

2023 IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2023)

**San Jose, California, USA
1 – 4 May 2023**



**IEEE Catalog Number: CFP23HOA-POD
ISBN: 979-8-3503-0063-5**

**Copyright © 2023 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:	CFP23HOA-POD
ISBN (Print-On-Demand):	979-8-3503-0063-5
ISBN (Online):	979-8-3503-0062-8
ISSN:	2835-5709

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

ProcessorFuzz: Processor Fuzzing with Control and Status Registers Guidance.....	1
<i>Sadullah Canakci, Chathura Rajapaksha, Leila Delshadtehrani, Anoop Nataraja, Michael Bedford Taylor, Manuel Egele, Ajay Joshi</i>	
Targeted Bitstream Fault Fuzzing Accelerating BiFI on Large Designs	13
<i>Susanne Engels, Maik Ender, Christof Paar</i>	
EC-CFI: Control-Flow Integrity Via Code Encryption Counteracting Fault Attacks.....	24
<i>Pascal Nasahl, Salmin Sultana, Hans Liljestrand, Karanvir Grewal, Michael Lemay, David M. Durham, David Schrammel, Stefan Mangard</i>	
Low-Latency Masking with Arbitrary Protection Order Based on Click Elements	36
<i>Mateus Simões, Lilian Bossuet, Nicolas Bruneau, Vincent Grosso, Patrick Haddad, Thomas Sarno</i>	
A Low-Randomness First-Order Masked Xoodoo.....	48
<i>Shuohang Peng, Bohan Yang, Shuying Yin, Hang Zhao, Cankun Zhao, Shaojun Wei, Leibo Liu</i>	
Security Order of Gate-Level Masking Schemes	57
<i>Sofiane Takarabt, Javad Bahrami, Mohammad Ebrahimabadi, Sylvain Guilley, Naghmeh Karimi</i>	
SCALE: Secure and Scalable Cache Partitioning.....	68
<i>Nadja Ramhöj Holtryd, Madhavan Manivannan, Per Stenström</i>	
Advanced Covert-Channels in Modern SoCs.....	80
<i>Lilian Bossuet, Carlos Andres Lara-Nino</i>	
Lightweight Countermeasures Against Original Linear Code Extraction Attacks on a RISC-V Core	89
<i>Théophile Gousselot, Olivier Thomas, Jean-Max Dutertre, Olivier Potin, Jean-Baptiste Rigaud</i>	
CIFER: Code Integrity and Control Flow Verification for Programs Executed on a RISC-V Core	100
<i>Anthony Zgheib, Olivier Potin, Jean-Baptiste Rigaud, Jean-Max Dutertre</i>	
Improving Single-Trace Attacks on the Number-Theoretic Transform for Cortex-M4.....	111
<i>Guilhèm Assael, Philippe Elbaz-Vincent, Guillaume Reymond</i>	
Detour: Layout-Aware Reroute Attack Vulnerability Assessment and Analysis	122
<i>Minyan Gao, Domenic Forte</i>	
Dual Channel EM/Power Attack Using Mutual Information and Its Real-Time Implementation.....	133
<i>Yunkai Bai, Jungmin Park, Mark Tehranipoor, Domenic Forte</i>	
Dual-Leak: Deep Unsupervised Active Learning for Cross-Device Profiled Side-Channel Leakage Analysis.....	144
<i>Honggang Yu, Shuo Wang, Haoqi Shan, Maximillian Panoff, Michael Lee, Kaichen Yang, Yier Jin</i>	
Hardware-Software Co-Design for Side-Channel Protected Neural Network Inference.....	155
<i>Anuj Dubey, Rosario Cammarota, Avinash Varna, Raghavan Kumar, Aydin Aysu</i>	

TripletPower: Deep-Learning Side-Channel Attacks Over Few Traces	167
<i>Chenggang Wang, Jimmy Dani, Shane Reilly, Austen Brownfield, Boyang Wang, John M. Emmert</i>	
Uprooting Trust: Learnings from an Unpatchable Hardware Root-Of-Trust Vulnerability in Siemens S7-1500 PLCs	179
<i>Yuanzhe Wu, Grant Skipper, Ang Cui</i>	
OMT: A Run-Time Adaptive Architectural Framework for Bonsai Merkle Tree-Based Secure Authentication with Embedded Heterogeneous Memory	191
<i>Rakin Muhammad Shadab, Yu Zou, Sanjay Gandham, Mingjie Lin</i>	
MagHop: Magnetic Spectrum Hopping for Securing Voltage and Current Magnetic Sensors.....	203
<i>Anomadarshi Barua, Mohammad Abdullah Al Faruque</i>	
Gadgets of Gadgets in Industrial Control Systems: Return Oriented Programming Attacks on PLCs.....	215
<i>Adeen Ayub, Nauman Zubair, Hyunguk Yoo, Wooyeon Jo, Irfan Ahmed</i>	
Disassembling Software Instruction Types Through Impedance Side-Channel Analysis	227
<i>Md Sadik Awal, Md Tauhidur Rahman</i>	
Bits to BNNs: Reconstructing FPGA ML-IP with Joint Bitstream and Side-Channel Analysis.....	238
<i>Brooks Olney, Robert Karam</i>	
LEDA: Locking Enabled Differential Analysis of Cryptographic Circuits	249
<i>Devanshi Upadhyaya, Maël Gay, Ilia Polian</i>	
Design of Quantum Computer Antivirus	260
<i>Sanjay Deshpande, Chuanqi Xu, Theodoros Trochatos, Hanrui Wang, Ferhat Erata, Song Han, Yongshan Ding, Jakub Szefer</i>	
Fast Fingerprinting of Cloud-Based NISQ Quantum Computers	271
<i>Kaitlin N. Smith, Joshua Vizslai, Lennart Maximilian Seifert, Jonathan M. Baker, Jakub Szefer, Frederic T. Chong</i>	
Towards Secure Classical-Quantum Systems.....	283
<i>Daniel Volya, Tao Zhang, Nashmin Alam, Mark Tehranipoor, Prabhat Mishra</i>	
FHE-Booster: Accelerating Fully Homomorphic Execution with Fine-Tuned Bootstrapping Scheduling.....	293
<i>Tommy White, Charles Gouert, Chengmo Yang, Nektarios Georgios Tsoutsos</i>	
Generating Lower-Cost Garbled Circuits: Logic Synthesis Can Help	304
<i>Mingfei Yu, Giovanni De Micheli</i>	
V_{PP} : Privacy Preserving Machine Learning Via Undervolting	315
<i>Md Shohidul Islam, Behnam Omid, Ihsen Alouani, Khaled N. Khasawneh</i>	
A Privacy-Preserving Protocol Level Approach to Prevent Machine Learning Modelling Attacks on PUFs in the Presence of Semi-Honest Verifiers	326
<i>Owen Millwood, Fei Hongming, Prosanta Gope, Oguz Narli, Meltem Kurt Pehlivanoglu, Elif Bilge Kavun, Biplab Sikdar</i>	

Author Index