

2026 IEEE International Symposium on Hardware Oriented Security and Trust (HOST 2026)

**Washington, District of Columbia, USA
4-7 May 2026**

IEEE Catalog Number:
ISBN:

CFP26HOA-POD
979-8-3195-0895-9



Copyright © 2026, IEEE

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:	CFP26HOA-POD
ISBN (Print-On-Demand):	979-8-3195-0895-9
ISBN (Online):	979-8-3195-0894-2
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

TABLE OF CONTENTS

Erasing Is Not Enough: Data Leakage From Sanitized Charge-Trap NOR Flash Devices	1
<i>Anjali Murali, Matchima Buddhano, Mondol Anik Kumar, Aleksandar Milenkovic, Indrajit Ray</i> <i>Sudeep Pasricha, Biswajit Ray</i>	
SnoopyPower! Remote Power Attacks on Cache and Coherence Paths	12
<i>Elliott Quéré, Maria Méndez Real, Alessandro Palumbo, Thomas Rokicki, Lilian Bossuet, Rubén Salvador</i>	
Vtrack: Defending Against All Rowhammer Attack Patterns by Tracking Victim Rows	25
<i>Tejeshwar Bhagatsing Thorawade, Varun Venkitaraman, Keerthi Sagar Kokkiligadda, Samiksha Verma</i> <i>Virendra Singh</i>	
Rowhammer Vulnerabilities in 3D NAND Flash Induced by Hot Carrier Injection	36
<i>Habib Ur Rahman, Matchima Buddhano, Mondal Anik Kumar, Sudeep Pasricha, Biswajit Ray</i>	
LEAH: Lightweight and Efficient Hardware Accelerator for Code-Based PQC Scheme HQC	47
<i>Yazheng Tu, Jiafeng Xie</i>	
Cash: Lightweight Keyed Hash Function Design for Reconfigurable Hardware	58
<i>Arman Allahverdi, Adil Farooq, Anias Pullen, Yongyu Qiang, Vincent John Mooney, Santiago Grijalva</i>	
Efficient Low-Latency Masking of Ascon Without Fresh Randomness	69
<i>Srinidhi Hari Prasad, Florian Mendel, Martin Schl��ffer, Rishub Nagpal</i>	
Fault Injection Attacks and Countermeasures on TinyML Algorithms	81
<i>Anthony Etim, Srilalith Nampally, Aubtin Rasouli, Dustin Mazza, Krishna Chilakapati, Tinghung Chiu</i> <i>Ferhat Erata, Leyla Nazhandali, Wenjie Xiong, Jakub Szefer</i>	
Exploring Laser Fault Injection in System-on-Chips: A New Approach for CPU and Cache Attacks	92
<i>Soline Casavecchia, Driss Aboukassimi, Jessy Cl��di��re, Jean-Max Dutertre, Simon Pont��</i>	
CHAPATI: End-to-End Methodology to Conduct Multi-Faults Injection Campaigns	103
<i>Antoine Gicquel, Ludovic Claudepierre, Damien Hardy, Karine Heydemann, Erven Rohou</i>	
WaLi: Can Pressure Sensors in HVAC Systems Capture Human Speech?	116
<i>Tarikul Islam Tamiti, Biraj Joshi, Rida Hasan, Anomadarshi Barua</i>	
LiDAR Spoofing for Compromising SLAM on ROS2 Using Statistical Beam Adjustment & Temporal Modeling	130
<i>Finn Schaefer, Ryan Lam, Sidarth Kumar, Jimmy Tram, Neil Sharma, Md Tanvir Arafin</i>	
From Uncertainty to Insight: Exploring Circuit-Level Privacy Preservation for Healthcare Applications	142
<i>Mashrafi Kajol, Nishanth Chennagouni, Wei Lu, Qiaoyan Yu</i>	
MCM-Leak: Exploiting Mid-Circuit Measurement Control for Covert Quantum Information Leakage	153
<i>Donald Lushi, Samah Mohamed Saeed</i>	
QubitHammer: Remotely Inducing Qubit State Change on Superconducting Quantum Computers	164
<i>Yizhuo Tan, Navnil Choudhury, Kanad Basu, Jakub Szefer</i>	
Formal Firmware Verification of an At-Scale VM-level TEE Architecture	175
<i>Sophia Zhang, Bo-Yuan Huang, Sayak Ray, Jason Fung, Aarti Gupta, Sharad Malik</i>	

Fuzz'EMup: Leveraging EM Side-Channel Emanation to Guide Black-Box Embedded Firmware Fuzzing	187
<i>Fatemeh Moradihaghighi, Zihao Zhan, Yanan Guo, Ziming Zhao, Mashrur Chowdhury, Zhenkai Zhang</i>	
Golden-Free Hardware Trojan Detection Using Multi-Modal Contrastive Learning	199
<i>Zhixin Pan, Amberbir Alemayoh, Linh Nguyen, Ziyu Shu</i>	
BlindMarket: Enabling Verifiable, Confidential, and Traceable IP Core Distribution in Zero-Trust Settings	210
<i>Zhaoxiang Liu, Samuel Judson, Raj Dutta, Mark Santolucito, Xiaolong Guo, Ning Luo</i>	
PermuteV: A Performant Side-Channel-Resistant RISC-V Core Securing Edge AI Inference	222
<i>Nuntipat Narkthong, Xiaolin Xu</i>	
GhostTrace: A Membership Inference Attack via Hardware Performance Counters as a Side-Channel	233
<i>Amisha Srivastava, Anand Menon, Sanjay Das, Kanad Basu</i>	
InterPUF: Distributed Authentication via Physically Unclonable Functions and Multi-Party Computation for Reconfigurable Interposers	244
<i>Ishraq Tashdid, Tasnuva Farheen, Sazadur Rahman</i>	
TwinAttest: A Digital Twin-Driven Attestation Framework for Programmable Logic Controllers in Industrial Internet of Things	256
<i>Syed Owais Athar, Muhammad Naveed Aman</i>	
Spatial RowHammer Fingerprints: DRAM-based PUFs for Robust Device Identification	267
<i>Vineet Suresh Kumar, Mohammad Farmani</i>	
AdvProtego: A Unified Framework to Safeguard Deep Learning Models Against Side Channel Leakage	273
<i>Xiaobei Yan, Chip Hong Chang, Shangwei Guo, Tianwei Zhang</i>	
Double Strike: Breaking Approximation-Based Side-Channel Countermeasures for DNNs	285
<i>Lorenzo Casalino, Maria Méndez Real, Jean-Christophe Prévotet, Rubén Salvador</i>	
Talking Traces: Audio Reconstruction Power Side-Channel Attack on Neural Network FPGA Accelerators	297
<i>Johannes Reibold, Vincent Meyers, Mehdi Tahoori</i>	
HeatGuard: Securing NoC-Based MPSoCs Against Analog Thermal Anomalies	309
<i>Mahdi Hasanazadeh, Mahdi Fazeli, Kasem Khalil, Cynthia Sturton, Ahmad Patooghy</i>	
RuntimeShield: Power Distribution Network-Based Root of Trust for Embedded System Security	320
<i>Kejun Chen, Zhaowen Chen, Huifeng Zhu, Xuan Zhang, Yuntao Liu, Xiaolong Guo, Xianglong Feng</i>	
SecureCoin: Preserving Confidentiality in Decentralized Hardware Power Management	332
<i>Ryan Piersma, Karthik Swaminathan, Martin Cochet, Pradip Bose, Simha Sethumadhavan</i>	
ObfusBFA: A Holistic Approach to Safeguarding DNNs From Different Types of Bit-Flip Attacks	344
<i>Xiaobei Yan, Han Qiu, Tianwei Zhang</i>	
FlipLLM: Efficient Bit-Flip Attacks on Multimodal LLMs Using Reinforcement Learning	356
<i>Khurram Khalil, Khaza Anuarul Hoque</i>	
BitFlipScope: Scalable Fault Localization and Recovery for Bit-Flip Corruptions in LLMs	367
<i>Muhammad Zeeshan Karamat, Sadman Saif, Christiana Chamon</i>	

Forgotten but Not Gone: Residual Data Exfiltration Attack Against on-Chip FPGA Memories	383
<i>Bharadwaj Madabhushi, Chandra Sekhar Mummidi, Sandip Kundu</i>	
Beyond Defense: A Rowhammer Mitigation That Boosts Performance	394
<i>Samiksha Verma, Virendra Singh</i>	
Covert Information Leakage Via Hardware-Induced Spectral Shaping	405
<i>Apostolos Kontarinis, Sameer Raju Dhole, Kiruba Sankaran Subramani, Aria Nosratinia, Yiorgos Makris</i>	
The Glitch for Majorities: Breaking Spatial Redundancy Countermeasures	416
Synthesis of RTL-Based Characterization Programs for Fault Injection	427
<i>Jonah Alle Monne, Guillaume Bouffard, Damien Couroussé, Mathieu Jan</i>	
Logic Infusion: Exploiting Topology as a Power Side-Channel Countermeasure in FPGA-Based AES	438
<i>Kazi Mejbaul Islam, Emmanuel Elias, Debayan Das, Baibhab Chatterjee, Sandip Ray</i>	