements of RO-PUFs with a Partial Reconfiguration Framework on Xilinx Zynq-7000 SoC FPGAs
Andreas Herkle, Holger Mandry, Joachim Becker and Maurits Ortmanns