Mark M. Tehranipoor

IEEE/ACM Fellow
Intel Charles E. Young Preeminence Endowed Chair Professor in Cybersecurity
Chair, Department of Electrical and Computer Engineering, University of Florida
Program Director of Cybersecurity at UF; Director, Florida Institute for Cybersecurity (FICS) Research; Co-director, AFOSR/AFRL Center of Excellence on Enabling Cyber Defense in Analog and Mixed Signal Domain (CYAN); Co-Director, National Microelectronic Security Training Center (MEST); Director, Edaptive Computing Inc. Transition Center (ECI-TC); President and CTO, Caspia Technologies

Office: 352-392-2585, **Mobile**: 860-942-4047
FICS Research: http://fics.institute.ufl.edu/, Personal: https://tehranipoor.ece.ufl.edu/
Email: tehranipoor@ece.ufl.edu, Gmail: tehranipoormark@gmail.com

Research Interests

Hardware and Cyber Security, IoT Security, Supply Chain Security, Counterfeit Electronics Detection and Prevention, Reliable Circuit Design and Analysis, and Integrated Circuits and Systems Testing

Non-academic Appointments

2/20-present President and CTO, Caspia Technologies, http://caspiatechnologies.com/

Academic Appointments

05/22-present Chair, Department of Electrical and Computer Engineering, University of Florida

06/20-09/21 Co-director, Center for Aerospace Resilience (CAR)

04/20-present Founding Director, Edaptive Computing Inc Transition Center (ECI-TC)
URL: https://ecitc.org/

07/19-05/22 Program Director of Cybersecurity Program at the University of Florida

07/17-7/2019 Associate Chair for Research and Strategic Initiatives (ACR), ECE Department, University of Florida

05/19-present Co-director, AFOSR/AFRL Center of Excellence on Enabling Cyber Defense in Analog and Mixed Signal Domain (CYAN)

008/19-08/22 Term Professorship

01/19-present Affiliate Professor and Executive Committee Members, SECURE center, Prairie View A&M University

07/15-Present Intel Charles E. Young Preeminence Endowed Chair Professor in Cybersecurity, University of Florida

07/15-Present Founding Director, Florida Institute in Cybersecurity (FICS) Research
URL: http://fics.institute.ufl.edu/

11/13-07/15 Professor, University of Connecticut

12/11-07/15 Founding Director, Center for Hardware Assurance, Security and Engineering (CHASE), University of Connecticut

06/12-07/17 Founding Director, Comcast Center of Excellence on Security Innovation (CSI), Sponsored by Comcast, University of Connecticut

11/12-08/13 Charles H. Knapp Associate Professor in Elecrical Engineering, University of Connecticut

04/12-11/12 F.L. Castleman Associate Professor in Engineering Innovation, University of Connecticut

08/10-08/13 Associate Professor, Electrical and Computer Department, University of Connecticut

08/06-08/10 Assistant Professor, Electrical and Computer Department, University of Connecticut

08/08-08/11 Term member of Graduate Faculty, Duke University

08/04-08/06 Assistant Professor, Department of Computer Science and Electrical Engineering (CSEE), University of Maryland Baltimore County (UMBC)

Major Initiatives and Accomplishments (2004-2022)

Oct. 2021 Estabished a workshop between UF and USF to enable more collaboration between researchers in the field of cybersecurity.

April 2021 FICS TDC 2021: A virtual conference was established to enable demonstration of the technologies developed in FICS to the sponsors

Sept 2020 Established CAR, Center for Aerorespace Resilience, in collaboration with Embry-Riddle Aeronautical University (ERAU) sponsored by FL DOE, and serves in collaboration with Dr. Remzi Seker of ERAU. $1.75M (no indirect)

August 2020 Ranked #3 in the entire University of Florida funding in 2019-2020 fiscal year with almost $15M. The top two faculty were from Medical Schools. Note the total funding of UF in 2019-2020 fiscal year was $900M.

July 2020 Established the first **certificate on Hardware Security offered through MEST Center**. This certificate includes none hours of presentation on nine topics in the domain of hardware security.

May 2020 Teamed up with Synopsys (Prime) to successfully compete on **DARPA Automated Implementation of Secure Silicon (AISS) BAA**. Synopsys was awarded $48M, of which FICS will receive $8M. Other team members include Boeing, ARM, UC San Diego, Purdue University, and Texas A&M.

April 2020 Established ***Edaptive Computing Inc. Transition Center (ECI-TC), $15M+***, This unique partnership between the University of Florida (UF) and Edaptive Computing has two main goals. Firstly, the proposed center will continue the groundbreaking work taking place in FICS Research—using automation, computer vision, and machine learning to test and verify the designs of microelectronics in all phases of the lifecycle. This work is fundamentally aimed at verifying that hardware (IoT devices, chips, circuit boards, systems) has been manufactured to the exact specifications of the designers, that the system does not suffer from any hardware related vulnerabilities, and that the designs themselves have not been compromised in any way. These efforts to ascertain the trustworthiness of devices entering the supply chain have become increasingly critical as more and more manufacturing has moved to East Asia, where oversight is less stringent. https://news.ece.ufl.edu/2020/04/29/15m-technology-transition-center-kicks-off-virtually/

July 2019 Founder, President, and CTO, Caspia Technologies, LLC. http://caspiatechnologies.com/

June 2019 Led the establishment of the National MicroElectronic Security Training (**MEST**) Center, Sponsored by Nimbis/AFRL (https://mestcenter.org/). This center mission is to establish collaboration between multiple universities, establishing an ecosystem of training modules and options to suit the need for diverse government and industry employees, place strong emphasis on hands-on learning, offer major courses and certificate programs, Provide comprehensive coverage of all security topics, Offering major courses and certificate programs, unique in the nation, and establish self-learning kits for hardware and systems security topic available for remote training and busy professionals.

May 2019 Led establishment of **AFOSR/AFRL Center of Excellence** on Enabling Cyber Defense in Analog and Mixed Signal Domain (**CYAN**). This center focuses on identifying opportunities in the analog and mixed signal doamin to establish end to end security for electronic devices and systems.

March 2019 Led the **2019 FICS Research Annual Conference on Cybersecurity** (https://fics.institute.ufl.edu/conference/). 180 people attended the conference from academia, industry, and government. The event was sponsored by 11 companies.

Nov. 2018 Co-authored the **first ever textbook** on Hardware Security, published by Morgan Kauffman

https://www.elsevier.com/books/hardware-security/bhunia/978-0-12-812477-2

Feb 2018 Led the **2018 FICS Research Annual Conference on Cybersecurity** (http://fics-institute.org/outreach/conference/). More than 230 people attended the conference from academia, industry, and government. The event was sponsored by 18 companies.

Aug 2017 Established a program to increase the number of awards and scholarships (NSF, SRC, IBM, etc.) among faculty and FICS Research students.

Aug 2017 Led establishing the Trusted and Assured MicroElectronics (**TAME**) Forum (http://www.tameforum.org/). TAME Forum's objective is to provide a bi-annual platform to researchers in academia, and practitioners in industry and government to discuss innovative solutions in the domain of trusted microelectronics in today's globalized and complex supply chain, discuss grand challenges and identify collaboration opportunities. One major outcome of the TAME Forum is expected to be the first ever "National Technology Roadmap for Trusted and Assured Microelectronics".

Dec. 2017 Co-founded IEEE PAINE (International Conference on Physical Attacks and Inspection of Electronic Systems). http://paine-conference.org/

Aug 2017 ACR: Established ECE **Faculty Mentoring Program**. This program is intended to build a strong foundation for the success of junior faculty (assistant and associate professors). Many new faculty have had little or no exposure to the different and new aspects of their profession, and desire an experienced voice to guide them in tailoring the initial stages of a successful career. It is critical to continually provide opportunities for career development through a strong voluntary mentor/mentee relationship. As a result, we established flexible career guidance and mentoring program to create a nurturing environment within the ECE department.

June 2017 **Proposal Writing and Review Process**: Instituted a CAREER/PECASE/YIP proposal writing review process internally for the ECE Department. Through this program, young faculty in the ECE department received NSF CAREER, YIP, and PECASE awards.

March 2017 Led the **2017 FICS Research Annual Conference on Cybersecurity** (http://fics-institute.org/outreach/conference/). More than 210 attended the conference from academia, industry, and government. The event was supported by 13 companies, more than 20 demos and 50 posters were presented, with many companies and government labs active in recruiting students for full time and summer intern positions.

Jan 2017 Helped establish **CyberGatorZ**, and currently secrving as the faculty advisor. CyberGatorZ is a fully student-run organization at the FICS Research Institute. CyberGratorZ group includes four major committees namely Incident Analysis and Reporting, IoT Hacking, Outreach and Diversity, and Professional Development. CyberGators mission is to advance the state of art in cybersecurity and increase students professional development by providing opportunities to communicate with experts from academia, industry, and government. CyberGatorZ are also active members of the K-12 initiative run by FICS Research.

Dec. 2016 Worked closely with the lead PI Prof. Bhunia on an **NSF Scholarship for Service (SFS)**. The accepted proposal, in collaboration with FIU, received $4.6M to recruit BS, MS and PhD students for a new program called *Hardware and Systems Security (HSS)* jointly developed at the UF ECE/CISE and FIU ECE department. The target program will be made available online through UF EDGE (online) program. The EDGE capability will allow FIU students to take the basic HSS classes and then continue with other cybersecurity courses in their respective departments. The program is available nation wide to all students from ECE, CSE, ME, BME, and other departments.

August 2016 Led establishment of **SCAN Lab under FICS Research Institute**. The lab includes $10M+ equipment with capabilities for physical inspection, imaging capabilities, attack assessment, electrical tests and measurement, bio-medical tests, thermal test, device characterization, etc.

April 2016 The topic of hardware security has seen major growth over the past decade or so. However, the community never enjoyed a dedicated journal on this topic, hence my colleague Prof. Bhunia and I took on this challenge and established the first ever journal supported by Springer called **Journal of Hardware and Systems Security (HASS),** http://www.editorialmanager.com/hass

April 2016 Helped establish **IEEE Symposium on Asian Hardware-Oriented Security and Trust (HOST)**. AsianHOST Symposium brings together experts from Asia, Europe and North America together to establish collaboration on topics related to Hardware Security. http://asianhost.org/

Feb 2016 **UF-TESCAN Partnership**: Led this effort to establish a partnership with one of the leading electron microscope companies in the world. This partnership is worth about $5M. The partnership includes significant donation, 5-year waranty, monthly meeting with TESCAN to develop strategies for collaboration and joint proposals to government and industry, student training, joint publications, etc. http://fics.institute.ufl.edu/facilities/

Feb 2016 Led the establishment of the **2016 FICS Annual Conference on Cybersecurity**. The goal of this conference was to put together a program consisting of experts from industry, government, and academia to discuss cybersecurity problems, engage with students via poster sessions and evalaution, project demos, panels, competitions, etc. The first year event brought togerther more than 155 experts on campus. The 2016 conference was sponsored by more than 12 companies. http://fics.institute.ufl.edu/conference/

July 2015 Founded the **Florida Institue for Cybersecurity (FICS) Research** to become a premier institute on cybersecurity that covers device to systems, human, mobile, network, software, and enterprise security. http://fics.institute.ufl.edu/ . Currenly serving as Director for FICS Research.

Nov. 2015 **CDC Tool** became part of **SAE international standard, AS6171**. The CDC project was sponsored in part by Honeywell, Comcast, and Missile Defense Agency (MDA). The tool is the first of its kind to evaluate the efficiency of test and inspection techniques for counterfeit and fake chips. *The tool was acquired by SAE International.*

April 2015 Initiated **Connecticut Cybersecurity Center (C3)** at the University of Connncticut. I led a proposal for a total of $1M+ funded by the State of Connecticut. The fund allowed for recruting two new faculty and a full time staff. https://ccc.engr.uconn.edu/

Nov 2014 Helped with the effort to establish a **Center of Excellence in Microscopy** at the University of Conencticut. This is a multi million dollar ($20M+) partnetship between UConn and FEI. http://today.uconn.edu/blog/2014/10/new-collaboration-to-create-world-class-microscopy-center/

Oct. 2014 Led establishment of **CyberSEED (Cybersecurity, Education, and Diversity Challenge Week)**. http://www.csi.uconn.edu/cybersecurity-week. CyberSEED, supported by more than a dozen companies, brought together students (undergraduate and graduate) from more than 45 schools and colleges around the nation to compete on many cybersecurity problems on campus at UConn. The students competed on capture the flag (CTF), software security, and hardware security.

May 2014 **Lead PI** for **MURI grant from DOD AFOSR**. The U.S. Department of Defense awarded a $7.5 million grant to the University of Connecticut, University of Maryland, and Rice University to support research that will analyze and upgrade security protections for nanoscale computer hardware. UCONN with 6 PIs is the lead institution and University of Maryland (2PIs) and Rice University (1 PI) are the other collaborators. http://news.engr.uconn.edu/muri-grant-to-improve-the-security-of-nanoscale-computer-devices.php. **This was the single largest grant brought to the University of Connecticut.**

2012-2015 Led establishment of **CHASE Consortium**: Established a consortium by bringing together several companies and agencies including Missile Defense Agency (MDA), Honeywell, Juniper, Comcast, and Semiconductor Research Corporation (SRC), UTAS, etc.

April 2014 **Founding Director for CSI Center at UConn:** In partnership with Comcast, I led the establishment of the **Center of Excellence in Security Innovation (CSI)**. The CSI was was established to lead research, teaching and workforce development in hardware, software, and network security and address Comcast's much needed security needs. CSI was established in April 2014 with main support from Comcast ($2M/year). http://www.csi.uconn.edu/

June 2012 Established the **Center for Hardware Assurance, Security, and Engineering (CHASE)**. The Center was established in 2012 to provide the University of Connecticut with a physical and intellectual environment necessary for interdisciplinary hardware-oriented research and applications to meet the challenges of the future in the field of assurance and security. CHASE is a research consortium with member companies from across the nation committed to enabling knowledge breakthroughs that shape future electronic systems. Current members include Honeywell, Comcast, Missile Defense Agency (MDA), and Juniper Networks. Other sponsors include Synokey, LSI, Qualcomm, Cisco, Samsung, Mangolia, R3Logic, Freescale, SRC, GRC, and more. https://www.chase.uconn.edu/

Feb. 2012 Established a series of **Workshops on Hardware and Systems Security at UConn**. The workshop grew quite fast that went from 60 participants in 2012 to 220 in 2014. We were able to bring together experts from academia, industry, and government to discuss the challenging problems of hardware and cyber security.

Feb 2011 Led establishment of **Trust-Hub** (www.trust-hub.org) funded by the National Science Foundation (NSF). Trust-Hub is a website where members of the IC hardware security community can share their discoveries and other information that accelerates hardware security research and developments. Trust-Hub serves as a clearing house and community-building tool where researchers can exchange papers, benchmarks, hardware platforms, source codes and tools.

Jan 2008 Led the establishmeant of the IEEE Workshop on **Hardware-Oriented Security and Trust (HOST)**, with Dr. Jim Plusquellic of UNM. In 2010, HOST became a symposium and is now the premier event on hardware security. HOST moved to Washington DC area in 2013 and grew to become an event with more than 350 attendees by 2017. http://www.hostsymposium.org/

2006-present Published the **first series of books on Hardware Security and Trust**. Two of the books is currently being used as text book in the domain of hardware security. http://tehranipoor.ece.ufl.edu/publications.html

Education

1/02 – 8/04 Ph.D, Electrical and Compueter Eng., University of Texas at Dallas, 2002-2004

9/97 – 8/00 M.Sc. Electrical Engineering, University of Tehran, 1997-2000

1/92 – 8/97 B.Sc. Electrical Engineering, Tehran Polytechnic University, 1992-1997

Project Sponsors

1. National Science Foundation (NSF)
2. Semiconductor Research Corporation (SRC)
3. Global Research Corporation (GRC)
4. National Institute of Standards and Technology (NIST)
5. Office of Naval Research (ONR)
6. Army Research Office (ARO)
7. Air Force Research Laboratory (AFRL)
8. Air Force Base Eglin
9. Missile Defense Agency (MDA)
10. GAANN, Department of Education
11. Defense Advanced Research Projects Agency (DARPA)
12. Air Force Office of Scientific Research (AFOSR) – MURI
13. KCP, Department of Energy (DOE)
14. AFOSR / DURIP
15. OSD/ONR SBIR
16. DRAPER
17. Raytheon
18. Tektronix
19. Texas Instruments
20. Cisco
21. Qualcomm
22. LSI Corporation
23. Freescale Semiconductor
24. MediaTek
25. Comcast
26. Honeywell
27. Juniper
28. BRIDG
29. Mentor Graphics
30. Intel
31. R3Logic
32. Synokey
33. UF Office of Research
34. CRI/Rambus Donation

35. Verigy, Inc. Donation
36. Xilinx Donation
37. Agilent Donation
38. EPSRC of United Kingdom
39. UConn Research Foundation
40. UMBC RAS/RIS
41. EYL Partners & Korean Institute for Information, Communication Technology Promotion (IITP)
42. Edaptive Computing Inc.
43. Bosch
44. Nimbis Services
45. Analog Devices (ADI)
46. DMEA
47. AFWERX
48. Dynetics
49. Battelle
50. Lockheed Martin
51. Synopsys
52. Department of Education (DOE), FL
53. Ansys
54. Arm
55. Meta (Facebook)
56. ***Small donations/Services:***
    - IBM
    - Intel
    - Raytheon
    - Draper
    - TESCAN
    - ZEISS
    - Thales E-security
    - Texas Instruments
    - Rambus
    - Mentor Graphics
    - NREL
    - Hammamatsu
    - Microphotonics

- Cisco
- Angstrom Scientific
- Cybraics
- Athena Groups
- Raith
- Bruker
- United Technology Research Center
- Microsemi
- Applied DNA Sciences
- Micronet Solutions
- PFP Technologies
- ARA
- Edaptive Computing
- Synopsys
- Onespin
- Battelle
- Arm
- Riscure

Research Supports and Donations (PI and Co-PI), $100M+

2022	Analog Devices, Security Enginer Assessment, $150K, Lead PI
2022	AFB Egin, Inter-layer PCB Impaging and Assurance, Lead PI, $330K
2022	Cisco, FPGA Bitstream Protection Against Optical Attacks, Co-PI, $200K
2021	Scanning Acoustic Microscope for Advanced Packaging Physical Assurance (SAPPA), $280K, ONR, Co-PI
2021	Facebook gift, $75K, co-PI
2021	Synopsys gift, $65K, PI
2021-2023	Extensible Secure SoC Architectures, SRC-Arm, $200K, Co-PI
2021-2024	SAIPA: Security Aware Interposer Design for Heterogeneous Packaging, ONR, $900K, Co-PI
2020-2021	Model-based PCB Attestation, KC-NSC, $150K, Co-PI
2021-2022	SHINE: Security Aware High-Level Synthesis, DARPA, $500K, Co-PI
2020-2021	TrustGuard: Trusted Embedded Systems using Power Side Channel Signal Analysis, ADI, $100K, gift, Co-PI
2020-2022	Fault Injection Assessment, ANSYS, Co-PI, $80K, gift
2020-2021	Center for Aerospace Resilience (CAR), DOE FL, $1,750,000, Co-PI, Co-director
2020-2021	Secure Assessment of AI Hardware and Accelerators, AFOSR, $1M, Lead PI
2020-2021	PCB Assurance Using Multi-Modal Data Infusion Based on Vulnerability/Risk Analysis, Cisco, $100K, Co-PI

2020-2021 A Holistic Approach for PCB Physical Inspection Using Learning Based Methods, Cisco, $100K, Co-PI

2020-2023 CCRI: ENS: Collaborative Research: Trust-Hub: Development of Benchmarks, Tools, Metrics, and Validation Platforms for Hardware Security, and a Web-based Dissemination Portal, NSF, $1.8M, Lead PI

2020-2021 PCB Assurance Using Multi-Modal Data Infusion Based on Vulnerability/Risk Analysis, Cisco, Co-PI, $100K

2020-2021 A Holistic Approach for PCB Physical Inspection Using Learning Based Methods, Cisco, Co-PI, $100K

2019-2023 DARP AISS ABIL – AISS By Industry Leaders, DARPA, ~$8M, Lead PI for UF FICS (Total: $48M)

2020 SBIR Navy, collaborate with Edaptive

20202-2022 Blockchain-Enabled Electronic Supply Chain Security, Nimbis Services, $1.1M, Lead PI

2020-2022 Hardware Vulnerability Ontology and Database for the Trusted Silicon Stratus, Battelle, HVD/HVO, $1.1M, Co-PI

2020-2021 Security Analysis and Implementation of DOSC Architecture, DARPA, $680K, Lead PI

2020-2021 ECI-TC Project on PCB and IC Assurance, $1.35M

2020 Lockheed Martin, Gift, $50K

2020-2023 STAMP: A Holistic Backward/Forward Trust Framework for Protecting Microelectronics Throughout Lifecycle, AFRL, $5.4M, Lead PI

2020-2022 Automated Delayering-Image Capture System (ADICS), MicroNet/DMEA, $300K, co-PI

2019 Ultra Backside Thinning of Integrated Circuits for Physical Assurance and Inspection, AFOSR DURIP, $290K, Lead PI

2019-2020 Side Channel Attack Testbench Emulator (SCATE), DARPA, $150K, Co-PI

2019-2022 CAD Framework for Analyzing and Mitigating Security Vulnerabilities in High-level Synthesis Flow, SRC, $250K, Lead PI

2019-2020 Microelectronics Security, Analog Devices, $90K, Lead PI

2019-2024 National Microelectronics Security Training Center (MEST), Year 1: $906K, Year 2-4: $12M, Total: ~13M, Lead PI

2019-2021 HARDEN: Hardware-Assisted ML-based Anomaly Detection for Cyber Defense, Cisco, $175K, Lead PI

2019-2021 HAWKS: Hardware Knowledge-Oriented Software Security Verification, Cisco, $200K, Co-PI

2019-2022 Pre-Silicon Security Verification and Backside Protection Schemes for Microelectronic Devices, AvMC/Dynetics, $2.15M, Lead PI

2019 Analog Devices, Establishing FICS Speaker Series on Cybersecurity, $15K, Gift, Lead

2019 Test Vehicle Design for HT Detection Validation, KCP Honeywell, $91K, Co-PI

2019-2020 Design Security Rule Check for SoCs, DARPA, $420K, Lead PI

2019-2024 University Center of Excellence: CYAN: Enabling Cyber Defense in Analog and Mixed Signal Domain, AFOSR/AFRL, $8.4M (with cost share), Co-directors: Waleed Khalil and Mark Tehranipoor

2019 AI Based Dynamic Encoding and Encryption Optimizer Powered by Quantum Entropy Chip, AFWERX Challenge on Microelectronic Design, $1.2M, Co-PI

2019-2020	ISIP: A Comprehensive Framework for Information Security for Intellectual Property and System-on-Chip Verification, Cisco, $100K, Lead PI
2019	Automated In-situ Large-area De-processing of ICs with High Throughput Electronic, STTR with Navid Asadi, DMEA / MicroNet Solutions, $44K, Co-PI
2019-20121	AutoBoM: Intelligent Framework for Automated Bill of Material Generation and Physical Inspection of PCBs, Edaptive / AFRL, $3M+, Lead PI
2019	Hardware Security Assessment, Bosch, $36K, Lead PI
2018-2021	Disciplined Microarchitectural Side Channel Detection, Intel, $165K (+ Option Years 2 and 3, Total: ~$500K), Co-PI
2018-2021	STV: Automated SoC Trust Validation Using Dynamic Trojan Benchmark Generation, Penn Test, and Deep Learning, Edaptive Computing, $1.4M, Lead PI
2018-2019	Protecting Obfuscated Circuits against Attacks that Utilize Test Infrastructure, DARPA, $380K, Lead PI
2018-2021	A Holistic Approach for Device to System Authentication, Air Force Eglin, $300K, PI
2018-2021	A Framework for Scalable Software Integrity Verification on Clear Hardware Assumptions, Texas Instruments/SRC, $450K, co-PI
2018-2021	EMLA: Metrics and Tools for Automated EM-Leakage Analysis at Pre-Silicon, NIST, $260K, Co-PI
2018-2021	Developing Firmware Security Testing Technology for IoT Devices, Korean Institute for Information and Communication Technology Promotion, Co-PI, Total: $2.54M, UF Share: ~$600K
2018-2019	BRAND: A Basic Framework for PCB Reverse Engineering, Analysis, and Defect Diagnosis, Cisco, $100K, Co-PI
2018	ARA, $10K
2018	2018 FICS conference support, $42K
2018-2019	A Framework for Automatic Detection of Fault Attack Vulnerabilities, Cisco, $100K, Co-PI
2018-2019	CRI/Rambus, DPA/EM Workstation, Donation, $187K Lead PI
2018-2019	DURIP, ONR Nano-probing Integrated Circuits for Physical Attacks and Hardware Security Assessment, ONR, Co-PI, $285K
2017-2018	MRI: Acquisition of a High-Resolution Photon Emission/Electro-Optical Microscope for Non-invasive Evaluation of Electronic Devices and Systems Security, NSF, Lead PI, $1M + $400K Cost Share from UF
2017-2020	NSF-SRC STARSS, SaTC: STARSS: Small: iPROBE - An Internal Shielding Approach for Protecting against Frontside and Backside Probing Attacks, Co-PI, $440K
2017-2019	Hardware IP Protection through Provably Secure State-Space Obfuscation, DARPA, Co-PI, $560K
2017-2018	PHASE II: FORTIS: Establishing Forward Trust for Protecting IPs and ICs in Today’s Complex Supply Chain, Cisco, $100K, Co-PI
2017-2019	A Comprehensive Framework for IoT Security and Privacy Evaluation Through Quantitative Metric, Cisco, $220K, IoT Vulnerability Database, Co-PI,
2017-2018	PHASE II: Scalable Hardware Trojan Detection using Statistical Test Generation and Side Channel Analysis, Raytheon, $100K, Co-PI
2017-2018	PHASE II: A Framework for Automatic Fine-Grain Timing Attack Vulnerability Evaluation, Draper, $20K, Co-PI
2017-2020	ASiLA: Automated Side-Channel Leakage Analysis: Metrics and Tools, NIST, $500K, Lead PI

2017 2017 FICS conference sponsorship, $28K

2017-2019 Security Validation of Integrated Circuits by Detailed Parameter Analysis Using Probe Station, ARO DURIP, $250K, Lead PI

2017-2018 Test Chip Design for Evaluating Trust, Honeywell, Lead PI, $210K

2017-2022 NSF SFS, SURPASS: NSF SFS Unique Scholarship Program in Hardware and Systems Security, Co-PI, $4.5M

2016-2018 Design Security Rule Check, SRC, Lead PI, $200K

2016-2019 Utilizing NIST Entropy as a Service and Chaotic Circuits for Management of Electronic Component Supply Chain, National Institute of Standards and Technologies (NIST), Co-PI, $500K

2016-2017 Timing Side-channel Analysis of Integrated Circuits, Draper, Co-PI, $50K

2016-2017 Self-referencing in Space and Time for Golden-Free Hardware Trojan Detection, Raytheon, Co-PI, $100K

2016 2016 FICS Conference support, $25K

2016 Donation from Tektronix (electrical test instruments), $150K

2016-2019 Establishing HACE (Hardware Security, Attack, and Countermeasure Evaluation Lab) Lab, NSF SaTC Education, PI, $300K

2016-2017 Gift from Intel for purchasing Servers and Workstations, $50K

2016-2019 Combating Counterfeit Analog and Mixed Signal ICs with Lightweight Embedded Mechanisms and Innovative Electrical Tests, NSF, Co-PI, $400K

2016 In-kind Contribution for ZEISS Orion, ZEISS, $1M

2016 Precise nano-fabrication and advanced circuit edit, DURIP, AFOSR, Lead PI, $1M

2016 TESCAN, in-kind contribution and gift to establishing INSPECT center at UF, $2.2M

2016-2018 Led the effort for establishing collaboration between FICS and Cisco in three areas: (1) IP Security and Trust, (2) Design for Security, and (3) Establishing forward trust from 3PIP to OEM, Cisco, Research Gift, $500K

2015-2018 Computer Systems Security, GAANN program, Department of Education (DOE), $591K, Co-director

2015-2018 CI-EN: Trust-Hub: Development of Benchmarks, Metrics, and Validation Platforms for Hardware Security, and a Web-based Dissemination Portal, NSF, Lead PI, $1.56M

2015-2017 Connecticut Cybersecurity Center (C3), State of Connecticut, Lead PI, $1M

2015 Security Rule Check: A Comprehensive Framework for Evaluating Security of Integrated Circuits, Semiconductor Research Corporation (SRC), Lead PI, $100K

2015-2018 REU Site: Research Experience in Cyber and Civil Infrastructure Security for Students with ADHD: Fostering Innovation, NSF, Co-PI, $344K

2014 2014 CHASE/CSI conference support + CyberSEED, $350K

2014-2019 Development of Universal Security Theory for Evaluation and Design of New Nanoscale Devices, DOD/AFOSR MURI, Lead PI, $7.5M

2014-2017 SHF:Small: GOALI: Advanced Physical Inspection of Counterfeit Integrated Circuits, NSF GOALI, Co-PI, $425K

2014-2017 Design of Low-Cost Memory-Based Security Primitives and Techniques for High-Volume Products, NSF/SRC STARSS, Lead PI, $460K

2014-2015	CHASE Membership, Juniper, Platinum Membership, $140K
2014	SBIR: Detecting Malicious Circuits in IP Cores, Office of Secretary of Defense (OSD), Co-PI, $150K
2013	2013 CHASE conference support, $30K
2014-2017	Comcast Center of Excellence in Security Innovation (CSI), $10M, Founding Director
2014-2017	Hardware Security and Security Assessment, Comcast, Lead PI, $185K
2014	Server Infrastructure, Donation to CHASE by Comcast, $300K
2013-2014	Physical Inspection equipment, Tech Park, $1M
2013-2014	Test Time Reduction for SOCs, LSI, Sole PI, $25K
2012	2012 CHASE workshop support, $20K
2013	Electrical Test Equipment, Tech Park, $140K
2013-2016	Low-Cost Self-Test Solutions for Improving Test Quality and Device Reliability and Resiliency, SRC, Sole PI, $300K
2013-2014	Comcast Lab, Hardware Security Assessment, Comcast, Lead PI, $285K
2013-2014	Equipment donation, Comcast, Lead PI, $170K
2013-2015	CHASE Membership, Honeywell, Platinum Membership, $200K
2013-2015	CHASE Membership, Comcast, Platinum Membership, $200K
2013-2014	Memory-based Physical Unclonable Function (PUF), Synokey, $90K
2013-2016	Development of Innovative Solutions for Hardware Security, and Detection and Prevention of Counterfeit Electronics Components, Missile Defense Agency (MDA), Sole PI, CHASE Funding, Platinum Membership, $292K
2013-2015	DOD IASP grant, Co-PI, $141K
2013-2014	Improving Hardware Security and Trust, Comcast, Lead PI, $93K
2013-2014	New Low-Cost LBIST for Improving Test Quality, GRC, Sole PI, $35K
2013-2016	A Multi-Level Test Approach for Improving Reliability and Performance of Nanometer Technology Designs, NSF/SRC, $270K, Sole PI, $270K
2012-2013	Technique to Measure Voltage Noise during Structural and Functional Testing of ASICs, Cisco, Sole PI (Gift, no indirect cost), $60K
2012-2015	Computer Systems Security, GAANN, Dept. of Education, (Co-PI), $400K
2013-2015	Efficient Test for Power Switches in Digital SOCs, EPSRC, Travel Grant to Southampton, UK, $10K
2012-2013	ARO Special Workshop on Counterfeit Electronics, $30K
2012-2013	Improving Security and Trustworthiness of IC Supply Chain, Comcast, $96K
2012-2013	CAREER: Novel Techniques for Detecting and Localizing Hardware Trojans in Integrated Circuits, NSF REU, $16K
2012-2013	High Quality Delay Tests for Nanometer Technology Designs, MediaTek, Sole PI (Gift, no indirect cost), $45K
2011-2014	Collaborative Research: CI-ADDO-NEW: Trust-Hub: Design of Trust Benchmarks, Hardware Validation Platforms and a Web-based Dissemination Portal, Lead PI, $1,230,000, NSF, $1.23M

2011-2014 Design-for-Hardware-Trust Techniques, Detection Strategies and Metrics for Hardware Trojans, Sole PI, Army Research office (ARO), $240K

2011-2012 Analysis and Measurement of Aging Effects on Circuit Performance in Nanometer Technology Designs, Cisco, Sole PI (Gift, no indirect cost), $60K

2011-2014 Exploratory Curriculum for Trustable Computing Systems Security Education (Co-PI), NSF, $200K

2011-2012 Correlating Structural Fmax with Functional Fmax, Qualcomm (Gift, no indirect cost), $30K

2011 Xilinx Equipment Donation, $5K

2010-2011 Effective Reliability and Variability Analysis of Sub-45nm Designs for Improving Yield and Product Quality, Cisco, Sole PI (Gift, no indirect cost), $60K

2011-2014 REU: Trustable Computing Systems Security Research and Education, NSF, (one of 5 PIs), $350K

2011-2012 UConn Intermediate Grant (one of 6 PIs), $99K

2010-2013 Test and Analysis for Critical Reliability and Variability Paths for Improving Yield, Product Quality and Reliability, Semiconductor Research Corporation (SRC), Sole PI, $300K

2010-2012 Collaborative Research: CI-ADDO-NEW: Trust-Hub: Design of Trust Benchmarks, Hardware Validation Platforms and a Web-based Dissemination Portal, NSF Planning Grant, Lead PI, $100K

2010 Agilent Equipment Donation, $40K

2010, 2011 Xilinx Equipment Donation, $10K

2010-2011 In-kind donation for Ocelot ZFP Tester, Verigy, $315K

2009-2014 CAREER: Novel Techniques for Detecting and Localizing Hardware Trojans in Integrated Circuits, NSF, Sole PI, $400K

2009-2012 Reliable Systems Design at Below 45-nm Technologies, SRC Custom Research, Freescale, Sole PI, $165K

2009-2012 Computer System Security, GAANN, Dept. of Education, (Co-PI), $525K

2009-2010 ARO Special Workshop on Hardware Assurance, Sole PI, $25K

2009-2013 High Quality Delay Test for VDSM Designs, LSI Logics, Sole PI, $150K

2009-2010 Root Cause of Timing Defects, Mentor Graphics, Sole PI, $43K

2008-2009 Intel Equipment Grant, Sole PI, $25K

2008-2012 GOALI (Industry-University Collaborative Project): Collaborative Research: Scalable Techniques for Detecting Small-Delay Defects in Nanometer Integrated Circuits, NSF, PI, $400K

2008-2012 CPA-DA: Dealing with Voltage Variations and Supply Noise During Performance Verification in Nanometer Technology Designs, NSF, Sole PI, $250K

2008-2009 Silicon Design Authentication and Malicious Alteration Detection in Integrated Circuits Using Delay Analysis, UConn Research Foundation, Sole PI, $24K

2007-2010 Collaborative Research: Detection and Isolation of Malicious Inclusions in Secure Hardware (DIMINISH), NSF, Lead PI, $300K

2007-2010 Timing-Aware ATPG for Maximizing Crosstalk/Signal Integrity on SOCs, Semiconductor Research Corporation (SRC), Sole PI, $282K

2005-2008 At-Speed Transition Fault Testing Using Low Cost Testers, SRC Custom Research, Texas Instruments, Sole PI, $152K

2005-2006 Frequency Driven Buffer Insertion (RAS, UMBC), $10K, PI

2005-2006 Securing Designs Against Non-Invasive Attacks (RAS, UMBC), $20K, PI

Industry Experience

1/98 – 11/01 **Advanced DSP Research Center, SAM Communications**

Designing emulator boards for TMS320C54x DSP, Implementing different programs on 'C54x emulator, internal memory BIST and implementation on 'C54x DSP.

In the Press

Is There a Practical Test for Rowhammer Vulnerability

https://semiengineering.com/is-there-a-practical-test-for-rowhammer-vulnerability/

Florida Trend: The one big threat when it comes to cyber-security has nothing to do with software

https://www.floridatrend.com/article/31635/the-one-big-threat-when-it-comes-to-cyber-security-has-nothing-to-do-with-software

CNN: Raid of former Florida Covid data scientist's home could affect other state employees, legal experts warn

https://www.cnn.com/2020/12/08/us/rebekah-jones-whistleblower-raid-invs/index.html

University of Florida Researcher Creates Innovative Training Platform That Makes
Cyberspace a Safer Place (UF Innovate)

http://innovate.research.ufl.edu/2020/11/10/tehranipoor-si2020-story/

UF researchers thrive despite the pandemic

https://www.alligator.org/news/uf-researchers-thrive-despite-the-pandemic/article_90c863e2-eb38-11ea-b3b1-bbc6f8f7bdf7.html

Interview with Semicon 2020

https://blog.semi.org/technology-trends/industry-expert-qa-the-key-to-chip-security-trust-and-verify-but-how

IEEE Spectrum Rcognizes Dr. Tehranipoor's technology at:

https://spectrum.ieee.org/computing/hardware/three-ways-to-hack-a-printed-circuit-board

University of Florida hits record $900 million in research awards

https://news.ufl.edu/2020/08/record-research-awards/

FICS Research Reveives $7.8M to Help Make On-Chip Security Pervasive

https://news.ece.ufl.edu/2020/05/13/tehranipoor-darpa-aiss/

Playing Digital Defense, Florida High Tech Corridor

https://floridahightech.com/playing-digital-defense/

This Tech Would Have Spotted the Secret Chinese Chip in Seconds: University of Florida Researchers use X-rays, optical imaging, and AI to spot spy chips in computer systems

https://spectrum.ieee.org/riskfactor/computing/hardware/this-tech-would-have-spotted-the-secret-chinese-chip-in-seconds

Interview with New York Times

Interview with the Florida Tend, Connected World

Vulnerability Note VU#739007

http://www.kb.cert.org/vuls/id/739007

Crypto Bugs in IEEE Standard Expose Intellectual Property in Plaintext

https://www.bleepingcomputer.com/news/security/crypto-bugs-in-ieee-standard-expose-intellectual-property-in-plaintext/

Flaws in IEEE P1735 electronics standard expose intellectual property

http://securityaffairs.co/wordpress/65184/hacking/ieee-p1735-electronics-standard-flaws.html

IEEE Spectrum, M. Tehranipoor, U. Guin, and S. Bhunia, "Invasion of the Hardware Snatchers: Fake Hardware Could Open the Door to Malicious Malware and Critical Failure," IEEE Spectrum, 2017.

http://spectrum.ieee.org/computing/hardware/invasion-of-the-hardware-snatchers-cloned-electronics-pollute-the-market

UF's Annual Cybersecurity Conference Focuses on Security of IoT

https://www.eng.ufl.edu/newengineer/ece/fics-2017/

Interview with Le Monde France: Fight against counterfeit electronic components

http://www.lemonde.fr/sciences/article/2016/12/05/lutter-contre-la-contrefacon-de-composants-electroniques_5043610_1650684.html

Pensacola News Journal: Cybersecurity must increase with automation

http://www.pnj.com/story/money/business/2016/11/28/cybersecurity-must-increase-automation/94546842/

UF Partners with TESCAN to create world-class hardware security lab

http://www.strategic-directions.com/_a/industry-news/?action=2&terms=&sdi=26f5e7d4-b522-47e8-8c6e-63a1474edbfc

University of Florida Cybersecurity Team Turns to Tektronix to Outfit Electronics Security Lab

http://finance.yahoo.com/news/university-florida-cybersecurity-team-turns-130000458.html

WUFT, Nov. 15, 2015, Cybersecurity Discussion Raises Concern For Experts

http://www.wuft.org/news/2015/11/15/cybersecurity-discussion-raises-concern-for-experts/

Cyber-security at Florida's public and private universities

http://www.floridatrend.com/article/19478/cyber-security-at-floridas-public-and-private-universities

IEEE Spectrum

http://spectrum.ieee.org/tech-talk/telecom/security/an-unhackable-qr-code-to-fight-bogus-chips

BusinessWire:

NIST Cybersecurity advisor visited CHASE center, Feb. 2014.

http://www.businesswire.com/news/home/20150219005203/en/NIST-Cybersecurity-Chief-Discuss-Threats-Framework-Implementation#.VOX_2MYsO8l

Yahoo Finance:

http://finance.yahoo.com/news/university-connecticut-comcast-sponsor-first-130000543.html

Washington Times

http://www.washingtontimes.com/news/2014/apr/29/universities-to-research-nanotechnology-security/

Wall Street Journal

http://online.wsj.com/article/PR-CO-20140410-912537.html

Universities beef up cybersecurity, identity theft research

http://gcn.com/blogs/pulse/2014/04/ut-uconn-cybersecurity-research.aspx

Credit Card Data Theft: Stopping the Hackers

http://today.uconn.edu/blog/2014/03/credit-card-data-theft-stopping-the-hackers/

Expert Discusses Steps to Address Threat of Cyber Attacks

http://today.uconn.edu/blog/2013/10/expert-discusses-steps-to-address-threat-of-cyber-attacks/

Cover Story, IEEE Spectrum, The Hidden Dangers of Chop-Shop Electronics

http://spectrum.ieee.org/semiconductors/processors/the-hidden-dangers-of-chopshop-electronics

Conference on Counterfeit Electronics Addresses Growing National Concern

http://www.chase.uconn.edu/conference-on-counterfeit-electronics-addresses-growing-national-concern.php

Sen. Lieberman Praises UConn Cybersecurity Labs

http://today.uconn.edu/blog/2012/02/sen-lieberman-praises-uconn-cybersecurity-labs/

Lieberman pushes for cyber security

http://www.dailycampus.com/news/lieberman-pushes-for-cyber-security-1.2794957#.T1P6RvEgdGM

Research Initiative Will Enhance Integrity of Integrated Circuits

http://today.uconn.edu/?p=34063

University of Connecticut and Duke University Develop Unique Method to Improve Testing for Small Delay Defects in Semiconductors

http://www.hartfordbusiness.com/news14048.html

http://www.physorg.com/news199362652.html

http://www.advfn.com/news_University-of-Connecticut-and-Duke-University-Develop-Unique-Method-to-Improve-T_43665962.html

http://www.forbes.com/feeds/businesswire/2010/07/20/businesswire142648135.html

http://www.src.org/newsroom/press-release/2010/86/

NYU-Poly and UConn Researchers Develop New Design Techniques to Protect Against Vulnerabilities in the Electronics Supply Chain

http://www.marketwatch.com/story/student-hackers-and-a-dose-of-skepticism-secure-vital-hardware-2011-11-08

Xuehui Zhang Received First Place Prize at the 2010 CSAW - Embedded Systems Challenge
http://www.brooklyneagle.com/categories/category.php?category_id=31&id=39204

http://www.poly.edu/press-release/2010/11/02/who-will-protect-our-digital-future-woman-high-school-videographer-student-

Interview with “The Economist”

Interview with EBN

Interview with NPR (twice)

Interview with WUFT

Academic Awards & Honors

2022 Best WiP Paper Award, K. Zamiri Azar, H. Kermani Mardani, F. Farahmandi, and M. Tehranipoor, “**Warm up before Circuit De-obfuscation? An Exploration of the Possibilities**” IEEE **HOST**, 2022

2021 **ACM Fellow**

2020 **Teacher/Scholar of the year**, Herbert Wertheim College of Engineering, University of Florida

2020 The paper titled “**SHADE: Automated Refinement of PCB Component Estimates Using Detected Shadows**,” received the best student paper award in IEEE Conference on Physical Assurance and Inspection of Electronics (**PAINE**), 2020.

2020 Ranked #3 among all PIs at the University of Florida in awarded funding for 2020

2020 Received **Inventor of the Year Award from UF Innovate**; Technology highlighted during the Standing InnOvation Event in September 2020

2018 Inducted into HOST Hall of Fame

2018 **Best Paper Award**, K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, M. Tehranipoor, “Hardware Trojans: Lessons Learned after One Decade of Research,” ACM Transaction on Design Automation of Electronic Systems (**TODAES**), 2017

2018 **IEEE Fellow**

2017 **Outstanding Paper Award,** E. L. Principe, N. Asadizanjani, D. Forte, M. Tehranipoor, R. Chivas, M. DiBattista, S. Silverman, M. Marsh, J. Mastovich, J. Odum, “**Steps Towards Automated Deprocessing of Integrated Circuits**,” International Symposium on Test and Failure Analysis (**ISTFA**), 2017

2017 **College of Engineering Excellence in Leadership Award**, University of Florida

2017 **ECE Research Excellence Award,** ECE Department, University of Florida

2017 **Best Paper Award**, X. Wang, Y. Guo, T. Rahman, D. Zhang, and M. Tehranipoor, “**DOST: Dynamically Obfuscated Wrapper for Split Test against IC Piracy**,” IEEE Asian Hardware-Oriented Security and Trust Symposium (**AsianHOST**), 2017.

2017 The article “**Hardware Trojans: Lessons Learned After One Decade of Research**" published in IEEE Transactions on Design Automation of Electronic Systems (**TODAES**) was included the **21st Annual Best of Computing** (http://www.computingreviews.com/recommend/bestof/notableitems.cfm?bestYear=2016).

2016 **TTTC Most Successful Event Award for HOST Symposium, Co-founded by Tehranipoor**

2016 **Best Paper Award,** Q. Shi, N. Asadi, D. Forte, and M. Tehranipoor, "**A Layout-driven Framework to Assess Vulnerability of ICs to Microprobing Attacks**," IEEE Symposium on Hardware-Oriented Security and Trust (HOST), 2016.

2016 **Best Paper Candidate**, K. Yang, D. Forte, and M. Tehranipoor, "**UCR: An Unclonable Chipless RFID Tag**," IEEE Symposium on Hardware-Oriented Security and Trust (HOST), 2016.

2015	**Best Paper Award**, "K. Xiao, D. Forte, and M. Tehranipoor, "**Efficient and Secure Split Manufacturing via Obfuscated Built-In Self-Authentication**," IEEE Hardware-Oriented Security and Trust (HOST), 2015"
2015	The paper titled "**Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead**" was recognized by **JETTA** as the most downloaded article in 2014
2015-present	Intel Charles E. Young Preeminence Endowed Professor in Cybersecurity, University of Florida
2015-present	Elected member of Connecticut Academy and Science and Engineering (**CASE**)
Nov. 2014	ISE North America, US and Canada, **Best Project finalist** for establishing CHASE and CSI centers
Nov. 2014	**Best paper Candidate**, International Symposium on Test and Failure Analysis (ISTFA), 2014
Oct. 2014	ISE Northeast, **Best Project finalist** for establishing CHASE and CSI centers
Aug 2014	Air Force Office of Scientific Research (AFOR) MURI Award (2014-2019)
Sep. 2014	UConn **ECE Research Excellence** Award
2012- 2014	Charles Knapp Associate Professor
May 2013	**Best Paper Award**, IEEE North Atlantic Test Workshop (**NATW**), 2013
2012	IEEE Computer Society **Golden Core Inductee**
Oct. 2012	**Best Student Paper Award,** IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT), 2012
2011- 2012	F.L. Castleman Associate Professor in Engineering Innovation
June 2012	IEEE Computer Society Outstanding Contribution Award
April 2012	SOE Outstanding Faculty Advisor Award
Jan 2012	**Best Special Session Award, IEEE VLSI Test Symposium (VTS), 2011**
2010-2013	**IEEE Computer Society Distinguished Speaker**
2010-2013	**ACM Distinguished Speaker**
May 2010	Recipient of the IEEE Computer Society TTTC **Most Successful Technical Event** for founding HOST Symposium
May 2010	Recipient of the 2009 **IEEE Computer Society Certificate of Appreciation**
May 2009	UConn **ECE Research Excellence** Award, 2009
Jan. 2009	**NSF CAREER Award**, 2009
May 2009	**Best Paper Award**, IEEE North Atlantic Test Workshop, 2009
Oct. 2008	IEEE **Computer Society Meritorious Service Award**, 2008
May 2008	**Best Paper Award**, IEEE North Atlantic Test Workshop, 2008
May 2008	Honorable Mention for **Best Paper Award**, IEEE North Atlantic Test Workshop, 2008
May 2007	**Best Panel Award**, IEEE VLSI Test Symposium (VTS), 2006
Nov. 2006	**Top Ten Recognition Paper**, ITC 2005
March 2006	**Best Paper Award,** IEEE VLSI Test Symposium (VTS), 2005
April 2006	**Best Paper Candidate,** Design Automation Conference, 2006
Sep. 2005	**Best Paper Candidate,** TI Symposium on Test (TIST), 2005

1/02 – 08/04 Received Texas Public Educational Grant, 2002-2004

July 1997 **Ranked 2nd**, Undergraduate Program, ECE Department, Tehran Polytechnic University

June 1992 **Ranked 1st**, High School, Among all high school students in Golestan province, Iran

Students Awards for their Projects under my Supervision

- My PhD student Nitin Pundir received the Best Dissertation Recognition Award, Title: **Security Verification for SoC Designs**, IEEE **HOST** 2022
- The Demo called **eChain: A Blockchain Based Ecosystem for Trusted Electronic Devices** won the Attendee's Choice Award, IEEE **HOST** 2022
- Team **Gator Hardware Oriented Security team (GHOST)** won first prize in IEEE **HOST** 2022 Microelectronic Security Challenge (IP Security Track).
- Andrew Stern received the 3rd place in the **2021 IEEE TTTC McCluskey Best Doctoral Thesis Award**
- Huanyu Wang received the 2nd place in the **2021 IEEE TTTC McCluskey Best Doctoral Thesis Award**
- The **Hardware Demo presented in HOST-2020** called "SPARTA: Laser Probing Approach for Trojan Detection" Received the judges best demo award
- The **Hardware Demo presented in HOST-2020** called "FPGA-As-A-Service Security" Received the attendees best demo award
- Andrew Stern received the second Prize for his hardware demo on "**Utilizing EM Emanation for Provenance Analysis of Microelectronic Devices**", IEEE International HOST, May 2018, Washington DC
- Andrew Stern, Received **best demo award** at the FICS 2018
- Fahim Rahman, Received **best poster award** at the FICS 2018
- Huanyu Wang, Received **best poster award** at the FICS 2018
- **Best Poster Award supported by DRAPER,** Andrew Stern, Haoting Shen, Xiaolin Xu, Domenic Forte, Mark Tehranipoor, **Near Field EM for Foundry of Origin Identification**, 2017 FICS Annual Conference on Cybersecurity
- **Best Poster Award,** Gustavo K. Contreras, Adib Nahiyan, Domenic Forte, Mark Tehranipoor, **Track and Extract: Information Flow Tracking for Security Vulnerability Analysis and Exploit Extraction**, 2017 FICS Annual Conference on Cybersecurity
- **Best Poster Award,** Troy Bryant, Sreeja Chowdhury, Domenic Forte, Mark Tehranipoor, Nima Maghari*,* **An All-Digital PUF (Physically Unclonable Functions) for AMS Applications Using Stochastic Comparator Voltage Offset**, 2017 FICS Annual Conference on Cybersecurity
- Adib Nahiyan and Gus Contreras receive **Best Poster Award** at the 2016 FICS Annual Conference on Cybersecurity, Title: **DSeRC: Design Security Rule Check**
- Mehdi Sadi received **Best in Session Award** from TECHCON, 2016 for his paper titled **BIST-Assisted In-field Aging Reliability Management of SoCs Using On-Chip Clock Sweeping and Machine Learning**
- G. Contreras received **Best in Session Award** from TECHCON, 2016 for his paper titled **Fault Deterministic Vector Analysis and Seed Extraction for LBIST**
- Tauhid Rahman received **Best in Session Award** from TECHCON, 2016 for his paper titled **SRAM Inspired Design and Optimization for Developing Robust Security Primitives**
- **Qihang Shi** received the Best TA Award from the ECE Department, UConn, 2012

- **Andrew Ferraiuolo, Adam Zimmer, and Rifat Chowdhury** won the first prize from ECE on their Senior Design Project under my supervision, 2012
- **Nicholas Tuzzio, Xuehui Zhang and Andrew Ferraiuolo**: Received the first place prize at the 2011 CSAW - Embedded Systems Challenge (Physical Unclonable Functions)
- **Xuehui Zhang, Nicholas Tuzzio, and Andrew Ferraiuolo**: Received the third place prize at the 2011 CSAW - Embedded Systems Challenge (Malicious Processor Design)
- **Junxia Ma**: Selected as one of the four finalists for Connecticut Women of Innovation (WOI)
- **Brian Helfer, Theodore Estwan, and Emilio Cepeda** won the first prize from ECE on their Senior Design Project under my supervision, 2011
- **Xuehui Zhang:** Received First Place Prize at the 2010 CSAW - Embedded Systems Challenge
- **Michel Wang:** Received Best in Session Award at TECHCON 2010
- **Nisar Ahmed:** Received UConn SOE Outstanding Graduate Thesis Award
- **Joseph Larosa, Corey Benoit, Andrew Tan, and Kevin Perkins** won the first prize from ECE on their Senior Design Project under my supervision, 2010
- **Junxia Ma:** Received Best in Session Award at TECHCON 2009
- **Jeremy Lee:** Received the TTTC Best Thesis Research Poster Award, 2008
- **Jeremy Lee:** Received the Best Computer Engineering Seminar Presentation, 2008
- **Paul Rago and Aaron Feldstein** won the second prize from ECE on their Senior Design Project under my supervision, 2008
- **Nisar Ahmed:** Received the TTTC 2007 Best Doctoral Dissertation Award
- **Kevin Tyler, Danny Ho, and Vimal Vachhani** won the first prize from ECE on their Senior Design Project under my supervision, 2007
- **Nisar Ahmed:** Received the UMBC-CSEE's Best PhD Thesis Award, 2006

Professional Activities

Founding Positions:

- **Co-founder**, IEEE International Physical Attacks and Inspection on Electronics (**PAINE**) Conference

  http://paine-conference.org/
- **Founder**, Trusted and Assured Microelectronics Forum (**TAME**)

  www.tameforum.org
- **Co-founder**, Journal of Hardware and Systems Security (**HASS**), 2016

  http://www.editorialmanager.com/hass
- **Co-founder**, IEEE Asian Symposium on Hardware-Oriented Security and Trust (**AsianHOST**), 2016

  http://asianhost.org/index.htm
- **Co-founder**, International Verification and Security Workshop (**IVSW**) and member of the steering committee,

  http://tima.imag.fr/conferences/ivsw/ivsw16/

- **Founder and Director**, Florida Institute for Cybersecurity (**FICS**), 2015-present
  http://www.institute.ufl.edu
- **Founding Director**, Center for Hardware Assurance, Security, and Engineering (**CHASE**), 2012-2015
  http://www.chase.uconn.edu/
- **Founding Director**, Comcast Center of Excellence in Security Innovation (**CSI**), 2013-2015
  http://www.csi.uconn.edu/
- **Co-founder**, IEEE Int. Symposium on Hardware-Oriented Security and Trust (**HOST**), 2008
  http://www.engr.uconn.edu/HOST/
- **Co-founder**, Trust-Hub, 2010

  http://www.trust-hub.org/

IEEE/ACM Events Chair Positions:

- **Co-general Chair,** IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2022
- **Vice-Program Chair**, IEEE International Worshop on Silicon Lifecycle Management (SLM), 2021
- **Co-general Chair,** IEEE International Hardware-Oriented Security and Trust (HOST) Summit, 2021
- **General Chair**, IEEE International Physical Assurance and Inspection of Electronics (PAINE) Conference, 2019, 2020, 2021
- **General Chair**, CAD4Sec Workshop, Co-located with DAC, 2022
- **Program Chair**, International Test Conference (ITC), 2019
- **Editor-in-Chief**, Journal of Hardware and Systems Security (HASS), 2016-present
- **Associate EIC**, IEEE Design & Test of Computers, 2012-2014
- **IEEE CS Fellow Evaluation Committee,** IEEE CS, 2018-2022
- **IEEE Cybersecurity Initiative Ambassador** (2016-2020)
- **Vice-program Chair**, International Test Conference (ITC), 2018
- **Co-Program Chair**, International Verification and Security Workshop (IVSW), 2016
- **Co-Program Chair**, IoT and Automotive Security Workshop (ISAW), 2017
- **Co-program Chair**, IEEE International Workshop on Cross-Layer Cyber-Physical Systems Security (CPSS), 2016
- **Co-program Chair**, IoT Security Workshop, co-located with IEEE HOST 2017
- **Vice-General Chair**, IEEE North Atlantic Test Workshop (NATW), 2011
- **General Chair**, IEEE Workshop on Defect and Data Driven Testing (D3T), 2009, Austin, TX
- **General Chair**, IEEE International Symposium on Defect and Fault Tolerance of VLSI Systems (DFT), 2009, Chicago, IL
- **General Chair,** IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2009, San Francisco, CA
- **General Chair,** 1st IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2008, Anaheim, CA

- **Steering Committee Chair**, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2008-present
- **Program Chair**, IEEE Workshop on Defect Based Testing (DBT), 2008, Santa Clara, CA
- **Program Chair**, IEEE International Symposium on Defect and Fault Tolerance of VLSI Systems (DFT), 2008, Boston, MA
- **Program Chair**, IEEE Workshop on Defect Based Testing (DBT), 2007, Santa Clara, CA
- **Local Arrangement Chair**, IEEE Int. Symp. on Defect and Fault Tolerance in VLSI Systems (DFT), 2006, Washington DC
- **Member, Steering Committee,** IEEE Workshop on Defect and Data Driven Testing (D3T), 2009-2010
- **Chair**, Hardware Security Subcommittee, Design Automation Conference (DAC), 2019, 2020
- **Member, Steering Committee,** International Test Conference (ITC), 2018-present
- **Member, Steering Committee,** IEEE Workshop on Defect and Adaptive Test Analysis (DATA), 2011-present
- **Member, Steering Committee,** IEEE International Verification and Security Workshop (IVSW), 2016-present
- **Vice-Chair,** TTTC Technical Activity group on Hardware Security and Trust
- **Vice-General Chair,** IEEE North Atlantic Test Workshop (NATW), 2012
- **Co-program Chair**, Internet of Things (IoT) and Automotive Security Workshop (IASW), co-located with HOST Symposium, 2017-present
- **Industry Liaison,** IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2014-present
- **Industry Liaison,** Workshop for Women in Hardware and Systems Security (WISE), 2017-present
- **Industry Liaison,** IEEE Asian Symposium on Hardware-Oriented Security and Trust (AsianHOST), 2016
- **Panel Chair,** IEEE Asian Symposium on Hardware-Oriented Security and Trust (AsianHOST), 2016-present
- **Security Special Session Track Chair**, IEEE International Microprocessor Test and Verification (MTV) conference, 2016
- **Security Track Co-chair**, International Test Conference (ITC), 2016-present
- **Security Track Chair**, Design Automation Conference (DAC), 2017-2018
- Design Automation Conference (DAC) **Security Special Focus Committee, 2018-2019**
- **Steering Committee**, Attacks and Solutions in Hardware Security (**ASHES**), Co-located with CCS 2017-present
- **Exhibit Chair,** IEEE International Hardware-Oriented Security and Trust (**HOST**), 2020

Non-IEEE Events Chair Positions:

- **Member**, Scientific Advisory Board, Center for Advanced Studies, LMU Munich
- **Chair**, Advisory Board, SECURE Center. Prairie View A&M University (PVAMU)
- Florida State University System (SUS) **Cybersecurity Steering Group (Governing Council)**, 2020-present
- **Co-Chair**, Trusted and Assured Microelectronics (TAME) Forum, Nov. 2017

- **Steering Committee,** Trusted and Assured Microelectronics (TAME) Forum
- **Chair**, FICS Annual Conference on Cybersecurity, March 2017. **13 companies sponsored this event. 210 attended.**
- **Chair**, FICS Annual Conference on Cybersecurity, February 2016. **12 companies sponsored this event. 155 attended.**
- **Chair**, CHASE Conference on Secure/Trustworthy Systems and Supply Chain Assurance, 2015. **10 companies sponsored this event.**
- **Co-organizer**, CyberSEED (http://www.csi.uconn.edu/cybersecurity-week), **More than a dozen companies sponsored this event.**
- **Chair**, CHASE Workshop on Secure/Trustworthy Systems and Supply Chain Assurance, 2014 (https://www.chase.uconn.edu/chase-workshop-2014.php). **8 companies sponsored this event.**
- **Chair**, ARO/CHASE Sponsored Workshop on Counterfeit Electronics, 2013
- **Chair**, 2nd ARO Sponsored Workshop on Hardware Assurance, 2011
- **Chair**, 1st ARO Workshop on Hardware Assurance, 2009

Editorial Board:

- **Associate Editor**, IEEE Transactions on Computers, 2019-present
- **Associate Editor**, IEEE Transactions on VLSI (**TVLSI**), 2015-present
- **Associate Editor**, ACM Transactions on Design Automation of Electronic Systems (**TODAES**), 2013-2020
- **Associate Editor**, IEEE Design & Test of Computer Magazine, 2009-2015, 2020-2021
- **Associate Editor**, Journal of Low Power Electronics (**JOLPE**), 2009-present
- **Associate Editor**, Journal of Electronic Testing: Theory and Applications (**JETTA**), 2007-present
- **Editor,** Test Technology Technical Council **(TTTC**) Newsletter, 2008-2011

Guest Editor:

- Special issue on CAD for Security: Pre-silicon Security Sign-off Solutions Through Design Cycle, ACM Journal on Emerging Technologies in Computing Systems (JETC), 2022, F. Farahmandi, A. Srivastava, G. Di Natale, and M. Tehranipoor
- Special issue on Physical Assurance and Inspection of Electronics, Springer Journal on Hardware and Systems Security (HaSS), 2020, N. Asadi, and M. Tehranipoor
- C. Chang, M. van Dijk, U. Ruhrmair, and M. Tehranipoor, Emerging Attacks and Solutions for Secure Hardware in the Internet of Things, IEEE Transactions on Dependable and Secure Computing (TDSC), May/June 2019
- IEEE Transactions on Multi-Scale Computing Systems, Special Issue on Hardware/Software Cross-Layer Technologies for Trustworthy and Secure Computing, Shiyan Hu (Michigan Technological University), Yier Jin (University of Central Florida), Mark M. Tehranipoor (University of Connecticut), Kenneth Heffner (Honeywell)
- IET Computers and Digital Techniques, Special Issue on Hardware Security, Ilia Polian (U of Passau) and M. Tehranipoor (UCONN), 2013-2014

- Special issue on "On-chip Structures for Smarter Silicon", IEEE Design & Test of Computers, Co-guest Editor: LeRoy Winemberg (Freescale Semiconductor), 2012
- IEEE Computer Society (CS) Computing Now on Hardware Security and Trust, September 2010
- IEEE Design & Test Special Issue on "Verifying Physical Trustworthiness of Integrated Circuits and Systems", Co-guest Editor: Farinaz Koushanfar (Rice University), 2009
- Special issue on "Test, Defect Tolerance, and Reliability of Nanoscale Devices", Journal of Electronic Testing: Theory and Applications (JETTA), 2007
- Special issue on "IR-Drop and power Supply Noise Effects on Design and Test of Very Deep Submicron Designs", IEEE Design & Test of Computers, Co-guest Editor: Ken Butler (Texas Instruments), 2008

Tutorials

- International Test Conference (ITC), **SoC Security Verification**, Oct. 2021
- IEEE International Hardware-Oriented Security and Trust (**HOST**), **CAD Solutions for SoC Security**, Dec. 12, 2021
- Design, Automation, and Test in Europe (**DATE**), CAD for SoC Security, Feb. 2021
- IEEE International Hardware-Oriented Security and Trust (**HOST**), **CAD for SoC Security**, Dec. 2020
- IEEE International Hardware-Oriented Security and Trust (**HOST**), **CAD for SoC Security**, Washington DC, May 2019
- IEEE International Hardware-Oriented Security and Trust (**HOST**), **Protecting Electronics Supply Chain from Throughout Lifecycle**, Washington DC, May 2018
- IEEE International Hardware-Oriented Security and Trust (**HOST**), **Protecting Electronics Supply Chain from Design to Resign**, Washington DC, May 2017
- International Test Conference (ITC), **Test Opportunities and Challenges for Secure Hardware and Verifying Trust in Integrated Circuits**, Dallas/Fort Worth, TX, 2016
- **Dagstuhl Seminar on Hardware Security**, Germany, Dagstuhl, 2016, Title: Hardware Security (http://www.dagstuhl.de/de/programm/kalender/semhp/?semnr=16202)
- International Test Conference (ITC), **Test Opportunities and Challenges for Secure Hardware and Verifying Trust in Integrated Circuits**, 2015
- Design Automation Conference (DAC), **Introduction to Hardware Security**, M. Potkonjak (UCLA), M. Tehranipoor (UCONN), 2015
- IEEE International System-on-Chip Conference (SOCC), **Electronic Component Supply Chain Security: Threats, Challenges, and Solution**, M. Tehranipoor (UCONN), 2014
- Design, Automation, and Test in Europe (DATE), **All You Need to Know About Hardware Trojans and Counterfeit ICs**, M. Tehranipoor and D. Forte (UCONN), 2014
- IEEE Conference on VLSI, 2014, **All You Need to Know About Hardware Trojans and Counterfeit ICs**, M. Tehranipoor and D. Forte (UCONN)
- IEEE International Reliability Physics Symposium (IRPS), 2013, **Chip to System Reliability Fundamentals**, M. Tehranipoor (UConn), Nemat Bidokhti (Cisco), and Bill Eklow (Cisco)

- International Test Conference (ITC), 2011, **Testing Low-Power Integrated Circuits: Challenges, Solutions, and Industry Practices**, Srivaths Ravi (Texas Instruments), M. Tehranipoor (UConn), and Rohit Kapur (Synopsys)
- International Test Conference (ITC), 2011, **High-Quality and Low-Cost Delay Testing for VDSM Designs: Challenges & Solutions**, M. Tehranipoor (UConn), Krish Chakrabarty (Duke University), and Jeff Rearick (AMD)
- Design Automation Conference (DAC), 2011, **Chip to System Reliability Fundamentals**, M. Tehranipoor (UConn), Nemat Bidokhti (Cisco), and Bill Eklow (Cisco)
- International Test Conference (ITC), 2010, **Testing Low-Power Integrated Circuits: Challenges, Solutions, and Industry Practices**, Srivaths Ravi (Texas Instruments), M. Tehranipoor (UConn), and Rohit Kapur (Synopsys)
- International Test Conference (ITC), 2010, **High-Quality and Low-Cost Delay Testing for VDSM Designs: Challenges & Solutions**, M. Tehranipoor (UConn), Krish Chakrabarty (Duke University), and Jeff Rearick (AMD)
- Design, Automation, and Test in Europe (DATE), 2010, **Testing Low-Power Integrated Circuits: Challenges, Solutions, and Industry Practices**, Srivaths Ravi (Texas Instruments), M. Tehranipoor (UConn), Rohit Kapur (Synopsys)
- International Conference on VLSI Design, Title: **High-Quality and Low-Cost Delay Test for VDSM Designs**, January 2009
- **IEEE MidWest Symposium on Circuits and Systems, Title:** High-Quality Delay Tests for Nanometer Technology Designs, Auguat 2008

Panelist

- Panelist: IEEE Workshop on Silicon Lifecycle Management (SLM), 2021
- Panelist: Microelectronics Security, Raytheon RX ISaC Technology Network Panel, May 2021
- Panel Co-moderator, High Level Synthesis: Facts, Myths, and fantacies, IEEE HOST, Dec. 2020
- Panelist: Quantifiable Assurance, IEEE HOST 2020
- Panelist: Hardware Security, SRC SIA DOE workshop on Decadal Plan for Semiconductors workshop on ICT Hardware Enabled Security
- Panelist: Education and Workforce Development, ERI Summit, August 2020
- Panelist: Assured AI, Trusted and Assured Microelectronic (TAME) Forum, Washington DC, May 2019
- Panelist: Hardware Supply Chain Security in Asia and Around the World, IEEE AsianHOST, 2018
- Panelist: Trusted and Assured Microelectronics (TAME), Vision for TAME (co-located with HOST), May 2018
- Panel Moderator with Edna Conway, Women in Hardware and Systems Security Workshop (WISE), May 2018
- Panelist, Global Electronic Supply Chain: What Can South East Asian do about it? IEEE AsianHOST, 2017
- Panelist: Internet of Things (IoT) and Automotive Security Workshop (IASW), 2017
- Panelist: NYU Alfred P. Sloan Foundation, Cybersecurity Lecture, with Wally Rhines, Chairman and CEO of Mentor Graphics, April 2017

- Panelist: International Workshop on Hardware Security, 2016, Title: Research Collaboration Opportunities in Hardware Security Areas
- Panelist: IEEE VLSI Test Symposium (VTS), 2016, Title: Test Challenges for Secure Hardware
- Panelist: International Symposium on Quality Electronic Design (ISQED), 2016, Title: Hardware and Systems Security Challenges in IoT Era
- Panelist: FIU Cybersecurity Conference, October, 2015
- Panelist: IEEE VLSI Test Symposium (VTS), 2015
- Panelist: IEEE S&P Symposium, San Jose, CA, May 2014
- Panelist: SRC STARSS, San Jose, CA, May 2014
- Panelist: Microprocessor Test and verification (MTV), Nov. 2013
- Panelist: IEEE North Atlantic Test Workshop (NATW), May 2013
- Panelist: Cisco innovation Test Conference (CITC), 2012
- Panelist: International Workshop on Defect and Adaptive Test Analysis (DATA), September 2011
- Panelist: International Test Conference (ITC), November 2010
- Panelist: IEEE Symposium on Hardware-Oriented Security and Trust (HOST), June 2010
- Panelist: International Test Conference (ITC), Nov. 2009
- Panelist: International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT), October 2009
- Panelist: IEEE Workshop on RTL Testing (WRTLT-08), Nov. 2008, Title: Power-Aware Testing in Integrated Circuits

Special Session Organizer

- **Special Session Organizer**, Hardware Security, International Test Conference (ITC), 2018
- **Special Session,** Emerging Topics in Security and Trust I, International Test Conference (ITC), 2017 (Speakers: Brian Dupaix (AFRL), Patrick Schaumont (Vriginia Tech), and An Chen (Semiconductor Research Corporation)
- **Special Session,** Emerging Topics in Security and Trust II, International Test Conference (ITC), 2017 (Domenic Forte (University of Florida), Jeyavijayan Rajendran (Texas A&M University), and Krishnendu Chakrabarty (Duke University))
- **Special Session,** Physical Attacks: Can Test Save Us? IEEE VLSI Test Symposium (VTS), 2017, Co-organized by Swarup Bhunia, University of Florida
- **Special Session** 1, IP Protection, IEEE Microprocessor Test and Verification, 2016
- **Special Session** 2, Test for Security and Trust, IEEE Microprocessor Test and Verification (MTV), 2016
- **Special Session**, Test for Security and Trust of Integrated Circuits, International Test Conference (ITC), 2016
- **Special Session**, IEEE VLSI Test Symposium (VTS), 2016, Title: Security Validation in IOT Space
- **Special Session,** IEEE VLSI Design, India, 2016, Title: New Topics in Hardware Security
- **Special Session**, IEEE Microprocessor Test and Verification Workshop (MTV), Austin, 2015, Title: New Directions in Hardware Security

- **HOT Topic Session on Counterfeit Electronics**, IEEE VLSI Test Symposium (**VTS**), May 2013 (with Prof. Ilia Polian, University of Passau)
- **HOT Topic Session on Smart Silicon**, IEEE VLSI Test Symposium (**VTS**), May 2011 (with LeRoy Windemberg, Freescale Semiconductor)
- **Moderator, Roundtable on Hardware Security and Trust,** IEEE Design & Test Magazine, September/October 2011

Panel and Tutorial Organizer/Moderator

- **Panel Organizer/Moderator**, GomacTech, Quantifiable Assurance: From IPs to SoCs, March 2022
- **Panel Organizer/Moderator**, International Test Conference (**ITC**), Perspectives on the Future of Hardware Security, 2019
- **Panel Moderator**, Chip to PCB Assurance: Detection and Prevention, International Conference on Physical Assurance and Inspection of Electronics (**PAINE**), 2019.
- **Panel Organizer**, AI-Enabled Security Validation and Test, IEEE VLSI Test Symposium (**VTS**), 2019
- **Panel Organizer/Moderator**, Physical Inspection and Attacks: New Frontiers in Hardware Security, International Test Conference (**ITC**), 2018
- **Panel Organizer/Moderator**: Crossroad Between Physical Inspection and Hardware Security, IEEE International Workshop on Physical Attacks and Inspection on Electronics (**PAINE**), San Francisco, June 2018.
- **Tutorial Organizer**: Security of Internet of Things (IoT) and Cyber-Physical Systems (CPS): A Hands-on Approach, Design Automation Conference (DAC), 2018, Presenter: Prof. Yier Jin, University of Florida
- **Fireside Interview** with Edna Conway, CSO, Global Value Chain, Cisco
- **Tutorial Organizer**, DAC, Security of Internet of Things (IoT) and Cyber-Physical Systems (CPS): A Hands-on Approach, **Presenter**: Yier Jin, June 2018
- **Panel Organizer**, AsianHOST, Co-organized by Dr. Yousef Iskander, Technical Lead, Cisco
- **Panel Organizer**, Automotive Safety and Security: The Impending Challenges and Hopes on the Horizon, International Test Conference (**ITC**), 2017, Co-organized by Yervant Zorian, Vice President, Synopsys
- **Panel Organizer**, Test and Security for IoTs, International Test Conference (**ITC**), 2016
- **Panel Organizer**, IEEE International Verification and Security Workshop (**IVSW**), 2016, DFT vs. Security – Is it a Contradiction? How Can we Get the Best of Both World?
- **Panel Organizer and Moderator**, IEEE International Hardware-Oriented Security and Trust (HOST), 2016, IP Protection from Chip-to-System Using Reverse Engineering
- **Panel Organizer**, IEEE International Hardware-Oriented Security and Trust (HOST), 2016, Hardware-based System Security
- **Panel Organizer**, IEEE VLSI Test Symposium (VTS), 2016, Test Opportunities for Secure Hardware
- **Panel Organizer**, Design Automation Conference (DAC), 2013 (**Panel 1**: Advanced Node Reliability: Are we in Trouble?)
- **Panel Organizer**, Design Automation Conference (DAC), 2013 (**Panel 2**: Is Security the New Design Dimension?)
- **Panel Organizer/Moderator**, IEEE Hardware-Oriented Security and Trust (HOST), June 2012
- **Moderator**, Special Session on Smart Silicon, IEEE VLSI Test Symposium (**VTS**), May 2011

- **Panel Moderator**, Title: *Low Power Testing,* IEEE VLSI Test Symposium (**VTS**), May 2011
- **Panel Organizer**, Title: *Test and Diagnosis for Parametric Failures,* Int. Workshop on Defect and Data Driven Testing, (**D3T**), Nov. 2009
- **Panel Organizer**, Title: *Challenges in Test Data Collection and Analysis,* Int. Workshop on Defect and Data Driven Testing, (**D3T**), Oct. 2008
- **Panel Organizer**, Title: *Zero Defect (Zero DPPM): How can we get there?,* Int. Symposium on Defect and Fault Tolerance in VLSI Systems (**DFT**), Oct. 2008
- **Panel Organizer** (with Kee Sup Kim from Intel), Title: *Three Questions to Oracle (Data required for test engineers and researchers in academia)***,** IEEE VLSI Test Symposium (**VTS**), 2006
- **Panel Organizer** (with Hank Walker, Texas A&M University), Title: *Process Variations + Systematic Defects: Can DBT Help?*, International Workshop on Defect-Based Testing (**DBT**), 2007.

Proposal Reviewer/Panelist

- **National Science Foundation (NSF)**
- **Army Research Office (ARO)**
- **Einstein Foundation, Germany**
- **Hong Kong Foundation**
- **Sultanate Oman, Dean of Research**

Membership:

- Fellow, IEEE
- Connecticut Academy of Science and Engineering (CASE)
- Golden Core Member, IEEE Computer Society
- Member, ACM
- Member, ACM SIGDA
- Member, TTTC

Program Committee Membership

- International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2017
- Microprocessor Test and Verification Workshop, 2012-present
- Smart City Security and Privacy (SCSP), 2016
- ASP-DAC, 2016
- EEE International Symposium on Computer Architecture and Digital Design (CADS), 2015
- IEEE Int. Symposium on VLSI Design and Test (VDAT), 2014-2015
- EDAA Outstanding Dissertation, European Design and Automation Association (EDAA), 2014-2015
- IEEE Latin American Test Workshop (LATW), 2015

- USENIX, 2014
- CSI International Symposium on Computer Architecture & Digital Systems (CADS 2017)
- Design Automation Conference (DAC), 2011-2014, 2017
- International Symposium on Quality Electronic Design (ISQED), 2014
- TRUDEVICE Workshop on Test and Fault Tolerance for Secure Devices, 2014
- Design Automation Conference (DAC) Panel Committee, 2013
- IEEE Conference on Very Large Scale Integration (VLSI-SoC), 2012-present
- IEEE CS Annual Symposium on VLSI (ISVLSI), 2012-present
- International Test Conference (ITC)-Asia, 2017-present
- International Test Conference (ITC), 2011-present
- Design, Automation, and Test in Europe (DATE), 2009-2010, 2013, 2016-present
- European Test Symposium (ETS), 2010-present
- IEEE VLSI Test Symposium (VTS), 2009-present
- ACM SIGDA PhD DAC Forum, 2008-2011, 2015
- IEEE Workshop on RTL and High Level Testing (WRTLT), 2009-2011
- ACM Great Lake Symposium on VLSI (GLSVLSI), 2008-present
- International Conference on Communication Theory, Reliability, and Quality of Service (CTRQ), 2008-2013
- IEEE Int. Workshop on Defect Based Testing (DBT), 2005-2010
- Int. Conference on Computer Design (ICCD), 2008-present
- North Atlantic Test Workshop (NATW) 2004-present
- IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT), 2005-present
- International Design and Test Workshop (IDT), 2006-present
- International Symposium on Nanoscale Architectures (NanoArch), 2007-2010
- IEEE Int. On-Line Testing Symposium (IOLTS), 2009
- Int. Workshop on Impact of Low-Power Design on Test and Reliability, 2009-present
- Workshop on Unique Chips and Systems (UCAS), 2009
- IEEE Workshop on Design for Reliability and Variability (DRV), 2009

Session Chair

- International Test Conference (ITC), 2015
- Design Automation Conference, 2015
- DMSMS, 2013
- International Test Conference (ITC), 2013
- Design Automation Conference (DAC), 2012

- Int. Workshop on Current and Defect-Based Testing (DBT), 2005
- Int. Workshop on Current and Defect-Based Testing (DBT'), 2005
- IEEE North Atlantic Test Workshop (NATW), 2006, 2007, 2008, 2009
- International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT), 2006
- Design Automation Conference (DAC), 2007
- International Symposium on Nanoscale Architectures (NanoArch), 2008
- International Test Conference (ITC), 2006, 2008, 2009
- IEEE Workshop on RTL and High Level Testing (WRTLT), 2008
- IEEE VLSI Test Symposium (VTS), 2010
- International Test Conference (ITC), 2013

Session Coordinator

- International Test Conference (ITC), 2011

Training

- MEST Center Training on Hardware Security, 2020 (9 hour teaching)

External Committee Membership

- NDIA Systems Security Engineering Committee

Additional Activities

- Robust Design Program (http://www.robust-designs.com/)
- Journal of Electronic Testing: Theory and Applications (JETTA) Best Paper Review Committee, 2018

Review Activity

- National Science Foundation (NSF)
- Army Research Office (ARO)
- Oman, Sultan Ghaboos University Foundation, Dean of Research
- IEEE Transactions on Computer-Aided Design of Integrated Circuits and Syatems (TCAD)
- IEEE Transactions on Very Large Scale Integration Systems (TVLSI)
- IEEE Transactions on Computers
- ACM Journal on Emerging Technologies in Computing Systems (JETC)
- ACM Transactions on Design Automation of Electronic Devices (TODAES)
- International Journal of Computers and Applications

- IEEE Circuits, Devices & Systems
- IEEE Design & Test of Computers Magazine
- Journal of Low Power Electronics (JOLPE)
- IBM Journal of Research and Developments
- IEEE Communication Magazine
- IEEE International Test Conference (ITC)
- IEEE VLSI Test Symposium (VTS)
- IEEE Asian Test Symposium (ATS)
- IEEE North Atlantic Test Workshop (NATW)
- IEEE Workshop on Defect-Based Testing (DBT)
- IEEE International Conference on Microelectronics (ICM)
- Design Automation Conference (DAC)
- IEEE Symp. on Defect and Fault Tolerance in VLSI Systems (DFT)
- Great Lake Symposium on VLSI (GLS-VLSI)

Publications

Books

1. N. Asadi and M. Tehranipoor, **Materials for Electronics Security and Assurance**, Elsevior, 2022.
2. K. Z. Azar, H. M. Kamali, F. Farahmandi, and M. Tehranipoor, **Understanding Logic Locking**, Springer, 2022.
3. N. Anandakumar, F. Farahmandi, and M. Tehranipoor, **Hardware Security Training, Hands-on!**, Springer 2022.
4. F. Farahmandi, S. Rajendran, and M. Tehranipoor, **CAD for Hardware Security**, Springer, 2022.
5. M. Tehranipoor, N. Vashistha, and F. Farahmandi, **Hardware Security Premitives**, Springer, 2022.
6. M. Tehranipoor, **Emerging Topics in Hardware Security**, Springer, 2021
7. N. Asadi, T. Rahman, and Mark Tehranipoor, **Physical Assurance for Electronic Devices and Systems**, Springer, 2021.
8. S. Bhunia and M. M. Tehranipoor, **Hardware Security: A Hands-on Learning Approach**, Elsevier, Morgan Kaufmann imprint, 2018.
9. S. Bhunia and M. Tehranipoor, **The Hardware Trojan War: Attacks, Myths, and Defenses**, Springer, Jan 2018.
10. M. Tehranipoor, D. Forte, G, Rose, and S. Bhunia, **Security Opportunities in Nano Devices and Emerging Technologies**, CRC Press, Dec. 2017.
11. P. Mishra, S. Bhunia, and M. Tehranipoor, **Hardware IP Security and Trust: Validation and Test**, Springer, Jan 2017.
12. D. Forte, S. Bhunia, and M. Tehranipoor, **Hardware Protection through Obfuscation**, Springer, Jan 2017.

13. M. Tehranipoor, U. Guin, and D. Forte, **Counterfeit Integrated Circuits: Detection and Avoidance,** Springer, Dec. 2014

14. M. Tehranipoor, H. Salmani, and X. Zhang, **IC Authentication: Hardware Trojan and Counterfeit Detection**, Springer, Jan. 2014.

15. M. Tehranipoor and C. Wang, **Introduction to Hardware Security and Trust**, Springer, June 2011.

16. M. Tehranipoor, K. Peng, and K. Chakrabarty, **High-Quality Test and Diagnosis for Small Delay Defects**, Springer, July 2011.

17. M. Tehranipoor, **Emerging Nanotechnologies: Test, Defect Tolerance, and Reliability**, Springer, Dec., 2007.

18. M. Tehranipoor and N. Ahmed, **Nanometer Technology Designs: High-Quality Delay Tests**, Springer, Nov. 2007.

Book Chapters

1. M. M. Hossain, F. Rahman, F. Farahmandi, and M. Tehranipoor, **Firmware Protection**, in Emerging Topics in Hardware Security, Springer, 2021.

2. M. M. Hossain, F. Rahman, F. Farahmandi, and M. Tehranipoor, **Software Security with Hardware in Mind**, in Emerging Topics in Hardware Security, Springer, 2021.

3. A. Nahiyan, M. He, Jungmin Park, and M. Tehranipoor, **CAD for Side-Channel Assessment**, in Emerging Topics in Hardware Security, Springer, 2021.

4. M. R. Makki, N. Pundir, M. Tehranipoor, and F. Farahmandi, **Security Assessment of High-Level Synthesis**, in Emerging Topics in Hardware Security, Springer, 2021.

5. P. Cui, U. Guin, and M. Tehranipoor, **Trillion Sensors Security**, in Emerging Topics in Hardware Security, Springer, 2021.

6. H. Wang, S. Chen, S. Islam Sami, F. Rahman, and M. Tehranipoor, **Digital Twin with a Perspective from Manufacturing Industry**, in Emerging Topics in Hardware Security, Springer, 2021.

7. M. Rahman and M. Tehranipoor, **Blockchain-Enabled Electronics Supply Chain Assurance**, in Emerging Topics in Hardware Security, Springer, 2021.

8. O. Arias, F. Rahman, M. Tehranipoor, and Yier Jin, "**IoT Device Authentication: From a Cross-Layer Perspective**" 2020.

9. Q. Shi, D. Forte, and M. Tehranipoor, "**Deterrent Approaches Against Hardware Trojan Insertion,"** in Hardware Trojan War, Springer, Jan. 2018.

10. S. Bhunia, A. Prasad Deb Nath, and M. Tehranipoor, "**Introduction to Hardware Trojans**," in Hardware Trojan War, Springer, Jan. 2018.

11. F. Rahman, A. Prasad Deb Nath, D. Forte, S. Bhunia, and M. Tehranipoor, "**Nano CMOS Logic-Based Security Primitive**," in Security Opportunities in Nano Devices and Emerging Technologies, CRC Press, Dec. 2017.

12. H. Shen, F. Rahman, M. Tehranipoor, and D. Forte, "**Carbon-Based Novel Devices for Hardware Security**," in Security Opportunities in Nano Devices and Emerging Technologies, CRC Press, Dec. 2017.

13. F. Rahman, A. Prasad Deb Nath, S. Bhunia, D. Forte, and M. Tehranipoor, "**Composition of Physical Unclonable Functions: From Device to Architecture**," in Security Opportunities in Nano Devices and Emerging Technologies, CRC Press, Dec. 2017.

14. B. Shakya, X. Xu, N. Asadi, M. Tehranipoor, and D. Forte, "**Leveraging Circuit Edit for Low-Volume Trusted Nanometer Fabrication**," in Security Opportunities in Nano Devices and Emerging Technologies, CRC Press, Dec. 2017.

15. U. Guin and M. Tehranipoor, **Obfuscation and Encryption for Securing Semiconductor Supply Chain** in Hardware Protection through Obfuscation, Jan 2017.

16. Q. Shi, K. Xiao, D. Forte, and M. Tehranipoor, **Obfuscated Built-in Self Authentication** in Hardware Protection through Obfuscation, Jan 2017.

17. T. Rahman, D. Forte, M. Tehranipoor, **Protection of Assets from Scan Chain Vulnerabilities through Obfuscation** in Hardware Protection through Obfuscation, Jan 2017.

18. Z. Guo, M. Tehranipoor, and F. Forte, **Permutation based Obfuscation** in Hardware Protection through Obfuscation, Jan 2017.

19. B. Shakya, M. Tehranipoor, S. Bhunia, and F. Forte, **Introduction to Hardware Obfuscation: Motivation, Methods and Evaluation** in Hardware Protection through Obfuscation, Jan 2017.

20. Q. Shi, D. Forte and M. Tehranipoor, **Analyzing Circuit Layout to Probing Attack**, in Hardware IP Security and Trust: Validation and Test, Jan 2017.

21. A. Nahiyan and M. Tehranipoor, **Code Coverage Analysis for IP Trust Verification**, in Hardware IP Security and Trust: Validation and Test, Jan 2017.

22. H. Salmani and M. Tehranipoor, **Digital Circuits Vulnerability to Hardware Trojans**, in Hardware IP Security and Trust: Validation and Test, Jan 2017.

23. A. Nahiyan, K. Xiao, D. Forte, and M. Tehranipoor, **Security Rule Check**, in Hardware IP Security and Trust: Validation and Test, Jan 2017.

24. P. Mishra, S. Bhunia, and M. Tehranipoor, **Security and Trust Vulnerabilities in Third-Party IPs**, in Hardware IP Security and Trust: Validation and Test, Jan 2017.

25. P. Mishra, S. Bhunia, and M. Tehranipoor, **The Future of Trustworthy Design**, in Hardware IP Security and Trust: Validation and Test, Jan 2017.

26. K. Xiao, D. Forte, and M. Tehranipoor, **Circuit Timing Signature (CTS) for Detection of Counterfeit Integrated Circuits,** in Secure System Design and Trustable Computing, by *Chip Hong Chang and Miodrag Potkonjak*, 2014.

27. M. Tehranipoor and J. Lee, **Protecting IPs Against Scan-Based Side-Channel Attacks**, in *Introduction to Hardware Security and Trust*, Springer, March 2011.

28. M. Tehranipoor and J. Lee, **Protecting IPs Against Scan-Based Side-Channel Attacks**, in *Introduction to Hardware Security and Trust*, Springer, March 2011.

29. M. Tehranipoor, **Built-In Self-Test and Defect Tolerance for Molecular Electronics-Based NanoFabrics**, in *Robust Nano-Computing* by Chao Huang, Springer 2010.

30. M. Tehranipoor and B. Sunar, **Hardware Trojan Horses**, in *Towards Hardware Intrinsic Security: Foundation and Practice*, by Ahmad R. Sadeghi, Springer, 2010.

31. M. Tehranipoor and N. Ahmed, **Faster-than-at-speed Test for Detecting SDDs**, in *Testing for Small-Delay Defects in Nanoscale CMOS Integrated Circuits* by S. Sandeep Goel and K. Chakrabarty, 2010.

32. K. Peng, M. Yilmaz, and M. Tehranipoor, **Path-Grading Considering Layout, Process Variations, and Crosstalk**, in *Testing for Small-Delay Defects in Nanoscale CMOS Integrated Circuits* by S. Sandeep Goel and K. Chakrabarty, 2010.

33. M. Kassab and M. Tehranipoor, **Test for Power Management Systems**, in Low Power Testable Design by P. Girard, N. Nicolici, and X. Wen, Springer, 2009.

34. M. Tehranipoor, **Test and Defect Tolerance for Nanoscale Crossbar-based Circuits**, in *System on Chip Test Architectures: Nanometer Design for Testability*, by L.T. Wang, Charles Stroud and Nur Touba, Elsevier, Target Publication Date: Oct. 2007.

35. M. Tehranipoor and R. Rad, **Defect Tolerance for Reconfigurable Nanoscale Architectures**, in *Emerging Nanotechnologies: Test, Defect Tolerance, and Reliability,* by M. Tehranipoor, Springer, 2007.

Patents

Granted:

1. **Embedded ring oscillator network for integrated circuit security and threat detection**, 2014, M. Tehranipoor, X. Wang, X. Zhang, US 8850608 B2, WO 2012122309 A3

2. **Methods and Systems for Hardware Piracy Prevention**, 2015, M. Tehranipoor and N. Tuzzio, 9071428

3. **Methods and Systems for Preventing Hardware Trojan Insertion**, 2015, M. Tehranipoor and K. Xiao, 92185061

4. **Photon-Counting Security Tagging and Verification Using Optically Encoded QR Codes**, B. Javidi, A. Markman, and M. Tehranipoor, US20150295711 A1

5. **Vanishing Via for Hardware IP Protection Against Reverse Engineering**, May 2019, S. Bhunia, M. Tehranipoor, D. Forte, N. Asadi, and H. Shen, 10283459

6. **Unclonable environmentally-sensitive chipless RFID tag with a plurality of slot resonators**, Jan 2019, Mark Tehranipoor, Kun Yang, Haoting Shen, and Domenic Forte, 10181065

7. **Layout-Driven Method to Assess Vulnerability of ICs to Microprobing Attacks**, 2020, M. Tehranipoor, D. Forte, N. Asadi, and Q. Shi, U.S. Patent No. 10573605

8. **Cross-registration of Unclonable RFID Tags**, Feb 2021, K. Yan, U. Boreto, D. Forte, H. Shen, and M. Tehranipoor, 10929741

9. **Circuit Edit and Obfuscation for Trusted Chip Fabrication**, June 2021, M. Tehranipoor, N. Asadi, D. Forte, and B. Shakya, 11030348

10. **Hardware Trojan Scanner,** June 2021, M. Tehranipoor, N. Asadi, D. Woodard, H. Shen, M. T. Rahman, and N. Vashistha, 11030737

11. **Covert Gates to Protect Gate-Level Semiconductors**, July 2021, M. Tehranipoor, D. Forte, B. Shakya, H. Shen, 11056448

12. **Prevention of Front-Side Probing Attacks**, July 2021, H. Wang. Q. Shi, H. Chen, D. Forte, and M. Tehranipoor, 11087058

13. **Protecting Obfuscated Circuits Against Attacks that Utilize Test Infrastructures,** January 2022, M. Tehranipoor, A. Nahiyan, D. Forte, S. Rahman, F. Farahmandi, and F. Rahman, 11222098

14. **Hardware Trojan Detection Through Information Flow Security Verification**, 2022, A. Nahyan, D. Forte, M. Tehranipoor, 11270002

15. **Image Processing for Printed Circuit Board Component Detection**, 2022, N. Asadi, M. Azhagan, M. Sathiaseelan, and M. Tehranipoor, 11308605

Submitted:

16. **Detection of Recovered Integrated Circuits**, 2014, M. Tehranipoor, N. Tuzzio, and X. Zhang, US 2014/0340112 A1, Publication number: 20140103344 (Application)

17. **Methods and Systems for Test Power Analysis**, 2014, M. Tehranipoor and W. Zhao, US20140365148 A1, Publication number: 20140365148 (Application)

18. **A Comprehensive Framework for Protecting Intellectual Property in the Semiconductor Industry**, 2016, M. Tehranipoor, D. Forte, and U. Guin (Application)

19. **Side-channel Leakage Analysis for Power, EM, Fault, and Timing**, S. Bhunia, M. Tehranipoor, and Jungmin Park

20. **Micro-probing Vulnerability Analysis**, M. Tehranipoor, D. Fote and Q. Shi

21. **SecureHDL Framework for Vulnerability Analysis**, S. Bhunia, G. Contreras, D. Capecci, H. Wang, and M. Tehranipoor

22. **Hardware Hacking Security Education Platform**, UF#17191 entitled, Swarup Bhunia, Shuo Yang, Mark Tehranipoor

23. **CAD Framework for Power-Side Channel Vulnerability Assessment**, M. Tehranipoor, A. Nahiyan, D. Forte, and J. Park

24. **Tampering, Snooping, and EM Attack Proof Coating on PCB**, Haoting Shen, Christian A. Zorman, Philip X.-L. Feng, Mark Tehranipoor, and Swarup Bhunia

25. **Hardness Amplification of Physical Unclonable Functions (PUFS)**, Fatemeh Ganji, Shahin Tajik, Jean-Pierre Seifert, Domenic Forte, Mark M. Tehranipoor, Provisional Appl. No. 62/836,829, filed April 22, 2019, A&B Ref. 049648/529675, UF Ref. T17664

26. **Techniques for PCB Component Detection (aka. Validating Component Estimates using Angled Light Sources)**, Nathan Jessurun and Olivia Paradis, M. Tehranipoor, and N. Asadi, A&B Ref. 049648/543022, UF Ref. T18041

27. **Nanopyramid: An Optical Scrambler Against Probing Attacks**, H. Shen. D. Forte, N. Asadi, and M. Tehranipoor, UF T17573

28. **Systems and Methods for Laser Probing For Hardware Trojan Detection**, A. Stern, S. Tajik, F. Farahmandi, and M, Tehranipoor, A&B Ref. 049648/534021, UF Ref. T18013US001

29. **In-Situ Thickness Measurement of Die Silicon Using Voltage Imaging**, N. Asadi, O. Paradi, N. Varshney, and M. Tehranipoor, T18042, 2020.

30. **SeRFI: Secure Remote FPGA Initialization in an Untrusted Environment**, M. Tehranipoor, A. Duncan, A. Nahiyan, F. Rahman, G. Skipper, M. Swany, A. Lukefahr, UF# - INV-200385, 2020.

31. **Knowledge-based Object Localization in Scanning Electron Microscopy Images for Hardware Assurance**, N. Asadi, H. Li, N. Vashistha, R. Wilson, D. Woodard, and M. Tehranipoor, 2021.

32. **Concealing Logic**, N. Asadi, M. T. Rahman, S. Tajik, and M. Tehranipoor, 2020

33. **He-Ion Imaging for Accurate Scanning**, N. Asadi, O. Paradis, N. Varshney, and M. Tehranipoor, 2020.

34. **Validating Component Estimates using Angled Light Sources**, N. Asadi, N. Jessurun, O. Paradis, and M. Tehranipoor, 2020.

35. **BODIFT: An Automated Framework for Exploitable Buffer Overflow Detection by Information Flow Tracking**, Farimah Farahmandi, Muhammad Monir Hossain, Fahim Rahman, Mark Tehranipoor, INV-210132, 2020

36. **Hardware-Assisted Dynamic Instruction Obfuscation for Firmware Protection**, Farimah Farahmandi, Muhammad Monir Hossain, Fahim Rahman, Mark Tehranipoor, INV-200422, 2020

37. **SoFI: Security Property-Driven Vulnerability Assessments of ICs Against Fault-Injection Attacks**, Farimah Farahmandi, Mark Tehranipoor, Huanyu Wang, INV-200394, 2020.

38. **RTL-PSC-Sim: RTL simulation-based power side channel analysis**, Farimah Farahmandi, Nitin Pundir, Fahim Rahman, Mark Tehranipoor, INV-200381, 2020.

39. **Hardware Deprocessing using Voltage Imaging for Hardware Assurance**, M. Tehranipoor, N. Asadi, O. P. Paradis, and N. Vashistha, Publication Number: 20210264082, 2021

40. **PINPOINT: An SMD Pin Localization Algorithm**, N. Asadi, N. Jessurun, J. Hsrrison, and M. Tehranipoor, T18756, 2022.

41. **Knowledge-based Object Localization in Images for Hardware Assurance**, M. Tehranipoor, N. Asadi, Nidish Vashistha, D. Woodard, H. Lu, R. Wilson, Publication Number: 20220130031, 2022

42. **System and Method for Computer Inspection of Surface-Mount Devices**, N. Asadi, M. Tehranipoor, N. Jessurun, J. Harrison, T18756US001, 2022

Editorial Notes

1. N. Asadi and M. Tehranipoor, **Physical Assurance and Inspection of Electronics**, Springer Journal on Hardware and Systems Security (HaSS), 2020.
2. C. H. Chang, M. van Dijk, Ul. Rührmair, M. Tehranipoor, **Emerging Attacks and Solutions for Secure Hardware in the Internet of Things,** IEEE Transactions on Dependable and Secure Computing (TDSC), 2019.
3. S. Bhunia and M. Tehranipoor, First Ever Issue of HaSS Journal, Journal of Hardware and Systems Security (HaSS), March 2017.
4. S. Hu, Y. Jin, K. Heffner, and M. Tehranipoor, **Hardware/Software Cross-Layer Technologies for Trustworthy and Secure Computing**, IEEE TMSCS, 2016.
5. I. Polian and M. Tehranipoor, Special Issue on **Hardware Security**, Guest Editorial, IET Computers and Digital Techniques, 2015.
6. M. Tehranipoor and F. Koushanfar, "**Hardware Security and Trust**," Guest Editorial, IEEE Computer Society Computing Now (CN), September 2010.
7. M. Tehranipoor and F. Koushanfar, "**Confronting the Hardware Trustworthiness Problem**," Guest Editorial, IEEE Design and Test of Computers, Jan 2010.
8. M. Tehranipoor and K. Butler, "**IR-Drop and Power Supply Noise Effects on Design and Test of Very Deep Submicron Designs**," Guest Editorial, IEEE Design and Test of Computers, July 2007.
9. M. Tehranipoor, "**Test, Defect Tolerance and Reliability of Nanoscale Devices,**" Guest Editorial, Journal of Electronic Testing: Theory and Applications (**JETTA**), Vol. 23, No. 2/3, pp. 115-116, June 2007.

Edited Conference Proceedings

1. S. Menon and M. Tehranipoor, Proceedings for IEEE Defect-Based Testing (**DBT**) Workshop, 2007.
2. N. Ahmed and M. Tehranipoor, Proceedings for IEEE Defect and Data Driven Testing (**D3T**) Workshop, 2008.
3. N. Ahmed and M. Tehranipoor, Proceedings for IEEE Defect and Data Driven Testing (**D3T**) Workshop, 2009.
4. D. Gizopolous, M. Tehranipoor, S. Tragoudas, Proceedings for IEEE Symposium on Defect and Fault Tolerance in VLSI Systems (**DFTS**), 2008.

5. D. Gizopolous, M. Tehranipoor, S. Tragoudas, Proceedings for IEEE Symposium on Defect and Fault Tolerance in VLSI Systems (**DFTS**), 2009.

6. J. Plusquellic and M. Tehranipoor, Proceedings for IEEE Symposium on Hardware-Oriented Security and Trust (**HOST**), 2008.

7. J. Plusquellic and M. Tehranipoor, Proceedings for IEEE Symposium on Hardware-Oriented Security and Trust (**HOST**), 2009.

Journal Papers

1. N. Vashistha, M. L. Rahman, S. Haque, A. Uddin, S. Islam Sami, A. Mazumder, P/ Calzada, F. Farahmandi, N. Asadi, F. Rahman, and M. Tehranipoor, "**ToSHI - Towards Secure Heterogeneous Integration: Security Risks, Threat Assessment, and Assurance**," IACR Cryptology ePrint Archive, August 2022, https://eprint.iacr.org/2022/984.pdf

2. S. Dey, J. Park, N. Pundir, D. Saha, A. mazumdar, D. Mehta, N. Asadi, F. Rahman, F. Farahmandi, and M. Tehranipoor, "**Secure Physical Design**," IACR Cryptology ePrint Archive, May 2022, https://eprint.iacr.org/2022/891

3. D. Mehta, J. True, O. Dizon-Paradis, N. Jessurun, D. Woodard, N. Asadi, and M. Tehranipoor, "**FICS PCB X-ray: A Dataset for Automated Printed Circuit Board Inter-Layers Inspection**," IACR Cryptology ePrint Archive, May 2022. https://eprint.iacr.org/2022/924

4. L. Biswas, L. Lavdas, T. Rahman, M. Tehranipoor, and N. Asadi, "**On Backside Probing Techniques and their Emerging Security Threats**," IEEE Design & Test of Computers (**D&T**), 2022.

5. M. M. Hossain, N. Vashistha, J. Allen, M. Allen, F. Farahmandi, F. Rahman, and M. Tehranipoor, "**Thwarting Counterfeit Electronics by Blockchain**," IEEE Blockchain, 2022.

6. N. Pundir, J. Park, F. Farahmandi, and M. Tehranipoor, "**Power Side-Channel Leakage Assessment Framework at Register-Transfer Level**," IEEE Transactions on VLSI (**TVLSI**), 2022.

7. J. Park, N. Anandakumar, D. Saha, D. Mehta, N. Pundir, F. Rahman, F. Farahmandi, and M. Tehranipoor, "**PQC-SEP: Power Side-channel Evaluation Platform for Post-Quantum Cryptography Algorithms**," IACR Cryptology ePrint Archive, May 2022, https://eprint.iacr.org/2022/527.pdf

8. K. Z. Azar, M. M. Hossain, A. Vafaei, H. Al Sheikh, N. Mondol, F. Rahman, M. Tehranipoor, and F. Farahmandi, "**Fuzz, Penetration, and AI Testing for SoC Security Verification: Challenges and Solutions**," IACR Cryptology ePrint Archive, March 2022, https://eprint.iacr.org/2022/394.pdf

9. Y. Bai, A, Stern, J. Park, M. Tehranipoor, and D. Forte, "**RASCv2: Enabling Remote Access to Side-Channels for Mission Critical and IoT Systems**," ACM Transactions on Design Automation of Electronic Systems (**TODAES**), 2022.

10. Y. Bai, J. Park, M. Tehranipoor, and D. Forte, "**Real-time Instruction-level Verification of Remote IoT/CPS Devices via Side-Channels**," Springer Discover Internet of Things, 2022.

11. H. A. Shaikh, M. B. Monjil, S. Chen, F. Farahmandi, N. Asadi, M. Tehranipoor, and F. Rahman, "**Digital Twin for Secure Semiconductor Lifecycle Management: Prospects and Applications**," IACR Cryptology ePrint Archive, March 2022, https://eprint.iacr.org/2022/258.pdf.

12. H. M. Kamali, K. Z. Azar, F. Farahmandi, and M. Tehranipoor, "**Advances in Logic Locking: Past, Present, and Prospects**," IACR Cryptology ePrint Archive, Feb. 2022, https://eprint.iacr.org/2022/260.pdf

13. N. N. Anandakumar, M. S. Rahman, M. M. M. Rahman, R. Kibria, U. Das, F. Farahmandi, F. Rahman, M. Tehranipoor, "**Rethinking Watermark: Providing Proof of IP Ownership in Modern SoCs**," IACR Cryptology ePrint Archive, Jan. 2022, https://eprint.iacr.org/2022/092.pdf

14. S. Khan, C. Xi, A. Khan, T. Rahman, M. Tehranipoor, and N. Asadi, “**Secure Interposer-Based Heterogenegous Integration**,” IEEE Design & Test of Computers (**D&T**), 2022.

15. N. Vashishta, M M. Hossain, R. Shahriar, F. Rahman, F. Farahmandi, and M. Tehranipoor, “**eChain: A Blockchain-enabled Ecosystem for Electronic Device Authenticity Verification**,” IEEE Transactions on Computer Electronics (**TCE**), Vol. 68, Issue 1, pp. 23-37, 2022.

16. J. He, X. Guo, M. Tehranipoor, A. Vassilev, and Y. Jin, “**EM Side Channel in Hardware Security: Attacks and Defenses**,” IEEE Design & Test of Computers (**D&T**), Vol. 39, Issue 2, April 2022.

17. N. Pundir, S. Aftabjahani, R. Cammarota, M. Tehranipoor, and F. Farahmandi, “**Analyzing Security Vulnerabilities Induced by High-level Synthesis**,” ACM Journal of Emerging Technologies in Computing Systems (**JETC**), Vol. 18, Issue 3, July 2022.

18. B. Ahmed, K. Bepary, N. Pundir, M. Borza, O. Raikhman, A. Garg, A. Cron, M. Abdel-Moneum, F. Farahmandi, F. Rahman, and M. Tehranipoor, “**Quantifiable Assurance: From IPs to Platforms**,” IACR Cryptology ePrint Archive, Dec. 2021, https://eprint.iacr.org/2021/1654.pdf

19. A. Stern, H. Wang, F. Rahim, F. Farahmandi, and M. Tehranipoor, “**ACED-IT: Assuring Confidential Electronic Design against Insider Threat in a Zero Trust Environment**,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems of Integrated Circuits and Systems (**TCAD**), Nov. 2021.

20. F. Rahman, F. Farahmandi, and M. Tehranipoor, “**An End-to-End Bitstream Tamper Attack Against Flip-chip Package**,” IACR Cryptology ePrint Archive, Nov. 2021, https://eprint.iacr.org/2021/1542.pdf

21. B. Park, D. Forte, M. Tehranipoor, and N. Maghari, “**A Metal-Via Resistance Based Physical Unclonable Function with Backend Incremental ADC**,” IEEE Transactions on Circuits and Systems I (**TCAS-I**), Vol. 68, Issue 11, pp. 4700-4709, November 2021.

22. N. Farzana, F. Farahmandi, and M. Tehranipoor, “**SoC Security Properties and Rules**,” IACR Cryptology ePrint Archive, Aug. 2021, https://eprint.iacr.org/2021/1014.pdf.

23. N. Vashishtha, H. Lu, Q. Shi, D. Woodard, N. Asdi, and M. Tehranipoor, “**Detecting Hardware Trojans using Combined Self Testing and Imaging**,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**), July 2021.

24. N. N. Anandakumar, M. S. Hashmi and M. Tehranipoor, “**FPGA-based Physical Unclonable Functions: Comprehensive Overview of Theory and Architectures**". Integration, the VLSI Journal, Elsevier, pp. 175-194, November 2021.

25. N. Pundir, F. Rahman, F. Rahman, and M. Tehranipoor, “**What is All the FaaS About? Remote Exploitation of FPGA-as-a-Service Platforms**,” IACR Cryptology ePrint Archive, June 2021, https://eprint.iacr.org/2021/746.

26. F. Ganji, U. Boreto, R. Wilson, M. T. Rahman, M. Azhagan, N. Asadi, M. Tehranipoor, D. Woodard, and D. Forte, “**Hardware Trust and Assurance through Reverse Engineering: A Tutorial and Outlook from Image Analysis and Machine Learning Perspective**,” ACM Journal of Emerging Technologies in Computing Systems (**JETC**), Vol. 17, Issue 4, pp. 1-53, October 2021.

27. J. Harrison, N. Asadi, and M. Tehranipoor, “**On Malicious Implants in PCBs Throughout the Supply Chain**,” VLSI Integration Journal, Vol. 79, pp. 12-22, March 2021.

28. H. Wang, H. Li, F. Rahman, M. Tehranipoor, and F. Farahmandi, “**SoFI: Security Property-Driven Vulnerability Assessments of ICs Against Fault-Injection Attacks**,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems of Integrated Circuits and Systems (**TCAD**), Vol. 41, Issue 3, pp. 452-465, 2021.

29. M. T. Rahman, N. F. Dipu, D. Mehta, S. Tajik, M. Tehranipoor, and N. Asadi, "**Concealing-Gate: Optical Contactless Probing Resilient Design**," ACM Journal of Emerging Technologies in Computing Systems (**JETC**), Vol. 17, Issue 3, pp. 1-25, July 2021.

30. M. S. Rahman, A. Nahiyan, F. Rahman, S. Fazzari, K. Plaks, F. Farahmandi, D. Forte, and M. Tehranipoor, "**Security Assessment of Dynamically Obfuscated Scan Chain Against Oracle-Guided Attacks**," ACM Transactions on Design Automation of Electronic Systems (**TODAES**), Vol. 26, Issue 4, March 2021.

31. D. Mehta, H. Lu, O. Paradis, M. Azhagan, T. Rahman, Y. Iskander, Praveen Chawla, D. Woodard, M. Tehranipoor, and N. Asadi, "**The Big Hack Explained: Detection and Prevention of PCB Supply Chain Implants**," ACM Journal of Emerging Technologies in Computing Systems (**JETC**), Vol. 16, Issue 4, Aug. 2020.

32. M. Alam, A. Nahiyan, M. Sadi, D. Forte, and M. Tehranipoor, "**Soft-HaT: Software-based Silicon Reprogramming for Hardware Trojan Implementation**," ACM Transactions on Design Automation of Electronic Systems (**TODAES**), Vol. 25, No. 4, June 2020.

33. F. Ganji, et. al., "**Rock'n'roll PUFs: Crafting Provably Secure PUFs from Less Secure Ones**," Journal of Cryptographic Engineering (**JCEN**), May 2020.

34. J. Park, S. Cho, T. Lim, and M. Tehranipoor, "**QEC: A Quantum Entropy Chip and Its Applications**," IEEE Transactions on VLSI (**TVLSI**), Vol. 28, Issue 6, pp. 1471-1484, June 2020.

35. A. Nahiyan, J. Park, M. He, Y. Iskander, F. Farahmandi, and M. Tehranipoor, "**SCRIPT: A CAD Framework for Power Side-channel Vulnerability Assessment using Information Flow Tracking and Pattern Generation**," ACM Transactions on Design Automation of Electronic Systems (**TODAES**), Vo. 25, issue 3, 2020.

36. Y. Yang, Z. Duan, and M. Tehranipoor, "**Identify Spoofing Attack of In-vehicle CAN Bus Based on Deep Features of ECU Fingerprint Signal**," Smart Cities, Vol. 3, No. 1, pp. 17-30, 2020.

37. M. T. Rahman, M. S. Rahman, H. Wang, S. Tajik, W. Khalil, F. Farahmandi, D. Forte, N. Asadi, and M. Tehranipoor, "**Defense-in-Depth: A Recipe for Logic Locking to Prevail**," Integration, the VLSI Journal, Vol. 72, pp. 39-57, May 2020.

38. Z. Guo, M. Tehranipoor, and D. Forte, "**Permutation Network De-obfuscation: A Delay-based Attack and Countermeasure Investigation**," ACM Journal on Emerging Technologies in Computing Systems (**JETC**), Vol. 16, No. 2, Jan. 2020.

39. H. Wang, Q. Shi, D. Forte, and M. Tehranipoor, "**A Physical Design Flow against Front-side Probing Attacks by Internal Shielding**," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**), Vol. 39, No. 10, pp. 2152-2165, Oct. 2020.

40. A. Stern, J. Ulberto, Fahim Rahman, D. Forte, and M. Tehranipoor, "**EMFORCED: EM-Based Fingerprinting Framework for Remarked and Cloned Counterfeit IC Detection using Machine Learning Classification**," IEEE Transactions on VLSI (**TVLSI**), Vol. 28, No. 2, pp. 363-375, Feb. 2020.

41. B. Shakya, X. Xu, M. Tehranipoor, D. Forte, "**CAS-Lock: A Security-Corruptibility Trade-off Resilient Logic Locking Scheme**," Transactions on Cryptographic Hardware and Embedded Systems (**TCHES**), pp. 175-202, 2020.

42. N. Pundir, M. Tehranipoor, and F. Rahman, "**RanStop: A Hardware-Assisted Runtime Crypto-Ransomeware Detection Technique**," 2020, arXiv, https://arxiv.org/abs/2011.12248

43. B. Shakya, X. Xu, M. Tehranipoor, and D. Forte, "**Defeating CAS-Unlock**," IACR Cryptology ePrint Archive, 2020, https://eprint.iacr.org/2020/324.pdf

44. H. Lu, D. Mehta, O. Paradis, N. Asadizanjani, M. Tehranipoor, and D. L. Woodard, "**FICS-PCB: A Multi-Modal Image Dataset for Automated Printed Circuit Board Visual Inspection**," https://eprint.iacr.org/2020/366, IACR Cryptology ePrint Archive, 2020.

45. L. Yu, X. Wang, F. Rahman, and M. Tehranipoor, "**Interconnect-based PUF with Signature Uniqueness Enhancement**," IEEE Transactions on VLSI (**TVLSI**), vol. 28, No. 2, pp. 339-352, Feb. 2020.

46. T. Hoque, K. Yang, R. Karam, S. Tajik, D. Forte, M. Tehranipoor, and S. Bhunia, "**Hidden in Plaintext: An Obfuscation-based Countermeasure against FPGA Bitstream Tampering Attacks**," ACM Transactions on Design Automation of Electronic Systems (**TODAES**), Vol. 25, Nov. 1, pp. 1-32, Nov. 2019.

47. J. Park. F. Rahman, A. Vassilev, D. Forte, and M. Tehranipoor, "**Leveraging Side Channel Information for Disassembly and Security**," ACM Journal on Emerging Technologies in Computing Systems (**JETC**), No. 6, Dec. 2019.

48. M. T. Rahman, S. Tajik, M. S. Rahman, M. Tehranipoor and N. Asadizanjani, "**The Key is Left under the Mat: On the Inappropriate Security Assumption of Logic Locking Schemes,**" https://eprint.iacr.org/2019/719, 2019 , IACR Cryptology ePrint Archive, 2019

49. M Tanjidur Rahman, M Sazadur Rahman, Huanyu Wang, Shahin Tajik, Waleed Khalil, Farimah Farahmandi, Domenic Forte, Navid Asadizanjani, Mark Tehranipoor, "**Defense-in-Depth: A Recipe for Logic Locking to Prevail**," https://arxiv.org/abs/1907.08863, 2019

50. U. Guin, N. Asadi, and M. Tehranipoor, "**Standards for Hardware Security**," Mobile Computing and Communications, vol. 23, issue 1, pp. 5-9, March 2019.

51. Y. Han, X. Wang and M. Tehranipoor, "**System-Level Counterfeit Detection Using On-Chip Ring Oscillator Array**," IEEE Transactions on VLSI (**TVLSI**), Vol. 27, Issue 12, pp. 2884-2896, Dec. 2019.

52. M. Alam, M. Tehranipoor, and D. Forte, "**Recycled FPGA Detection Using Exhaustive LUT Path Delay Characterization and Voltage Scaling**," IEEE Transactions on VLSI (**TVLSI**), vol. 27, pp. 2897-2910, Dec. 2019.

53. B. Shakya, H. Chen, M. Tehranipoor, and D. Forte, "**Covert Gates: Protecting Integrated Circuits with Undetectable Camouflaging**," Transactions on Cryptographic Hardware and Embedded Systems (**TCHES**), 86-118, 2019.

54. N. Karimian, D. Woodard, M. Tehranipoor, and D. Forte, "**Unlock Your Heart: Next Generation Biometric in Resource-Constrained Healthcare Systems and IoT**," IEEE Access, Vol. 7, Issue 1, pp. 49135-49149, Dec. 2019.

55. Q. Shi, M. Tehranipoor, and D. Forte, "**Obfuscated Built-In Self-Authentication with Secure and Efficient Wire-Lifting**," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**), Vol. 38, Issue 11, 1981-1994, Nov. 2019.

56. H. Wang, Q. Shi, D. Forte, and M. Tehranipoor, "**Probing Assessment Framework and Evaluation of Anti-probing Solutions**," IEEE Transactions on VLSI (**TVLSI**), Vol. 7, Issue 6, pp. 1239-1252, June 2019.

57. X. Xu, F. Rahman, B. Shakya, A. Vassilev, D. Forte, and M. Tehranipoor, "**Electronic Supply Chain Integrity Enabled by Blockchain**," ACM Transactions on Design Automation of Electronic Systems (**TODAES**), 2019.

58. U. Botero, M. Tehranipoor, and D. Forte, "**Upgrade/Downgrade: Efficient and Secure Legacy Electronic System Replacement**," IEEE Design & Test of Computers (**D&T**), Vol. 36, Issue 1, Jan 2019.

59. F. Ganji, D. Forte, N. Asadizanjani, M. Tehranipoor, D. Woodard, "**The power of IC Reverse Engineering for Hardware Trust and Assurance**", Electronic Device Failure Analysis (**EDFA**), May 2019.

60. K. Yang, U. Botero, H. Shen, D. Woodard, D. Forte, "**UCR: An Unclonable Environmentally-Sensitive Chipless RFID Tag for Protecting Supply Chain**," ACM Transactions on Design Automation of Electronic Systems (**TODAES**), Vol. 23, No. 6, Dec. 2018.

61. X. Xu, S. Keshavarz, D. Forte, M. Tehranipoor, and D. Holcomb, "**Bimodal Oscillation as a Mechanism for Automotive Majority Voting in PUFs**," IEEE Transactions on VLSI (**TVLSI**), Vol. 26, No. 11, Nov. 2018.

62. N. Karimian, Z. Guo, F. Tehranipoor, D. Woodard, M. Tehranipoor, and D. Forte, "**Noise Aware Biometric Key Generation in Resource-Constrained Systems and IoT**," IEEE Transactions on Signal Processing, 2018.

63. D. Zhang, X. Wang, T. Rahman, and M. Tehranipoor, "**An On-Chip Dynamically-Obfuscated Wrapper for Protecting Supply Chain Against IP and IC Piracy**," IEEE Transactions on VLSI (**TVLSI**), Vol. 26, Issue 11, 2018.

64. S. Amir, B. Shakya, X. Xu, Y. Jin, S. Bhunia, M. Tehranipoor, D. Forte, "**Development and Evaluation of Hardware Obfuscation Benchmarks**", Journal of Hardware and Systems Security (**HaSS**), Vol. 2, Issue 2, pp. 142-161, June 2018.

65. N. Vashistha, M. T. Rahman, H. Shen, D. Woodard, N. Asadi and M. Tehranipoor, "**Detecting Hardware Trojans Inserted by Untrusted Foundry using Physical Inspection and Advanced Image Processing Techniques**," Journal of Hardware and Systems Security (**HaSS**), Vol. 2, Issue 4, pp. 333-344, Dec. 2018.

66. A. Nahiyan, F. Farahmandi, P. Mishra, D. Forte, and M. Tehranipoor, "**Security-Aware FSM Design Flow for Identifying and Mitigating Vulnerabilities to Fault Attacks**," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**), May 2018.

67. K. Yang, D. Forte, and M. Tehranipoor, "**ReSC: An RFID-Enabled Solution for Defending IoT Supply Chain**," ACM Tfransactions on Design Automation of Electronic Systems (**TODAES**), Vol 23, Issue 3, 2018.

68. M. Alam, S. Choudhury, B. Park, D. Munzer, N. Maghari, M. Tehranipoor, and D. Forte, "**Challenges and Opportunities in Analog and Mixed Signal (AMS) Integrated Circuit (IC) Security**," Journal of Hardware and Systems Security (**HaSS**), Vol. 2, Issue 1, pp. 15-32, 2018.

69. Z. Guo, X. Xu, T. Rahman, M. Theranipoor, and D. Forte, "**SCARe: An SRAM based Countermeasure Against IC Recycling Framework**," IEEE Transactions on VLSI (**TVLSI**), Vol. 36, Issue 4, 2018.

70. X. Wang, D. Zhang, M. He, and M. Tehranipoor, "**Secure Scan and Test Using Obfuscation Throughout Supply Chain**," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**), Vol. 37, Issue 9, Sep. 2018.

71. E. Principe, N. Asadi, D. Forte, R. Chivas, M. DiBattista, and S. Silverman, "**Plasma FIB Deprocessing of Integrated Circuits from the Backside**," Electronic Device Failure Analysis (**EDFA**), Jan 2018.

72. K. Yang, H. Shen, D. Forte, S. Bhunia, and M. Tehranipoor, "**Hardware-Enabled Pharmaceutical Supply Chain Security**," ACM Transactions on Design Automation of Electronic Systems (**TODAES**), Vol. 23, Issue 2, 2018.

73. S. Ray, S. Bhunia, and M. Tehranipoor, "**System-on-Chip Platform Security Assurance: Architecture and Validation**," Proceedings of IEEE, Volume 106. Issue 1, 2018.

74. M. Alam, M. Tehranipoor, and U. Guin, "**TSensors Vision, Infrastructure, and Security Challenges in Trillion Sensor Era**," Journal of Hardware and Systems Security (**HaSS**), Vol. 1, Issue 4, 2017.

75. T. Rahman, A. Hosey, J. Carrol, D. Forte, and M. Tehranipoor, "**Systematic Correlation and Cell Neighborhood Analysis of SRAM-PUF for Robust and Unique Key Generation**," Journal of Hardware and Systems Security (**HaSS**), Vol. 1, Issue 2, June 2017.

76. F. Rahman, B. Shakya, X. Xu, D. Forte, and M. Tehranipoor, "**Security Beyond CMOS: Fundamentals, Applications, and Roadmap**," IEEE Transactions on VLSI (**TVLSI**), Vol. 25, Issue 12, 2017.

77. M. Sadi, G. Contreras, J. Chen, L. Winemberg, and M. Tehranipoor, "**Design of Reliable SoCs with BIST Hardware and Machine Learning**," IEEE Transactions on VLSI (**TVLSI**), Vol. 25, Issue 11, 2017.

78. H. Shen, F. Rahman, B. Shakya, X. Xu, M. Tehranipoor, and M. Tehranipoor, "**Poly-Si Based Physical Unclonable Functions**," IEEE Transactions on VLSI (**TVLSI**), Vol. 25, Issue 11, 2017.

79. H. Wang, Q. Shi, D. Forte, M. Tehranipoor, "**Probing Attacks on Integrated Circuits: Challenges and Research Opportunities**," IEEE Design & Test of Computers, Vol. 34, Issue 5, 2017.

80. M. He and M. Tehranipoor, "**An Access Mechanism for Embedded Sensors in Modern SoCs**," Journal of Electronics Testing: Theory and Applications (**JETTA**), Vol. 33, Issue 4, 2017.

81. T. He, G. Contreras, D. Tran, L. Winemberg, and M. Tehranipoor, "**Test-Point Insertion Efficiency Analysis for LBIST in High-Assurance Application**s," IEEE Transactions on VLSI (**TVLSI**), Vol. 25, Issue 9, 2017.

82. M. Tehranipoor, U. Guin, and S. Bhunia, "**Invasion of the Hardware Snatchers: Fake Hardware Could Open the Door to Malicious Malware and Critical Failure**," IEEE Spectrum, 2017.

83. B. Shakya, H. Salmani, D. Forte, S. Bhunia, and M. Tehranipoor, "**Benchmarking of Hardware Trojans and Maliciously Affected Circuits**," Journal of Hardware and Systems Security (**HaSS**), Vol. 1, Issue 1, March 2017.

84. J. Wurm, Y. Jin, Y. Liu, S. Hu, K. Heffner, F. Rahman, and M. Tehranipoor, "**Introduction to Cyber Physical System Security: A Cross-Layer Perspective**," IEEE Trans. on Multi-Scale Computing Systems (**TMSCS**), September 2017.

85. N. Karimian, Z. Guo, M. Tehranipoor, and D. Forte, "**Highly Reliable Key Generation from Electrocardiogram (ECG)**," IEEE Transactions on Biomedical Engineering (**TBME**), Vol. 64, Issue 6, June 2017.

86. K. Yang, D. Forte, and M. Tehranipoor, "**CDTA: A Comprehensive Solution for Counterfeit Detection, Traceability and Authentication in IoT Supply Chain**," ACM Transactions on Design Automation of Electronic Systems (**TODAES**), Vol. 22, Issue 3, May 2017.

87. M. Sadi, L. Winemberg, S. Kannan, and M. Tehranipoor, "**SoC Speed Binning Using Machine Learning and On-chip Slack Sensors**," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**), vol. 36, issue 5, pp. 842-854, May 2017.

88. Z. Guo, J. Di, M. Tehranipoor, and D. Forte, "**Obfuscation-based Protection Framework Against Printed Circuit Boards Unauthorized Operation and Reverse Engineering**," ACM Transactions on Design Automation of Electronic Systems (**TODAES**), Vol. 22, Issue 3, May 2017.

89. X. Wang, P. Jiao, M. Sadi, L. Winemberg, and M. Tehranipoor, "**TRO: An On-chip Ring Oscillator Based GHz Transient IR-Drop Monitor**," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**), vol. 36, issue 5, pp. 855-868, May 2017.

90. U. Guin, S. Bhunia, D. Forte, and M. Tehranipoor, "**SMA: A System-Level Mutual Authentication for Protecting Electronic Hardware and Firmware**," Transactions on Dependable and Secure Computing (**TDSC**), pp. 265-278, May 2017.

91. M. Alam, H. Shen, N. Asadi, M. Tehranipoor, and D. Forte, "**Impact of X-ray Tomography on the Reliability of Integrated Circuits**," IEEE Transaction on Device and Materials Reliability, vol. 7, Issue 1, March 2017.

92. N. Asadi, M. Tehranipoor, and D. Forte, "**PCB Reverse Engineering Using Non-destructive X-ray Tomography and Advanced Image Processing**," IEEE Transactions on Components, Packaging and Manufacturing Technology (**TCPMT**), Vol. 7, Issue 2, Feb. 2017.

93. K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, "**Hardware Trojans: Lessons Learned After One Decade of Research**," ACM Transactions on Design Automation of Electronic Systems (**TODAES**), Vol. 22, Issue 1, Dec. 2016. **Made the 2016 most notable computing articles list, Computingreviews.com. The paper also received the Best Paper Award from TODAES.**

94. K. Xiao, A. Nahiyan, and M. Tehranipoor, "**Security Rule Checking in IC Design**," IEEE Computer Magazine, Vol. 49, Issue 8, Aug. 2016.

95. Y. Xie, C. Bao, C. Serafy, T. Lu, A. Srivastava, and M. Tehranipoor, "**Security and Vulnerability Implications of 3D ICs**," IEEE Trans. on Multi-Scale Computing Systems (**TMSCS**), Vol. 2, Issue 2, June 2016.

96. U. Guin, Q. Shi, D. Forte, and M. Tehranipoor, "**FORTIS: A Comprehensive Solution for Establishing Forward Trust for Protecting IPs and ICs**," ACM Transactions on Design Automation of Electronic Systems (**TODAES**), May 2016.

97. Q. Shi, X. Wang, L. Winemberg, and M. Tehranipoor, "**On-Chip Sensor Selection for Effective Speed-Binning**," Int. Journal on Analog Integrated Circuits and Signal Processing, Vol. 88, Issue 2, Aug. 2016.

98. H. Salmani and M. Tehranipoor, "**Vulnerability Analysis of a Circuit Layout to Hardware Trojan Insertion**," IEEE Transactions on Information Forensics & Security (**TIFS**), Vol. 11, Issue 6, June 2016.

99. M. Sadi and M. Tehranipoor, "**Design of a Network of Digital Sensor macros for Extracting Power Supply Noise Profile in SoCs**," IEEE Transactions on VLSI (**TVLSI**), Vol. 24, Issue 5, May 2016.

100. X. Wang, D. Zhang, D. Su, L. Winemberg, and M. Tehranipoor, "**A Novel Peak Power Supply Noise Measurement and Adaptation System for Integrated Circuits**," IEEE Transactions on VLSI (**TVLSI**), Vol. 24, Issue 5, May 2016.

101. T. Rahman, F. Rahman, D. Forte, and M. Tehranipoor, "**An Aging-Resistant RO-PUF for Reliable Key Generation**," IEEE Transactions on Emerging Topics in Computing (**TETC**), Vol. 4, Issue 3, July 2016.

102. U. Guin, D. Forte, and M. Tehranipoor, "**Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling**," IEEE Transactions on VLSI (**TVLSI**), Vol. 24, Issue 4, April 2016.

103. S. Quadir, J. Chen, D. Forte, N. Asadi, S. Shahbaz, L. Wang, J. Chandy, and M. Tehranipoor, "**A Survey on Chip to System Reverse Engineering**," ACM Journal on Emerging Technologies in Computing Systems (**JETC**), Vol 13, Issue 1, Dec. 2016.

104. S. Kelly, X. Zhang, M. Tehranipoor, and A. Ferraiuolo, "**Detecting Hardware Trojans using On-chip Sensors in an ASIC Design**," Journal of Electronic Testing: Theory and Applications (**JETTA**), Vol. 31, Issue 1, Feb. 2015.

105. X. Wang, D. Tran, S. George, L. Winemberg, N. Ahmed, S. Palosh, L. Dobia, M. Tehranipoor, "**Aging Adaption in Integrated Circuits Using a Novel Built-In Sensor**," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**), 2015.

106. K. Xiao, D. Forte, and M. Tehranipoor, "**A Novel Built-In Self-Authentication Technique to Prevent Inserting Hardware Trojans**," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**), vol. 33, no. 12, pp. 1178-1791, 2014.

107. A. Tomita, X. Wen, Y. Sato, S. Kajihara, K. Miyase, S. Holst, P. Girard, M. Tehranipoor, L.T. Wang, "**On Achieving Capture Power Safety in At-Speed Scan-Based Logic BIST**," **IEICE** Transactions, vol. E97-D, no.10, pp.2706-2718. 2014.

108. U. Guin, K. Huang, D. DiMase, J. Carulli, M. Tehranipoor, Y. Makris, "**Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain**," Proceedings of IEEE, vol. 102, no. 8, pp. 1207-1228, 2014.

109. Z. Collier, D. DiMase, S. Walters, M. Tehranipoor, J. Lambert, and I. Linkov, "**Risk-Based Cybersecurity Standards: Policy Challenges and Opportunities**," IEEE Computer Magazine, pp. 70-76, Jan. 2014.

110. U. Guin, D. DiMase, and M. Tehranipoor, "**Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead**," Journal of Electronic Testing: Theory and Applications (**JETTA**), vol. 30, no. 1, pp. 9-23, Feb. 2014 (**Most Downloaded Article in 2014**).

111. A. Markman, B. Javidi, and M. Tehranipoor, "**Photon-Counting Security Tagging and Verification Using Optically Encoded QR Codes**," IEEE Photonics Journal, vol. 6, no. 1, Feb. 2014.

112. U. Guin, D. DiMase, and M. Tehranipoor, "**A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment**," Journal of Electronic Testing: Theory and Applications (**JETTA**), vol. 30, no. 1, pp. 25-40, Jan. 2014 (**6th Most Downloaded Article in 2014**).

113. J. Chen, S. Wang, and M. Tehranipoor, "**Critical-Reliability Path Identification and Delay Analysis**," ACM Journal on Emerging Technologies in Computing Systems (**JETC**), vol. 10, no. 2, Feb. 2014.

114. X. Zhang and M. Tehranipoor, "**Design of On-chip Light-weight Sensors for Effective Detection of Recycled ICs**," IEEE Transactions on VLSI (TVLSI), vol. 22, no. 5, pp. 1016-1029, May 2014.

115. S. Wang and M. Tehranipoor, "**A Light-Weight On-Chip Structure for Measuring Timing Uncertainty Induced by Noise in Integrated Circuits**," IEEE Transactions on VLSI (TVLSI), vol. 22, no. 5, pp. 1030-1041, May 2014.

116. F. Bao, K. Peng, M. Tehranipoor, and K. Chakrabarty, "**Generation of Effective 1-Detect TDF Patterns for Detecting Small-Delay Defects**," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**), vol. 32, no. 10, pp. 1583-1594, Oct. 2013.

117. W. Zhao, J. Ma, M. Tehranipoor, and S. Chakravarty, "**Power-Safe Application of TDF Patterns to Flip-Chip Designs during Wafer Test**," ACM Transactions on Design Automation of Electronic Systems (**TODAES**), vol. 18, no. 3, July 2013.

118. M. Li, A. Davoodi, and M. Tehranipoor, "**A Sensor-Assisted Self-Authentication Framework for Hardware Trojan Detection**," IEEE Design & Test, pp. 74-82, Oct. 2013.

119. J. Villasenor and M. Tehranipoor, "**The Hidden Dangers of Chop Shop Electronics**" IEEE Spectrum, Sep. 2013.

120. K. Xiao, X. Zhang, and M. Tehranipoor, "**A Clock Sweeping Technique for Detecting Hardware Trojans Impacting Circuits Delay**," IEEE Design & Test, vol. 30, no. 2, pp. 26-34, April 2013.

121. F. Bao, K. Peng, M. Yilmaz, K. Chakrabarty, L. Winemberg, and M. Tehranipoor, "**Efficient Pattern Generation for Small-Delay Defects Using Selection of Critical Faults**," Journal of Electronic Testing: Theory and Applications (**JETTA**), vol. 29, no. 1, pp. 35-48, 2013.

122. K. Peng, M. Yilmaz, K. Chakrabarty, and M. Tehranipoor, "**Crosstalk- and Process Variations-Aware High-Quality Tests for Small-Delay Defects**," IEEE Transactions on VLSI (**TVLSI**), vol. 21, no. 6, pp. 1129-1142, 2012.

123. X. Zhang, A. Ferraiuolo, and M. Tehranipoor, "**Detection of Hardware Trojans using a Combined Ring Oscillator Network and Off-chip Transient-Power Analysis**," ACM Journal on Emerging Technologies in Computing Systems (**JETC**), vol. 9, no. 3, 2012.

124. M. Abramovici, et. al., "**Protecting Against Hardware Trojan Attacks: Towards a Comprehensive Solution**," IEEE Design & Test of Computers, vol. 30, no. 3, pp. 6-17, 2012.

125. W. Zhao, M. Tehranipoor, and S. Chakravarty, "**Ensuring Power-Safe Application of Test Patterns Using An Effective Gating Approach Considering Current Limits**," Journal of Low Power Electronics (**JOLPE**), vol. 8, no. 2, pp. 235-247, 2012.

126. X. Wang, M. Tehranipoor, S. George, D. Tran and L. Winemberg, "**Design and Analysis of a Delay Sensor Applicable to Process/Environmental Variations and Aging Measurement**," IEEE Transactions on VLSI (**TVLSI**), vol. 20, no. 8, pp. 1405-1418, 2012.

127. H. Salmani, W. Zhao, M. Tehranipoor, S. Chakravarty, P. Girard, and X. Wen, "**Layout-Aware Pattern Evaluation and Analysis for Power-Safe Application of TDF Patterns**," Journal of Low Power Electronics (**JOLPE**), vol. 8, no. 2, pp. 248-258, 2012.

128. H. Salmani, M. Tehranipoor, and J. Plusquellic, "**A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time**," IEEE Transactions on VLSI (**TVLSI**), vol. 20, no. 1, pp. 112-125, 2012.

129. H. Salmani and M. Tehranipoor, "**A Layout-Aware Approach for Improving Localized Switching to Detect Hardware Trojans in Digital Integrated Circuits**," IEEE Transactions on Information Forensics & Security (**TIFS**), vol. 7, no. 1, pp. 76-87, 2011

130. J. Ma, M. Tehranipoor, and P. Girard, "**A Layout-Aware Pattern Grading Procedure for Critical Paths Testing Considering Crosstalk and Power Supply Noise**," Journal of Electronics Testing: Theory and Applications (**JETTA**), vol. 28, no. 2, pp. 201-2014, 2012.

131. J. Ma and M. Tehranipoor, "**Layout-Aware Critical Path Delay Test under Maximum Power Supply Noise Effects**," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**), vol. 30, no. 12, pp. 1923-1934, 2011.

132. C. Lamech, R. Rad, J. Plusquellic, and M. Tehranipoor, "**An Experimental Analysis of Power and Delay Signal-to-Noise Requirements for Detecting Trojans and Methods for Achieving the Required Detection Sensitivities**," IEEE Transactions on Information Forensics & Security (**TIFS**), vol. 6, no. 3, pp. 1170-1179, 2011.

133. M. Yilmaz, K. Chakrabarty, and M. Tehranipoor, "**Adaptation and Evaluation of the Output-Deviations Metric to Target Small-Delay Defects in Industrial Circuits**," IEEE Design and Test of Computers, vol. 28, no. 2, pp .52-61, 2011.

134. M. Tehranipoor, H. Salmani, X. Zhang, X. Wang, R. Karri, J. Rajendran, and K. Rosenfeld, "**Trustworthy Hardware: Trojan Detection Solutions and Design-for-Trust Challenges**," IEEE Computer Magazine, vol. 44, no. 7, pp. 66-74, 2010.

135. R. Karri and M. Tehranipoor, "**Trustworthy Hardware: Identifying and Classifying Hardware Trojans**," IEEE Computer Magazine, vol. 43, no. 10, pp. 39-46, 2010.

136. F. Wu, L. Dilillo, A. Bosio, P. Girard, S. Pravossoudovitch, A. Virazel, M. Tehranipoor, X. Wen, and N. Ahmed, "**A Comprehensive Analysis of Transition Fault Coverage and Test Power Dissipation for LOS and LOC Schemes**," Journal of Low Power Electronics (**JOLPE**), vol. 6, no. 2, pp. 289-300, 2010.

137. M. Tehranipoor and F. Koushanfar, "**A Survey of Hardware Trojan Taxonomy and Detection**," IEEE Design and Test of Computers, vol. 27, no. 1, pp. 10-25, 2010.

138. N. Ahmed and M. Tehranipoor, "**A Novel IR-drop Tolerant Transition Delay Fault Test Pattern Generation Procedure**," Journal of Low Power Electronics (**JOLPE**), vol. 6, no. 1, pp. 150-159, 2010.

139. M. Yilmaz, K. Chakrabarty, and M. Tehranipoor, "**Test-Pattern Selection Small-Delay Defects in Very-Deep Submicron Integrated Circuits**," IEEE Transactions on CAD, vol. 29, no. 5, pp. 760-773, 2010.

140. M. Tehranipoor and K. Butler, "Power Supply Noise: A **Survey on Effects and Research**," IEEE Design and Test of Computers, vol. 27, no. 2, pp. 51-67, 2010.

141. N. Ahmed and M. Tehranipoor, "**A Novel Faster-than-at-speed Transition Delay Test Method Considering IR-drop Effects**," IEEE Transactions on CAD, vol. 28, no. 10, pp. 1573-1582, 2009.

142. J. Lee and M. Tehranipoor, "**Layout-Aware Transition-Delay Fault Pattern Generation with Evenly Distributed Switching Activity**," Journal of Low Power Electronics (**JOLPE**), vol. 4, pp. 1-12, 2008.

143. R. Rad, J. Plusquellic, and M. Tehranipoor, "**A Sensitivity Analysis of Power Signal Methods for Detecting Hardware Trojans under Real Process and Environmental Conditions**," IEEE. Trans. on VLSI, vol. 18, no. 12, pp. 1735-1744, 2010.

144. K. Miyase, X. Wen, H. Furukawa, Y. Yamato, S. Kajihara, P. Girard, L.–T. Wang, and M. Tehranipoor, "**High Launch Switching Activity Reduction in At- Speed Scan Testing using CTX: A Clock-Gating-**

Based Test Relaxation and X-Filling Scheme," IEICE Trans. Fundamentals/Commun./Electron/Inf. & Syst., vol. E93-D, no. 1, pp. 2-9 , 2010.

145. M. Tehranipoor and R. Rad, "**Defect Tolerance for Nanoscale Crossbar-based Devices**," IEEE Design & Test of Computers, vol. 25, no. 6, pp. 549-559, 2008.

146. R. Rad and M. Tehranipoor, "**SCT: A Novel Approach for Testing and Configuring Nanoscale Devices**," ACM Journal on Emerging Technologies in Computing Systems (**JETC**), vol. 4, no. 3, pp. 370-377, 2008.

147. M. Nourani, M. Tehranipoor and N. Ahmed, "**Low-Transition Test Pattern Generation for BIST-Based Applications**," IEEE Transactions on Computers, vol. 57, no. 3, pp. 303-315, March 2008.

148. J. Lee, M. Tehranipoor, C. Patel and J. Plusquellic, "**Securing Designs Against Scan-Based Side-Channel Attacks**," IEEE Transactions on Dependable and Secure Computing (**TDSC**), vol. 4, no. 4, pp. 325-336, 2007.

149. R. Rad and M. Tehranipoor, "**Evaluating Area and Performance of a Hybrid FPGA with Nanoscale Clusters and CMOS Routing**," ACM Journal on Emerging Technologies in Computing Systems (**JETC**), vol. 3, no. 3, 2007.

150. M. ElShoukry and M. Tehranipoor and C.P. Ravikumar, "**A Critical-Path Aware Partial Gating Approach for Test Power Reduction**," ACM Transactions on Design Automation of Electronic Systems (**TODAES**), vol. 12, issue 2, 2007.

151. N. Ahmed, M. Tehranipoor, C.P. Ravikumar and K. Butler, "**Local At-Speed Scan Enable Generation for Transition Fault Testing Using Low-Cost Testers**," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**CAD/ICAS**), vol. 26, no. 5, pp. 896-906, 2007.

152. M. Tehranipoor and R. M.P. Rad, "**Built-In Self-Test and Recovery Procedures for Molecular Electronics-Based NanoFabrics**," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**CAD/ICAS**), vol. 26, no. 5, pp. 943-958, May 2007.

153. N. Ahmed and M. Tehranipoor, "**Improving Quality of Transition Delay Test Using Hybrid Scan-Based Technique**," IEEE Design and Test of Computers, 2006.

154. D. Acharyya, A. Singh, M. Tehranipoor, C. Patel and J. Plusquellic, "**Quiescent Signal Analysis: a Multiple Supply Pad I_{DDQ} Method**," IEEE Design and Test of Computers, vol. 23, no. 4, pp. 278-293, 2006.

155. M. Tehranipoor, M. Nourani and K. Chakrabarty, "**Nine-Coded Compression Technique for Testing Embedded Cores in SoCs**," IEEE Transactions on Very Large Scale Integration Systems (**TVLSI**), vol. 13, no. 6, pp. 719-731, June 2005.

156. M. Nourani and M. H. Tehranipour, "**RL-Huffman Encoding for Test Compression and Power Reduction in Scan Application**," ACM Transactions on Design Automation of Electronic Systems (**TODAES**), vol. 10, no. 1, pp. 91-115, Jan. 2005.

157. M. H. Tehranipour, N. Ahmed and M. Nourani, "**Testing SoC Interconnects for Signal Integrity Using Extended JTAG Architecture**," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**CAD/ICAS**), vol. 23, issue 5, pp. 800-811, May 2004.

158. M. H. Tehranipour, S. M. Fakhraie, Z. Navabi and M. R. Movahedin, "**A Low-Cost At-Speed BIST Architecture for Embedded Processor and SRAM Cores**," Journal of Electronic Testing: Theory and Applications (**JETTA**), vol. 20, pp. 155-168, April 2004.

159. M. H. Tehranipour, S. M. Fakhraie, M. Nourani, M. R. Movahedin and Z. Navabi, "**Embedded Test for Processor and Memory Cores in System-on-Chips**," International Journal of Science and Technology, vol. 10, no. 4, pp. 486-494, Oct. 2003.

Conference Papers

1. R. Muttaki, M. Tehranipoor, and F. Farahmandi, "**FTC: A Universal Low-Overhead Fault-Injection Attack Detection Solution**," International Symposium for Testing and Failure Analysis (**ISTFA**), 2022.

2. N. Pundir, H. Li, L. Lin, N. Chang, "**SPILI: Security Properties and Machine Learning Assisted Pre-silicon Laser Fault Injection Assessment**," International Symposium for Testing and Failure Analysis (**ISTFA**), 2022.

3. R. Kibria, S. Rahman, F. Farahmandi, and M. Tehranipoor, "**RTL-FSMx: Fast and Accurate Finite State Machine Extraction ar the RTL for Security Application**," International Test Conference (**ITC**), 2022.

4. U. Das, R. Muttaki, m. Tehranipoor, and F. Farahmandi, "**ADWIL: A Zero-Overhead Analog Device Watermarking Using Inherent IP Features**," International Test Conference (**ITC**), 2022.

5. A. Mazumder Shuvo, N. Pundir, J. Park, F. Farahmandi, and M. Tehranipoor, "**LDTFI: Layout-Aware Timing Fault-Injection Attack Assessment Against Differential Fault Analysis**," IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2022.

6. N. Jessurun, J. Harrison, M. Tehranipoor, and N. Asadi, "**PinPoint: An SMD Pin Localization Method**" IEEE International Symposium pn Physical and Failure Analysis (**IPFA**), 2022.

7. K. Zamiri Azar, H. Kamali, F. Farahmandi, and M. Tehranipoor, "**Warm Up before Circuit De-obfuscation? An Exploration of Possibilities**," IEEE International Symposium on Hardware-Oriented Security and Trust (**HOST**), 2022.

8. R. Muttaki, M. Tehranipoor, and F. Farahmandi, "**FTC: A Universal Fault Injection Attack Detection Sensor**," IEEE International Symposium on Hardware-Oriented Security and Trust (**HOST**), 2022.

9. N. Pundir, L. Lin, N. Chang, F. Farahmandi, and M. Tehranipoor, "**Security Property Driven Pre-Silicon Laser Fault Injection Assessment**," IEEE International Symposium on Hardware-Oriented Security and Trust (**HOST**), 2022.

10. S. Rahman, R. Guo, H. M. Kamali, M. Abdel-Moneum, F. Farahmandi, F. Rahman, and M. Tehranipoor, "**O'Clock: Lock the Clock via Clock-gating for SoC IP Protection**," Design Automation Conference (**DAC**), 2022.

11. R. Kibira, N. Farzana, F. Farahmandi, and M. Tehranipoor, "**FSMx: Finite State Machine Extraction from Flattened Netlist with Application to Security**," IEEE VLSI Test Symposium (**VTS**), 2022.

12. C. Xi, N. Jessurun, A. Khan, M. Tehranipoor, and N. Asadi, "**A Naturally Inherent Tracking Methodology for Secure Packaging Using Geo-Magnetic Signatures**," GomacTech, 2022.

13. P. Calzada, J. Harrison, P. Chawla, N. Asadi, and M. Tehranipoor, "**PCB Trojan Detection using Optical Imaging**," GOMACTech, 2022.

14. M. Farmani, J. Harrison, F. Rahman, and M. Tehranipoor, "**Efficient Rowhammer-Aware DRAM Test Under Reduced Voltage and Increased Temperature**," GOMACTech, 2022.

15. M. Azhagan, M. Y. Vutukuru, O. Paradis, M. Tehranipoor, N. Asadi, "**Logo Detection and Localization for IC Authentication, Marking Recognition, and Counterfeit Detection**," GOMACTech, 2022.

16. N. Vashishta, Al Hassan, Md. Mahfuz, F. Rahman, N. Asadi, and M. Tehranipoor, "**Trust Validation of Chiplets using a Physical Inspection Based Certificate Authorithy**," Electronic Components and Technology Conference (**ECTC**), 2022.

17. D. Mehta, N. Mondol, F. Farahmandi, and M. Tehranipoor, "**AIME: Watermarking AL Models by Leveraging Errors**," Design, Automation, and Test in Europe (**DATE**), 2022.

18. T. Zhang, F. Rahman, M. Tehranipoor, and F. Farahmandi, "**FPGA-Chain: Enabling Holistic Protection of FPGA Supply Chain with Blockchain Technology**," IEEE Workshop on Silicon Lifecycle Management (**SLM**), Oct. 2021.

19. H. Wang, H. Li, F. Rahman, F. Farahmandi, and M. Tehranipoor, "**Security Property-Driven Fault-Injection Vulnerability Assessment of Modern SoCs**," iSecCon, 2021.

20. S. U. Sami, F. Rahman, D. Donchin, A. Cron, M. Borza, F. Farahmandi, and M. Tehranipoor, "**POCA: First Power-on Chip Authentication in Untrusted Foundry and Assembly**," IEEE International Symposium on Hardware-Oriented Security and Trust (**HOST**), 2021.

21. S. Rahman, H. Li, R. Guo, F. Rahman, F. Farahmandi, and M. Tehranipoor, "**LL-ATPG: Logic-Locking Aware Test Using Valet Keys in an Untrusted Environment**," International Test Conference (**ITC**), 2021.

22. A. Vafaei, N. Hooten, M. Tehranipoor, and F. Farahmandi, "**Symba: Symbolic Execution at C-level for Hardware Trojan Detection**," International Test Conference (**ITC**), 2021.

23. B. Ahmed, F. Rahman, N. Hooten, F. Farahmandi, and M. Tehranipoor, "**AutoMap: Automated Mapping of Security Properties Between Different Levels of Abstraction in Design Flow**," International Conference on Computer-Aided Design (**ICCAD**), 2021.

24. N. Pundir, S. Shi, M. Tehranipoor, and F. Farahmandi, "**HLS-Induced Information Leakage Verification**," SRC TECHCON, 2021.

25. J. True, N. Jessurun, D. Mehta, M. Tehranipoor, N. Asadizanjani, "**Q.U.A.I.N.T.P.E.A.X. QUantifying Algorithmically INTrinsic Properties of Electronic Assemblies via X-ray CT**", Microscopy and Microanalysis (**M&M),** August 2021.

26. J. True, C. Xi, N. Jessurun, K. Ahi, M. Tehranipoor, N. Asadizanjani, "**Terahertz Based Machine Learning Approach to Integrated Circuit Assurance**" Electronic Components and Technology Conference (**ECTC**), June 2021

27. M. M. Al Hasan, N. Vashistha, S. Taheri, M. Tehranipoor, N. Asadizanjani "**Generative Adversarial Network for Integrated Circuits Physical Assurance Using Scanning Electron Microscopy**", IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (**IPFA**), September 2021.

28. M. M. Rahman, S. Mohammad, J. Vosatka, J. Allen, M. Allen, F. Farahmandi, F. Rahman, and M. Tehranipoor, "**HEXON: Protecting Firmware Using Hardware-Assisted Execution-Level Obfuscation**," International Symposium on VLSI (**ISVLSI**), 2021.

29. T. Farheen, U. Boreto, N. Varshney, H. Shen, D. Woodard, M. Tehranipoor, and D. Forte, "**Proof of Reverse Engineering Barrier: SEM Image Analysis on Covert Gates**," International Sympoium on Test and Failure Analysis (**ISTFA**), 2021.

30. S. Aftabjahani, R. Kastner, M. Tehranipoor, F. Farahmandi, J. Oberg, A. Nordstrom, N. Fern, A. Alric, "**CAD for Hardware Security – Automation is Key to Adoption of Solution**," IEEE VLSI Test Symposium (**VTS**), 2021.

31. H. Wang, F. Farahmandi, and M. Tehranipoor, "**SoFI: Security Property-Driven Vulnerability Assessment of ICs Against Fault-Injection Attacks**," SNUG, 2021.

32. Md. S. Ul Islam, F. Rahman, Farimah Farahmandi, A. Cron, M. Borza, and Mark Tehranipoor, "**End-to-End Secure SoC Lifecycle Management**," Design Automation Conference (**DAC**), 2021.

33. T. Zhang, J. Park, M. Tehranipoor, and F. Farahmandi, "**PSC-TG: RTL Power Side-Channel Leakage Assessment with Test Pattern Generation**," Design Automation Conference (**DAC**), 2021.

34. R. Muttaki, M. Tehranipoor, and F. Farahmandi, "**HLock: Locking IPs at the High-Level Language**," Design Automation Conference (**DAC**), 2021.

35. M. Farmani, F. Rahman, and M. Tehranipoor, "**RHAT: Efficient RowHammer-Aware Test for Modern DRAM Modules**," IEEE European Test Symposium (**ETS**), 2021.

36. N. Dipu, A. Ayalasomayajula, F. Rahman, F. Farahmandi, and M. Tehranipoor, "**SAIF: Automated Asset Identification for Security Verification ar the Register Transfer Level**," IEEE VLSI Test Symposium (**VTS**), 2021.

37. J. Harrison, P. Calzada, N. Asadi, and Mark Tehranipoor, "**A Comprehensive Benchmark Suite for PCB Assurance**," GoamcTech 2021.

38. A. Khan, C. Xi, N. Asadi, and Mark Tehranipoor, "**Security Assessment of Interposer in Advanced Packaging**," GomacTech 2021.

39. H. Wang, H. Li, F. Farahmandi, and Mark Tehranipoor, "**SOFI: Security Property-Driven Vulnerability Assessment of ICs Against Fault-Injection Attacks**," GoamcTech 2021.

40. O. Paradis, D. Woodard, M. Tehranipoor, and N. Asadi, "**Frameowrk for Automatic OCB Marking Detection and Recognition for Hardware Assurance**," GOMACTech 2021.

41. N, Jessurrun, O. Paradis, M. Tehranipoor, N. Asadi, "**Improvements on the SHADE Algorithm for PCB Component Estimate Refinement**," GOMACTech 2021.

42. N. Pundir, F. Farahmandi, and M. Tehranipoor, "**Secure High-Level Synthesis: Challenges and Solutions**," International Symposium on Quality Electronics Design (**ISQED**), 2021.

43. M. M. Hossain, F. Farahmandi, M. Tehranipoor and F. Rahman, "**BOFT: Exploitable Buffer Overflow Detection by Information Flow Tracking**," Design, Automation, and Test in Europe (**DATE**), 2021.

44. O. Paradis, N. Jessurun, M. Tehranipoor, and N. Asadi, "**Color Normalization for Robust Automatic Bill of Materials Generation and Visual Inspection of PCBs**," International Symposium on Test and Failure Analysis (**ISTFA**), 2020.

45. L. Lavdas, M. T. Rahman, M. Tehranipoor, and N. Asadi, "**On Optical Attacks Making Logic Obfuscation Fragile,**" International Test Conference, Asia (**ITC-Asia**), 2020.

46. A. Stern, D. Mehta, S. Tajik, F. Farahmandi, and M. Tehranipoor, "**SPARTA: A Laser Probing Approach for Trojan Detection**," International Test Conference (**ITC**), 2020.

47. A. Stern, D. Mehta, S. Tajik, U. Guin, F. Farahmandi, and M. Tehranipoor, "**Trust Assessment for Electronic Components using Laster and Emission-based Microscopy**," IEEE RAPID, 2020.

48. J. Vosatka, A. Stern, M. Hossain, F. Rahman, J. Allen, M. Allen, F. Farahmandi, and M. Tehranipoor, "**Confidence Modeling and Tracking of Recycled Integrated Circuits, Enabled by Blockchain**," IEEE RAPID, 2020.

49. H. Lu, N. Vashishta, N. Asadi, M. Tehranipoor, D. Woodard, "**Knowledge-based Object Localization in Scanning Electron Microscopy Images for Hardware Assurance**," International Symposium on Test and Failure Analysis (**ISTFA**), 2020.

50. O. Paradis, N. Jessurun, M. Tehranipoor, and N. Asadi, "**Color Normalization for Robust Automatic Bill of Materials Generation and Visual Inspection of PCBs**," International Symposium on Test and Failure Analysis (**ISTFA**), 2020.

51. N. Jessurun, O. Paradis, M. Tehranipoor, and N. Asadi, "**SHADE: Automated Refinement of PCB Component Estimates Using Detected Shadows**," IEEE Conference on Physical Assurance and Inspection of Electronics (**PAINE**), 2020. (Received Best Student Paper Award)

52. J. Vosatka, A. Stern, M. M. Hossain, F. Rahman, F. Allen, M. Allen, F. Farahmandi, and M. Tehranipoor, "**Tracking Cloned Elecronic Components using a Consortium-based Blockchain Infrastructure**," IEEE Conference on Physical Assurance and Inspection of Electronics (**PAINE**), 2020.

53. A. Stern, D. Mehta, S. Tajik, U. Guin, F. Farahmandi, and M. Tehranipoor, "**SPARTA: Laser Probing Approach for Sequential Trojan Detection in COTS Integrated Circuits**," IEEE Conference on Physical Assurance and Inspection of Electronics (**PAINE**), 2020.

54. A. Duncan, A. Nahiyan, F. Rahman, G. Skipper, M. Swany, A. Lukefahr, F. Farahmandi, and M. Tehranipoor, "**SERFI: Secure Remote FPGA Initialization in an Untrusted Environment**," IEEE VLSI Test Symposium (**VTS**), 2020.

55. N. Pundir, F. Rahman, M. Tehranipoor, and F. Farahmandi, "**Analyzing Security Vulnerabilities Induced by High-Level Synthesis**," GomacTech 2020.

56. J. Vosatka, M.M. Hossain, F. Rahman, J. Allen, M. Allen, F. Farahmandi, and M. Tehranipoor, "**Modeling Risk in Electronics Supply Chains Enabled by Blockchain**," GomacTech 2020.

57. A. Stern, A. Duncan, S. Tajik, F. Farahmandi, and M. Tehranipoor, "**Sequential Hardware Trojan Detection usong Clock Activity Analysis**," GomacTech, 2020.

58. A. Duncan, A. Nahiyan, F. Rahman, G. Skipper. M. Swany, A. Lukefahr, F. Farahmandi, and M. Tehranipoor, "**SERFI: Secure Remote FPGA Initialization**," GomacTech, 2020.

59. T. Rahman, S. M. Rahman, S. Tajik, M. Tehranipoor, and N. Asadi, "**The Key is Left Under the Mat: On the Inappropriate Security Assumption of Logic Locking Schemes**," IEEE International Hardware-Oriented Security and Trust (**HOST**), 2020.

60. M. Azhagan, M. D. Mehta, H. Lu, S. Agrawal, M. Tehranipoor, D. Woodard, N. Asadizanjani, "**A Review on Automatic Bill of Material Generation and Visual Inspection on PCBs**," International Symposium for Testing and Failure Analysis (**ISTFA**), Portland, NV, 2019.

61. D. Forte, S. Bhunia, Ramesh Karri, J. Plusquellic, and M. Tehranipoor, "**IEEE International Hardware-Oriented Security and Trust (HOST): Past, Present, and Future**" International Test Conference (**ITC**), 2019.

62. N. Farzana, F. Rahman, M. Tehranipoor, and F. Farahmandi, "**Security Verification of System on Chip using Property Checking**," International Test Conference (**ITC**), 2019.

63. A. Duncan, F. Rahman, A. Lukefahr, F. Farahmandi, and M. Tehranipoor, "**FPGA Bitstream Security: A Day in the Life**," International Test Conference (**ITC**), 2019.

64. M. Azhagan, D. Mehta, H. Lu, S. Agrawal, P. Chawla, M. Tehranipoor, D. Woodard, and Navid Asadi, "**A New Framework for Automated Bill of Material Generation and Visual Inspection**," International Symposium on Test and Failure Analysis (**ISTFA**), 2019.

65. M. Alam, F. Ganji, S. Tajik, M. Tehranipoor, and D. Forte, "**RAM-Jam: Remote Temperature and Voltage Fault Attack on FPGAs using Memory Collisions**," Fault Diagnosis and Tolerance in Cryptography (**FDTC**), 2019.

66. F. Ganji, S. Tajik, J. P. Seifert, M. Tehranipoor, and D. Forte, "**Approaches for Hardness Amplification of PUFs**," PROOFS, 2019.

67. J. Park, S. Cho, T. Lim, S. Bhunia, M. Tehranipoor, "**SCR-QRNG: Side-Channel Resistant Design using Quantum Random Number Generator**," International Conference on Computer-Aided Design (**ICCAD**), 2019.

68. T. Aravin, H. Shen, M. Tehranipoor, and Q. Qu, "**LPN-based Device Authentication Using Resistive Memory**," ACM GLS-VLSI, 2019.

69. A. Duncan, A. Skipper, A, Stern, F. Rahman, A. Nahiyan, A. Lukefahr, M. Swany, and M. Tehranipoor, "**FLATS: Filling Logic and Testing Spatially for FPGA Authentication and Tamper Detection,**" IEEE International Hardware-Oriented Security and Trust (**HOST**), 2019.

70. X. Guo, M. Tehranipoor, and Y. Jin, "**QIF-Verilog: Quantitative Information-Flow based Hardware Description Languages for Pre-Silicon Security Assessment**," IEEE International Hardware-Oriented Security and Trust (**HOST**), 2019.

71. B. Park, M. Tehranipoor, D. Forte, and N. Maghari, "**A Metal-Via Resistance Based Physically Unclonable Function with 1.18% Native Instability**," IEEE Custom Integrated Circuits Conference (**CICC**), 2019.

72. J. Park, T. Miao, A. Nahiyan, A. Vassilev, Y. Jin, and M. Tehranipoor, "**RTL-PSC: Automated Power Side-Channel Leakage Assessment at Register-Transfer Level**," IEEE VLSI Test Symposium (**VTS**), 2019.

73. A. Stern, K. Yang, J. Vosatka, A. Duncan, J. Park, D. Forte, and M. Tehranipoor, "**RASC: Enabling Remote Access to Side-Channels for Mission Critical Systems**," GomacTech, 2019.

74. A. Duncan, A. Lukefahr, A. Sterm, M. Tehranipoor, and M. Swany, "**Lifetime Physical Authentication of FPGAs Through Infrared Watermarking**," GomacTech, 2019.

75. Q. Shi, H. Wang, N. Asadi, M. Tehranipoor, and D. Forte, "**A Comprehensive Analysis on Vulnerability of Active Shields to Tilted Microprobing Attacks**," IEEE Asian HOST (2018).

76. M. T. Rahman, Q. Shi. S. Tajik, H. Shen, D. Woodard, M. Tehranipoor, and N. Asadi, "**Physical Inspection and Attacks: New Frontier in Hardware Security**," IEEE International Verification and Security Workshop (**IVSW**), 2018.

77. A. Stern, U. Botero, B. Shakya, H. Shen, and M. Tehranipoor, "**EMFORCED: EM-based Fingerprinting Framework for Counterfeit Detection with Demonstration on Remarked ICs**," International Test Conference (**ITC**), 2018.

78. Y. Han, X. Wang, and M. Tehranipoor, "**CIPA: Concurrent IC and PCB Authentication Using On-Chip Ring Oscillator Array**," IEEE Asian Test Symposium (**ATS**), 2018.

79. H. Shen, N. Asadi, M. Tehranipoor, and D. Forte, "**Nanopyramid: An Optical Scrambler Against Backside Probing Attacks**," International Symposium on Test and Failure Analysis (**ISTFA**), 2018.

80. H. Shen, M. Tehranipoor, and S. Bhunia, "**Tampering, Snooping, and Electromagnetic Attack Proof Coating on Printed Circuit Boards**," International Symposium on Test and Failure Analysis (**ISTFA**), 2018.

81. N. Vashistha, H. Shen, T. Rahman, D. Woodard, N. Asadi, and M. Tehranipoor, "**Trojan Scanner: Detecting Hardware Trojans with Rapid Imaging Combined with Image Processing and Machine Learning**," International Symposium on Test and Failure Analysis (**ISTFA**), 2018.

82. H. Wang, Q. Shi, D. Forte, and M. Tehranipoor, "**Metrics and Physical Design Flow for Internal Shielding Against Front Side Probing Attack**," SRC TECHCON, 2018.

83. A. Nahiyan, D. Forte, and M. Tehranipoor, "**Framework for Automated and Systematic Security Assessment of Modern SoCs**," SRC TECHCON, 2018.

84. K. Yang, J. Park, M. Tehranipoor, and S. Bhunia, "**Robust Timing Attack Countermeasure on Virtual Hardware**," IEEE Computer Society Annual Symposium on VLSI (**ISVLSI**), 2018.

85. J. Park, X. Xu, Y. Jin, D. Forte, and M. Tehranipoor, "**Power-based Side-channel Instruction-level Disassembler**," Design Automation Conference (**DAC**). 2018.

86. M. Alam, S. Chowdhury, M. Tehranipoor, and U. Guin, "**Robust, Low-Cost, and Accurate Detection of Recycled ICs using Digital Signatures**", IEEE International Symposium on Hardware Oriented Security and Trust (**HOST**), 2018

87. K. Yang, J. Park, M. Tehranipoor, and S. Bhunia, "**Hardware Virtualization for Protection against Power Analysis Attack**," IEEE International Symposium on Hardware-Oriented Security and Trust (**HOST**), 2018.

88. O. Arias, F. Rahman, M. Tehranipoor, and Y. Jin, "**Device Attestation: Past, Present, and Future**," Design Automation, and Test in Europe (**DATE**), 2018.

89. E. Principe, N. Asadi, D. Forte, M. Tehranipoor, R. Chivas, M. DiBattista, S. Silverman, M. Marsh, N. Piche, J. Mastovich, "**Steps Toward Computational Guided Deprocessing of Integrated Circuits**," GomacTech, 2018.

90. D. Capecci, G. Contreras, D. Forte, M. Tehranipoor, and S. Bhunia, "**Automated SoC Security from Design to Fabrication**," GomacTech, 2018.

91. S. Beireddy, N. Asadi, M. Tehranipoor, D. Woodard, and D. Forte, "**Automated Detection of Counterfeit IC Defects Using Image Processing**," GomacTech, 2018 (poster).

92. J. He, X. Guo, M. Tehranipoor, and Y. Jin, "**Golden Chip Free Electromagnetic Simulation and Statistical Analysis for Hardware Security**," GomacTech, 2018 (poster).

93. U. Botero, M. Tehranipoor, and D. Forte, "**Downgrade: A Framework for Obsolescence Handling through Backwards Compatibility**," GomacTech, 2018.

94. F. Rahman, M. Farmani, M. Tehranipoor, and Y. Jin, "**Hardware-assisted Cybersecurity for IoT Devices**," IEEE Microprocessor Test, Security, and Verification (**MTV**), 2017.

95. X. Wang, L. Yu, F. Rahman, and M. Tehranipoor, "**IV-PUF: Interconnect Variations PUF with Self-Masking Circuit for Performance Enhancement**," IEEE Microprocessor Test and Security Conference (**MTV**), 2017

96. S. Choudhury, X. Xu, M. Tehranipoor, and D. Forte, "**Aging-Resistant RO PUF with Increased Reliability in FPGA**," Int. Conference on Reconfigurable Computing and FPGAs (**Reconfig**), 2017.

97. A. Chhotaray, A. Nahiyan, T. Shrimpton, D. Forte, and Mark Tehranipoor, "**Standardizing Bad Cryptographic Practice - A teardown of the IEEE standard for protecting electronic-design intellectual property**," ACM Conference on Computer and Communication Security (**CCS**), 2017.

98. X. Wang, Y. Guo, T. Rahman, D. Zhang, and M. Tehranipoor, "**DOST: Dynamically Obfuscated Wrapper for Split Test against IC Piracy**," IEEE Asian Hardware-Oriented Security and Trust Symposium (**AsianHOST**), 2017. **Received Best Paper Award.**

99. Z. Guo, X. Xu, M. Tehranipoor, and D. Forte, "**MPA: Model-assisted PCB Attestation via Board-level RO and Temperature Compensation**," IEEE Asian Hardware-Oriented Security and Trust Symposium (**AsianHOST**), 2017.

100. K. Yang, H. Shen, D. Forte, and M. Tehranipoor, "**A Split Manufacturing Approach for Unclonable Chipless RFIDs for Pharmaceutical Supply Chain Security**," IEEE Asian Hardware-Oriented Security and Trust Symposium (**AsianHOST**), 2017.

101. E.L. Principe, N. Asadizanjani, D. Forte, M. Tehranipoor, R. Chivas, M. DiBattista, S. Silverman, M. Marsh, J. Mastovich, J. Odum, "**Steps Towards Automated Deprocessing of Integrated Circuits**," International Symposium on Test and Failure Analysis (**ISTFA**), 2017. **Received Outstanding Paper Award**.

102. A. Nahiyan, M. Sadi, R. Vittal, G. Contreras, D. Forte, and M. Tehranipoor, "**Hardware Trojan Detection Through Information Flow Security Verification**," International Test Conference (**ITC**), 2017.

103. X. Xu, B. Shakiya, M. Tehranipoor, and D. Forte, "**Novel Bypass Attack and BDD-based Tradeoff Analysis Against all Known Logic Locking Attacks**," Conference on Cryptographic Hardware and Embedded Systems (**CHES**), 2017.

104. Z. Guo, M. Tehranipoor, and D. Forte, "**Memory-based Counterfeit IC Detection Framework**," SRC TECHCON, 2017.

105. A. Nahiyan, D. Forte, and M. Tehranipoor, "**Framework for Automated and Systematic Security Assessment of Modern SoCs**," SRC TECHCON, 2017.

106. J. Park, M. Corba, A. E. de la Serna, R. Vigeant, M. Tehranipoor, and S. Bhunia, "**ATAVE: A Framework for Automatic Timing Attack Vulnerability Evaluation**," IEEE Mid-West Symposium on Circuits and Systems (**MWSCAS**), 2017.

107. S. Amir, B. Shakya, D. Forte, M. Tehranipoor, and S. Bhunia, "**Comparative Analysis of Hardware Obfuscation for IP Protection**," ACM Great Lake Symposium on VLSI (**GLS-VLSI**), 2017.

108. Q. Shi, K. Xiao, D. Forte, and M. Tehranipoor, "**Securing Split Manufactured ICs with Wire Lifting Obfuscated Built-In Self-Authentication**," ACM Great Lake Symposium on VLSI (**GLS-VLSI**), 2017.

109. M. Sadi, S. Kannan, and M. Tehranipoor, "**Design of a Digital IP for 3D-IC Die-to-Die Clock Synchronization**," IEEE International Symposium on Circuits & Systems (**ISCAS**), 2017.

110. Z. Guo, M. Tehranipoor, and D. Forte, "**FFD: A Framework for Fake Flash Detection**," Design Automation Conference (**DAC**), 2017.

111. T. Bryant, S. Chowdhury, D. Forte, M. Tehranipoor and N. Maghari, "**A Stochastic All-Digital Weak Physically Unclonable Function for Analog/Mixed-Signal Applications**," IEEE Int. Symposium on Hardware-Oriented Security and Trust (**HOST**), 2017.

112. N. Karimian, M. Tehranipoor, and D. Forte, "**Non-Fiducial PPG-based Authentication for Healthcare Application**," Engineering in Medicine and Biology Conference (**EMBC**), 2017.

113. N. Karimian, M. Tehranipoor, and D. Forte, "**Noise Assessment Framework for Optimizing ECG Key Generation**," International Conference on Technologies for Homeland Security, 2017.

114. D. Zhang, X. Wang, T. He, and M. Tehranipoor, "**A Novel Dynamic Obfuscation Scan Design for Protecting IPs against Scan-Based Attack**," IEEE VLSI Test Symposium (**VTS**), 2017.

115. Q. Shi, N. Asadi, D. Forte, and M. Tehranipoor, "**Layout-based Microprobing Vulnerability Assessment for Security Critical Applications**," **GOMACTech**, 2017.

116. N. Kariminan, Z. Guo, M. Tehranipoor, and D. Forte, "**Human Recognition from Photoplethysmography (PPG) Based on Non-fiducial Features**," IEEE International Conference on Acoustics, Speech, and Signal Processing (**ICASSP**), 2017.

117. G. K. Contreras, A. Nahiyan, S. Bhunia, D. Forte, M. Tehranipoor, "**Security Vulnerability Analysis of Design-for-Test Exploits for Asset Protection in SoCs**," Asia and South Pacific Design Automation Conference (**ASP-DAC**), 2017.

118. R. Karam, T. Hoque, S. Ray, M. Tehranipoor, S. Bhunia, "**MUTARCH: Architectural Diversity for FPGA Device and IP Security**," Asia and South Pacific Design Automation Conference (**ASP-DAC**), 2017.

119. Z. Guo, M. Tehranipoor, and D. Forte, "**Aging Attacks for Key Extraction on Permutation-Based Obfuscation**," IEEEE Asian Hardware-Oriented Security and Trust (**AsianHOST**), 2016.

120. T. Rahman, D. Forte, X. Wang, and M. Tehranipoor, "**Enhancing Noise Sensitivity of Embedded SRAMs for Robust True Random Number Generation in SoCs**," IEEEE Asian Hardware-Oriented Security and Trust (**AsianHOST**), 2016.

121. R. Karam, T. Hoque, S. Ray, M. Tehranipoor and S. Bhunia, "**Robust Bitstream Protection in FPGA-based Systems through Low-Overhead Obfuscation**," **ReConFig** 2016.

122. M. Sadi, G. Contreras, D. Tran, J. Chen, L. Winemberg, and M. Tehranipoor, "**BIST-RM: BIST-Assisted Reliability Management of SoCs Using On-Chip Clock Sweeping and Machine Learning**," International Test Conference (**ITC**), 2016.

123. M. Alam, M. Tehranipoor, and D. Forte, "**Recycled FPGA Detection using Exclusive LUT Path Delay Characterization**," International Test Conference (**ITC**), 2016.

124. T. Bryant, S. Chowdhury, D. Forte, M. Tehranipoor, and N. Maghari, "**A Stochastic Approach to Analog Physical Unclonable Function**," IEEE Midwest Symposium on Circuits and Systems (**MWSCAS**), 2016.

125. B. Shakya, N. Asadi, D. Forte, and M. Tehranipoor, "**Chip Editor: leveraging Circuit Edit for Logic Obfuscation and Trusted Fabrication**," IEEE International Conference on Computer-Aided Design (**ICCAD**), 2016.

126. N. Karimian, D. Woodard, M. Tehranipoor, and D. Forte, "**Biometrics for Authentication in Resource-Constrained Systems**," Annual International Conference of the IEEE Engineering in Medicine and Biology Society (**EMBC**), 2016.

127. G. Contreras and M. Tehranipoor, "**Fault Deterministic Vector Analysis and Seed Extraction for LBIST**," SRC TECHCON, 2016. **Received Best in Session Award.**

128. M. He and M. Tehranipoor, "**Test-Point Insertion Efficiency Analysis for LBIST Applications**," SRC TECHCON, 2016.

129. M. Sadi and M. Tehranipoor, "**BIST-Assisted In-field Aging Reliability Management of SoCs Using On-Chip Clock Sweeping and Machine Learning**," SRC TECHCON, 2016. **Received Best in Session Award.**

130. T. Rahman, D. Forte, and M. Tehranipoor, "**SRAM Inspired Design and Optimization for Developing Robust Security Primitives**," SRC TECHCON, 2016. **Received Best in Session Award.**

131. N. Asadizanjani, D. Forte, and M. Tehranipoor, "**Non-destructive Bond Pull and Ball Shear Failure Analysis Based on Real Structural Properties**," Int. Symposium on Testing and Failure Analysis (**ISTFA**), 2016.

132. N. Asadizanjani, H. Chen, B. Shakya, D. Forte, S. Bhunia, and M. Tehranipoor, "**A New Methodology to Protect PCBs from Non-destructive Reverse Engineering**," Int. Symposium on Testing and Failure Analysis (**ISTFA**), 2016.

133. N. Asadizanjani, S. Gattigowda, N. Dunn, D. Forte, and M. Tehranipoor, "**A Database for Counterfeit Electronics and Automatic Defect Detection Based on Image processing and Machine Learning**," Int. Symposium on Testing and Failure Analysis (**ISTFA**), 2016.

134. S. Ray, S. Bhunia, Y. Jin, and M. Tehranipoor, "[Extended Abstract] **Security Validation in IoT Space**," IEEE VLSI Test Symposium (**VTS**), 2016.

135. H. Shen, F. Rahman, B. Shakya, M. Tehranipoor, and D. Forte, "**Selective Enhancement of Randomness at the Materials Level: Poly-Si Based Physical Unclonable Functions (PUFs)**," IEEE Computer Society Annual Symposium on VLSI (**ISVLSI**) 2016.

136. T. Li, J. Di, M. Tehranipoor, D. Forte, and L. Wang, "**Tracking Data Flow at Gate-Level through Structural Checking**," ACM **GLS-VLSI**, 2016.

137. A. Zaghi and Mark Tehranipoor, "**Major Observations from a Specialized REU Program for Engineering Students with ADHD**," American Society for Engineering Education (**ASEE**), 2016.

138. F. Rahman, D. Forte, and Mark Tehranipoor, "**Reliability vs. Security: Challenges and Opportunities for Developing Reliable and Secure Integrated Circuits**," International Reliability Physics Symposium (**IRPS**), 2016.

139. M. Sadi and M. Tehranipoor, "**BIST-Assisted Reliability Management of SoC Using On-chip Clock Sweeping and Machine Learning**," IEEE Reliability Innovations Conference (**IRIC**), 2016 (extended abstract).

140. K. Yang, D. Forte, and M. Tehranipoor, "**UCR: An Unclonable Chipless RFID Tag**," IEEE Symposium on Hardware-Oriented Security and Trust (**HOST**), 2016.

141. Q. Shi, N. Asadi, D. Forte, and M. Tehranipoor, "**A Layout-driven Framework to Assess Vulnerability of ICs to Microprobing Attacks**," IEEE Symposium on Hardware-Oriented Security and Trust (**HOST**), 2016. **(Best Paper Award)**

142. Z. Guo, T. Rahman, M. Tehranipoor, and D. Forte, "**A Zero-cost Approach to Detect Recycled SoC Chips Using Embedded SRAM**," IEEE Symposium on Hardware-Oriented Security and Trust (**HOST**), 2016. **(Best Paper Nominate)**

143. A. Nahiyan, K. Xiao, K. Yang, D. Forte, Y. Jin, and M. Tehranipoor, "**AVFSM: A Framework for Identifying and Mitigating Vulnerabilities in FSMs**," Design Automation Conference (**DAC**), 2016.

144. Z. Guo, N. Karimian, M. Tehranipoor, and D. Forte, "**Hardware Security Meets Biometrics for the Age of IoT**," Int. Symposium on Circuits and Systems (**ISCAS**), 2016.

145. T. Meade, Y. Jin, M. Tehranipoor, S. Zhang, "**Gate-Level Netlist Reverse Engineering for Hardware Security: Control Logic Register Identification**," Int. Symposium on Circuits and Systems (**ISCAS**), 2016.

146. L. Yu, X. Wang, P. Jiao, A. Chen, D. Su, L. Winemberg, M. Sadi, and M. Tehranipoor, "**An Efficient All-Digital Alarmer for DVFS-based SOC**," Int. Symposium on Circuits and Systems (**ISCAS**), 2016.

147. L. Wu, X. Wang, D. Su, A. Chen, Q. Shi, and M. Tehranipoor, "**AES Design Improvement Toward Information Safety**," Int. Symposium on Circuits and Systems (**ISCAS**), 2016.

148. M. He, G. Contreras, M. Tehranipoor, D. Tran, and L. Winemberg, "**Test Point Insertion Efficiency Analysis for LBIST Applications**," IEEE VLSI Test Symposium (**VTS**), 2016.

149. T. Meade, S. Zhang, M. Tehranipoor, and Y. Jin, "**A Comprehensive Netlist Reverse Engineering Toolset for IC Trust**," GomacTech, 2016.

150. N. Asadi, S. Shahbazi, D. Forte, and M. Tehranipoor, "**Nondestructive X-ray Tomography Based Bond Pull and Ball Shear Analysis**," GomacTech, 2016.

151. Z. Guo, N. Karimian, M. Tehranipoor, and D. Forte, "**Biometric Based Human-to-Device (H2D) Authentication**," GomacTech, 2016.

152. M. Alam, N. Asadi, S. Shahbazi, D. Forte, and M. Tehranipoor, "**The Impact of X-ray Tomography on the Reliability of FPGAs**," GomacTech, 2016.

153. B. Shakya, F. Rahman, M. Tehranipoor, and D. Forte, "**Security in Nanoscale Regime – A Perspective Paper**," IEEE Microprocessor Test and Verification (**MTV**), 2015.

154. K. Ahi, N. Asadi, M. Tehranipoor, and M. Anwar, "**Authentication of electronic components by time domain THz Techniques**," Connecticut Microelectronic Symposium (**CMOC**), 2015 (extended abstract).

155. K. Yang, D. Forte, and M. Tehranipoor, "**Protecting Endpoint Devices in IoT Supply Chain**," International Conference on Computer-Aided Design (ICCAD), 2015.

156. Q. Shi, R. Tekumalla, and M. Tehranipoor, "**Concurrent Testing of Logic and Memory, and Detection of Memory Functional Paths in SOCs**," International Test Conference, 2015 (inovted).

157. B. Shakya, U. Guin, M. Tehranipoor, and D. Forte, "**Performance Optimization for On-Chip Sensors to Detect Recycled ICs**," IEEE Int. Conference on Computer Design (ICCD), 2015.

158. T. Rahman, F. Rahman, D. Forte, and M. Tehranipoor, "**A Pair Selection Algorithm for Robust RO-PUF Against Environmental Variations and Aging**," IEEE Int. Conference on Computer Design (ICCD), 2015.

159. G. Contreras, L. Winemberg, M. Tehranipoor, and N. Ahmed, "**Predictive LBIST Model and partial ATPG for Seed Extraction**," IEEE Defect and Fault Tolerant Systems (DFTS), 2015.

160. S. Chen, J. Chen, D. Forte, J. Di, M. Tehranipoor, and L. Wang, "**Chip Level Anti-reverse Engineering using Transformable Interconnects**," IEEE Defect and Fault Tolerant Systems (DFTS), 2015.

161. N. Asadi, S. Shahbaz, M. Tehranipoor, and D. Forte, "**Non-destructive PCB Reverse Engineering Using X-ray Micro Computed Tomography**," Int. Symposium for Testing and Failure Analysis (ISTFA), 2015.

162. H. Dogan, N. Asadi, S. Shahbaz, D. Forte, and M. Tehranipoor, "**Analyzing the Impact of X-ray Tomography for Non-destructive Counterfeit Detection**," Int. Symposium for Testing and Failure Analysis (ISTFA), 2015.

163. K. Ahi, N. Asadi, S. Shahbaz, M. Tehranipoor, and M. Anwar, "**Terahertz Characterization of Electronic Components and Comparison of Terahertz Imaging with X-ray Imaging Techniques**," Terahertz Physics, Devices, and Systems, 2015.

164. K. Yang, D. Forte, and M. Tehranipoor, "**ReSC: RFID-enabled Supply Chain Management and Traceability for Network Devices**," RFID Security, 2015.

165. T. Rahman, D. Forte, and M. Tehranipoor, "**Robust SRAM-PUF: Cell Stability Analysis and Novel Bit-Selection Algorithm**," TECHCON, 2015.

166. M. Sadi and M. Tehranipoor, "**An Efficient Speed Binning Methodology for SoC Using On-chip Slack Sensors and Machine Learning**," TECHCON, 2015.

167. J. Chandy, et. al, "**Hardware Hacking: An Approach to Trustable Computing Systems Security Education**," The Colloquium for Information Systems Security Education (**CISSE**). Las Vegas, June 2015.

168. Z. Guo, J. Di, M. Tehranipoor, and D. Forte, "**Investigation of Obfuscation-based Anti-Reverse Engineering for Printed Circuit Boards**," Design Automation Conference (**DAC**), 2015.

169. M. Sadi, X. Wang, L. Winemberg, and M. Tehranipoor, "**Speed Binning using Machine Learning and On-chip Slack Sensors**," ACM Great Lake Symposium on VLSI (**GLSVLSI**), 2015.

170. M. Sadi and M. Tehranipoor, "**Timing Slack Extraction for SoC Reliability Monitoring with Robust Digital Sensor IP and Sensor Insertion Flow**," IEEE Reliability Innovations Conference (**IRIC**), 2015 (extended abstract).

171. T. Rahman, A. Hosey, K. Xiao, D. Forte, and M. Tehranipoor, "**Cell Stability Analysis and Novel Bit-Selection Algorithm for Robust SRAM-PUF**," Connecticut Microelectronic Symposium (**CMOC**), 2015 (extended abstract).

172. M. Sadi and M. Tehranipoor, "**A Robust Multipurpose Digital Sensor IP for In-situ Path Timing Slack Monitoring in SOCs**," IEEE VLSI Test Symposium (**VTS**), 2015.

173. K. Xiao, D. Forte, and M. Tehranipoor, "**Efficient and Secure Split Manufacturing via Obfuscated Built-In Self-Authentication**," IEEE Hardware-Oriented Security and Trust (**HOST**), 2015. (**Best Paper Award)**

174. K. Yang, D. Forte, and M. Tehranipoor, "**An RFID-based Technology for Electronic Component and System Counterfeit Detection and Traceability**," IEEE International Conference on Technologies for Homeland Security (**HST**), 2015.

175. G. Contreras, M. Tehranipoor, N. Ahmed, L. Winemberg, and Y. Zhao, "**LBIST Pattern Reduction by Learning ATPG Test Cube Properties**," International Symposium on Quality Electronic Design (**ISQED**), 2015.

176. S. Quadir, N. Asadi, D. Forte, and M. Tehranipoor, "**Rapid Non-destructive Reverse Engineering of Printed Circuit Boards by High Resolution X-ray Tomography**," GOMACTech, 2015.

177. T. Rahman, A. Hosey, F. Rahman, D. Forte, and M. Tehranipoor, "**RePa: A Pair Selection Algorithm for Reliable Keys from RO-based PUF**," GOMACTech, 2015.

178. H. Dogan, D. Forte, and M. Tehranipoor, "**Aging Analysis for Recycled FPGA Detection**," GOMACTech, 2015.

179. M. Sadi, Z. Conroy, B. Eklow, M. Kamm, N. Bidokhti, and M. Tehranipoor, "**An All-Digital Distributed Sensor Network Based Framework for Continuous Noise Monitoring and Timing Failure Analysis in SOCs**" IEEE Asian Test Symposium (**ATS**), pp. 269-274, 2014.

180. A. Hosey, T. Rahman, K. Xiao, D. Forte, and M. Tehranipoor, "**Advanced Analysis of Cell Stability for Reliable SRAM PUFs**," IEEE Asian Test Symposium (**ATS**), pp. 348-358, 2014.

181. H. Dogan, D. Forte, and M. Tehranipoor, "**Aging Analysis for Recycled FPGA Detection**," IEEE Int. Symposium on Defect and Fault Tolerance Symposium (**DFTS**), pp. 171-76, 2014.

182. M. He and M. Tehranipoor, "**SAM: A Comprehensive Mechanism for Accessing Embedded Sensors in Modern SoCs**," IEEE Int. Symposium on Defect and Fault Tolerance Symposium (**DFTS**), pp. 240-246, 2014.

183. T. Rahman, D. Forte, Q. Shi, G. Contreras, and M. Tehranipoor, "**CSST: Preventing Distribution of Unlicensed and Rejected ICs by Untrusted Foundry and Assembly**," IEEE Int. Symposium on Defect and Fault Tolerance Symposium (**DFTS**), pp. 46-51, 2014.

184. M. Sadi and M. Tehranipoor, "**A SOC Noise Monitoring and Diagnosis with Fully Digital On-Chip Distributed Sensor Network,"** SRC TECHCON 2014.

185. G. Contreras and M. Tehranipoor, "**Improving LBIST Pattern Quality and Test Point Reduction**," SRC TECHCON 2014.

186. Q. Shi, X. Wang, L. Winemberg, and M. Tehranipoor, "**On-Chip Sensor Selection for Effective Speed-Binning,**" IEEE Mid-West Symposium on Circuits and Systems (**MWSCAS**), Oct. 2014.

187. S. Shahbaz, D. Forte, and M. Tehranipoor, "**Advanced Physical Inspection Methods for Counterfeit Detection**," Int. Symposium for Testing and Failure Analysis (**ISTFA**), pp. 1073-1076, 2014 (**Best Paper Candidate**).

188. S. Shahbaz, D. Forte, and M. Tehranipoor, "**Advanced Physical Inspection Techniques for Counterfeit IC Detection**," Calce Symposium on Counterfeit Electronics and Supply Chain, pp. 55-64, 2014.

189. G. Contreras, N. Ahmed, L. Winemberg, and M. Tehranipoor, "**TAME-TPI: A Timing-Aware Metric for Efficient Test Point Insertion and Area Overhead Reduction**," IEEE North Atlantic Test Workshop (**NATW**), 2014.

190. T. Rahman, D. Forte, Q. Shi, G. Contreras, and M. Tehranipoor, "**CSST: An Efficient Secure Split-Test for Preventing IC Piracy**," IEEE North Atlantic Test Workshop (**NATW**), pp. 43-47, 2014.

191. X. Wang, L. Winemberg, A. Haggag, J. Chayachinda, A. Saluja and M. Tehranipoor, "**Fast Aging Degradation Rate Prediction During Production Test**," International Reliability Physics Symposium (**IRPS**), pp. 6B.5.1-6B.5.5, 2014.

192. M. Sadi and M. Tehranipoor, "**On-Chip Sensors for Chip Timing Failure Analysis**", Connecticut Symposium on Microelectronics and Optoelectronics (**CMOC**), 2014.

193. M. Sadi, Z. Conroy, M. Kamm, B. Eklow, N. Bidokhti and M. Tehranipoor "**System on Chip Noise Reliability Testing and Monitoring with Light-Weight Fully Digital Embedded Sensor Network**" IEEE International Reliability Innovation Conference (**IRIC**), 2014.

194. K. Xiao, T. Rahman, D. Forte, M. Tehranipoor, M. Su, and Y. Huang, "**Bit Selection Algorithm Suitable for High Volume Production of SRAM PUF**," IEEE International Symposium on Hardware-Oriented Security and Trust (**HOST**), pp. 101-106, 2014.

195. T. Rahman, K. Xiao, D. Forte, X. Zhang, Z. Shi, and M. Tehranipoor, "**TI-TRNG: Technology Independent True Random Number Generator**," Design Automation Conference (**DAC**), 2014.

196. U. Guin, X. Zhang, D. Forte, and M. Tehranipoor, "**Low-Cost On-Chip Structures for Combating Die and IC Recycling**," Design Automation Conference (**DAC**), 2014.

197. J. Chen, L. Winemberg, and M. Tehranipoor, "**Identification of Testable Representative Paths for Low-Cost Verification of Circuit Performance During Manufacturing Tests and in the Field**," IEEE VLSI Test Symposium (**VTS**), 2014.

198. S. Hamdiui, G. Di Natalie, G. van Battum, J. Danger, F. Smailbegovic, and M. Tehranipoor, "**Hacking and Protecting IC Hardware**," Design, Automation, and Test in Europe (**DATE**), 2014.

199. T. Rahman, D. Forte, M. Tehranipoor, and J. Fahrny, "**ARO-PUF: An Aging-Resistant Ring-Oscillator PUF Design**," Design, Automation, and Test in Europe (**DATE**), pp. 1-6, 2014.

200. K. Xiao, T. Rahman, D. Forte, M. Tehranipoor, Y. Huang, and M. Su, "**Low-cost Analysis of SRAM PUFs for Identification of Mass-Produced Electronic Devices**," **GOMACTech**, 2014.

201. U. Guin, D. Forte, D. DiMase, and M. Tehranipoor, "**Counterfeit IC Detection: Test Method Selection Considering Test Time, Cost, and Tier Level Risk**," **GOMACTech**, 2014.

202. U. Guin, D. Forte, and M. Tehranipoor, "**Low-cost On-Chip Structures for Combating Die and IC Recycling**," **GOMACTech**, 2014.

203. N. Bidokhti, M. Tehranipoor, J. Chen, and J. Lee, "**Life After Failure**," Reliability and Maintainability Symposium (**RAMS**), 2014.

204. U. Guin, D. Forte, and M. Tehranipoor, "**Anti-Counterfeit Techniques: From Design to Resign**," IEEE Microprocessor Test Verification (**MTV**), pp. 89-94, 2013.

205. J. Chen and M. Tehranipoor, "**Critical Paths Selection and Test Cost Reduction Considering Process Variations**," IEEE Asian Test Symposium (**ATS**), pp. 259 - 264, 2013.

206. F. Bao, H. Chen, and M. Tehranipoor, "**Worst-case Critical-Path Delay Analysis Considering Power-Supply Noise**," IEEE Asian Test Symposium (**ATS**), pp. 37-42, 2013.

207. A. Tomita, X. Wen, Y. Sato, S. Kajihara, P. Girard, M. Tehranipoor, and L.T. Wang, "**On Achieving Capture Power Safety in At-speed Scan-based Logic BIST**," IEEE Asian Test Symposium (**ATS**), pp. 19-24, 2013.

208. U. Guin and M. Tehranipoor, "**CDIR: Low-Cost Combating Die/IC Recycling Structures**," **DMSMS**, 2013 (Invited)

209. U. Guin, D. DiMase, and M. Tehranipoor, "**CDC: Counterfeit Defect Coverage Analysis**," **DMSMS**, 2013 (Invited)

210. A. Mazady, H. Chi Chou, M. Tehranipoor and M. Anwar, "**Terahertz Spectroscopy: A Technology Platform for the Detection of Counterfeit Electronics**," **DMSMS**, 2013 (Invited)

211. U. Guin, T. Chakraborty, and M. Tehranipoor, "**Novel DFTs for Circuit Initialization to Reduce Functional Fmax Test Time**," IEEE Int. Conference on Computer Design (**ICCD**), 2013. ??

212. H. Salmani, M. Tehranipoor, and R. Karri, "**Trust Benchmark and Design Vulnerability Analysis**," IEEE Int. Conference on Computer Design (**ICCD**), 2013 (poster).

213. G. Contreras, T. Rahman, and M. Tehranipoor, "**Secure Split-Test for Preventing IC Piracy by Untrusted Foundry and Assembly**," Int. Symposium on Defect and Fault Tolerance in VLSI Systems (**DFT**), pp. 196-203, 2013.

214. H. Salmani and M. Tehranipoor, "**Analyzing Circuit Vulnerability to Hardware Trojan Insertion at the Behavioral Level**," Int. Symposium on Defect and Fault Tolerance in VLSI Systems (**DFT**), pp. 190-195, 2013.

215. Q. Shi, J. Chen, and M. Tehranipoor, "**Silicon Data Based Delay Analysis and PDF Pattern Generation for Advanced Technology Node**," SRC TECHCON, September 2013.

216. M. Tehranipoor, "**An All-in-One Anti-Counterfeiting Technology for Integrated Circuits**," Symposium on Counterfeit Electronic Parts and Electronic Supply Chain, 2013.

217. Q. Shi, X. Wang, L. Winemberg, and M. Tehranipoor, "**Experimental Analysis of Variations' Impact on Integrated Circuits Performance in Advanced Technology Nodes**," North Atlantic Test Workshop (**NATW**), 2013.

218. U. Guin, T. Chakraborty, and M. Tehranipoor, "**Novel DFTs for Circuit Initialization to Reduce Functional Fmax Test Time**," North Atlantic Test Workshop (**NATW**), 2013.

219. U. Guin and M. Tehranipoor, "**On Selection of Counterfeit IC Detection Methods**," North Atlantic Test Workshop (**NATW**), 2013.

220. K. Xiao and M. Tehranipoor, "BISA: **Built-In Self-Authentication for Preventing Hardware Trojan Insertion**," Int. IEEE Symposium on Hardware-Oriented Security and Trust (**HOST**), pp. 45-50, 2013.

221. X. Zhang, K. Xiao, M. Tehranipoor, J. Rajendran, and R. Karri, "**A Study on the Effectiveness of Trojan Detection Techniques using a Red Team Blue Team Approach**," IEEE VLSI Test Symposium (**VTS**), 2013.

222. G. Contreras and M. Tehranipoor, "**ATPG Learning BIST for Increasing Pattern Effectiveness**," IEEE International Reliability Innovation Conference (**IRIC**), 2013.

223. J. Chen and M. Tehranipoor, "**Efficient Skew Reduction for Clock Tree Design Considering NBTI and Process Variation**," IEEE International Reliability Innovation Conference (**IRIC**), 2013.

224. M. Tehranipoor and U. Guin, "**Counterfeit Detection Technology Assessment**," GOMACTech-2013.

225. M. Tehranipoor and K. Xiao, "**BISA: Built-In Self-Authentication to Prevent Insertion of Trojans by Untrusted Foundry**," GOMACTech-2013.

226. J. Chen and M. Tehranipoor, "**A Novel Flow for Reducing Clock Skew Considering NBTI Effect and Process Variations**," Int. Symposium on Quality Electronics Design (ISQED), pp. 327-334, 2013.

227. W. Zhao and M. Tehranipoor, "**PowerMAX: Fast Power Analysis During Test**," IEEE Asian Test Symposium (**ATS**), pp. 227-232, 2012 (*invited*).

228. S. Wang and M. Tehranipoor, "**Representative Critical Reliability Paths for Low-Cost and Accurate On-Chip Aging Evaluation**," Int. Conf. on Computer-Aided Design (**ICCAD**), pp. 736-741, 2012.

229. A. Ferraiuolo, X. Zhang, and M. Tehranipoor, "**Experimental Analysis of a Ring Oscillator Network for Hardware Trojan Detection in a 90nm ASIC**," Int. Conf. on Computer-Aided Design (**ICCAD**), pp. 37-42, 2012.

230. X. Wang, D. Tran, S. George, L. Winemberg, N. Ahmed, S. Palosh, A. Dobin, and M. Tehranipoor, "**Radic: A standard-cell Based Sensor for On-Chip Aging and Flip-Flop Metastability Measurements**," Int. Test Conference (**ITC**), pp. 1-9, 2012.

231. X. Wen, Y. Nishida, K. Miyase, S. Kajihara, P. Girard, M. Tehranipoor, and L.T. Wang, "**On Pinpoint Capture Power Management in At-Speed Scan Test Generation**," Int. Test Conference (**ITC**), pp. 1-10, 2012.

232. X. Zhang, K. Xiao, and M. Tehranipoor, "**Path-Delay Fingerprinting for Identification of Recovered ICs**" in Proc. IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (**DFTS**), pp. 13-18, 2012. **Received Best Student Paper Award**

233. M. Tehranipoor, "**SST: Secure Split-Test for Preventing IC Piracy and Easy Detection**," DMSMS & Standardization, pp. 1-8, 2012.

234. N. Murphy, U. Guin, and M. Tehranipoor, "**Counterfeit Detection Technology Assessment**," DMSMS & Standardization, 2012.

235. X. Zhang, N. Tuzzio, and M. Tehranipoor, "**Identification of Recovered ICs using Fingerprints from a Light-Weight On-Chip Sensor**," Design Automation Conference (**DAC**), pp. 703-708, 2012.

236. S. Wang, Q. Shi, J. Chen, and M. Tehranipoor, "**On-Chip Structures and Test Methodologies for Analyzing Performance Degradation in Modern Designs**," SRC TECHCON, 2012.

237. N. Tuzzio, Kan Xiao, X. Zhang, and M. Tehranipoor, "**A Zero-Overhead IC Identification Technique using Clock Sweeping and Path Delay Analysis**," IEEE **GLSVLSI**, pp. 95-98, 2012.

238. S. Wang and M. Tehranipoor, "**TSUNAMI: "A Light-Weight On-Chip Structure for Measuring Timing Uncertainty Induced by Noise during Functional and Test Operations**," IEEE **GLSVLSI**, pp. 183-188, 2012.

239. J. Chen, S. Wang, and M. Tehranipoor, "**Efficient Selection and Analysis of Critical—Rreliability Paths and Gates**," IEEE **GLS-VLSI**, pp. 45-50, 2012.

240. M. Tehranipooor, "**Combating IC Recovery for Improving Reliability and Security of Digital Integrated Circuits,"** IEEE Int. Reliability Innovations Conference (**IRIC**), 2012 (*Extended Abstract*).

241. M. Tehranipoor and N. Bidokhti, "**Timing Analysis and On-Chip Measurement Considering Aging**," IEEE Int. Reliability Innovations Conference (**IRIC**), 2012 (*Extended Abstract*).

242. W. Zhao, S. Chakravarty, J. Ma, N. Devta-Prasanna, F. Yang, M. Tehranipoor, "**A Novel Method for Fast Identification of Peak Current during Test**," IEEE VLSI Test Symposium (**VTS**), pp. 191-196, 2012.

243. X. Zhang, N. Tuzzio, and M. Tehranipoor, "**CDR: Combating Die Recovery**," **GOMACTech**, Las Vegas, 2012.

244. M. Li, A. Davoodi, and M. Tehranipoor, "**A sensor-assisted self-authentication framework for hardware Trojan detection**", in Proc. Design, Automation, and Test in Europe (**DATE**), pp. 74-82, 2012.

245. X. Zhang, N. Tuzzio, and M. Tehranipoor, "**Red Team Design of Intelligent Hardware Trojans with Known Defense Schemes**," Int. Conference on Computer Design (**ICCD**), pp. 309-312, 2011.

246. F. Bao, K. Peng, K. Chakrabarty, and M. Tehranipoor, "**On Generation of 1-Detect TDF Pattern Set with Significantly Increased SDD Coverage**," IEEE Asian Test Symposium (**ATS**), pp. 120-125, 2011.

247. H. Salmani, W. Zhao, M. Tehranipoor, S. Chakravarty, P. Girard, X. Wen, "**Layout-Aware Pattern Evaluation and Analysis for Power-Safe Application of TDF Patterns**," IEEE LPonTR, pp. 248-258, 2011.

248. F. Wu, L. Dilillo, A. Bosio, P. Girard, M. Tehranipoor, K. Miyase, X. Wen, N. Ahmed, "**Mapping Test Power to Functional Power Through Smart X-Filling for LOS Scheme**," IEEE LPonTR, 2011.

249. J. Chen and M. Tehranipoor, "**On-Chip Structures and Methodologies for Reliable Circuit Design**," Poster, SRC TECHCON, 2011.

250. S. Wang, L. Winemberg, and M. Tehranipoor, "**In-Field Aging Measurement and Calibration for Power-Performance Optimization**," in Proc. Design Automation Conference (**DAC**), pp. 706-711, 2011.

251. W. Zhao and M. Tehranipoor, "**Peak Power Identification on Power Bumps During Test Application**," Low Power SOC Workshop (LPSOC), pp. 1-3, 2011 (*Invited*).

252. X. Zhang and M. Tehranipoor, "**Case Study: Detecting Hardware Trojans in Third-Party Digital IP Cores**," Int. IEEE Hardware-Oriented Security and Trust (**HOST**), pp. 67-70, 2011.

253. F. Bao, K. Peng, M. Yilmaz, K. Chakrabarty, and M. Tehranipoor, "**Critical Fault-Based Pattern Generation for Screening Small Delay Defects**," in proc. European Test Symposium (**ETS**), pp. 1177-182, 2011.

254. S. Wang and M. Tehranipoor, "**Aging Measurement and Calibration for Nanoscale VLSI Circuit**," Connecticut Symposium on Microelectronics and Optoelectronics (**CMOC**), 2011 (*Invited*).

255. J. Chen and M. Tehranipoor, "**Timing Analysis for Nanometer VLSI Designs Considering Aging Effects**," Connecticut Symposium on Microelectronics and Optoelectronics (**CMOC**), 2011 (*Poster*).

256. X. Zhang and M. Tehranipoor, "**RON: An On-chip Ring Oscillator Network for Hardware Trojan Detection**," Design, Automation, and Test in Europe (**DATE**), pp. 1-6, 2011.

257. F. Wu, L. Dilillo, A. Bosio, P. Girard, S. Pravossoudovitch, A. Virazel, M. Tehranipoor, K. Miyase, X. Wen, and N. Ahmed, "**Power Reduction Through X-filling of Transition Fault Test Vectors for LOS Testing**," in Design & Technology of Integrated Systems (**DTIS**), pp. 1-6, 2011.

258. W. Zhao, S. Chakravarty, and M. Tehranipoor, "**Power-Safe Test Application Using An Effective Gating Approach Considering Current Limits**," IEEE VLSI Test Symposium (**VTS**), pp. 160-165, 2011.

259. K. Peng, F. Bao, G. Shofner, L. Winemberg, and M. Tehranipoor, "**Case Study: Efficient SDD Test Generation for Very Large Integrated Circuits**," IEEE VLSI Test Symposium (**VTS**), pp. 78-83, 2011.

260. J. Ma, N. Ahmed, and M. Tehranipoor, "**Low-Cost Diagnostic Pattern Generation and Evaluation Procedures for Noise-Related Failures**," IEEE VLSI Test Symposium (**VTS**), pp. 309-314, 2011.

261. X. Wen, K. Enokimoto, K. Miyase, Y. Yamato, M. Kochte, S. Kajihara, P. Girard, M. Tehranipoor, "**Power-Aware Test Generation with Guaranteed Launch Safety for At-Speed Scan Testing**," IEEE VLSI Test Symposium (**VTS**), pp. 166-171, 2011.

262. M. Tehranipoor, "**Verifying Trustworthiness of Integrated Circuits**," **GOMACTech**, 2011 (*Invited*).

263. J. Chen, S. Wang, N. Bidokhti, and M. Tehranipoor, "**A Framework for Fast and Accurate Critical-Reliability Paths Identification**," IEEE North Atlantic Test Workshop (**NATW**), 2011.

264. F. Bao, K. Peng, K. Chakrabarty, L. Winemberg, and M. Tehranipoor, "**Increasing SDD Coverage without Increasing Pattern Count**," IEEE North Atlantic Test Workshop (**NATW**), 2011.

265. N. Reddy, S. Wang, L. Winemberg, and M. Tehranipoor, "**Experimental Analysis for Aging in Integrated Circuits**," IEEE North Atlantic Test Workshop (**NATW**), 2011.

266. J. Ma, M. Tehranipoor, O. Sinanoglu, and S. Almukhaizim, "**Identification of IR-drop Hot-spots in Defective Power Distribution Network Using TDF ATPG**," Int. Workshop on Design and Test (**IDT**), pp. 122-127, 2010.

267. M. Tehranipoor, "**Dealing with Reliability and Variability Issues in Nanometer Technology Designs**," Connecticut Symposium on Microelectronics and Optoelectronics (**CMOC**), 2010 (*Invited*).

268. H. Salmani, M. Tehranipoor, and J. Plusquellic, "**A Layout-Aware Approach for Improving Localized Switching to Detect Hardware Trojans in Integrated Circuits**," IEEE International Workshop on Information Forensics and Security (**WIFS**), pp. 1-6, 2010.

269. W. Zhao, J. Ma, M. Tehranipoor, and S. Chakravarty, "**Power-Safe Application of Transition Delay Fault Patterns Considering Current Limit during Wafer Test**," IEEE Asian Test Symposium (**ATS**), pp. 301-306, 2010.

270. K. Peng, M. Yilmaz, K. Chakrabarty, and M. Tehranipoor, "**A Noise-Aware Hybrid Method for SDD Pattern Grading and Selection**," IEEE Asian Test Symposium (**ATS**), pp. 331-336, 2010.

271. S. Goel, K. Chakrabarty, M. Yilmaz, K. Peng, and M. Tehranipoor, "**Circuit Topology-Based Test Pattern Generation for Small-Delay Defects**," IEEE Asian Test Symposium (**ATS**), pp. 307-312, 2010.

272. F. Wu, L. Dilillo, A. Bosio, P. Girard, S. Pravossoudovitch, A. Virazel, M. Tehranipoor, J. Ma, W. Zhao, X. Wen, "**Analysis of Power Consumption and Transition Fault Coverage for LOS and LOC Testing Schemes**," DDECS, pp. 376-381, 2010.

273. X. Wang and M. Tehranipoor, "**Low-Cost On-Chip Structures for Measuring NBTI Effects, Variations, Path Delay, and Noise**," SRC TECHCON, Poster Presentation, 2010.

274. F. Wu, L. Dilillo, A. Bosio, P. Girard, S. Pravossoudovitch, A. Virazel, M. Tehranipoor, K. Miyase, X. Wen, and N. Ahmed, "**Power reduction Through X-filling of Transition Fault Vectors for LOS Testing**," International Workshop on the Impact of Low Power design on Test and Reliability (LPonTR), pp. 1-6, 2010.

275. J. Ma and M. Tehranipoor, "**A Low-Cost Diagnostic Procedure for Parametric Failures Caused by Pattern-Induced Noises**," SRC TECHCON, Poster Presentation, 2010.

276. K. Peng, Y. Huang, W. T. Cheng, and M. Tehranipoor, "**Full-Circuit SPICE Simulation Based Validation of Dynamic Delay Estimation**," European Test Symposium (**ETS**), pp. 101-106, 2010.

277. J. Ma, J. Lee, N. Ahmed, P. Girard, and M. Tehranipoor, "**Pattern Grading for Testing Critical Paths Considering Power Supply Noise and Crosstalk Using a Layout-Aware Quality Metric**," Great-Lake Symposium on VLSI (**GLS-VLSI**), pp. 127-130, 2010

278. K. Peng, J. Thibodeau, M. Yilmaz, K. Chakrabarty, and M. Tehranipoor, "**A Novel Hybrid Method for SDD Pattern Grading and Selection**," IEEE VLSI Test Symposium (**VTS**), pp. 45-50, 2010.

279. K. Peng, M. Yilmaz, K. Chakrabarty, and M. Tehranipoor, "**High-Quality Pattern Selection for Screening Small-Delay Defects Considering Process Variations and Crosstalk**," Design, Automation, and Test in Europe (**DATE**), pp. 1426-1431, 2010.

280. X. Wang and M. Tehranipoor, "**Novel Physical Unclonable Function Based on Process and Environmental Variations**," Design, Automation, and Test in Europe (**DATE**), pp. 1065-1070, 2010.

281. K. Peng, Y. Huang, R. Guo, W. T. Cheng, and M. Tehranipoor, "**Emulating and Diagnosing IR-Drop by Using Dynamic SDF**," ASP-DAC, pp. 511-516, 2010.

282. X. Wang, M. Tehranipoor, and R. Datta, "**A Novel Architecture for On-Chip Path Delay Measurement**," International Test Conference (**ITC**), pp. 1-10, 2009.

283. J. Ma, J. Lee, and M. Tehranipoor, "**Extended Abstract: Developing a Novel Quality Metric for Path-Delay Fault Pattern Evaluation**," IEEE Int. Workshop on Defect and Data Driven Testing (**D3T**), 2009.

284. K. Peng, Y. Huan, W. T. Cheng, and M. Tehranipoor, "**Efficient Modeling of IR-Drop Using Dynamic SDF for Test and Diagnosis**," IEEE Workshop on RTL and High Level Testing (**WRTLT**), 2009.

285. K. Peng, M. Yilamaz, K. Chakrabarty, and M. Tehranipoor, "**Efficient Pattern Grading for Small Delay Defects in Digital Integrated Circuits**," IEEE North Atlantic Test Workshop, May 2009 **(Received Best Paper Award).**

286. H. Salmani, M. Tehranipoor, and J. Plusquellic, "**New Design Strategy for Improving Hardware Trojan Detection and Reducing Trojan Activation Time**," IEEE Workshop on Hardware-Oriented Security and Trust (**HOST**), pp. 67-73, 2009.

287. J. Ma, J. Lee, and M. Tehranipoor, "**Layout-Aware Pattern Generation for Maximizing Supply Noise Effects on Critical Paths**," in Proc. IEEE VLSI Test Symposium (**VTS**), pp. 221-226, 2009.

288. J. Ma, J. Lee, and M. Tehranipoor, "**Layout-Aware Pattern Generation for Critical Paths Considering Supply Voltage Noise**," Poster Presentation, SRC TECHCON, Austin, TX, 2009 (**Received Best in Session Award**).

289. H. Furukawa, X. Wen, K. Miyase, Y. Yamoto, S. Kajihara, P. Girard, L.T. Wang, M. Tehranipoor, "**CTX: A Clock-Gating-Based Test Relaxation and X-Filling Scheme for Reducing Yield Loss Risk in At-Speed Testing** ," IEEE Asian Test Symposium (**ATS**), pp. 197-402, 2008.

290. M. tehranipoor, "**ATPG for Increased Test Quality and In-Field Reliability**," **DRV** Workshop, 2008 (Invited).

291. J. Ma, J. Lee, M. Tehranipoor, X. Wen, A. Crouch, "**Identification of IR-drop Hot-spots in Defective Power Distribution Network Using TDF ATPG**," in Proc. Int. Workshop on Defect and Data Driven Testing (**D3T**), 2008.

292. X. Wang, M. Tehranipoor, and R. Datta, “**Path-RO: A Novel On-Chip Critical Path Delay Measurement Under Process Variations**,” International Conference on Computer-Aided Design (**ICCAD**), pp. 640-646, 2008.

293. R. Rad, X. Wang, J. Plusquellic, and M. Tehranipoor, “**Taxonomy of Trojans and Methods of Detection for IC Trust**,” International Conference on Computer-Aided Design (**ICCAD**), Nov. 2008.

294. X. Wang, H. Salmani, M. Tehranipoor, and J. Plusquellic, “**Hardware Trojan Detection and Isolation Using Current Integration and Localized Current Analysis**,” International Symposium on Fault and Defect Tolerance in VLSI Systems (**DFT**), pp. 87-95, Oct. 2008.

295. X. Wang, M. Tehranipoor, and R. Datta "**Accurate On-Chip Path Delay Measurement**," Texas Instruments Symposium on Test (**TIST**), Aug. 2008

296. J. Lee and M. Tehranipoor, "**A Novel Test Pattern Generation Framework for Inducing Maximum Crosstalk Effects on Delay-Sensitive Paths**," IEEE International Test Conference (**ITC**), pp. 1-10, Oct. 2008.

297. M. Yilmaz, K. Chakrabarty and M. Tehranipoor, "**Interconnect-Aware and Layout-Oriented Test-Pattern Selection for Small-Delay Defects**," IEEE International Test Conference (**ITC**), pp. 1-10, Oct. 2008.

298. J. Ma, J. Lee, and M. Tehranipoor, “**Power Distribution Failure Analysis Using Transition-Delay Fault Pattern Generation**,” Poster presentation at IEEE International Test Conference (**ITC**), Oct. 2008.

299. X. Wang, M. Tehranipoor, and R. Datta "**Path-RO: On-Chip Critical Path Delay Measurement Under Process Variations**," IEEE North Atlantic Test Workshop (**NATW**), May 2008 **(Received Best Paper Award)**.

300. J. Ma, J. Lee, M. Tehranipoor, and A. Crouch "**Test Pattern Generation for Open Defects in Power Distribution Networks**," IEEE North Atlantic Test Workshop (**NATW**), May 2008.

301. J. Lee, S. Narayan, and M. Tehranipoor, "**Low-Power Transition-Delay Fault Pattern Generation**," IEEE North Atlantic Test Workshop (**NATW**), May 2008 **(Received Honorable Mention for Best Paper Award)**.

302. X. Wang, M. Tehranipoor, and J. Plusquellic, “**Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions**,” IEEE Int. Hardware-Oriented Security and Trust (**HOST**), pp. 15-19, 2008.

303. R. Rad, J. Plusquellic, and M. Tehranipoor, “**Sensitivity Analysis to Hardware Trojans using Power Supply Transient Signals**,” IEEE Int. Hardware-Oriented Security and Trust (**HOST**), pp. 3-7, 2008.

304. J. Lee and M. Tehranipoor, “**LS-TDF: Low Switching Transition Delay Fault Test Pattern Generation**,” in Proc. IEEE VLSI Test Symposium (**VTS**), pp. 227-232, 2008.

305. M. Yilmaz, K. Chakrabarty, and M. Tehranipoor, “**Test Grading and Pattern Selection for Small Delay Defects**,” in Proc. IEEE VLSI Test Symposium (**VTS**), pp. 233-239, 2008.

306. J. Lee, S. Narayan, M. Kapralos, and M. Tehranipoor, “**Layout-aware, IR-drop Tolerant Transition Fault Pattern Generation**,” in Proc. Design, Automation, and Test in Europe (**DATE**), pp. 1172-1177, 2008.

307. J. Lee, K. Peng, and M. Tehranipoor, "**Inducing Maximum Crosstalk Effects on Delay-Sensitive Paths**," Poster presentation, SRC TECHCON, Austin, TX, 2008.

308. M. Yilmaz, K. Chakrabarty and M. Tehranipoor, “**Test Pattern Grading for Small Delay Defects**,” Int. Workshop on Defect-Based Testing (**DBT’07**), 2007.

309. R. Helinski, J. Plusquellic and M. Tehranipoor, “**Small Delay Defect Detection Using Self-Relative Timing Bounds**,” Int. Workshop on Defect-Based Testing (**DBT’07**), 2007.

310. J. Lee and M. Tehranipoor, “**Delay Fault Testing in Presence of Maximum Crosstalk**,” 16th IEEE North Atlantic Test Workshop (**NATW'07**), Boxborough, MA, 2007.

311. N. Ahmed, M. Tehranipoor and V. Jayaram, "**IR-drop Tolerant Transition Delay Fault Testing**," 16th IEEE North Atlantic Test Workshop (**NATW'07**), Boxborough, MA, 2007.

312. N. Ahmed, M. Tehranipoor and V. Jayaram, "**Transition Delay Fault Test Pattern Generation Considering Supply Voltage Noise in a SOC Design**," in Proc. Design Automation Conference (**DAC'07**), pp. 533-538, 2007.

313. N. Ahmed, M. Tehranipoor and V. Jayaram, "**Supply Voltage Noise Aware ATPG for Transition Delay Faults**," in Proc. IEEE VLSI Test Symposium (**VTS'07**), pp. 179-186, 2007.

314. N. Ahmed and M. Tehranipoor, "**Supply Voltage Noise Aware ATPG for Transition Delay Faults**," TECHCON, Austin, TX 2007.

315. N. Ahmed, M. Tehranipoor and V. Jayaram, "**Improving ATPG and Pattern Selection for Screening Small Delay Defects**," IEEE Int. Workshop on Current and Defect Based Testing (**DBT'06**), 2006.

316. J. Plusquellic, D. Acharyya, A. Singh, M. Tehranipoor and C. Patel, "**Multiple Supply Pad IDDQ_based Defect Detection Techniques Applied to Hardware Test Chips**," IEEE Int. Workshop on Current and Defect Based Testing (**DBT'06**), 2006.

317. J. Plusquellic, D. Acharyya, A. Singh, M. Tehranipoor and C. Patel, "**Triangulating to a Defect's Physical Coordinates Using Multiple Supply Pad IDDQs: Test Chip Results**," in Proc. International Symposium for Testing and Failure Analysis Conference **(ISTFA'06)**, pp. 36-42, 2006.

318. N. Ahmed, M. Tehranipoor and V. Jayaram, "**A Novel Framework for Faster-than-at-Speed Delay Test Considering IR-Drop Effects**," in Proc. Int. Conf. on Computer-Aided Design (**ICCAD'06**), pp. 198-203, 2006.

319. R. M. Rad and M. Tehranipoor, "**A Hybrid FPGA Using Nanoscale Cluster and CMOS Scale Routing**," in Proc. Design Automation Conference (**DAC'06**), pp. 727-730, 2006.

320. N. Ahmed, M. Tehranipoor and V. Jayaram, "**Timing-Based Delay Test for Screening Small Delay Defects**," in Proc. Design Automation Conference (**DAC'06**), pp. 320-325, 2006 **(Best Paper Award Candidate)**.

321. R. M. Rad and M. Tehranipoor, "**A Reconfiguration-based Defect Tolerance Method for Nanosclae Devices**," in Proc. Int. Symposium on Defect and Fault Tolerance of VLSI Systems (**DFT'06**), pp. 107-118, 2006.

322. R. M. Rad and M. Tehranipoor, "**SCT: An Approach for Testing and Configuring Nanoscale Devices**," in Proc. IEEE VLSI Test Symposium (**VTS'06**), pp. 372-377, 2006.

323. J. Lee, M. Tehranipoorand J. Plusquellic, "**A Low-Cost Solution for Protecting IPs Against Side-Channel Scan-Based Attacks**," In Proc. IEEE VLSI Test Symposium (**VTS'06**), pp. 94-99, 2006.

324. R. M. Rad and M. Tehranipoor, "**Test Time and Defect Map Analysis of PLA and LUT-Based Nano-Architectures**," IEEE North Atlantic Test Workshop (**NATW'06**), 2006.

325. N. Ahmed, M. Tehranipoor and V. Jayaram, "**A Case Study of IR-Drop Effects during Faster-than-at-Speed Delay Test**," IEEE North Atlantic Test Workshop (**NATW'06**), 2006.

326. J. Plusquellic, D. Acharyya, A. Singh, M. Tehranipoor and C. Patel, "**Triangulating to a Defect's Physical Coordinates Using Multiple Supply Pad IDDQs: Test Chip Results**," IEEE North Atlantic Test Workshop (**NATW'06**), 2006.

327. J. Lee, N. Ahmed, M. Tehranipoor, V. Jayaram and J. Plusquellic, "**A Novel Framework for Functionally Untestable Transition Fault Avoidance during ATPG**," IEEE North Atlantic Test Workshop (**NATW'06**), 2006.

328. R. M. P. Rad and M. Tehranipoor, "**Fine-Grained Island Style Architecture for Molecular Electronic Devices**," International Symposium on Field-Programmable Gate Arrays **(FPGA'06)** (Poster), pp. 226, 2006.

329. M. Tehranipoor and R. M. P. Rad, "**Test and Recovery for Fine-Grained Nanoscale Architectures**," International Symposium on Field-Programmable Gate Arrays **(FPGA'06)** (Poster), 2006.

330. M. ElShoukry, C.P. Ravikumar and M. Tehranipoor, "**Partial Gating Optimization for Power Reduction During Test Application**," in Proc. IEEE Asian Test Symposium (**ATS'05**), pp. 242-247, 2005.

331. M. Tehranipoor, M. Nourani and N. Ahmed, "**Low Transition LFSR for BIST-Based Applications**," in Proc. IEEE 14th Asian Test Symposium (**ATS'05**), pp. 138-143, 2005.

332. C.P. Ravikumar, N. Ahmed and M. Tehranipoor, "**Practicing Transition-Fault Testing with Physical-Design-Friendly Flows**," Texas Instruments India Technical Conference (**TIITC'05**), 2005.

333. J. Lee, M. Tehranipoor, C. Patel and J. Plusquellic, "**Securing Scan Design Using Lock & Key Technique**," in Proc. International Symposium on Defect and Fault Tolerance in VLSI Systems (**DFT'05**), pp. 51-62, 2005.

334. N. Ahmed and M. Tehranipoor, "**Improving Transition Delay Fault Coverage Using Hybrid Scan-Based Technique**," in Proc. International Symposium on Defect and Fault Tolerance in VLSI Systems (**DFT'05**), 2005.

335. M. Tehranipoor, "**Defect Tolerance for Molecular Electronics-Based NanoFabrics Using Built-In Self-Test Procedure**," in Proc. International Symposium on Defect and Fault Tolerance in VLSI Systems (**DFT'05**), pp. 4886-495, 2005.

336. M. Alisafaee, S. M. Fakhraie and M. Tehranipoor, "**Architecture of an Embedded Queue Management Engine for High-Speed Network Devices**," in Proc. IEEE MidWest Symposium on Circuits and Systems (**MWSCAS'05**), Cincinnati, pp. 1907-1910, 2005.

337. H. Esmaeilzadeh, F. Farzan, N. Shahidi, S. M. Fakhraie, C. Lucas and M. Tehranipoor, "**NnSP: Embedded Neural Networks Stream Processor**," in Proc. IEEE MidWest Symposium on Circuits and Systems (**MWSCAS'05**), Cincinnati, pp. 223-226, 2005.

338. N. Ahmed, M. Tehranipoor and C.P. Ravikumar, "**Addressing At-speed Fault Coverage and Test Cost Issues Using Enhanced Launch-off-Capture**," Texas Instruments Symposium on Test (**TIST'05**), 2005.

339. N. Ahmed, M. Tehranipoor and C.P. Ravikumar, "**At-Speed Local Scan Enable Generation for Transition Fault Testing Using Low-Cost Testers**," Texas Instruments Symposium on Test (**TIST'05**), 2005 **(Ranked 5th Among 89 Presentations)**.

340. N. Ahmed, M. Tehranipoor and C.P. Ravikumar, "**Enhanced Launch-off-Capture Transition Fault Testing**," in Proc. IEEE International Test Conf. (**ITC'05**), pp. 225-234, 2005 **(Received top ten recognition)**.

341. N. Ahmed, M. Tehranipoor, C.P. Ravikumar and J. Plusquellic, "**At-Speed Transition Fault Testing Using Low Speed Testers With Application to Reduced Scan Enable Routing Area**," IEEE North Atlantic Test Workshop (**NATW'05**), pp. 112-119, 2005.

342. D. Acharyya, A. singh, M. Tehranipoor, C. Patel and J. Plusquellic, "**Sensitivity Analysis of Quiescent Signal Analysis for Defect Detection**," IEEE. Int. Workshop on Defect Based Testing (**DBT'05**), pp. 3-10, 2005.

343. M. Nourani, M. Tehranipoor and N. Ahmed, "**Pattern Generation and Estimation for Power Supply Noise Analysis**," in proc. IEEE VLSI Test Symposium (**VTS'05**), pp. 439-444, 2005.

344. N. Ahmed, C.P. Ravikumar, M. Tehranipoor and J. Plusquellic, "**At-Speed Transition Fault Testing With Low Speed Scan Enable**," in proc. IEEE VLSI Test Symposium (**VTS'05**), pp. 42-47, 2005 **(Received Best Paper Award)**.

345. M. H. Tehranipour, M. Nourani and K. Chakrabarty, "**Nine-Coded Compression Technique with Application to Reduced Pin-Count Testing and Flexible On-Chip Decompression**," in proc. IEEE/ACM Design, Automation and Test in Europe (**DATE'04**), Paris, France, vol. 2, pp. 1284-1289, 2004.

346. M. H. Tehranipour, M. Nourani, K. Arabi and A. Afzali-Kusha, "**Mixed RL-Huffman Encoding for Power Reduction and Data Compression in Scan Test**," in proc. IEEE International Symposium on Circuits And Systems (**ISCAS'04**), Vancouver, Canada, vol. 2, pp. 681-684, 2004.

347. N. Ahmed, M. H. Tehranipour and M. Nourani, "**Low-Power Pattern Generation for BIST Architecture**," in proc. IEEE International Symposium on Circuits And Systems (**ISCAS'04**), Vancouver, Canada, vol. 2, pp. 689-692, 2004.

348. N. Ahmed, M. H. Tehranipour, D. Zhou and M. Nourani, "**Frequency Driven Repeater Insertion for Deep Submicron**," in proc. IEEE International Symposium on Circuits And Systems (**ISCAS'04**), Vancouver, Canada, vol. 5, 181-184, 2004.

349. M. H. Tehranipour, N. Ahmed and M. Nourani, "**Testing SoC Interconnects for Signal Integrity Using Boundary Scan**," in proc. IEEE VLSI Test Symposium (**VTS'03**), Napa, CA, pp. 158-163, 2003.

350. N. Ahmed, M. H. Tehranipour and M. Nourani, "**Extending JTAG for Testing Signal Integrity in SoCs**," in proc. IEEE/ACM Design, Automation and Test in Europe (**DATE'03**), Messe Munich, Germany, pp. 218-223, 2003.

351. M. H. Tehranipour, N. Ahmed and M. Nourani, "**Multiple Transition Model and Enhanced Boundary Scan Architecure to Test Interconnects for Signal Integrity**," in proc. IEEE International Conference on Computer Design (**ICCD'03**), San-Jose, pp. 554-559, CA, 2003.

352. M. H. Tehranipour, M. Nourani and S. M. Fakhraie, "**Systematic Test Program Generation for SoC Testing Using Embedded Processor**," in proc. IEEE International Symposium on Circuits And Systems (**ISCAS'03**), Bangkok, Thailand, vol. 5, pp. 541-544, 2003.

353. G. R. Chaji, R. M. Pourrrad, S. M. Fakhraie and M. H. Tehranipour, "**eUTDSP: A Design Study of a New VLIW-Based DSP Architecture**," in proc. IEEE International Symposium on Circuits And Systems (**ISCAS'03**), Bangkok, Thailand, vol. 4, pp. 137-140, 2003.

354. M. H. Tehranipour and M. Nourani, "**Signal Integrity Loss in SoC's Interconnects: A Diagnostic Approach Using Embedded Microprocessor**," in proc. IEEE International Test Conference (**ITC'02**), Baltimore, MD, pp.1093-1102, 2002.

355. S. M. Fakhraie, M. H. Tehranipour, M. R. Movahedin and M. Nourani, "**Fast Prototyping of a DSP Core**," in proc. IEEE MidWest Symposium on Circuits and Systems (**MWSCAS'02**), Tulsa, Oklahoma, vol. 2, pp. 215-218, 2002.

356. M. H. Tehranipour, M. Nourani, S. M. Fakhraie and C. A. Papachristou, "**Test Optimization of Bus-Structured SoCs Using Embedded Microprocessor**," in proc. IEEE MidWest Symposium on Circuits and Systems (**MWSCAS'02**), Tulsa, Oklahoma, vol. 1, pp. 168-171, 2002.

357. M. Tehranipour, Z. Navabi and S. M. Fakhraie, "**An Efficient BIST for Embedded SRAM Testing**," in proc. IEEE International Symposium on Circuits and Systems (**ISCAS'01**), Sydney, Australia, Vol 5, pp. 73-76, 2001.

358. M. Tehranipour, Z. Navabi and S. M. Fakhraie, "**A Low-Cost BIST Architecture for Processor Cores**," in proc. IEEE Electronic Circuits and Systems Conference (**ECS'01**), Bratislava, Slovakia, pp. 11-14, 2001.

359. M. Tehranipour and Z. Navabi, "**Zero-Overhead BIST for Internal SRAM Testing**," in proc. IEEE International Conference on Microelectronics (**ICM'00**), Tehran, Iran, pp. 109-112, 2000.

Technical Reports and Invited Poster Presentations

1. U. Guin, M. Tehranipoor, D. DiMase, and M. Megrdician, "**Counterfeit IC Detection and Challenges Ahead**," ACM SIGDA, March 2013.
2. N. Reddy and M. Tehranioor, "**Reliability Analysis for 90nm Test Chips**," Technical Reports, CADT-20110110, 2011.
3. F. Wu, L. Dilillo, A. Bosio, P. Girard, S. Pravossoudovitch, A. Virazel, M. Tehranipoor, K. Miyase, X. Wen, N. Ahmed, "**Is Test Power Reduction Through X-Filling Good Enough?**," Poster presentation, Int. Test Conference (**ITC**), 2010.
4. J. Lee and M. Tehranipoor, "**Low-power Transition Delay Fault Test Pattern Generation**," IEEE VLSI Test Symposium (**VTS**), 2008, PhD Thesis Poster Presentation.
5. M. Tehranipoor, "**Trojan Detection and Isolation in Integrated Circuits**," NSF Cyber Trust meeting, New Haven, March 2008
6. N. Ahmed, M. Tehranipoor, and V. Jayaram, "**Considering IR-Drop Effects During Faster-than-at-Speed Delay Test**," presented in Special Session (Elevator Talk), IEEE VLSI Test Symposium (**VTS**), 2006.
7. N. Ahmed and M. Tehranipoor, "**On-chip Scan Enable Generation for Transition Fault Testing**," Poster Presentation, University Booth, ITC 2005.
8. J. Plusquellic, D. Acharyya, C. Patel, A. Singh and M. Tehranipoor, "**Hardware Investigation of Defect Sensitivity of a Multiple Supply Pad IDDQ Method**," Poster Presentation, University Booth, ITC 2005.
9. N. Ahmed and M. Tehranipoor, "**Enhanced Launch-off-Capture with Improved Fault Coverage and Reduced Pattern Count**," Presented in UT-Austin Poster Session, ITC 2005.
10. M. H. Tehranipour and M. Nourani, "**Low-Power Test pattern generation for BIST Architecture**," University of Texas at Dallas, 2003.
11. M. H. Tehranipour and M. Nourani, "**Test Compression and Power Reduction in Scan Using RL-Huffman Encoding**," University of Texas at Dallas, 2002.

Consulting

1. **Consulting** with many companies (OCMs, OEMs, and EDA) and universities worldwide
2. Served on the **advisory board** of several companies with focus on cybersecurity

Invited Talks and Keynote Addresses

- **Invited Talk**, SRC HWS e-Workshop, Hardware Security: A Vision for the Next Decade, May 2022
- **Invited Talk**, Accellera IPSA, Quantifiable Assurance: From IPs to SoCs, April 19, 2022
- **Visionary Talk**, Silicon Lifecycle Management (SLM) Workshop, March 18, 2022
- **Invited Talk**, Intel, Quantifiable Assurance: From IPs to SoCs, Feb. 2022
- **Keynote Address**, Synopsys User Group, SNUG, March, 2022
- **Invited Talk**, NIST, State of the Microelectronics Security and Trust, Jan 2022
- Interview with Dr. Jay Lewis, Partner, Microsoft, 2021
- Interview with Serge Leef, MTO Program Manager, DARPA, MEST Center, 2021

- Interview with Dr. Wally Rhines, CEO of CORNAMI, MEST Center, 2021
- **Invited Speaker**, Microelectronics Packaging & Test Engineering Council (MEPTEC), Nov. 3, 2021 (https://www.youtube.com/watch?v=SQlgdezOw_Q&t=4s)
- **Keynote Address**, Workshop on RTL and High Level Testing (WRTLT), Nov. 2021
- **Invited Talk**, UF AI Speaker Series, Nov. 2021 (https://www.youtube.com/watch?v=gZxyb45jnLM)
- **Invited Talk**, Dynetics, Nov. 2021
- **Invited Talk**, Design Automation Conference (DAC), Dec. 2021
- **Keynote Address**, IEEE Microelectronics Design and Test Symposium (MDTS), May 2021
- **Keynote Address**, Workshop on Securing the Nation's 5G Supply Chain Though Measurement Countermeasure, NIST, 2021
- **Invited Talk**, Microsoft, Title: State of the Microelectronics Security, March 2021
- **Keynote Address**, ACM Workshop on Attacks and Solutions for Hardware Security (**ASHES**), November 2020
- **Invited Talk**, KBR Center of Excellence on Microelectronic Trust, October 16, 2020
- **Invited Talk**, NIST's Cybersecurity and Privacy Federal Advisory Board, October 15, 2020
- **Keynote Address**, MOST (Ministry of Science and Technology, R.O.C.), ESD Alliance and SEMI, Security on Chip Summit in **SEMICON** Taiwan on September 25th, 2020 in TaiNEX1, Taiwan.
- **Keynote Address**, International Test Conference (**ITC**) Asia, September 2020.
- **Invited Talk**, DOD Technical Executives, Education and Workforce Development, Aug, 2020
- **Invited Talk**, Cyber Security and Information Assurance (CSIA) IWG, Aug. 2020
- **Keynote Address**, SRC/SIA/DoE Decadal Plan workshop on ICT Hardware Enabled Security, Aug, 26, 2020
- **Invited Talk,** ACM SIGDA / IEEE CEDA webinar, Design Automation WebiNar (**DAWN**), Title: *Automatic Implementation of Secure Silicon (AISS)*, Aug 2020
- **Invited Talk**, Global Foundries Executive Talk, July 2020
- **Invited Talk,** Texas Instruments Gator Day, July 2020
- **Invited Talk**, IEEE Oregon Section, The Pursuit of Happyness: Root of Trust for Cybersecurity, June 2020
- **Invited Talk**, DARPA, Automated Rule Checking for Hardware Security, May 2020
- **Keynote Address**, Cyber Resilient Supply Chain Technologies (**CReSCT**), May 2020
- **Invited Webinar**, MEST Center, Title: Supply Chain Security, 2019
- **Invited Talk**, OSD Quantifiable Assurance (QA), Title: Quantifiable Assurance under Zero Trust, Washington DC, Oct. 2019
- **Invited Talk**, ERI Summit – Hardware Security Workshop, July 2019, Title: Securing Supply Chain from Chips to PCBs

- **Invited Talk**, Qualcomm, June 2019, SoC Supply Chain Security
- **Invited Talk**: Gator 100 Conference, March 2019
- **Keynote Address**, GomacTech 2019, Title*: The Pursuit of Happiness: Establishing hardware root of Trust for cybersecurity*
- **Invited Talk:** DARPA OMG Meeting, Feb. 2019, Title: Defense-in-Depth for Secure Obfuscation
- **Invited Talk**, NXP, Chandler, AZ, October 2018, Title: *New Trends and Challenges in Securing Hardware*
- **Keynote Address**, ISTFA 2018, Phoenix, AZ, October 2018*,* Title*: Hardware Root-of-Trust for Cyber Security: Uncovering the Role of Test and Failure Analysis in Enabling Cyber Defense*
- **Keynote Address**, Asian Test Symposium (ATS), Hefei, China, October 2018, Title: *Securing SoCs: Current Practices and Challenges*
- **Invited Talk**, GeorgiaTech, September 2018
- **Keynote Address**, IEEE World Conference on Information Security Applications, Jeju, Korea, August 2018
- **Invited Presentation**, GeorgiaTech, IoT Summer School, August 2018
- **Invited Talk, Distinguished Speaker Series**, Navy Crane, IN, August 2018
- **Keynote Address**, SRC Workshop on Fabrics of the Security, Fremont, CA, July 2018
- **Invited Talk, NSF SCCS Workshop,** Title: *SoC Security Validation*, Washington DC, March 2017
- **Invited Talk, Cisco CRC workshop on Hardware Security**, San Jose, CA, Dec. 2017
- **Keynote Speaker, Groundswell Conference on Cybersecurity,** Melbourne, FL, Nov. 2017
- **Invited Talk, Qualcomm**, San Diego, October 2017, Title: SoC Security
- **Invited Talk, Tsinghua University**, Beijing, October 2017, Title: *When it Comes to Security, Do not Forget about Hardware*
- **Keynote Speaker, Int. IEEE Verification and Security Workshop (IVSW)**, July 2017
- **Invited Talk: Air Force Research Laboratory (AFRL),** Dayton, OH, Title: *Trusted and Assured Microelectronics*, 2017
- **Invited Talk: Air Force Research Laboratory (AFRL),** Dayton, OH, Title: *Test and Design-for-Anti-Counterfeit*, 2017
- **Invited Talk: Ohio State University**, Columbus, OH, Title: *When It Comes to Cybersecurity, Do Not Forget About Hardware*, 2017
- **IEEE Ambassador talk at the Harris Corporation**, Melbourne, FL, March 2017, Title: *When It Comes to Cybersecurity, Do Not Forget About Hardware*
- **RSA Conference**, San Francisco, CA, February 2017, Title: *Securing Electronic Supply Chain from Design to Resign*
- **Keynote Speaker**, IEEE Asian HOST, Dec. 2016, Taiwan, Title: Security Rule Check

- **Keynote Speaker,** Microprocessor Test and Verification (MTV) Workshop, Austin, TX, Dec. 2016, Title: Security Rule Check: A Closer Look at the Automated Test for Security
- **Global Foundries, CTO Speaker Series**, Dec. 2016
- **Invited Talk: SRC e-Workshop,** July 2016
- **Invited Talk: Chinese Academy of Science (CAS)**, June 2016
- **Keynote Speaker:** International Workshop on on Hardware Security, 2016, Organized jointly by Tsinghua University and Beihang University, **Title**: Hardware Security: Past, Present, and the Future
- **Invited Talk: Peking University**, June 2016
- **Invited Talk: Beihang University**, June 2016
- **Invited Talk, Dagstuhl Seminar**, Germany, May 2016
- **Invited Talk: IEEE International Reliability Physics Symposium (IRPS)**, 2016, **Title**: *Security vs. Reliability: Where Do These Two Road Converge?*
- **Keynote Speaker: IEEE Workshop on CPS Security,** April 2016
- **Keynote Speaker: US-Brazil Joint Workshop on Cybersecurity,** April 2016, Orlando, FL
- **Invited Talk: Florida Institute of Technology (FIT),** Host: Dr. Fareena Saqib, March 2016
- **Invited Talk: Florida Energy Systems Consortium (FESC)**, March 2016
- **Keynote Speaker: International Symposium on Quality Electronic Design (ISQED**), Santa Clara, March 2016, **Title**: *New Frontiers in Hardware Security and Trust*
- **Invited Talk: Northrop Grumman,** Nov. 2015
- **Invited Talk: IEEE/ACM International Conference on Computer-Aided Design (ICCAD)**, Nov. 2015, Austin, TX
- **Invited Talk: Potomac Institute for Policy (PIP)**, October 2015
- **Invited Talk: DHS Software and Supply Chain Assurance Forum**, Sep. 2015
- **NSF WATCH Talk**, July 2015, Host: Jeremy Epstein
- **Invited Talk: Global Foundries**, Malta, NY, Dec. 2014
- **Keynote Speaker: Freescale Semiconductors' Technical Enrichment Conference,** Austin, TX, Dec. 2014
- **Invited Talk: Cadence,** Austin, TX, Dec. 2014
- **Invited Talk: Missile Defense Agency (MDA),** Nov. 2014, Huntsville, Alabama
- **Invited Talk: Beihang University**, Nov. 2014, HOST: Prof. Michel Wang
- **Invited Talk: IEEE Asian Test Symposium (ATS)**, Nov. 2014
- **Invited Talk: Army Research Office (ARO) Workshop**, NYC, Nov. 2014
- **Invited Talk: CSI CyberSEED event,** University of Connecticut, Oct. 2014
- **Invited Talk: Honeywell International,** Oct. 2014

- **Invited Talk: ISE Northeast**, Oct. 2014, NYC
- **Invited Talk: Sharif University of Technology**, July 2014, HOST: Dr. Siavash Bayat
- **Invited Talk: Shahid Beheshti University,** July 2014, HOST: Dr. Ali Jahanian
- **Invited Talk: Amirkabir University of Technology**, June 2014, HOST: Drs. Saheb Zamani and Hamid Zarandi
- **Invited Talk: Cisco Corporation**, May 2014, Host: Dr. Wei Zhao
- **Invited Talk: Xilinx Corporation**, May 2014, Host: Dr. Amit Majumdar
- **Keynote Speaker: IEEE North Atlantic Test Workshop (NATW)**, May 2014
- **Invited Talk: Design, Automation, and Test in Europe (DATE)**, March 2014
- **Keynote Speaker: IEEE Int. Workshop on Reliability-Aware System Design and Test (RASDAT)**, Jan. 2014.
- **Invited Talk: IEEE Microprocessor Test Workshop,** Austin, TX, Dec. 2013
- **Invited Talk: DMSMS**, Dec. 2013, Counterfeit Detect Coverage
- **Invited Talk: DMSMS**, Dec. 2013, Combating Die/IC Recovery
- **Invited Talk: Missile Defense Agency (MDA), PMPB,** Nov. 2013
- **Invited Talk: ARO Workshop,** NYC, Nov. 2013
- **Invited Talk: Honeywell, Cyber Security Group Meeting,** Nov. 2013
- **Invited Talk: National Chao Tung University**, Taiwan, Nov. 2013
- **Invited Talk: MediaTek**, Taiwan, Nov. 2013
- **Invited Talk: CALCE Symposium on Counterfeit Electronic Parts and Electronic Supply Chain,** June 2013
- **Invited Talk: CS1 ICT Supply Chain Risk Management**, June 2013
- **Invited Talk: United Technologies Research Center (UTRC),** May 2013
- **Invited Talk: NASA Quality Leadership Forum,** March 2013
- **Invited Talk: Trusted Supplier Industry,** March 2013
- **Invited Talk: Cisco,** Security Group, March, 2013, Title: SiliconAP: A novel Platform for Counterfeit Prevention
- **Invited Talk: ARO/CHASE Workshop on Counterfeit Electronics**, Jan. 2013, Counterfeit Detection Assessment
- **Invited Talk: ARO/CHASE Workshop on Counterfeit Electronics**, Jan. 2013, Silicon Authentication Platform
- **Invited Talk: NSF/SRC SA+TS Workshop**, Washington DC, Jan. 2013
- **Invited Talk: Microelectronics Reliability and Qualification proposal (MRQW)**, Dec. 2012

- **Invited Talk: DMSMS Standardization Conference**, Nov. 2012, Title: Secure Split Test for Counterfeit Avoidance
- **Invited Talk: DMSMS Standardization Conference**, Nov. 2012, Title: Counterfeit Test Technology Readiness Assessment
- **Invited Talk: IEEE Asian Test Symposium (ATS)**, Nov. 2012
- **Invited Talk: SRC e-Workshop**, Nov. 2012
- **Invited Talk: University of Arkansas**, Oct. 2012, Host: Prof. Jia Di
- **Invited Talk: Symposium on Counterfeit Electronic Parts and Electronic Supply Chain**, June 2012
- **Invited Talk: University of Pittsburgh**, April 2012, Host: Prof. Kartik Mohanram
- **Invited Talk: University of Illinois at Chicago**, March 2012, Host: Prof. Wenjing Rao
- **Invited Talk: Missile Defense Agency**, March 2012, Host: Fred Schipp
- **Invited Talk: San Jose State University**, March 2012, Host: Prof. Shahab Ardalan
- **Invited Talk: G-19A Test Laboratory Standards Development Committee,** March 2012, Host: Daniel DiMase, Honeywell
- **Invited Talk: IEEE International Reliability Innovations Conference (IRIC)**, March 2012 (Talk on Security)
- **Invited Talk: IEEE International Reliability Innovations Conference (IRIC)**, March 2012 (Talk on Reliability)
- **Invited Talk: IEEE Workshop on Defect and Adaptive Data Analysis (DATA)**, September 2011
- **Invited Talk: Air Force Research laboratory (AFRL)**, Rome, September 2011
- **Invited Talk: University of South Florida**, July 2011, Host: Prof. Sanjukta Bhanja
- **Invited Talk: Low Power SOC Workshop (LPSOC)**, July 2011
- **Invited Talk: IBM TJ Watson**, June 2011, Host: Dr. Peilin Song
- **Invited Talk: Qualcomm,** June 2011, Host: Dr. Sagar Sabade
- **Invited Talk: Cisco,** May 2011, Host: Nemat Bidokhti and Bill Eklow
- **Invited Talk: IEEE VLSI Test Symposium (VTS)**, May 2011, Dana Point, CA
- **Invited Talk: Virginia Tech**, April 22, 2011, Host: Prof. Patrick Schaumont
- **Invited Talk: NYU-Abu Dhabi Workshop on Test**, New York, NY, April 2011, Host: Prof. Ozgur Sinanoglu
- **Invited Talk: University of Maryland**, April 2011, Host: Prof. Gang Qu
- **Invited Talk: ARO Workshop on Hardware Assurance**, Washington, DC, April 2010
- **Invited Talk: University of South Florida**, March 2011, IEEE CS Tampa Chapter, IEEE DVP program
- **Invited Talk: GOMACtech Conference**, March 2011, Orlando, FL

- **Invited Talk: LSI**, March 4, 2011, **Invited by:** Sreejit Chakrabarty, Title: On-chip Measurement Structures: Opportunities and Challenges
- **Invited Talk: LSI**, March 10, 2011, **Invited by:** Arun Gunda, Title: Detection of SDDs in Nanoneter Technology Designs
- **Invited Talk: University of Wisconsin, Madison**, Feb. 2011
- **Invited Talk: Freescale**, Austin, TX, Nov. 2010, Host: LeRoy Winemberg
- **Invited Talk: Texas Instruments**, Dallas, TX, September, 2010, Host: Dr. Nisar Ahmed
- **Invited Talk: University of Texas at Arlington**, September 2010, Arlington, TX, HOST: Prof. Robert Magnusson, Title: Design for Hardware Security and Trust
- **Invited Talk: Air Force Research Lab (AFRL)**, Nov. 2011
- **Invited Talk: MediaTek**, Boston, Nov. 2010. Hosts: Jeff Roher and Harry Chen
- **Invited Talk: Cisco,** October 2010, Hosts: Carson Stuart and Nemat Bidokhti, Title: New Threats to Hardware: Detection and Prevention Challenges
- **Invited Talk: Brown University**, Providence, RI, October 2010, Host: Prof. Sherief Reda, Title: Design for Hardware Security and Trust
- **Invited Talk: NYU-Poly**, New York, NY, August 2010, Host: Prof. Ramesh Karri
- **Invited Talk: Qualcomm**, San Diego, CA, August 2010, Host: Mike Laisne
- **Invited Talk: LSI**, June 2010, San Jose, CA, Host: Dr. Sreejit Chakravarty
- **Invited Talk: Cisco**, June 2010, San Jose, CA, Host: Nemat Bidokhti
- **Invited Talk: IBM**, May 2010, Invited by: Dr. Phil Nigh
- **Invited Talk:** NASA/ESA Conference on Adaptive Hardware and Systems (**AHS**-2010)
- **Invited Talk:** Connecticut Microelectronics and Optoelectronics Consortium (**CMOC**), 2010
- **Invited Talk: University of Massachusetts, Lowell**, March 2010, HOST: Prof. Martin Margala
- **Invited Talk: LSI Logic**, Jan 2010, Host: Dr. Sreejit Chakravarty
- **Invited Talk:** Information Security Council (**INFOSEC**), Jan 2010
- **Invited Talk: IBM-Austin Research Lab** (**IBM-ARL**), Nov. 2009, Host: Dr. Anne Gattiker
- **Invited Talk: ARO Special Workshop** on Hardware Assurance, 2009
- **Invited Talk: AMD**, July 2009, Host: Dr. Mahmut Yilmaz / Jeff Fitzgerald
- **Invited Talk: Amirkabir University of Technology**, July 2009, Host: Dr. A. Bagheri
- **Invited Talk: Cisco**, May 2009, Host: Nemat Bidokhti
- **Invited Talk: Southwest DFT** (SWDFT-2009), Austin, TX
- **Invited Talk: Duke University**, April 2009, Host: Prof. Krishnendu Chakrabarty
- **Invited Talk: University of Rhode Island**, April 2009, Host: Prof. Resit Sendag

- **Invited Talk: Worcester Polytechnic Institute (WPI)**, March 2009, Host: Prof. Xinming Huang
- **Invited Talk: Mentor Graphics**, Feb 2009, Host: Dr. Yu Huang
- **Invited Talk: IBM TJ Watson**, Nov. 2008, Host: Dr. Jinjun Xiong
- **Invited Talk: Intel**, Nov. 2008, Title: *Small Delay Fault Detection and On-Chip Measurement*
- **Invited Talk: FIST**, Japan, Dec. 2008, Title: *Dealing with Power and Signal Integrity Issues During Test in Nanometer Technology Designs*
- **Invited Talk: University of Connecticut,** Title: *Hardware-Trust: Challenges and Solutions*
- **Invited Talk:** IP/IC Trust, University **of Connecticut, Northrop Grumman visit**
- **Invited Talk:** Fukuoka Industry, Science & Technology Foundation (**FIST**), Japan, Dec. 2008, Title: *Verifying Trustworthiness of Integrated Circuits*
- **Invited Talk:** Industry, Science & Technology Foundation (**FIST**), Japan, Dec. 2008, Title: *ATPG for Testing Power Supply Noise and Crosstalk*
- **Invited Talk:** IEEE Workshop on Design for Reliability and Variability (**DRV**), Oct. 2008, Title: *ATPG for Increased Quality and In-Field Reliability*
- **Invited Talk: University of Tehran**, Host: Prof. Mahmoud Hashemi, Title: *ATPG for Increased Test Quality and In-field Reliability*
- **Invited Talk: University of Tehran**, Host: Prof. Mahmoud Hashemi, Title: *Verifying the Trustworthiness on Integrated Circuits*
- **Invited Talk: Sharif University of Technology**, Host: Prof. S. Ghassem Miremadi, Title: *ATPG for Increased Test Quality and In-field Reliability*
- **Invited Talk: Babol University of Technology**, Host: Prof. Miar Naimi, Title: *Verifying the Trustworthiness on Integrated Circuits*
- **Invited Talk: IBM**, Aug. 2008, Invited by: Dr. Phil Nigh
- **Invited Talk: Magma**, April 2008, Host: Dr. Sandeep Goel
- **Invited Talk: SRC e-Workshop**, Feb. 2008, **Title:** *High-Quality Delay Tests for Nanotechnology Designs*
- **Invited Talk: Freescale**, Austin, TX, Dec. 2007, Host: Dr. Magdy Abadir/Dr. Raj Raina
- **Invited Talk: Texas Instruments**, Dallas, TX, Dec. 2007, Hosts: Vinay Jayaram / Dr. Ken Butler
- **Invited Talk: TranSwitch**, Bedford, MA, Nov. 2007, Host: Zahi Abuhamdeh
- **Invited Talk: AMD**, Boston, MA, Nov. 2007, Host: Dr. Kamran Zarrineh
- **Invited Talk: Analog Devices**, Boston, MA, Nov. 2007, Host: Harry Chen
- **Keynote Speaker: Magma**'s Luncheon Event at International Test Conference (ITC), San Jose, CA, Tuesday Oct. 23, 2007
- **Invited Talk: Cadence,** June 2007, **Title**: *IR-drop Tolerant AT-speed Tests for Nanometer Technology Designs*, Host: Dr. Krishna Chakravadhanula

- **Invited Talk: LSI Logic,** June 2007, **Title**: *Generating High Quality At-speed Tests for Nanometer Technology Designs: Challenges and Solutions*, Invited by: Dr. Sreejit Chakravarty
- **Invited Talk: Qualcomm** (San Diego, CA), June 2007, **Title**: *At-speed Test for Nanotechnology: Challenges and Solutions*, Host: Dr. Sagar Sabade
- **Invited Talk:** Guest Lecturer for VLSI System Testing Course of ECE Department at **Duke University**, Instructor: Prof. Krish Chakrabarty
- **Invited Talk: Mentor Graphics** (Wilsonville, OR), Nov. 2006, **Title**: *At-speed Test for Nanotechnology: Challenges and Solutions*, Host: Dr. Nilanjan Mukherjee
- **Invited Talk: LSI Logic** (San Jose, CA), Nov. 2006, **Title**: *High Quality At-speed Tests for Nanotechnology Designs*, Host: Dr. Arun Gunda
- **Invited Talk: AMD** (Sunnyvale, CA), Oct. 2006, **Title**: *High Quality At-speed Tests for Nanometer High-speed Designs,* Host: Dr. Anuja Sehgal
- **Invited Talk: Texas Instruments** (Dallas, TX), April 2004, **Title**: Enhanced Scan Architectures for Reducing Power and Test Application Time

Technology Transfer

1. On-chip Monitors was successfully implemented on few products
2. Small-delay defect generation tool is used by semiconductor and EDA companies
3. LTG Cell for implementing LOS using low-speed scan enable signal
4. SAE International, the CDC tool on counterfeit detection
5. Test point insertion technology for LBIST to semiconductor industry

Teaching Experience

University of Florida

Spring 2018	EEL 4714/5716 Introduction to Hardware Security and Trust
Spring 2016	Introduction to Hardware Security and Trust

University of Connecticut

Semester & Year	Course No. & Title
Fall 2006	ECE 290: Senior Design
Spring 2007	ECE 291: Senior Design
Spring 2007	ECE 300: VLSI Design Verification and Test
Fall 2007	ECE 290: Senior Design
Spring 2008	ECE 291: Senior Design
Spring 2008	ECE 300: VLSI Design Verification and Test
Fall 2008	ECE 4901: Senior Design

Fall 2008	ECE 6094: VLSI CAD Algorithms
Spring 2009	ECE 3421: VLSI Design and Simulation
Fall 2010	ECE 6094: VLSI Design Verification and Test
Fall 2010	ECE 4901: Senior Design
Spring 2010	ECE 4095/6095: Intro. Hardware Security and Trust
Spring 2010	ECE 4902: Senior Design
Fall 2010	ECE 4095/6095: VLSI CAD Algorithms
Fall 2010	ECE 4901: Senior Design
Spring 2011	ECE 3421: VLSI Design and Simulation
Spring 2011	ECE 4902: Senior Design
Fall 2011	ECE 6432: VLSI Design Verification and Testing
Fall 2011	ECE 4901: Senior Design
Fall 2011	ECE 6094: Computer Engineering Seminar
Spring 2012	ECE 3401: Digital Systems Design
Spring 2012	ECE 4902: Senior Design
Spring 2012	ECE 6094: Computer Engineering Seminar
Fall 2012	ECE 4451/5451: Intro. to Hardware Security and Trust
Fall 2012	ECE 4901: Senior Design
Spring 2013	ECE 3401: Digital Systems Design
Spring 2013	ECE 4095: Hardware Hacking
Spring 2013	ECE 4902: Senior Design
Fall 2013	ECE 4901: Senior Design
Spring 2014	ECE 3401: Digital Systems Design
Spring 2014	ECE 4095: Hardware Hacking
Spring 2014	ECE 4902: Senior Design
Fall 2014	ECE 4451/5451: Intro. to Hardware Security and Trust
Fall 2014	ECE 4901: Senior Design
Spring 2015	ECE 4902: Senior Design
Spring 2016	EEL 4930: Introduction to Hardware Security and Trust
Spring 2018	EEL 4714/5716: Introduction to Hardware Security and Trust

New Courses Developed and Taught at UMBC (2004-2006):

SOC Design and Test

CAD Algorithms

VLSI Design Verification and Testing

New Courses Developed and Taught at UConn:

VLSI Design Verification and Testing

CAD Algorithms

Introduction to Hardware Security and Trust

Hardware Hacking

New courses Developed at UF:

Introduction to Hardware Security and Trust

Research Group

Current Post-Doctoral Fellows and Visiting Researchers:

1. **Dr. Sukanta Dey**, September 2021
2. **Dr. Hadi Mardani**, July 2021, Jointly supervised with Prof. Farimah Farahmandi
3. **Dr. Kimia Zamiri Azar**, July 2021, Jointly supervised with Prof. Farimah Farahmandi
4. **Dr. Sree R. Rajendran**, Dec. 2020, Jointly supervised with Prof. Farimah Farahmandi
5. **Dr. Nalla Nachimuthu**, Nov. 2020, Jointly supervised with Prof. Farimah Farahmandi
6. **Dr. Jungmin Park**, Research Assistant Professor (PhD, Iowa State University)
7. **Dr. Fahim Rahman**, Research Assistant Professor (PhD, University of Florida)

Technicians:

8. **Nitin Varshney**, Lab engineer, 2017-present
9. **Daniel Johnson,** Lab Engineer, 2020-present

Current Students:

10. **Sazadur Rahman**, PhD Student, Spring 2018
11. **Nusrat Farzana,** PhD Student, Spring 2019
12. **Monir Rahman,** PhD Student, Spring 2019
13. **Jacob Harrison**, PhD Student, Fall 2019
14. **Md. Sami Ul Islam**, PhD Student, Fall 2019
15. **Bulbul Ahmed**, PhD Student, Fall 2019
16. **Paul Calzada**, PhD Students, Fall 2020
17. **Henian Li**, PhD Student, Spring 2020
18. **Shang Shi**, PhD Student, Fall 2020
19. **Tanvir Rahman**, PhD Student, Fall 2020
20. **Hasan Al-Sheikh,** PhD Student, Spring 2021
21. **Md Saad Haque,** PhD Student, Spring 2021

22. **Md Latifur Rahman,** PhD Student, Spring 2021
23. **Amit Mazumder,** PhD Student, Spring 2021
24. **Shuva Saha,** PhD Student, Spring 2021
25. **Nurun Mondol,** PhD Student, Spring 2021
26. **Azim Uddin,** PhD Student, Spring 2021
27. **Rasheed Kibira,** PhD Student, Spring 2021
28. **Kawser Bepary,** PhD Student, Spring 2021
29. **Pantha Sarker,** PhD Student, Spring 2021
30. **Katayoon Yahyaie,** PhD Student, Summer 2021
31. **Mohammad Monjil**, PhD Student, Fall 2021
32. **Arun Basu**, PhD Student, Fall 2021
33. **Habibur Rahman**, PhD Student, Spring 2022
34. **Ahmed Alhurubi**, PhD Student, Spring 2022
35. **Sai Kiran Lade**, MSc Student, Fall 2021
36. **Sumaiya**
37. **+ 10 OPS students**

Former Students / Post-doctoral Fellows/Visitors:

Post-doctoral fellow and visiting researchers:

1. **Dr. Sean Taheri,** Jointly supervised with Prof. Asadi
2. **Dr. Shahed Quadir**, Currently with Monmouth Colege
3. **Dr. Rakib Shahriar**, Currently with Cisco
4. **Dr. Shahin Tajik**, Post-doctoral fellow (PhD, TU Berlin), Curretnly with WPI
5. **Dr. Qihang Shi**, Post-doctoral fellow (PhD, University of Connecticut), Jointly supervised with Prof. Domenic Forte, Currently with Tsinghua University
6. **Prof. Yun Yang,** Visiting Researcher, Currently with Chang'An University
7. **Dr. Haoting Shen,** Post-doctoral Fellow (PhD, Penn State University), Jointly supervised with Prof. Domenic Forte, Currently with University of Nevada, Reno
8. **Dr. Xiaolin Xu,** Post-doctoral Fellow, 2016-2018, Currently with University of Illinois at Chicago
9. **Adam Dundan**, Visiting Researcher, May-August 2018, Navy Crane
10. **Dr. Navid Asadi Zanjani,** Post-doctoral Fellow, 2014-2017, Currently with University of Florida
11. **Dr. Sina Shahbaz,** Post-doctoral Fellow, 2013-2014, Currently with University of Connecticut
12. **Dr. Shuo Wang**, Post-doctoral Fellow, 2010-2012, Currently with Qualcomm
13. **Dr. Hassan Salmani**, Post-doctoral Fellow, 2011-2013, Currently with Howard University

Graduated PhD Students:

1. **Nisar Ahmed**, PhD, Oct. 2007, Currently with Apple
2. **Junxia Ma**, Dec. 2010, Currently with Intel
3. **Ke Peng**, Dec. 2010, Currently with ARM
4. **Xiaoxiao (Michel) Wang**, Dec. 2010, Currently with Beihang University as Full Professor as one of China's top 1000 talent
5. **Jeremy Lee**, Dec. 2010, Currently with Texas Instruments
6. **Hassan Salmani**, August 2011, Howard University
7. **Wei Zhao**, 2013, Currently with Nvidia
8. **Xuehui Zhang**, 2013, Currently with Oracle
9. **Jifeng Chen**, 2013, Currently with Samsung Research America
10. **Fang Bao**, 2014, Currently with Intel
11. **Kan Xiao,** 2015, Currently with Intel
12. **Ujjwal Guin**, 2016, Currently an Assistant Professor at Auburn University
13. **Mehdi Sadi,** 2017, Currently with Intel
14. **Gustavo Contreras,** 2017, Currently with Intel
15. **Qihang Shi**, 2017, Currently a post-doc at the University of Florida
16. **Tauhidur Rahman**, 2017, Currently with the University of Alabama
17. **Kun Yang**, Jan 2018, Currently with Nvidia
18. **Fahim Rahman,** July 2018, CTO, Caspia Technologies
19. **Tony (Miao) He,** July 2018
20. **Adib Nahiyan**, Aug 2019, Currently with Intel
21. **Huanyu Wang**, April 2021, Currently with Apple
22. **Jason Vosatka**, April 2021, Scientist, AFB Eglin
23. **Andrew Stern**, August 2021, CEO, Coremeleon
24. **Dhwani Mehta,** July 2022, Currently with AMD
25. **Nidish Vashistha,** July 2022, Currently with Micron
26. **Nitin Pundir**, Currently with IBM
27. **Mohammad Farmani**

<u>Graduated M.Sc. Students:</u>

1. **Hector Crespo,** May 2022
2. **Ashley Tramble**, Masters, May 2021
3. **Halit Dogan**, Sep. 2013, Currently with University of Connecticut
4. **Niranjan Kayam**, M.S., Sep. 2011, Currently with Synopsys
5. **Prasath Periyasamy**, M.S. Thesis, Aug 2006, Currently with Qualcomm

6. **Smita Patil**, M.S. Project, Aug 2006, Currently with Atmel
7. **Mohammed ElShoukry**, M.S. Thesis, Aug 2006, Currently with Micron
8. **Eun Chung,** M.S. Project, Dec. 2004

<u>Undergraduate Students:</u>

1. Brandon Wand, Undergraduate, Summer 2020
2. Luran Manfino, Undergraduate, Summer 2020
3. Anna Raymaker, Undergraduate, May 2020-Jan 2022
4. Paul Calzada, Undergraduate, Fall 2019-Spring & Summer 2020
5. Risham Sidhu, 2018
6. Wesley Steven, 2014
7. Dan Guerrera, 2014
8. Ryan Nesbit, 2014
9. Shane Tobey, 2013
10. Shane Kelly, 2013-2014
11. Nathan Murphy, 2013
12. Jacquelyn Khajah, 2014
13. Andrew Ferraiuolo, REU-Sponsored Undergraduate Student, Summer & Fall 2011, Spring 2012
14. Ashley Calder, Undergraduate Student, Spring 2012
15. Michael Calvo, Eastern Conn. Univ., REU-Sponsored Undergraduate Student, Summer 2011
16. Sagar Patil, Undergraduate Researcher, Summer 2010
17. Ryan Fitterman (CMPE), Senior Design, 2012
18. Jeffrey Foster (EE), Senior Design, 2012
19. Alvin Sanabria (EE), Senior Design, 2012
20. Michael Stettenbenz (EE), Senior Design, 2012
21. Rifat Chowdhury (CMPE/MATH), Senior Design, 2012
22. Andrew Ferraiuolo (EE/CMPE), Senior Design, 2012
23. Adam Zimmer (CSE), Senior Design, 2012
24. Carl Hinkle (EE), Senior Design, 2011
25. Dan Matosian (CMPE), Senior Design, 2011
26. Ryan Wilson (EE), Senior Design, 2011
27. Emilio Cepeda (EE), Senior Design, 2011
28. Theodore Estwan (EE), Senior Design, 2011
29. Brian Helfer (EE), Senior Design, 2011
30. Sagar Patel (EE), Senior Design, 2010

31. Michael Runde (CMPE), Senior Design, 2010
32. Ton Thomas (CMPE), Senior Design, 2010
33. Nicholas Tuzzio (CMPE), Senior Design, 2010
34. Corey Benoit (EE), Senior Design, 2010
35. Joesph Larosa (EE), Senior Design, 2010
36. Kevin Perkins (EE), Senior Design, 2010
37. Andrew Tan (EE/MGMT), Senior Design, 2009
38. Colin Gladding (EE), Senior Design, 2009
39. Harpreet Mankoo (EE), Senior Design, 2009
40. Joe Mascola (EE), Senior Design, 2009
41. Elvis Anes (CMPE), Senior Design, 2009
42. Jeff Chua (CMPE), Senior Design, 2009
43. Ali Faraz (EE), Senior Design, 2009
44. Samantha Logue (CMPE), Senior Design, 2009
45. Poorak Mody (CMPE), Senior Design, 2008
46. Jonathan Schindler (CMPE), Senior Design, 2008
47. Jason Thibodeau (CMPE), Senior Design, 2008
48. Aaron Feldstein (EE), Senior Design, 2008
49. Paul Rago (EE), Senior Design, 2008
50. Danny Ho (EE), Senior Design, 2007
51. Kevin Tyler (EE), Senior Design, 2007
52. Vimal Vacchani (EE), Senior Design, 2007
53. Michael Kelley (EE), Senior Design, 2007
54. Benjamin Romeo (EE), Senior Design, 2007
55. Jeffrey Travis (EE), Senior Design, 2007
56. Pedro Almaida, B.S., 2005

Thesis Advisory Committee

PhD Advisory Committee:

Nisar Ahmed (Chair), Jianwei Dai (Adivosr: Lei Wang, UConn), Wei-Gu Tang (Adivosr: Lei Wang, UConn), Janardhan Singaraju (Adivosr: John Chandy, UConn), Junxia Ma (Chair), Ke Peng (Chair), Michel Wang (Chair), Xuan Guan (Adivosr: Yunsi Fei), Jeremy Lee (Chair), Hai Lin, Shou Wang, Tina John (Adivosr: John Chandy, UConn), Abhishek Singh (Adivosr: Jim Plusquellic, UMB), Ajith Kumar (Adivosr: john Chandy, UConn), Robert Karam (Adivosr: Swarup Bhunia, UF, 2017), Zimu Guo (Advisor: Domenic Forte, UF), Gustavo Contreras (Chair), Tauhid Rahman (Chair), Mahmut Yilmaz (Advisor: Krishnendu Chakrabarty, Duke University); Nolen Scaife (Advisor: Patrick Traynor, UF, 2018), Kai Yang (Advisor: Swarup Bhunia, UF, 2018), Fangchao Zhang (Advisor: Swarup Bhunia, UF, 2018), Nima Karimian (Adivosr: Domenic Forte, UConn, 2018), Zimu Guo (Advisor: Domenic Forte, UF), Abdulrahman Alql (Advisor: Swarup Bhunia), Mukhil Azhagan (Advisor: Navid Asadi), Alice Hangwei (Advisor: Damon Woodard), Ana Covic (Advisor: Domenic Forte), Tamzidul Hoque (Advisor: Swarup Bhunia), Christian Peeters (Advisor: Patrick Traynor), Alice Lu (Advisor: Damon Woodard), Rabin Acharya (Advisor: Domenic Forte)

International: Fatemeh Ganji (Advisor: Jean-Pierre Seifert, TU Berlin, 2018), Shahin Tajik (Advisor: Jean-Pierre Seifert, TU Berlin, 2018)

M.S. Advisory Committee:

Halit Dogan (Chair), Niranjan Kayam (Chair), Prasath Periyasamy (Chair), Smita Patil (Chair), Mohammed ElShoukry (Chair), Eun Chung (Chair), Pushkar Pulastya, Michael Wolk, Jitin Tharian, Adhruva Acharyya, Niranjan Reddy, Shruti Khare, Michael Runda, Hitesh Sharma

B.Sc. Advisory Committee:

Jackson Carrol

Institutional Service

UF: ECE/CISE Department Chair, Wally Rhines Chair Professorship in Homomorphic Professorships (2021)

UF: ECE Department, Chair, Semotto IoT Chair Professorship Search Committee (2018-2019)

UF: College of Engineering, Tenure & Promotion (T&P) Committee (2017-2019)

UF: ECE Department, Chair, Tenure & Promotion (T&P) Committee (2017-2019)

UF: ECE Department, Associate Chair for Research and Strategic Initiatives (2017-present)

UF: College of Engineering, Member, Research Advancement Committee, RAC (2017-present)

UF: ECE Department, Chair, Faculty Development Committee (2017-present)

UF: ECE Department, Member, Semotto IoT Chair Professorship Search Committee (2017-2018)

UF: College of Engineering, Tenure & Promotion (T&P) Committee (2017-2020)

UConn: Chair, Computer Engineering Search Committee (2012-2014)

UConn: ECE Search Committee (2011-2012, 2013-2014)

UConn: ECE Department Library Liaison, January 2009-Present

UConn: C&C Committee (2007-present)

UMBC: Member, Equipment Committee (Oct. 2004–2006)

UMBC: Member, Graduate Admission Committee (Jan 2005-2006)

UMBC: Member, ABET Visiting Committee (Oct. 2004–2006)

Supervising Undergraduate Senior Design Projects

2006-2007 **Project 1:** Redesign of Solitec Track System (Sponsored by Phonon)

Project 2: Speech Control System for Persons with Disabilities (Sponsored by ECE Department) First Prize in ECE Department

2007-2008 **Project 1:** Wafer Processing Track Upgrade (Sponsored by Phonon) Second Prize in ECE Department

Project 2: CAD2XML (Sponsored by QualTech)

2008-2009 **Project 1:** Digital Temperature Controller (DTC) Design (Sponsored by Phonon)

Project 2: UConn Peronal ATE (Sponsored by ECE Department)

2009-2010 **Project 1:** Surface Contour Profiler (Sponsored by Phonon) First Prize in ECE Department

Project 2: UConn Personal ATE (Sponsored by ECE Department)

2010-2011 **Project 1:** Enhanced Surface Contour Profiler (Sponsored by Phonon) First Prize in ECE Department

Project 2: Distributed Aviation Control and Communication System (Sponsored by Hamilton Sundstrand)

2011-2012 **Project 1:** Automated Trojan Insertion and Detection Evaluation (Sponsored by ECE Department) First Prize in ECE Department

Project 2: Distributed Aviation Control and Communication System (Sponsored by Hamilton Sundstrand)

2013-2014 **Project 1:** Virtual Laboratir for Hardware Security (Sponsored by ECE Department)

2013-2014 **Project 2:** Automated Counterfeit IC Physical Defect Characterization (Sponsored by ECE Department)