2023 IEEE Physical Assurance and Inspection of Electronics (PAINE 2023)

Huntsville, Alabama, USA
24-26 October 2023

IEEE Catalog Number: CFP23S83-POD
ISBN: 979-8-3503-3932-1

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:	CFP23S83-POD
ISBN (Print-On-Demand):	979-8-3503-3932-1
ISBN (Online):	979-8-3503-3931-4

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

Exploiting Hardware Imperfections for GPS Spoofing Detection using Clock Variations . . . 1
Mirza Athar Baig and Muhammad Aman

Attest: Non-Destructive Identification of Counterfeit FPGA Devices . . . 8
Whitney Batchelor, James Koiner, Cody Crofford, Kevin Paar, Margaret Winslow, Mia Taylor and Scott Harper

Aging of SRAM PUFs: Mitigation and Advancements through Machine Learning Techniques . . . 13
Niraj Prasad Bhatta, Harshdeep Singh, Ashutosh Ghimire, Md Tauhidur Rahman and Fathi Amsaad

PQC Cloudization: Rapid Prototyping of Scalable NTT/INTT Architecture to Accelerate Kyber . . . 19
Mojtaba Bisheh-Niasar, Daniel Lo, Anjana Parthasarathy, Blake Pelton, Bharat Pillilli and Bryan Kelly

IPRec and Isoblaze: Fuzzy Subcircuit Isomorphism for IP Detection in Physical Netlists . . 26
Dallin Dahl, Corey Simpson, Keenan Faulkner, Brent Nelson and Jeffrey Goeders

Exploring Security of Embedded SRAM in PIC and RISC-V Chips: Insights from Image Processing of Low-Cost Photon Emission Microscopy . . . 33
Bahareh Ebrahimi Sadrabadi and Catherine Gebotys

Rectification for Computed Tomography Scans of Printed Circuit Boards Using Vias as Landmarks . . . 40
Alexander Fafard Ph.D.

Cycle-to-Cycle Variation Suppression in ReRAM-Based AI Accelerators . . . 47
Jingyan Fu, Zhiheng Liao and Jinhui Wang

Identification and Localization of Quantum Electromagnetic Fields of Hardware Trojan Attacks using QDM-based Unsupervised Deep Learning . . . 53
Ashutosh Ghimire, Al Amin Hossain, Niraj Prasad Bhatta and Fathi Amsaad

Potential of Unsupervised Deep Learning for Detection of EM Side-Channel Attacks . . . 60
Ashutosh Ghimire, Harshdeep Singh, Niraj Prasad Bhatta and Fathi Amsaad

DeepICLogo: A Novel Benchmark Dataset for Deep Learning-Based IC Logo Detection . . . 66
Shajib Ghosh, Patrick Craig, Jake Julia, Nitin Varshney, Hamed Dalir and Navid Asadizanjani

X-Ray Fault Injection in non-volatile memories on Power OFF devices . . . 74
Paul Grandamme, Lilian Bossuet and Jean-Max Dutertre

A sense of self for power side-channel signatures: Time-series Side-channel Disassembler (TSD) and Integrity Monitor (TSD-IM) . . . 81
Random Gwinn

SHI-Lock: Enabling Co-Obfuscation for Secure Heterogeneous Integration against RE and Cloning 88
Md Saad Ul Haque, Rui Guo, Mohammad Sazadur Rahman, Hadi Mardani Kamali, Farimah Farahmandi and Mark Tehranipoor

IED_PUF Probe: A PUF-based Hardware Fingerprint Extraction Equipment for IEDs 95
Vishal Jadhav, Narahari N. Moudhgalya, Tapabrata Sen and T. V. Prabhakar

Simulation-Based Approach to Generating Golden Data for PCB-Level Hardware Trojan Detection Using Capacitive Sensor 102
Shugo Kaji, Daisuke Fujimoto and Yuichi Hayashi

RI-SAR: Randomized Input SAR ADC Resilient to Power Side Channel Attacks 109
Sumanth N Karanth, Sirish Oruganti, Meizhi Wang and Jaydeep P Kulkarni

CMX-Ray: An X-ray Compatibility Metric for Advanced Packages to facilitate Design-for-Inspection 116
M Shafkat M Khan, Chengjie Xi, Nitin Varshney, Aslam A Khan, Antonio Serna, Hamed Dalir, Volker Sorger and Navid Asadizanjani

Towards a Comprehensive System for Physical Hardware Inspection for Trust 123
Bernhard Lippmann, Matthias Ludwig, Detlef Houdeau, Horst Gieser and Nicola Kovac

Microstructural Investigation and Serial Section Tomography on ASIC chips for Assurance through Reverse Engineering Applications 130
Shuvodip Maitra, Abhishek Chakraborty and Debdeep Mukhopadhyay

PALLET: Protecting Analog Devices using a Last-Level Edit Technique 138
Md Rafid Muttaki, Hadi Mardani Kamali, Mark Tehranipoor and Farimah Farahmandi

Nanoscale X-ray Tomography of Integrated Circuits using a Hybrid Electron/X-ray Microscope: Results and Prospects 145
Nathan Nakamura, Paul Szypryt, Joseph W Fowler, Zachary H Levine and Daniel S Swetz

An Assessment of Sample Preparation Challenges in 3D Stacked Integrated Circuit Devices for Post-Silicon Verification and Validation 152
Noah Padro, Yash Patel, Jon Scholl, John Kelley, Adam R. Waite, Matt Sale and Adam Kimura

Experimental Characterization of Two-Photon Optical Beam Induced Current Imaging for Microelectronics Assurance 159
Ryan Patton, Anthony George, Adam Kimura and Jamin McCue

Investigating the Effect of Electromagnetic Fault Injections on the Configuration Memory of SRAM-based FPGA Devices 164
Alexandre Proulx, Jacob Thibodeau, Bastien Bourgault, Jean-Yves Chouinard, Amine Miled and Paul Fortier

PLaNe: Reverse Engineering of Planar Layouts to Gate-Level Netlists 171
Maximilian Putz, Matthias Ludwig, Bernhard Lippmann and Helmut Graeb

Robust Measurements for RF Fingerprinting with Constellation Patterns of Radiated Waveforms . . . 178
Améya Ramadurgakar, Jacob Rezac, Lennart Heijnen, Kate Remley, Dylan Williams, Melinda Piket-May and Robert Horansky

Non-Destructive Hardware Trojan Circuit Screening by Backside Near Infrared Imaging . . 184
Junichi Sakamoto, Hirofumi Sakane, Yohei Hori, Shinichi Kawamura, Yuichi Hayashi and Makoto Nagata

Evaluating the Robustness of SRAM Physical Unclonable Functions: Empirical Investigations . . . 191
Harshdeep Singh, Niraj Prasad Bhatta, K M Tawsik Jawad, Ashutosh Ghimire, Md Tauhidur Rahman and Fathi Amsaad

MicroBitstreams: Reducing Configuration Time of Encrypted Bitstreams . . . 198
Christopher Sozio, Grant Skipper, Daniel Hansen, Andrew Lukefahr and Adam Duncan

MeLPUF: Memory-in-Logic PUF Structures for Low-Overhead IC Authentication . . . 205
Christopher Vega, Patanjali Slpsk, Shubhra Deb Paul, Atri Chatterjee and Swarup Bhunia

A Modular Blockchain Framework for Enabling Supply Chain Provenance . . . 212
Yadi Zhong, Amaar Ebrahim, Ujjwal Guin and Vivek Menon