

# **2024 IEEE Physical Assurance and Inspection of Electronics (PAINE 2024)**

**Huntsville, Alabama, USA  
12-14 November 2024**



**IEEE Catalog Number: CFP24S83-POD  
ISBN: 979-8-3315-4226-9**

**Copyright © 2024 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:	CFP24S83-POD
ISBN (Print-On-Demand):	979-8-3315-4226-9
ISBN (Online):	979-8-3315-4225-2

**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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

## Table of Contents

Fault-Injection Countermeasures, Deployed at Scale .....	1
<i>Daniel Nemiroff and Carlos Tokunaga</i>	
Towards reducing costs of side channel analysis for real time algorithm detection .....	8
<i>Kevin Pintong and Douglas Summerville</i>	
3D Interconnect Inspection for Chiplet Packaging using White-light Scanning and Phase-Shifting Interferometry .....	15
<i>Shahab Chitchian, Seyong Song, Hyejin Song, Hyunmin Lee, Mingu Kang and Sangyoon Lee</i>	
Improving Workforce Development with Laboratory Automation .....	19
<i>Edward Carlisle, Scott Harper and Jonathan Graf</i>	
Overview of PUFs and Emerging Chaotic Structures .....	24
<i>David Tindall, Aubrey Beal and Tommy Morris</i>	
Dendritic Identifiers as Oracles in Microelectronics .....	31
<i>Michael Kozicki</i>	
Success Thresholds for Power Analysis Attacks Across Multiple Data Encryption Standard (DES) Implementations on a Microcontroller .....	38
<i>David Ingalls, Barrett Tieman and Andrew Lukefahr</i>	
Applying a Trusted Microelectronics Post-Silicon Verification & Validation Workflow to Legacy Integrated Circuit Design Recovery .....	45
<i>Jon Scholl, Noah Padro, Yash Patel, Tim McDonley, Adam R. Waite, John Kelley, Christian Eakins, Tamara Juntiff and Adam Kimura</i>	
Assuring the Cybersecurity of COTS Processors in Space Systems .....	52
<i>Jeffery Lim, Allan Nesathurai, Benjamin Nahill, Michael Vai, Rick Skowrya, Keith Bergevin and Pawan Gogna</i>	
Cover to Uncover: Comprehensive Study of Occlusion in DL-based SCA .....	58
<i>Emanuele Strieder and Benjamin Pfanz</i>	
Adversarial Attack Against Golden Reference-Free Hardware Trojan Detection Approach ..	65
<i>Ashutosh Ghimire, Mohammed Alkurdi, Karma Gurung and Fathi Amsaad</i>	
Enhancing Product Assurance and Reliability through a Machine Learning-Based Data Analysis System .....	72
<i>Dohun Kim and Wonjong Kim</i>	
Reverse-Engineering and Data Extraction from SRAM using Photon Emission Analysis...	79
<i>Rodrigo Silva Lima, Raphael Viera, Jean-Max Dutertre, William Magrini, Matthieu Pommies and Anthony Bertrand</i>	
In-Situ FPGA Fault Injection with Short-Circuits .....	86
<i>Garren Dutto, Daniil Lytkov and Vincent Immler</i>	
Pre-Silicon Side-Channel Analysis of AI/ML Systems .....	93
<i>Furkan Aydin, Emre Karabulut and Aydin Aysu</i>	

Securing Silicon Photonics Supply Chain Threats and Opportunities.....	100
<i>Liton Kumar Biswas, Rouhan Noor, Nitin Varshney, Hamed Dalir, Rayhane Ghane-Motlagh, Johnnie A Greene, Bahareh Ghane-Motlagh and Navid Asadizanjani</i>	
Evaluation of Terahertz Time Domain Spectroscopy for Uncovering Dosimetric Properties of Microelectronic Materials.....	107
<i>Daniel Heligman, Tyler Thompson, Rajind Mendis and Christine Wang</i>	
ChiPICA: Chiplet Physical Inspection Certification Authority for Trust Verification in Heterogeneous Integration.....	113
<i>Mohammad Bin Monjil, Jingbo Zhou, Nitin Varshney, Navid Asadi Zanjani, Farimah Farahmandi and Mark Tehranipoor</i>	
Better security requirements for physically unclonable functions .....	120
<i>Nick Egbert, Jon Mellott and Dan Toohey</i>	
Physical Layout Extraction via Ion Milling based IC Delaying for Reverse Engineering Applications .....	125
<i>Shuvodip Maitra, Tishya Sarma Sarkar, Abhishek Chakraborty and Debdeep Mukhopadhyay</i>	
Third-Party IP Verification and Validation for Post-Silicon Recovered Designs .....	134
<i>Joshua Delozier, Noah Taylor, Tim McDonley, Katie Liszewski, Richard Ott, Matt Sale and Adam Kimura</i>	
Vision Transformers for Counterfeit IC Detection.....	142
<i>Chaitanya Bhure, Dhruvakumar Aklekar, Wenjie Che and Fareena Saqib</i>	
Broadening the Semiconductor Talent Pipeline with Non-Engineering Students .....	149
<i>George Clark, Jeffery McDonald and Todd Anel</i>	
Expert Knowledge based Segmentation Algorithm for IC Layout SEM Images .....	156
<i>Bernhard Lippmann, Johannes Mutter and Georg Sigl</i>	
A Quantitative Framework for Assessing and Enhancing Hardware Security Resilience ....	163
<i>Arvind Sharma and Shao-Fang Wen</i>	
Physical Security Assessment of Advanced Packaging Structures.....	170
<i>Liton Kumar Biswas, Nitin Varshney, Rouhan Noor, Shajib Ghosh, Yashan Peng, Jiaqi Tang and Navid Asadizanjani</i>	
Using Near-Field Electromagnetic Side Channels for Efficiently Fingerprinting Wireless Modules .....	177
<i>Vishnuvardhan Iyer, Jacob Rezac and James Booth</i>	
Evaluating the Efficacy of the ResCav System in Distinguishing Integrated Circuits Across Manufacturers, Series, and Lots.....	183
<i>Aditya Nechiyil, Robert Lee and Gregg Chapman</i>	
Isolation Forest Based TinyML for Detecting Hardware Trojans on FPGA in Real Time ..	190
<i>Mani Rupak Gurram, Mithun Kumar Pk and Fathi Amsaad</i>	

SPICED: Syntactical Bug and Trojan Pattern Identification in A/MS Circuits using LLM-Enhanced Detection .....	195
<i>Jayeeta Chaudhuri, Dhruv Thapar, Arjun Chaudhuri, Farshad Firouzi and Krishnendu Chakrabarty</i>	
Assessing Magnetic Attack on Commercial 40nm pMTJ STT-MRAM.....	202
<i>M. Sojib Ahmed and Biswajit Ray</i>	
Case Study: Fault-Injection Vulnerability Assessment at RTL Level .....	208
<i>Azim Uddin, Sujan Kumar Saha, Farimah Farahmandi and Mark Tehranipoor</i>	
Mechanical Sample Preparation for Heterogeneous Integration(HI) Packaging.....	215
<i>Chengjie Xi, M Shafkat M Khan, Nitin Varshney, Aslam A Khan, Chris Richardson and Navid Asadizanjani</i>	
Architecting the Quantum Future: Key Devices and Layers in Quantum Network Design .	223
<i>Mansoor Ali Khan, Muhammad Naveed Aman and Biplab Sikdar</i>	
CAKE-SiP: Chiplet Authenticate & Key Exchange for Secure Provisioning in System-in-Package .....	230
<i>Md Sami Ul Islam Sami, M Shafkat M Khan, Farimah Farahmandi, Navid Asadizanjani and Mark Tehranipoor</i>	
Data Remanence Vulnerabilities in Commercial SRAM at Low Temperature.....	238
<i>Farzana Hoque, Izak Halseide, Aleksandar Milenkovic and Biswajit Ray</i>	
United We Protect: Protecting IP Confidentiality with Integrated Transformation and Redaction.....	245
<i>Md Moshir Rahman, Rasheed Almajzan, Aritra Dasgupta, Sudipta Paria and Swarup Bhunia</i>	
Feature Analysis and Model Evaluation for Classification of Hardware Trojans.....	252
<i>Niraj Parsad Bhatta, Sufian Al Majmaie and Fathi Amsaad</i>	