

2025 IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2025)

**San Jose, California, USA
5-8 May 2025**



**IEEE Catalog Number: CFP25HOA-POD
ISBN: 979-8-3315-4199-6**

**Copyright © 2025 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:	CFP25HOA-POD
ISBN (Print-On-Demand):	979-8-3315-4199-6
ISBN (Online):	979-8-3315-4198-9
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

An Input Recovery Side-Channel Attack on DNN Accelerator with Three-Dimensional Power Surface.....	1
<i>Le Wu, Liji Wu, Zhiwei Ba, Xiangmin Zhang</i>	
MACPruning: Dynamic Operation Pruning to Mitigate Side-Channel DNN Model Extraction.....	12
<i>Ruyi Ding, Cheng Gongye, Davis Ranney, Aidong A. Ding, Yunsi Fei</i>	
EyeHearYou: Probing Location Identification via Occluded Smartphone Cameras and Ultrasound.....	23
<i>Nina Shamsi, Yan Long, Kevin Fu</i>	
Betrayed by Light: How Photon Emission Microscopy Empowers Register Bit-Level Laser Attacks on Microcontrollers	35
<i>Hugo Perrin, Jean-Max Dutertre, Jean-Baptiste Rigaud</i>	
ReFID: A System-Aware Remote Fault-Injection Attack Detection & Mitigation for Secure Heterogeneous System	46
<i>Amit M. Shuvo, M. Latifur Rahman, Jingbo Zhou, Farimah Farahmandi, Mark Tehranipoor</i>	
ML-EMFI: A Machine Learning-Driven Pre-Silicon Electromagnetic Fault Injection Security Evaluation for Robust IC Design.....	57
<i>Pantha P. Sarker, Tianze Kan, Jingchen Liang, Ozgur Tuncer, Bo He, Zelin Lu, Sudarshan Mallu, Lang Lin, Norman Chang, Riku Hasegawa, Kazuki Monta, Makoto Nagata, Farimah Farahmandi, Mark Tehranipoor</i>	
E-LoQ: Enhanced Locking for Quantum Circuit IP Protection.....	67
<i>Yuntao Liu, Jayden John, Qian Wang</i>	
STIQ: Safeguarding Training and Inferencing of Quantum Neural Networks from Untrusted Cloud.....	78
<i>Satwik Kundu, Swaroop Ghosh</i>	
Undermining Quantum Circuit Obfuscation: Insights from Structural Analysis.....	88
<i>Donald Lushi, Samah M. Saeed</i>	
3D Bioprinter Firmware Attacks: Categorization, Implementation, and Impacts.....	99
<i>Muhammad Ahsan, Barry Najjarro-Blancas, Johanna T. Ebode, Nastassja Lewinski, Irfan Ahmed</i>	
Reverse Engineering DVFS Mechanisms	111
<i>Ryan Piersma, Tawhid Bhuiyan, Tanvir A. Khan, Simha Sethumadhavan</i>	
FanBleed: Stealing Your Secrets via Observing Your Cooling Fan.....	123
<i>Sisheng Liang, Zhengxiong Li, Zihao Zhan, Zhenkai Zhang</i>	
USBSnoop - Revealing Device Activities via USB Congestions	135
<i>Davis Ranney, Yufei Wang, A. Adam Ding, Yunsi Fei</i>	
Traffic Analysis Attacks on Wireless NoC-Based SoCs.....	146
<i>Hansika Weerasena, Prabhat Mishra</i>	
DOMe: Automated Validation of Data-Oblivious Program Execution.....	157
<i>Donayam Benti, Todd Austin</i>	

WaveSleuth: Retrospective PLC Memory for Anomaly Detection in Industrial Control Systems.....	170
<i>Nehal Ameen, Ramyapandian Vijayakanthan, Adeen Ayub, Aisha Ali-Gombe, Irfan Ahmed</i>	
EvoWeight: Sponge Poisoning of FPGA-Based DNN Accelerators in Differential Private Secure Federated Learning.....	182
<i>Muhammad S. Akram, Vincent Meyers, Mehdi Tahoori, Bogaraju S. Varma, Dewar Finlay</i>	
LAPD: Lifecycle-Aware Power-Based Malware Detection	194
<i>Alexander Cathis, Mulong Luo, Mohit Tiwari, Andreas Gerstlauer</i>	
Michscan: Black-Box Neural Network Integrity Checking at Runtime Through Power Analysis.....	205
<i>Robi Paul, Michael Zuzak</i>	
AccessShadow: Leveraging Adversarial Samples to Counter Deep Learning-Assisted Cache Timing Attacks	216
<i>Xiang Zhang, Ziyue Zhang, Aidong A. Ding, Yunsi Fei</i>	
Input-Triggered Hardware Trojan Attack on Spiking Neural Networks.....	227
<i>Spyridon Raptis, Paul Kling, Ioannis Kaskampas, Ihsen Alouani, H.-G. Stratigopoulos</i>	
Trojan Localization in Generic AMS Circuits from Combined Power and Functional Queries.....	239
<i>Dipali Jain, Shakil Ahmed, Guangwei Zhao, Rajesh Datta, Kaveh Shamsi</i>	
Evaluating the Effectiveness of Hardware Trojan Detection Approaches at RTL.....	250
<i>Ruo Chen Dai, Zhaoxiang Liu, Orlando Arias, Xiaolong Guo, Tuba Yavuz</i>	
Amplifying Electromagnetic Leakage by Hardware Trojans Through Cable Geometry Manipulation	261
<i>Hayato Ide, Shohei Matsumoto, Taiki Kitazawa, Shugo Kaji, Daisuke Fujimoto, Takashi Kasuga, Yuichi Hayashi</i>	
Sourcing Trust from Peers with Physical Unclonable Functions.....	268
<i>M. Sadman Siraj, Aisha B. Rahman, Cyrus Minwalla, Eirini E. Tsiropoulou, Jim Plusquellic</i>	
On the Impact of Metastability in Jitter Based TRNG	279
<i>Florian Pebay-Peyroula, Licinius-Pompiliu Benea, Mikael Carmona, Romain Wacquez</i>	
Quantization Schemes for PUFs: The Entropy-Area Trade-Off.....	289
<i>Jens Nöpel, Tim Music, Niklas Stein, Christoph Frisch, Michael Pehl</i>	
cuOT: Accelerating Oblivious Transfer on GPUs for Privacy-Preserving Computation.....	300
<i>Andrew Gan, Setsuna Yuki, Timothy Rogers, Zahra Ghodsi</i>	
Cryptographic Least Privilege Enforcement for Scalable Memory Isolation.....	312
<i>Martin Unterguggenberger, David Schrammel, Lukas Maar, Lukas Lamster, Vedad Hadžic, Stefan Mangard</i>	
CHESS: Compiling Homomorphic Encryption with Scheme Switching.....	324
<i>Rostin Shokri, Nektarios G. Tsoutsos</i>	
SoCureLLM: An LLM-Driven Approach for Large-Scale System-on-Chip Security Verification and Policy Generation	335
<i>Shams Tarek, Dipayan Saha, Sujan K. Saha, Mark Tehranipoor, Farimah Farahmandi</i>	
Low-Entropy Packed Binary Detection via Accurate Hardware Events Profiling	346
<i>Erika Leal, Mengfei Ren, Shijia Li, Jiang Ming</i>	

RLFuzz: Accelerating Hardware Fuzzing with Deep Reinforcement Learning	358
<i>Raphael Götz, Christoph Sendner, Nico Ruck, Mohamadreza Rostami, Alexandra Dmitrienko, Ahmad-Reza Sadeghi</i>	
Reward-Based Blockchain Infrastructure for 3D IC Supply Chain Provenance	370
<i>Sulyab T. Valapu, Aritri Saha, Bhaskar Krishnamachari, Vivek Menon, Ujjwal Guin</i>	
RRR: Rethinking Randomized Remapping for High Performance Secured NVM LLC	381
<i>Prathamesh N. Tanksale, Guru R. S. Seethiraju, Shirshendu Das, Venkata K. Tavva</i>	
Efficient CPA Attack on Hardware Implementation of ML-DSA in Post-Quantum Root of Trust	392
<i>Merve Karabulut, Reza Azarderakhsh</i>	
Code Encryption for Confidentiality and Execution Integrity Down to Control Signals	403
<i>Théophile Gousselot, Jean-Max Dutertre, Olivier Potin, Jean-Baptiste Rigaud</i>	
Termite Attacks: Gnawing on Logs to Extract Secret Information.....	415
<i>Hyun B. Lee, Tushar M. Jois, Christopher W. Fletcher, Carl A. Gunter</i>	
Securing Smart Manufacturing: Detection of Cyber-Physical Attacks in CNC-Based Systems	427
<i>Bethanie Williams, Rima A. Awad, Clifton Mulkey, Gabriela Ciocarlie, Muhammad Ismail, Kyle Saleeby</i>	
Wattshield: A Power Side-Channel Framework for Detecting Malicious Firmware in Fused Filament Fabrication.....	438
<i>Muhammad Ahsan, Irfan Ahmed</i>	
Breaking Confidentiality of XTS-AES Encrypted Data at Rest on Microprocessors using Electromagnetic Side-Channel Attacks	450
<i>Paul Krüger, Stefan Wildermann, Jürgen Teich</i>	
Micropower: Micro Neural Networks for Side-Channel Attacks	462
<i>Logan Reichling, Ryan Evans, Mabon Ninan, Phuc Mai, Boyang Wang, Yunsi Fei, John M. Emmert</i>	

Author Index