

2025 IEEE Physical Assurance and Inspection of Electronics (PAINE 2025)

**Denver, Colorado, USA
14-16 October 2025**

IEEE Catalog Number: CFP25S83-POD
ISBN: 979-8-3315-6788-0



Copyright © 2025, 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:	CFP25S83-POD
ISBN (Print-On-Demand):	979-8-3315-6788-0
ISBN (Online):	979-8-3315-6787-3

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

TABLE OF CONTENTS

Enabling Algorithm Detection in the Presence of Interrupts: Using HAL for Side-Channel Interrupt Detection and Mitigation	1
<i>Kevin Pintong, Douglas Summerville</i>	
Machine Learning for Counterfeit Chip Detection in Edge Devices	8
<i>Pavani Manchala, Seungyeon Paik</i>	
A Defense Electronics Supply Chain Root Cause Analysis-Based Model to Identify Data Features that are Viable for Counterfeit Predictive Analytics	14
<i>Konstantinos Belesis</i>	
FirmEM: Firmware Flashing Detection via Unintentional Electromagnetic Emissions	21
<i>Elvan M. Ugurlu, Baki B. Yilmaz, Angelos D. Keromytis</i>	
X-Ray Fault Injection Localization with a Shield on Powered and Unpowered Devices	28
<i>P. Grandamme, S. Anceau, N. Bochard, L. Salvo, L. Bossuet, J.M. Dutertre</i>	
Precision Strike: Targeted Misclassification of Accelerated CNNs with a Single Clock Glitch	35
<i>Arsalan Ali Malik, Furkan Aydin, Aydin Aysu</i>	
Analysis of Temperature Effect on SRAM PUF for Low Cost Applications	42
<i>Sayan Samanta, Biswajit Ray, Aleksandar Milenkovic</i>	
AuthEM: Authenticating and Monitoring ECUs Through Electromagnetic Signatures	49
<i>Baki B. Yilmaz, Zahir Khan, Elvan M. Ugurlu, Donald Greene, Angelos D. Keromytis</i>	
Combined Trace Neural Network for Improved Design Extraction in Integrated Circuit Post-Silicon Verification and Validation Workflows	56
<i>Emily Haines, Preston Pozderac, J. Timothy Balint, Yash Patel, Ryan Mattei, James Schaffranek Adam R. Waite, Tamara Juntiff, Matt Sale, Adam Kimura</i>	
PUF-Based Tamper Protection for Global Satellite Navigation	62
<i>Valentin Huber, Alexander Sedlmaier, Alaa Abdellah, Fabian Benschuh, Alexander Rügamer Matthias Hiller</i>	
Integrated-Circuit Supply Chain Verification Using Mask Set Comparison in the Open Source Context	69
<i>Olivier Thomas, Florent Gomez, Julien Barbate, Clarisse Ginet, Stephane Gauri</i>	
PINCLASS: Pinhole-Centric Counterfeit Classification of IC Packages	75
<i>Md Shah Imran Shovon, Shajib Ghosh, Patrick J Craig, Chih-Yun Pai, Chien-Chia Huang Navid Asadizanjani</i>	
Anomaly-Based Hardware Trojan Detection in PCB Supply Chains Using One-Class SVM Analysis of Capacitance Sensor Data	82
<i>Rikuo Haga, Shugo Kaji, Daisuke Fujimoto, Yuichi Hayashi</i>	
Toward In-House 3D Nanoscale X-Ray Tomography of Integrated Circuits for Quality Control and Hardware Security at Speed of Need	88
<i>Jordan Fonseca, Nathan Nakamura, Paul Szypryt, Joseph W. Fowler, Zachary H. Levine, Andras E. Vladar John Henry Scott, Felix H. Kim, Daniel S. Swetz</i>	

Smart Automated Optical Inspection of PCBs	95
<i>Pratham Parlecha, Soma Biswas, Gayathry S V, T V Prabhakar</i>	
Magnetic Field Imaging Using Diamond Nitrogen-Vacancy Centers for Fault Detection and Security of Semiconductor and Superconductor Electronics	102
<i>Pauli Kehayias, Rohan T. Kapur, Michael Gold, Jennifer M. Schloss, Danielle A. Braje</i>	
Towards Improving Side-Channel Analysis in FPGAs Using the Hardware Response	107
<i>Meghana Jain, Douglas Summerville</i>	
Power Spectrum Analysis-Based Counterfeit Screening: A Hardware Comparison	114
<i>Devon R. Richman, Connor P. Dempsey, Steven J. Dourmaskin, Michael H. Azarian, Diganta Das</i>	
Survey on Counterfeit and Malicious Design Alterations to Integrated Circuits	119
<i>William Oswald, George Clark, J. Todd McDonald</i>	
AuthenTree: A Scalable MPC-Based Distributed Trust Architecture for Chiplet-Based Heterogeneous Systems	126
<i>Ishraq Tashdid, Tasnuva Farheen, Sazadur Rahman</i>	
RADPIC: A Radiation-Aware Design-Space Exploration and Simulation Framework for SOI-Based Photonic Integrated Circuits	133
<i>Kevin Mienta, Biswajit Ray, Mahdi Nikdast</i>	
Project Foxtrot: Abstracting the Complexity of Bitstream Reverse Engineering Through ML	140
<i>Alexandre Proulx, Tarek Ould-Bachir, Nora Boulahia-Cuppens, Frédéric Cuppens</i>	
Evaluating Multimodal Foundation Models for Few-Shot PCB Identification and Reasoning	148
<i>Zachary Burns, Gregorios Katsios, Samuel Merten</i>	
Efficient Side-Channel Leakage Assessment Using Deep Learning-Based Feature Extractor and ANOVA	155
<i>Yuta Fukuda, Kota Yoshida, Yohei Hori, Takeshi Fujino</i>	
Metaheuristic Color Scheme Strategies for Enhanced Visual Inspection of 3D IC Layouts	161
<i>Jie Zhang, Zhansen Shi, Hanchen Wang, Zhuoyang Zhang, Lucas Lum, Quanhao Gan, Shaoyu Cai</i> <i>Eng Tat Khoo, Yeow Kheng Lim</i>	
Post-Silicon Functional Verification and Validation: Chip to RTL Analysis	170
<i>Tim McDonley, Josh Delozier, Noah Taylor, Tamara Juntiff, Christian Eakins, Adam Kimura</i>	
Analyzing Sources of Fingerprints in Wireless Modules Using Microwave Measurements	176
<i>Vishnuvardhan V. Iyer, Jacob D. Rezac, James C. Booth</i>	
A Quantitative Means for Assessing Failure in SnBi-Based Solder Joints During Current Stressing	182
<i>Sitaram Panta, Javier Flores, Silas Wieland, Babak Arfaei, Anola Semndili, Frances Holcomb, Eric Cotts</i>	
Implementation of Machine Learning-Based Dynamic Logic Locking	188
<i>Nahush Tambe, Naseeruddin Lodge, Vineet Chadavalada, Fareena Saqib</i>	
Counterfeit IC Detection via Federated Learning: Exposure to Byzantine Data Poisoning	195
<i>Naseeruddin Lodge, Nahush Tambe, Dhruva Aklekar, Fareena Saqib</i>	
Timing-Based Side-Channel Attack on DDR4 Memory in FPGA Cloud Environments	202
<i>Vineet Chadavalada, Naseeruddin Lodge, Dhruva Aklekar, Fareena Saqib</i>	

Lurking in the Shadows: Challenges for X-Ray Inspection to Uncover Electromigration-Based Hardware Trojans in Advanced Packaging	209
<i>Katayoon Yahyaei, Susann Rothe, Mahmood Vawoo Dawood Naina, Antika Roy, M. Shafkat M. Khan Ozgur Sinanoglu, Jens Lienig, Johann Knechtel, Navid Asadizanjani</i>	
Trust Anchor to Mitigate a Physical-Material-Based Denial-of-Service Attack on Electronics Hardware Post-Manufacturing	216
<i>Jared Ott, Carlos Moreno, Michael Mayer, Sebastian Fischmeister</i>	
DeepAttack: X-Deep Side-Channel Attacks on Encryption Algorithm	223
<i>Nouf Nur Nabilah, Sartaj Jamal Chowdhury, Ahmed Oun, Akshay Raghavendra Kulkarni Annamalai Annamalai</i>	
Multi-Granular Information Flow Tracking in RISC-V Based SoCs	230
<i>Dhruvakumar Aklekar, Vineet Chadalavada, Nahush Tambe, Fareena Saqib</i>	
Advancing Microelectronics Evidence-Based Assurance While Preserving Confidentiality: Copia	237
<i>Nikhil S. Shenoy, Nicholas Pattengale, Nathan J. Edwards, Kelly E. Glebus, Cameron Patterson Evan M. Lally, Tyler E. Olson</i>	
Magnetic Field-Driven Physically Unclonable Function in 40nm p-MTJ STT-MRAM	246
<i>Md Sojib Ahmed, Biswajit Ray</i>	
Exploiting Electron-Beam Probing for Information Leakage in Advanced-Node Integrated Circuits	252
<i>M Shafkat M Khan, Liton Kumar Biswas, Istiaq Firoz Shiam, Neel Leslie, Jeffrey Block</i>	
Addressing STEM Specimen Preparation Challenges in Advanced-Node FinFET Devices	258
<i>Matthew Cheng, Abinash Kumar, Stephen Schwarz, Ed Perko, Henry Williams, Brenda Prenitzer</i>	