2020 IEEE Physical Assurance and Inspection of Electronics (PAINE 2020)

Virtual Event
15 – 16 December 2020

IEEE Catalog Number: CFP20S83-POD
ISBN: 978-1-7281-6122-8

****** 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: CFP20S83-POD
ISBN (Print-On-Demand): 978-1-7281-6122-8
ISBN (Online): 978-1-7281-6121-1

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

PAINE 2020 Program (All Times are in EST)

Day 1 (December 15, 2020)

08:45 - 09:00

Opening Remarks

General Chair and Program Chair

Plenary Session

09:00 - 09:30

Keynote Talk I: Attack and Parry – What Chance Do the White Hats have in a World Full of

Black Hats?

Mike Borza – Synopsys Inc.

09:30 - 09:40

Break

SESSION I: Supply Chain Security

09:40 - 10:00

Assurance – From Integrated Circuits to Printed Circuit Boards.....N/A

Dr. Richard Ott – Air Force Research Lab

10:00 - 10:20

Replicating a Nation-State-Style Chipping Attack on Cisco Firewalls.....N/A

Monta Elkins – Foxguard Solutions/Sans Institute

10:20 - 10:40

Practical Design and Implementation of Zero-Trust Supply Chain for Electronic Products.....N/A

Phil Vachon and Joel Even – Bloomberg

10:40 - 11:00

The Secret Life of Supply Chains – Security at Hardware Level.....N/A

Sophia d'Antoine – Margin Research

11:00 - 11:10

Break

SESSION II: PCB Assurance

11:10 - 11:30

Electronic Component Solderability Assessment Algorithm by Deep External Visual Inspection.....1

Dr. Eyal Weiss – Cybord Inc.

11:30 - 11:50

Techniques to Thwart Surreptitiously Altered PCBs.....7

Dr. Samuel Russ – University of South Alabama

11:50 - 12:10

SHADE: Automated Refinement of PCB Component Estimates Using Detected Shadows.....11

Nathan Jessurun – University of Florida

12:10 - 13:10

Lunch and Learn – 12:10 – 13:10

Live Demo (Cyberoptics): 12:40 – 13:10

13:10 - 13:40

Keynote Talk II: “Intrinsic and Extrinsic Process Modalities for IC Security”

Ezra hall, GlobalFoundaries

13:40 - 13:50

Break

SESSION III: Panel Discussion

13:50 - 14:50

Package Security

Panelists: Dr. John Allgair (BRIDG), David Kehlet (Intel), Wes Hansford (Boeing Research & Technology),

and Dr. Norman Chang (Ansys)

Moderator: Dr. Waleed Khalil, Ohio State University

14:50 - 15:00

Break

SESSION IV: Side-Channel Attacks

15:00 - 15:20

Toward an RF Side-Channel Reverse-Engineering Tool.....17

Dr. Stergios Papadakis – Johns Hopkins University

15:20 - 15:40

Strengthening Side-Channel Attacks: Combined Distinguishers using Preprocessing Techniques.....N/A

Dr. Selçuk Köse – University of Rochester

15:40 - 16:00

Detection and Prevention of Power Side-Channel Attack.....N/A

Dr. Swaroop Ghosh – Penn State University

16:00 - 16:20

Reverse Engineering Neural Networks through Physical Side-Channels.....N/A

Dr. Aydin Aysu – NC State University

16:20 - 16:40

Compromising Devices Security via NVM Controller Vulnerability.....23

Dr. Sergei Skorobogatov – University of Cambridge

Closing Day 1

Day 2 (December 16, 2020)

09:00 - 09:30

Keynote Talk III: “Fast, 100% 3D Wafer Bump Metrology and Inspection to Improve Yields and

3D System Integration”

Timothy Skunes, CyberOptics

09:30 - 09:40

Break

SESSION V: IC Assurance

09:40 - 10:00

Trust and Assurance Challenges for Heterogeneous Integration and Packaging Technologies.....N/A

Dr. John Allgair – BRIDG

10:00 - 10:20

Decoding & Defending the Trusted Platform Module Against Malicious Hardware Implants.....N/A

Suehayla (Sue) Mohieldin – River Loop Security

10:20 - 10:40

From Silicon to Simulation: A Full End-to-End Decomposition of a Fabricated 130 nm Serial Peripheral Interface for Establishing a Hardware Assurance Baseline Root-of-Trust.....29

Dr. Adam Kimura, Battelle

10:40 - 11:00

Automated Detection and Localization of Counterfeit Chip Defects by Texture Analysis in Infrared (IR) Domain.....35

Pallabi Ghosh – University of Florida

11:00 - 11:20

Tracking Cloned Electronic Components using a Consortium-Based Blockchain Infrastructure.....41

Jason Vosatka – University of Florida

11:20 - 11:30

Break

SESSION VI: SoC Protection and Vulnerabilities

11:30 - 11:50

Security along SoC Design Lifecycle: Current Practices and Challenges Ahead.....N/A

Dr. Magdy Abadir – Caspia Technologies

11:50 - 12:10

ReCon: From the Bitstream to Piracy Detection.....47

Grant Skipper – Indiana University

12:10 - 12:30

SPARTA-COTS: A Laser Probing Approach for Sequential Trojan Detection in COTS Integrated Circuits.....53

Andrew Stern – University of Florida

12:30 - 13:30

Lunch/Sponsor Showcase

13:30 - 14:00

Keynote Talk IV: “Machine Learning for Circuit Extraction Based on IC Images”

Dr. Bah-Hwee Gwee – Nanyang Technological University, Singapore

14:00 - 14:10

Break

SESSION VII: Advanced Imaging and Sample Preparation

14:10 - 14:30

Sample Mounting Methods for Precision Delayering of 130 nm Integrated Circuit Devices.....59

Jon Scholl – Battelle

14:30 - 14:50

New Physical Analysis Capability for Counterfeit Electronics and Reverse Engineering.....64

Gregory M. Johnson – Zeiss

14:50 - 15:10

Semi-Supervised Automated Layer Identification of X-ray Tomography Imaged PCBs.....69

Ulbert Botero – University of Florida

15:10 - 15:20

Break

SESSION VIII: IP Protection

15:20 - 15:40

ATPG-Guided Fault Injection Attacks on Logic Locking.....75

Dr. Ujjwal Guin – Auburn University

15:40 - 16:00

Challenges and Opportunities in Physical Attacks on Logic Locking.....N/A