

2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2021)

**Virtual Symposium
13 – 14 December 2021**



**IEEE Catalog Number: CFP21HOA-POD
ISBN: 978-1-6654-1358-9**

**Copyright © 2021 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:	CFP21HOA-POD
ISBN (Print-On-Demand):	978-1-6654-1358-9
ISBN (Online):	978-1-6654-1357-2

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

TABLE OF CONTENTS

SAFEGUARDING THE INTELLIGENCE OF NEURAL NETWORKS WITH BUILT-IN LIGHT-WEIGHT INTEGRITY MARKS (LIMA).....	1
<i>Fateme S. Hosseini, Qi Liu, Fanruo Meng, Chengmo Yang, Wujie Wen</i>	
HW2VEC: A GRAPH LEARNING TOOL FOR AUTOMATING HARDWARE SECURITY	13
<i>Shih-Yuan Yu, Rozhin Yasaei, Qingrong Zhou, Tommy Nguyen, Mohammad Abdullah Al Faruque</i>	
AUTOMATED DETECTION OF SPECTRE AND MELTDOWN ATTACKS USING EXPLAINABLE MACHINE LEARNING.....	24
<i>Zhixin Pan, Prabhat Mishra</i>	
SINGLE-TRACE SIDE-CHANNEL ATTACKS ON ω -SMALL POLYNOMIAL SAMPLING: WITH APPLICATIONS TO NTRU, NTRU PRIME, AND CRYSTALS-DILITHIUM	35
<i>Emre Karabulut, Erdem Alkim, Aydin Aysu</i>	
FAULTLINE: SOFTWARE-BASED FAULT INJECTION ON MEMORY TRANSFERS	46
<i>Joseph Gravellier, Jean-Max Dutertre, Yannick Tegli, Philippe Loubet Moundi</i>	
SECWALK: PROTECTING PAGE TABLE WALKS AGAINST FAULT ATTACKS	56
<i>Robert Schilling, Pascal Nasahl, Stefan Weiglhofer, Stefan Mangard</i>	
PROTECTING INDIRECT BRANCHES AGAINST FAULT ATTACKS USING ARM POINTER AUTHENTICATION	68
<i>Pascal Nasahl, Robert Schilling, Stefan Mangard</i>	
ITIMED: CACHE ATTACKS ON THE APPLE A10 FUSION SOC.....	80
<i>Gregor Haas, Seetal Potluri, Aydin Aysu</i>	
CROSS-VM INFORMATION LEAKS IN FPGA-ACCELERATED CLOUD ENVIRONMENTS.....	91
<i>Ilias Giechaskiel, Shanquan Tian, Jakub Szefer</i>	
TIME SERIES-BASED MALWARE DETECTION USING HARDWARE PERFORMANCE COUNTERS	102
<i>Abraham Peedikayil Kuruvila, Sayar Karmakar, Kanad Basu</i>	
A COMPARISON OF NEURAL NETWORKS FOR PCB COMPONENT SEGMENTATION	113
<i>Abinai Pasunuri, Nathan Jessurun, Olivia P. Paradis, Navid Asadizanjani</i>	
POCA: FIRST POWER-ON CHIP AUTHENTICATION IN UNTRUSTED FOUNDRY AND ASSEMBLY.....	124
<i>Md Sami Ul Islam Sami, Fahim Rahman, Adam Cron, Dale Donchin, Mike Borza, Farimah Farahmandi, Mark Tehranipoor</i>	
3D UNCLONABLE OPTICAL IDENTITY FOR UNIVERSAL PRODUCT VERIFICATION	136
<i>Chenxing Wang, Lily Raymond, Yifei Jin, Alireza Tavakkoli, Haoting Shen</i>	
SYNCIRC: EFFICIENT SYNTHESIS OF DEPTH-OPTIMIZED CIRCUITS FOR SECURE COMPUTATION	147
<i>Arpita Patra, Thomas Schneider, Ajith Suresh, Hossein Yalame</i>	

USING UNDERVOLTING AS AN ON-DEVICE DEFENSE AGAINST ADVERSARIAL MACHINE LEARNING ATTACKS.....	158
<i>Saikat Majumdar, Mohammad Hossein Samavatian, Kristin Barber, Radu Teodorescu</i>	
LIGHTWEIGHT ENCRYPTION USING CHAFFING AND WINNOWING WITH ALL-OR-NOTHING TRANSFORM FOR NETWORK-ON-CHIP ARCHITECTURES	170
<i>Hansika Weerasena, Subodha Charles, Prabhat Mishra</i>	
CONTRASTIVE GRAPH CONVOLUTIONAL NETWORKS FOR HARDWARE TROJAN DETECTION IN THIRD PARTY IP CORES.....	181
<i>Nikhil Muralidhar, Abdullah Zubair, Nathanael Weidler, Ryan Gerdes, Naren Ramakrishnan</i>	
CONNOC: A PRACTICAL TIMING CHANNEL ATTACK ON NETWORK-ON-CHIP HARDWARE IN A MULTICORE PROCESSOR.....	192
<i>Usman Ali, Omer Khan</i>	
HERMES: HARDWARE-EFFICIENT SPECULATIVE DATAFLOW ARCHITECTURE FOR BONSAI MERKLE TREE-BASED MEMORY AUTHENTICATION.....	203
<i>Yu Zou, Amro Awad, Mingjie Lin</i>	
RUDBA: REUSABLE USER-DEVICE BIOMETRIC AUTHENTICATION SCHEME FOR MULTI-SERVICE SYSTEMS.....	214
<i>Zhonghao Liao, Yong Guan</i>	
MORPHEUS II: A RISC-V SECURITY EXTENSION FOR PROTECTING VULNERABLE SOFTWARE AND HARDWARE.....	226
<i>Austin Harris, Tarunesh Verma, Shijia Wei, Lauren Biernacki, Alex Kisil, Misiker Tadesse Aga, Valeria Bertacco, Baris Kasikci, Mohit Tiwari, Todd Austin</i>	
TRRSOPE: UNDERSTANDING TARGET ROW REFRESH MECHANISM FOR MODERN DDR PROTECTION.....	239
<i>Yichen Jiang, Hui Feng Zhu, Haoqi Shan, Xiaolong Guo, Xuan Zhang, Yier Jin</i>	
NEUROBFUSCATOR: A FULL-STACK OBFUSCATION TOOL TO MITIGATE NEURAL ARCHITECTURE STEALING	248
<i>Jingtao Li, Zhezhi He, Adnan Siraj Rakin, Deliang Fan, Chaitali Chakrabarti</i>	
METHODOLOGY OF ASSESSING INFORMATION LEAKAGE THROUGH SOFTWARE-ACCESSIBLE TELEMETRIES	259
<i>Chen Liu, Monodeep Kar, Xueyang Wang, Nikhil Chawla, Neer Roggel, Bilgiday Yuce, Jason M. Fung</i>	
MULTIPHYSICS SIMULATION OF EM SIDE-CHANNELS FROM SILICON BACKSIDE WITH ML-BASED AUTO-POI IDENTIFICATION.....	270
<i>Lang Lin, Deqi Zhu, Jimin Wen, Hua Chen, Yu Lu, Norman Chang, Calvin Chow, Harsh Shrivastav, Chia-Wei Chen, Kazuki Monta, Makoto Nagata</i>	
FUN-SAT: FUNCTIONAL CORRUPTIBILITY-GUIDED SAT-BASED ATTACK ON SEQUENTIAL LOGIC ENCRYPTION.....	281
<i>Yinghua Hu, Yuke Zhang, Kaixin Yang, Dake Chen, Peter A. Beerel, Pierluigi Nuzzo</i>	
JANUS: BOOSTING LOGIC OBFUSCATION SCOPE THROUGH RECONFIGURABLE FSM SYNTHESIS	292
<i>Leon Li, Shuyi Ni, Alex Orailoglu</i>	

FORMAL EVALUATION AND CONSTRUCTION OF GLITCH-RESISTANT MASKED
FUNCTIONS..... 304
*Sofiane Takarabt, Sylvain Guilley, Youssef Souissi, Khaled Karray, Laurent Sauvage, Yves
Mathieu*

Author Index