# Domenic J. Forte

Department of Electrical and Computer Engineering
216 Larsen Hall, P.O. Box 116200
University of Florida, Gainesville, FL 32611-6200
Phone: 352-392-1525 E-mail: dforte@ece.ufl.edu

## Research Interests

**Counterfeit Electronic Component Detection and Avoidance**: Includes physical inspection, electrical tests, and sensor design; provenance and supply chain tracking; from device level to system level
**Physically Unclonable Functions (PUFs)**: Design, fabrication, and applications
**Hardware Trojans**: Pre-silicon prevention and post-silicon detection
**Design Tools, Rules, Metrics, and Benchmarking**: Hardware security assessment, mitigation, and obfuscation
**Biometrics in IoT Applications**: Includes emerging medico-chemical biometrics such as electrocardiogram (ECG) and photoplethysmograph (PPG)
**PCB and IC Reverse and Anti-Reverse Engineering**
**Nanoscale Integration Challenges**: 3D integration, thermal issues, security, and manufacturing variations in CMOS and beyond CMOS

## Education

**University of Maryland**, College Park, MD
Ph.D., Electrical Engineering, August 2013

**University of Maryland**, College Park, MD
M.S., Electrical Engineering, December 2010

**Manhattan College**, Riverdale, NY
B.S., Electrical Engineering, *Summa Cum Laude*, May 2006

## Professional Experience

**University of Florida, ECE Department**, Gainesville, FL

*Associate Director, Florida Institute for National Security (FINS)*, August 2022 – present
*Steven A. Yatauro Faculty Fellow*, May 2021 – present
*Associate Professor*, August 2019 – present
*FICS Research Security and Assurance (SCAN) Lab Director*, August 2016 – July 2021
*Assistant Professor*, July 2015 – August 2019

**University of Connecticut, ECE Department**, Storrs, CT

*Assistant Professor*, August 2013 – July 2015

**University of Maryland, ECE Department**, College Park, MD

*Research Assistant*, June 2009 – August 2013

**University of Maryland, ECE Department**, College Park, MD

*Teaching Assistant*, August 2006 – December 2010

**National Institutes of Health CIT DCB CBEL SPIS**, Bethesda, MD

*Co-op Student Intern*, June 2007 – May 2009

**Maryland Engineering Research Internship Teams (MERIT)**, College Park, MD

*REU Student*, Summer 2005

## Honors and Distinctions

*External Faculty Awards*

- 2017 Presidential Early Career Award for Scientists and Engineers (PECASE) by Department of Defense, 2019
- 2017 Early Career Award for Scientists and Engineers (ECASE-Army) by Army Research Office, 2019
- NSF Faculty Early Career Development (CAREER) Award, 2017
- Army Research Office (ARO) Young Investigator Award, 2016
- Schloss Dagstuhl - NSF Support Grant for Junior Researchers, Awarded, 2016

*Internal Faculty Awards*

- HWCOE Doctoral Dissertation Advisor/Mentoring Award (2021-2022), 2021
- Steven Yatauro Faculty Fellow, 2021
- Pramod R. Khargonekar Award, 2019
- Excellence in Teaching Award, University of Florida ECE Graduate Student Organization, 2019
- Provost Awards UF Term Professorship, 2019
- UF Provost's Excellence Award for Assistant Professors, 2018

*Best Paper Awards and Nominations*

- EDFAS Virtual Workshop (International Symposium for Testing and Failure Analysis 2020) Outstanding Paper Award, 2020
- ACM TODAES Best Paper Award, 2018
- International Symposium for Testing and Failure Analysis (ISTFA) Outstanding Paper Award, 2017
- International Joint Conference on Biometrics (IJCB) Best Student Paper Award, 2017
- ACM Computing Reviews Notable Computing Books and Articles – 2016, Hardware Category
- IEEE International Symposium on Hardware Oriented Security and Trust (HOST) Best Paper Award, 2016
- IEEE International Symposium on Hardware Oriented Security and Trust (HOST) Best Paper Nomination ($\times$2), 2016
- IEEE International Symposium on Hardware Oriented Security and Trust (HOST) Best Paper Award, 2015
- Design Automation Conference (DAC) Best Paper Nomination, 2012
- NASA/ESA Conference on Adaptive Hardware and Systems (AHS) Best Student Paper Award, 2011

*Graduate School Awards*

- Jacob K. Goldhaber Travel Award, University of Maryland, 2013
- Northrop Grumman Fellowship, 2012-2013 (Awarded to a top student in ECE)
- TA Teaching and Development (TATD) Fellow, University of Maryland, 2010–2011, 2011–2012
- George Corcoran Outstanding Teaching Award, University of Maryland, 2008 (Presented to two ECE graduate teaching assistants in 2008)
- Distinguished Teaching Assistant Award, University of Maryland, 2007-2008 (Awarded to top 10% of all graduate teaching assistants in the university)

*Undergraduate School Awards*

- Co-recipient of medal for Electrical Engineering, Manhattan College, 2006 (Awarded at graduation to top two EE students in 2006)

- Next in Merit: Draddy Medal for General Excellence in Engineering, Manhattan College, 2006
- Society of Military Engineers (SAME) Scholarship, 2005
- Manhattan College Presidential Scholarship, 2002
- NY State Academic Excellence Scholarship, 2002

### Awards Received by Student Advisees

- David Koblah: Received scholarship under the Science, Mathematics, and Research for Transformation (SMART) Scholarship-for-Service Program, 2022
- Rabin Acharya: Received Best Poster Award in "AI Architectures and Algorithms" track at IBM-IEEE AI Compute Symposium (AICS), 2021
- Ana Covic: Received the ECE Graduate Student Excellence in Service Award, 2021
- Ulbert (Joey) Botero: Received Outstanding Paper Award from EDFAS Virtual Workshop, 2020
- Sumaiya (Jyoti) Shomaji: Awarded first place for poster in "IoT Technology" category at the Warren B. Nelms Annual IoT Conference, 2019
- Sumaiya (Jyoti) Shomaji: Three Minute Thesis (3MT) Competition Finalist and People's Choice Award Winner at the University of Florida, 2019
- Sumaiya (Jyoti) Shomaji: Received best oral presentation award at UF Diversity Graduate Research Symposium, 2019
- Sreeja Chowdury: Awarded first place in poster competition at the Third Workshop for Women in Hardware and Systems Security (WISE), 2019
- Sumaiya (Jyoti) Shomaji: Awarded honorable mention in poster competition at the Third Workshop for Women in Hardware and Systems Security (WISE), 2019
- Ulbert (Joey) Botero: Awarded best poster in "Hardware Verification and Authentication" category at FICS Research Annual Conference on Cybersecurity, 2019
- Mahbub Alam: Awarded best poster in "Physical Attacks and Countermeasures" category at FICS Research Annual Conference on Cybersecurity, 2019
- Ulbert (Joey) Botero: NSF Graduate Research Fellowship Program (GRFP), 2018
- Sreeja Chowdury: Three Minute Thesis (3MT) Competition Finalist at the University of Florida, 2018
- Sreeja Chowdury: $ISC^2$ Graduate Cybersecurity Scholarship, 2018
- Sreeja Chowdury: Awarded second place in poster competition at the Second Workshop for Women in Hardware and Systems Security (WISE), 2018
- Ulbert (Joey) Botero: Awarded best poster at FICS Research Annual Conference on Cybersecurity, 2018
- Nima Karimian: Awarded best student paper at International Joint Conference on Biometrics (IJCB) 2017
- Zimu Guo: Awarded best demo at FICS Research Annual Conference on Cybersecurity, 2017
- Sreeja Chowdury: Awarded best hardware primitive poster at FICS Research Annual Conference on Cybersecurity, 2017
- Zimu Guo and Nima Karimian: Awarded best hardware security poster at FICS Research Annual Conference on Cybersecurity, 2016

## Books

B1. M. Tehranipoor, **D. Forte**, G. Rose, S. Bhunia, "Security Opportunities in Nano Devices and Emerging Technologies", CRC Press, 2017. *[Edited and Contributed]*

B2. **D. Forte**, S. Bhunia, M. Tehranipoor, "Hardware Protection through Obfuscation", Springer, 2017. *[Edited and Contributed]*

B3. M. Tehranipoor, U.J. Guin, **D. Forte**, "Counterfeit Integrated Circuits: Detection and Avoidance", Springer, 2015. *[Authored]*

## Book Chapters

BC1. A. Covic, S. Chowdhury, RY Acharya, F. Ganji, **D. Forte**, "Post-Quantum Hardware Security: Physical Security in Classic vs. Quantum Worlds", in Emerging Topics in Hardware Security by Mark M. Tehranipoor, Springer, 2020.

BC2. H. Lu, DE Capecci, P. Ghosh, **D. Forte**, DL Woodard, "Computer Vision for Hardware Security", in Emerging Topics in Hardware Security by Mark M. Tehranipoor, Springer, 2020.

BC3. Q. Shi, **D. Forte**, M. Tehranipoor, "Deterrent Approaches Against Hardware Trojan Insertion," in The Hardware Trojan War by Swarup Bhunia, and Mark M. Tehranipoor, Springer, 2018.

BC4. F. Rahman, A. Nath, **D. Forte**, S. Bhunia, and M Tehranipoor, "Nano CMOS Logic-Based Security Primitive Design", in Security Opportunities in Nano Devices and Emerging Technologies by Mark M. Tehranipoor, Domenic Forte, Garrett Rose, and Swarup Bhunia, CRC Press, 2017.

BC5. H.T. Shen, F. Rahman, M. Tehranipoor, **D. Forte**, "Carbon-Based Novel Devices for Hardware Security", in Security Opportunities in Nano Devices and Emerging Technologies by Mark M. Tehranipoor, Domenic Forte, Garrett Rose, and Swarup Bhunia, CRC Press, 2017.

BC6. F. Rahman, A. Nath, S. Bhunia, **D. Forte**, M. Tehranipoor, "Composition of Physical Unclonable Functions: From Device to Architecture", in Security Opportunities in Nano Devices and Emerging Technologies by Mark M. Tehranipoor, Domenic Forte, Garrett Rose, and Swarup Bhunia, CRC Press, 2017.

BC7. B. Shakya, X. Xu, N. Asadizanjani, M. Tehranipoor, **D. Forte**, "Leveraging Circuit Edit for Low-Volume Trusted Nanometer Fabrication", in Security Opportunities in Nano Devices and Emerging Technologies by Mark M. Tehranipoor, Domenic Forte, Garrett Rose, and Swarup Bhunia, CRC Press, 2017.

BC8. B. Shakya, M. Tehranipoor, S. Bhunia, **D. Forte**, "Introduction to Hardware Obfuscation: Motivation, Methods and Evaluation," in Hardware Protection through Obfuscation by Domenic Forte, Swarup Bhunia, and Mark M. Tehranipoor, Springer, 2017.

BC9. Z. Guo, M. Tehranipoor, **D. Forte**, "Permutation-Based Obfuscation," in Hardware Protection through Obfuscation by Domenic Forte, Swarup Bhunia, and Mark M. Tehranipoor, Springer, 2017.

BC10. M. T. Rahman, **D. Forte**, M. Tehranipoor, "Protection of Assets from Scan Chain Vulnerabilities through Obfuscation," in Hardware Protection through Obfuscation by Domenic Forte, Swarup Bhunia, and Mark M. Tehranipoor, Springer, 2017.

BC11. Q. Shi, K. Xiao, **D. Forte**, M. Tehranipoor, "Obfuscated Built-in Self Authentication," in Hardware Protection through Obfuscation by Domenic Forte, Swarup Bhunia, and Mark M. Tehranipoor, Springer, 2017.

BC12. A. Nahiyan, K. Xiao, **D. Forte**, M. Tehranipoor, "Security Rule Check," in Hardware IP Security and Trust by Prabhat Mishra, Swarup Bhunia and Mark Tehranipoor, Springer, 2017.

BC13. Q. Shi, **D. Forte**, M. Tehranipoor, "Analyzing Circuit Layout to Probing Attack," in Hardware IP Security and Trust by Prabhat Mishra, Swarup Bhunia and Mark Tehranipoor, Springer, 2017.

BC14. K. Xiao, **D. Forte**, 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, Springer, 2016.

Peer-Reviewed Journal Publications (accepted)

J1. D. Koblah, R. Acharya, D. Capecci, O. Dizon-Paradis, S. Tajik, F. Ganji, D. Woodard, **D. Forte**, "A Survey and Perspective on Artificial Intelligence for Security-Aware Electronic Design Automation", to appear *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 2022.

J2. S. Amir and **D. Forte**, "EigenCircuit: Divergent Synthetic Benchmark Generation for Hardware Security Using PCA and Linear Programming", to appear *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, 2022.

J3. Y. Bai, A. Stern, J. Park, M. Tehranipoor, **D. Forte**, "RASCv2: Enabling Remote Access to Side-Channels for Mission Critical and IoT Systems", *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, Vol. 27, No. 1, Nov. 2022.

J4. Y. Bai, J. Park, M. Tehranipoor, **D. Forte**, "Real-time Instruction-level Verification of Remote IoT/CPS Devices Via Side Channels", *Discover Internet of Things Journal*, Vol. 2, No. 1, March 2022.

J5. S. Shomaji, P. Ghosh, F. Ganji, DL Woodard, **D. Forte**, "An Analysis of Enrollment and Query Attacks on Hierarchical Bloom Filter-based Biometric Systems", *IEEE Transactions on Information Forensics and Security (TIFS)*, Vol. 16, Nov. 2021.

J6. B. Park, **D. Forte**, M. Tehranipoor, N. Maghari, "A Metal-Via Resistance based Physically Unclonable Function with Backend Incremental ADC", *IEEE Transactions on Circuits and Systems I*, Vol. 68, No. 11, Nov. 2021.

J7. S. Shomaji, Z. Guo, F. Ganji, N. Karimian, DL Woodard, **D. Forte**, "BLOcKeR: A Biometric Locking Paradigm for IoT and the Connected Person", *Journal of Hardware and Systems Security (HaSS)*, Vol. 5, No. 3, October 2021.

J8. S. Shomaji, NVR Masna, DJ Ariando, SD Paul, K. Horace-Herron, **D. Forte**, S. Mandal, S. Bhunia, "Detecting Dye-Contaminated Vegetables using Low-Field NMR Relaxometry", *Foods*, Vol. 10, No. 9, September 2021.

J9. R. Wilson, H. Lu, M. Zhu, **D. Forte**, DL Woodard, "REFICS: Assimilating Data-Driven Paradigms into Reverse Engineering and Hardware Assurance on Integrated Circuits", *IEEE Access*, Vol. 9, September 2021.

J10. UJ Botero, R. Wilson, H. Lu, MT Rahman, MA Mallaiyan, F. Ganji, N. Asadizanjanizanjani, MM Tehranipoor, DL Woodard, **D. Forte**, "Hardware Trust and Assurance through Reverse Engineering: A Tutorial and Outlook from Image Analysis and Machine Learning Perspectives", to appear *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, Vol. 17, No. 4, June 2021

J11. MS Rahman, A. Nahiyan, F. Rahman, S. Fazzari, K. Plaks, F. Farahmandi, **D. Forte**, M. Tehranipoor, "Security Assessment of Dynamically Obfuscated Scan Chain Against Oracle-guided Attacks", *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, Vol. 26, No. 4, March 2021.

J12. S. Chowdhury, A. Covic, R. Acharya, S. Dupee, F. Ganji, **D. Forte**, "Physical Security in the Post-quantum Era: A Survey on Side-channel Analysis, Random Number Generators, and Physically Unclonable Functions", *Journal of Cryptographic Engineering (JCEN)*, 2021.

J13. H. Wang, Q. Shi, A. Nahiyan, **D. Forte**, 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, October 2020.

J14. S. Chowdury, F. Ganji, **D. Forte**, "Recycled SoC Detection using LDO Degradation" *SN Computer Science*, September 2020.

J15. N. Karimian, D. Woodard, **D. Forte**, "ECG Biometric: Spoofing and Countermeasures," *IEEE Transactions on Biometrics, Behavior, and Identity Science (T-BIOM)*, Vol. 2, No. 3, July 2020.

J16. M. Alam, A. Nahiyan, M. Sadi, **D. Forte**, 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.

J17. F. Ganji, S. Tajik, P. Stauss, J.-P. Seifert, M. Tehranipoor, **D. Forte**, "Rock'n' roll PUFs: Crafting Provably Secure PUFs from Less Secure Ones (Extended Version)," *Journal of Cryptographic Engineering*, May 2020.

J18. A. Nahiyan, J. Park, H. Miao, Y. Iskander, F. Farahmandi, **D. Forte**, 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)*, Vol. 25, No. 3, May 2020.

J19. MT Rahman, MS Rahman, H. Wang, S. Tajik, W. Khalil, F. Farahmandi, **D. Forte**, N. Asadizanjanizanjani, M. Tehranipoor, "Defense-in-Depth: A Recipe for Logic Locking to Prevail", *Integration, the VLSI Journal*, Vol. 72, May 2020.

J20. A. Stern, U.J. Botero, F. Rahman, **D. Forte**, M. Tehranipoor, "EMFORCED: EM-Based Fingerprinting Framework for Remarked and Cloned Counterfeit IC Detection using Machine Learning Classification", *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, Vol. 28, No. 2, February 2020.

J21. Z. Guo, S. Chowdury, M. Tehranipoor, **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, January 2020.

J22. B. Shakya, X. Xu, M. Tehranipoor, **D. Forte**, "CAS-Lock: A Security-Corruptibility Trade-off Resilient Logic Locking Scheme", *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, No. 1, 2020.

J23. J. Park, F. Rahman, A. Vassilev, **D. Forte**, M. Tehranipoor, "Leveraging Side-channel Information for Disassembly and Security", *ACM Journal on Emerging Technologies in Computing (JETC)*, Vol. 16, No. 1, December 2019.

J24. T. Hoque, K. Yang, R. Karam, S. Tajik, **D. Forte**, M. Tehranipoor, 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, No. 1, December 2019.

J25. M. Alam, M. Tehranipoor, **D. Forte**, "Recycled FPGA Detection Using Exhaustive LUT Path Delay Characterization and Voltage Scaling", *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, Vol. 27, No 12. December 2019.

J26. F. Ganji, **D. Forte**, JP Seifert, "PUFmeter: A Property Testing Tool for Assessing the Robustness of Physically Unclonable Functions to Machine Learning Attacks", *IEEE Access*, Vol. 7, No. 1, December 2019.

J27. BM Talukder, B. Ray, **D. Forte**, MT Rahman, "PreLatPUF: Exploiting DRAM Latency Variations for Generating Robust Device Signatures", *IEEE Access*, Vol. 7, No. 1, December 2019.

J28. N. Karimain, M. Tehranipoor, D. Woodard, **D. Forte**, "Unlock Your Heart: Next Generation Biometric in Resource-Constrained Healthcare Systems and IoT", *IEEE Access*, Vol. 7, No. 1, December 2019.

J29. Q. Shi , M. Tehranipoor, **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, No. 11, November 2019.

J30. S. Shomaji, P. Dehghanzadeh, A. Roman, **D. Forte**, S. Bhunia, S. Mandal, "Early Detection of Cardiovascular Diseases Using Wearable Ultrasound Device" *IEEE Consumer Electronics Magazine*, Vol. 8, No. 6, November 2019.

J31. P. Ghosh, A. Bhattacharyay, **D. Forte**, RS Chakraborty,"Automated Defective Pin Detection for Recycled Microelectronics Identification" *Journal of Hardware and Systems Security (HaSS)*, Vol. 3, No. 3, September 2019.

J32. B. Shakya, H. Shen, M. Tehranipoor, **D. Forte**, "Covert Gates: Protecting Integrated Circuits with Undetectable Camouflaging", *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, August 2019.

J33. X. Xu, F. Rahman, B. Shakya, A. Vassilev, **D. Forte**, M. Tehranipoor, "Electronics Supply Chain Integrity Enabled by Blockchain", *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, Vol. 24, No. 3, June 2019.

J34. H. Wang, Q. Shi. **D. Forte**, M. Tehranipoor, "Probing Assessment Framework and Evaluation of Anti-probing Solutions", *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, Vol. 27, No. 6, June 2019.

J35. A. Nahiyan, F. Farahmandi, P. Mishra, **D. Forte**, 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)*, Vol. 38, No. 6, June 2019.

J36. U. J. Botero, M. Tehranipoor, **D. Forte**, "Upgrade/Downgrade: Efficient and Secure Legacy Electronic System Replacement", *IEEE Design & Test*, Vol. 36, No. 1, February 2019.

J37. K. Yang, U. Botero, H. Shen, D. Woodard, **D. Forte**, M. Tehranipoor, "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, December 2018.

J38. X. Xu, S. Keshavarz, **D. Forte**, M. Tehranipoor, D.E. Holcomb, "Bimodal Oscillation as a Mechanism for Autonomous Majority Voting in PUFs", *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, Vol. 26, No. 11, November 2018.

J39. 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, No. 2, June 2018.

J40. Z. Guo, X. Xu, M. Tehranipoor, **D. Forte**, "SCARe: An SRAM-based Countermeasure Against IC Recycling Framework" *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, Vol. 26., No. 4, April 2018.

J41. M.M. Alam, S. Chowdhury, B. Park, D. Munzer, N. Maghari, M. Tehranipoor, **D. Forte**, "Challenges and Opportunities in Analog and Mixed Signal (AMS) Integrated Circuit (IC) Security", *Journal of Hardware and Systems Security (HaSS)*, Vol. 2, No. 1, March 2018.

J42. K. Yang, **D. Forte**, M. Tehranipoor, "ReSC: An RFID-Enabled Solution for Defending IoT Supply Chain", *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, Vol. 23, No. 3, February 2018.

J43. K. Yang, H. Shen, **D. Forte**, S. Bhunia, M. Tehranipoor, "Hardware-Enabled Pharmaceutical Supply Chain Security", *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, Vol. 23, No. 3, January 2018.

J44. F. Rahman, B. Shakya, Bicky, X. Xu, **D. Forte**, M. Tehranipoor,"Security Beyond CMOS: Fundamentals, Applications, and Roadmap", *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, Vol. 25, No. 12, December 2017.

J45. H. Shen, F. Rahman, B. Shakya, X. Xu, M. Tehranipoor, **D. Forte**,"Poly-Si Based Physical Unclonable Functions", *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, Vol. 25, No. 11, November 2017.

J46. H. Wang, Q. Shi, **D. Forte**, M. Tehranipoor, "Probing Attacks on Integrated Circuits: Challenges and Research Opportunities", *IEEE Design & Test*, Vol. 34, No. 5, October 2017.

J47. M.T. Rahman, A. Hosey, Z. Guo, J. Carroll, **D. Forte**, 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, No. 2, June 2017.

J48. N. Karimian, Z. Guo, M. Tehranipoor, **D. Forte**, "Highly Reliable Key Generation from Electrocardiogram (ECG)," *IEEE Transactions on Biomedical Engineering (TBME)*,Vol. 64, No. 6, June 2017.

J49. U.J. Guin, S. Bhunia, **D. Forte**, M. Tehranipoor, "SMA: A System-Level Mutual Authentication for

Protecting Electronic Hardware and Firmware," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, Vol. 14, No. 3, May-June 1 2017.

J50. Z. Guo, J. Di, M. Tehranipoor, **D. Forte**, "Obfuscation based Protection Framework Against Printed Circuit Boards Privacy Violation," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, Vol. 22, No. 3, April 2017.

J51. K. Yang, **D. Forte**, 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, No. 3, April 2017.

J52. B. Shakya, T. He, H. Salmani, **D. Forte**, S. Bhunia, M. Tehranipoor, "Benchmarking of Hardware Trojans and Maliciously Affected Circuits", *Journal of Hardware and Systems Security (HaSS)*, Vol. 1, No. 1, April 2017.

J53. M. Alam, H. Shen, N. Asadizanjani, M. Tehranipoor, **D. Forte**, "Impact of X-ray Tomography on the Reliability of Integrated Circuits", *IEEE Transactions on Device and Materials Reliability (TDMR)*, Vol. 17, No. 1, March 2017.

J54. N. Asadizanjani, M. Tehranipoor, **D. Forte**, "PCB Reverse Engineering Using Non-destructive X-ray Tomography and Advanced Image Processing", *IEEE Transactions on Components, Packaging and Manufacturing (CPMT)*, Vol. 7, No. 2, February 2017.

J55. K. Xiao, **D. Forte**, Y. Jin, R. Karri, S. Bhunia, M. Tehranipoor, "Hardware Trojans: Lessons Learned After One Decade of Research", *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, Vol. 22, No. 1, June 2016. **[2018 ACM TODAES Best Paper, ACM Computing Reviews Notable Computing Books and Articles – 2016, Hardware Category]**

J56. U Guin, Q. Shi, **D. Forte**, M. Tehranipoor, "FORTIS: A Comprehensive Solution for Establishing Forward Trust for Protecting IPs and ICs," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, Vol. 21, No. 4, June 2016

J57. U.J. Guin, **D. Forte**, M. Tehranipoor, "Design of Accurate Low-Cost On-Chip Structures for protecting Integrated Circuits against Recycling," *IEEE Transactions on VLSI Systems (TVLSI)*, Vol. 24, No. 4, April 2016.

J58. S. E. Quadir, J. Chen, **D. Forte**, N. Asadizanjanizanjani, S. Shahbazmohamadi, L. Wang, J. Chandy, M. Tehranipoor, "A Survey on Chip to System Reverse Engineering," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, Vol. 13, No. 1, April 2016.

J59. C. Bao, **D. Forte**, A. Srivastava, "On Reverse Engineering-Based Hardware Trojan Detection," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, Vol. 35, No.1, January 2016

J60. C. Bao, **D. Forte**, A. Srivastava, "Temperature Tracking: Towards Robust Run-time Detection of Hardware Trojans," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)* Vol. 34, No. 10, October 2015.

J61. M.T. Rahman, F. Rahman, **D. Forte**, M. Tehranipoor, "An Aging-Resistant RO-PUF for Reliable Key Generation," *IEEE Transactions on Emerging Topics in Computing (TETC)*, September 2015.

J62. A. Mazady, M.T. Rahman, **D. Forte**, M. Anwar,"Memristor Nano-PUF A Security Primitive: Theory and Experiment," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems (JETCAS)*, Vol. 5, No. 2, June 2015.

J63. K. Xiao, **D. Forte**, 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. 32, No. 12, November 2014.

J64. **D. Forte** and A. Srivastava, "Improving the Quality of Delay-based PUFs via Optical Proximity Correction," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, Vol. 32, No. 12, December 2013.

J65. **D. Forte** and A. Srivastava, "Thermal-Aware Sensor Scheduling for Distributed Estimation," *ACM Transactions on Sensor Networks (TOSN)*, Vol. 9, No. 4, July 2013.

J66. **D. Forte** and A. Srivastava, "Energy and Thermal-Aware Video Coding via Encoder/Decoder Workload Balancing", *IEEE Transactions on Embedded Computing Systems (TECS)*, Vol. 12, No. 2, May 2013.

J67. **D. Forte** and A. Srivastava, "Resource-Aware Architectures for Adaptive Particle Filter Based Visual Target Tracking", *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, Vol. 18, No. 2, April 2013.

Peer-Reviewed Conference/Workshop Publications

C1. M. Hashemi, S. Roy, F, Ganji **D. Forte**, "Garbled EDA: Privacy Preserving Electronic Design Automation", to appear *International Conference on Computer-Aided Design (ICCAD)*, November 2022.

C2. T. Farheen, S. Tajik, **D. Forte**, "SPREAD: Spatially Distributed Laser Fault Injection Resilient Attack Detector", to appear *International Symposium for Testing and Failure Analysis (ISTFA)*, November 2022.

C3. M. Choudhury, M. Gao, S. Tajik, **D. Forte**, "TAMED: Transitional Approaches for LFI Resilient State Machine Encoding", to appear *IEEE International Test Conference (ITC)*, September 2022.

C4. RY Acharya, **D. Forte**, "Joint Optimization of NCL PUF Using Frequency-based Analysis and Evolutionary Algorithm", *International Symposium on Quality Electronic Design (ISQED)*, April 2022.

C5. S. Roy, T. Farheen, S. Tajik, **D. Forte**, "Self-timed Sensors for Detecting Static Optical Side Channel Attacks", *International Symposium on Quality Electronic Design (ISQED)*, April 2022.

C6. R. Wilson, H. Lu, M. Zhu, **D. Forte**, DL Woodard, "REFICS: A Step Towards Linking Vision with Hardware Assurance", *Winter Conference on Applications of Computer Vision (WACV)*, January 2022.

C7. U. Botero, F. Ganji, D. Woodard, **D Forte**, "Automated Trace and Copper Plane Extraction of X-ray Tomography Imaged PCBs, *IEEE International Conference on Physical Assurance and Inspection of Electronics (PAINE)*, December 2021.

C8. T. Farheen, U. Botero, N. Varshney, HT Shen, DL Woodard, M. Tehranipoor, **D. Forte**, "Proof of Reverse Engineering Barrier: SEM Image Analysis on Covert Gates", *International Symposium for Testing and Failure Analysis (ISTFA)*, November 2021.

C9. M. Choudhury, S. Tajik, **D. Forte**, "SPARSE: Spatially Aware LFI Resilient State Machine Encoding", *Hardware and Architectural Support for Security and Privacy (HASP)*, October 2021.

C10. RY Acharya, M. Levin, **D. Forte**, "LDO-based Odometer to Combat IC Recycling", *IEEE International System-on-Chip Conference (SOCC)*, September 2021.

C11. RY Acharya, N. Charlot, MM Alam, F. Ganji, D. Gauthier, **D. Forte**, "Chaogate Parameter Optimization using Bayesian Optimization and Genetic Algorithm", *International Symposium on Quality Electronic Design (ISQED)*, April 2021.

C12. M. Choudhury, S. Tajik, **D. Forte**, "PATRON: A Pragmatic Approach for Encoding LFI Resistant FSMs", *Design, Automation and Test in Europe (DATE)*, February 2021.

C13. R. Acharya, S. Chowdhury, F Ganji, **D. Forte**, "Attack of the Genes: Finding Keys and Parameters of Locked Analog ICs Using Genetic Algorithm", *IEEE IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, December 2020.

C14. U. Botero, F. Ganji, N. Asadizanjanizanjani, D. Woodard, **D. Forte**, "Semi-Supervised Automated Layer Identification of X-ray Tomography Imaged PCBs", *IEEE International Conference on Physical Assurance and Inspection of Electronics (PAINE)*, December 2020.

C15. P. Ghosh, U. Botero, F. Ganji, D. Woodard, RS Chakraborty, **D. Forte**, "Automated Detection and Localization of Counterfeit Chip Defects by Texture Analysis in Infrared (IR) Domain", *IEEE*

*International Conference on Physical Assurance and Inspection of Electronics (PAINE)*, December 2020.

C16. UJ Botero, D. Koblah, DE Capecci, F. Ganji, N. Asadizanjani, DL Woodard, **D. Forte**, "Automated Via Detection for PCB Reverse Engineering", *International Symposium for Testing and Failure Analysis (ISTFA)*, December 2020. **[EDFAS Virtual Workshop (ISTFA 2020) Outstanding Paper Award]**

C17. R. Wilson, **D. Forte**, N. Asadizanjani, D. Woodard, "LASRE: A Novel Approach to Large area Accelerated Segmentation for Reverse Engineering on SEM images", *International Symposium for Testing and Failure Analysis (ISTFA)*, December 2020.

C18. S. Chowdhury, R. Acharya, W. Boullion, M. Howard, A. Felder, J. Di, **D. Forte**, "A Weak Asynchronous RESet (ARES) PUF Using Start-up Characteristics of Null Conventional Logic Gates", *IEEE International Test Conference (ITC)*, November 2020

C19. S. Amir, **D. Forte**,"Adaptable and Divergent Synthetic Benchmark Generation for Hardware Security", *International Conference on Computer-Aided Design (ICCAD)*, November 2020.

C20. S. Chowdhury, F Ganji, **D. Forte**,"Low-Cost Remarked Counterfeit IC Detection Using LDO Regulators", *IEEE International Symposium on Circuits and Systems (ISCAS)*, October 2020.

C21. F Ganji, S. Amir, S. Tajik, **D. Forte**, JP Seifert, "Pitfalls in Machine Learning-based Adversary Modeling for Hardware Systems", *Design, Automation, and Test in Europe (DATE)*, March 2020.

C22. A. Covic, Q. Shi, H. Shen, **D. Forte**, "Contact-to-Silicide Probing Attacks on Integrated Circuits and Countermeasures", *IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, December 2019.

C23. A. Alaql, **D. Forte**, S. Bhunia, "Sweep to the Secret: A Constant Propagation Attack on Logic Locking", *IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, December 2019.

C24. S. Chowdhury, F. Ganji, T. Bryant, N. Maghari, **D. Forte**, "Recycled Analog and Mixed Signal Chip Detection at Zero Cost Using LDO Degradation", *IEEE International Test Conference (ITC)*, November 2019.

C25. R. Wilson, RY Acharya, **D. Forte**, N. Asadizanjani, D. Woodard, "A Novel Approach to Unsupervised Automated Extraction of Standard Cell Library for Reverse Engineering and Hardware Assurance", *International Symposium for Testing and Failure Analysis (ISTFA)*, November 2019.

C26. S. Shomaji, F. Ganji, D. Woodard, **D. Forte**, "Hierarchical Bloom Filter Framework for Security, Space-efficiency, and Rapid Query Handling in Biometric Systems", *IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, September 2019.

C27. M. Alam, S. Tajik, F. Ganji, M. Tehranipoor, **D. Forte**, "RAM-Jam: Remote Temperature and Voltage Fault Attack on FPGAs using Memory Collisions", *Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, August 2019.

C28. F. Ganji, S. Tajik, P. Stauss, JP Seifert, **D. Forte**, M. Tehranipoor, "Approaches for Hardness Amplification of PUFs", *International Workshop on Security Proofs for Embedded Systems (PROOFS)*, August 2019.

C29. P. Ghosh, F. Ganji, **D. Forte**, D. Woodard, RS Chakraborty"Automated Framework for Unsupervised Counterfeit Integrated Circuit Detection by Physical Inspection", *International Conference on Physical Assurance and Inspection of Electronics (PAINE)*, July 2019.

C30. S. Chowdhury, H. Shen, B. Park, N. Maghari, **D.Forte**, "Aging Analysis of Low Dropout Regulator for Universal Recycled IC Detection", *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, July 2019.

C31. A. Gorbenko, N. Noor, S. Muneer, R. Khan, F. Dirisaglik, A. Cywar, B. Shakya, **D. Forte**, M. van Dijk, A. Gokirmak, H. Silva, "Resistance Drift and Crystallization in Suspended and On-Oxide Phase Change Memory Line Cells", *IEEE International Conference on Nanotechnology (IEEE-NANO)*, July 2019.

C32. B. Park, M. Tehranipoor, **D. Forte**, N. Maghari, "A Metal-Via Resistance Based Physically Unclonable Function with 1.18% Native Instability", *IEEE Custom Integrated Circuits Conference (CICC)*, April 2019.

C33. A. Alaql, T. Hoque, **D. Forte**, S. Bhunia, "Quality Obfuscation for Reliable and Adaptive Hardware IP Protection", *IEEE VLSI Test Symposium (VTS)*, April 2019.

C34. Q. Shi, H. Wang, N. Asadizanjani, M. Tehranipoor, **D. Forte**, "A Comprehensive Analysis on Vulnerability of Active Shields to Tilted Microprobing Attacks", *IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, December 2018.

C35. A. Stern, U.J. Botero, B. Shakya, H. Shen, **D. Forte**, M. Tehranipoor, "EMFORCED: EM-based Fingerprinting Framework for Counterfeit Detection with Demonstration on Remarked ICs", *IEEE International Test Conference (ITC)*, October-November 2018.

C36. H. Shen, N. Asadizanjanizanjani, M. Tehranipoor, **D. Forte**, "Nanopyramid: An Optical Scrambler Against Backside Probing Attacks", *International Symposium for Testing and Failure Analysis (ISTFA)*, October 2018.

C37. P. Ghosh, **D. Forte**, D. Woodard, R.S. Chakraborty, "Automated Detection of Pin Defects on Counterfeit Microelectronics", *International Symposium for Testing and Failure Analysis (ISTFA)*, October 2018.

C38. J. Park, X. Xu, Y. Jin, **D. Forte**, M. Tehranipoor, "Power-based Side-Channel Instruction-level Disassembler", *Design Automation Conference (DAC)*, June 2018.

C39. S. Chowdhury, X. Xu, M. Tehranipoor, **D. Forte**, "Aging Resistant RO PUF with Increased Reliability in FPGA", *International Conference on Reconfigurable Computing and FPGAs (ReConFig)*, December 2017.

C40. E.L. Principe, N. Asadizanjanizanjani, **D. Forte**, M. Tehranipoor, R. Chivas, M. DiBattista, S. Silverman, M. Marsh, N. Piche, J. Mastovich, "Steps Toward Automated Deprocessing of Integrated Circuits," *International Symposium for Testing and Failure Analysis (ISTFA)*, November 2017. [**ISTFA 2017 Outstanding Paper Award**]

C41. A. Chhotaray, A. Nahiyan, T. Shrimpton, **D. Forte**, M. Tehranipoor, "Standardizing Bad Cryptographic Practice - A Teardown of the IEEE Standard for Protecting Electronic-Design Intellectual Property," *ACM Conference on Computer and Communications Security (CCS)*, November 2017.

C42. Z. Guo, X. Xu, M. Tehranipoor, **D. Forte**, "MPA: Model-assisted PCB Attestation via Board-level RO and Temperature Compensation", *IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, October 2017.

C43. K. Yang, U.J. Botero, H. Shen, **D. Forte**, M.Tehranipoor, "A Split Manufacturing Approach for Unclonable Chipless RFIDs for Pharmaceutical Supply Chain Security", *IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, October 2017.

C44. A. Nahiyan, M. Sadi, R. Vittal, G. Contreras, **D. Forte**, M.Tehranipoor, "Hardware Trojan Detection through Information Flow Security Verification," *IEEE International Test Conference (ITC)*, October 2017.

C45. N. Karimian, D. Woodard, **D. Forte**, "On the Vulnerability of ECG Verification to Online Presentation Attacks," *IEEE International Joint Conference on Biometrics (IJCB)*, October 2017. [**IJCB 2017 Best Student Paper Award**]

C46. X. Xu, B. Shakya, M. Tehranipoor, **D. Forte**, "Novel Bypass Attack and BDD-based Tradeoff Analysis Against all Known Logic Locking Attacks," *International Conference on Cryptographic Hardware and Embedded Systems (CHES)*, September 2017.

C47. Z. Guo, X. Xu, M. Tehranipoor, **D. Forte**, "FFD: A Framework for Fake Flash Detection", *Design Automation Conference (DAC)*, June 2017.

C48. Q. Shi, K. Xiao, **D. Forte**, M. Tehranipoor, "Securing Split Manufactured ICs with Wire Lifting Obfuscated Built-In Self-Authentication", *GLSVLSI*, May 2017.

C49. S. Amir, B. Shakya, **D. Forte**, M. Tehranipoor, S. Bhunia, "Comparative Analysis of Hardware Obfuscation for IP Protection", *GLSVLSI*, May 2017.

C50. T. Byrant, S. Chowdhury, **D. Forte**, M. Tehranipoor, N. Maghari, "A Stochastic All-Digital Weak Physically Unclonable Function for Analog/Mixed-Signal Applications", *Hardware-Oriented Security and Trust (HOST)*, May 2017

C51. N. Karimian, F. Tehranipoor, Z. Guo, M. Tehranipoor, **D. Forte**, "Noise Assessment Framework for Optimizing ECG Key Generation", *IEEE International Conference on Technologies for Homeland Security (HST)*, April 2017.

C52. N. Karimian, Z. Guo, M. Tehranipoor, **D. Forte**, "Human Recognition from Photoplethysmography (PPG) Based on Non-fiducial Features", *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, March 2017.

C53. N. Karimian, M. Tehranipoor, **D. Forte**, "Non-Fiducial PPG-based Authentication for Healthcare Application", *International Conference on Biomedical and Health Informatics (BHI)*, February 2017.

C54. 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)*, January 2017.

C55. Z. Guo, M. Tehranipoor, **D. Forte**, "Aging Attacks for Key Extraction on Permutation-Based Obfuscation," *IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, December 2016.

C56. T. Rahman, **D. Forte**, X. Wang, M. Tehranipoor, "Enhancing Noise Sensitivity of Embedded SRAMs for Robust True Random Number Generation in SoCs," *IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)*, December 2016.

C57. M. M. Alam, M. Tehranipoor, **D. Forte** "Recycled FPGA Detection Using Exclusive LUT Path Delay Characterization," *IEEE International Test Conference (ITC)*, November 2016.

C58. B. Shakya, N. Asadizanjani, **D. Forte**, M. Tehranipoor, "Chip Editor: Leveraging Circuit Edit for Logic Obfuscation and Trusted Fabrication," *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, November 2016.

C59. Z. Guo, B. Shakya, H. Shen, S. Bhunia, N. Asadizanjanizanjani, **D. Forte**, M. Tehranipoor, "A New Methodology to Protect PCBs from Non-destructive Reverse Engineering", *International Symposium for Testing and Failure Analysis (ISTFA)*, November 2016.

C60. N. Asadizanjanizanjani, **D. Forte**, M. Tehranipoor, "Non-destructive Bond Pull and Ball Shear Failure Analysis Based on Real Structural Properties" *International Symposium for Testing and Failure Analysis (ISTFA)*, November 2016.

C61. N. Asadizanjanizanjani, S. Gattigowda, N. Dunn, M. Tehranipoor, **D. Forte**, "A Database for Counterfeit Electronics and Automatic Defect Detection Based on Image Processing and Machine Learning," *International Symposium for Testing and Failure Analysis (ISTFA)*, November 2016.

C62. T. Bryant, S. Chowdhury, **D. Forte**, M. Tehranipoor, N. Maghari, "A Stochastic Approach to Analog Physical Unclonable Function," *IEEE Midwest Symposium on Circuits and Systems (MWSCAS)*, October 2016.

C63. N. Karimian, M. Tehranipoor, D. Woodard, **D. Forte**, "Biometrics for Authentication in Resource-Constrained Systems," *International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, August 2016.

C64. H. Shen, F. Rahman, B. Shakya, M. Tehranipoor, **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)*, July 2016.

C65. A. Nahiyan, K. Xiao, K. Yang, Y. Jin, **D. Forte**, M. Tehranipoor, "AVFSM: A Framework for Identifying and Mitigating Vulnerabilities in FSMs", *Design Automation Conference (DAC)*, June 2016.

C66. Z. Guo, N. Karimian, M. Tehranipoor, **D. Forte**, "Hardware Security Meets Biometrics for the Age of IoT", *IEEE International Symposium on Circuits and Systems (ISCAS)*, May 2016.

C67. T. Le, J. Di, M. Tehranipoor, **D. Forte**, L. Wang, "Tracking Data Flow at Gate-Level through Structural Checking", *GLSVLSI*, May 2016.

C68. Q. Shi, N. Asadizanjanizanjani, **D. Forte**, M.Tehranipoor, "A Layout-driven Framework to Assess Vulnerability of ICs to Microprobing Attacks", *Hardware-Oriented Security and Trust (HOST)*, May 2016. [**HOST 2016 Best Paper Award**]

C69. Z. Guo, M. T. Rahman, M. Tehranipoor, **D. Forte**, "A Zero-cost Approach to Detect Recycled SoCs Using Embedded SRAM", *Hardware-Oriented Security and Trust (HOST)*, May 2016.

C70. K. Yang, **D. Forte**, M. Tehranipoor, "UCR: Unclonable Chipless RFID Tag", *Hardware-Oriented Security and Trust (HOST)*, May 2016. [**HOST 2016 Best Paper Nomination**]

C71. 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)*, April 2016

C72. B. Shakya, F. Rahman, M. Tehranipoor, **D. Forte**, "Harnessing Nanoscale Device Properties for Hardware Security", *Microprocessor Test and Verification (MTV)*, December 2015.

C73. K. Yang, **D. Forte**, and M. Tehranipoor, "Protecting Endpoint Devices in IoT Supply Chain", *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, November 2015.

C74. H. Dogan, M. Alam, N. Asadizanjanizanjani, S. Shahbazmohamadi, **D. Forte**, and M. Tehranipoor, "Analyzing the Impact of X-ray Tomography for Non-destructive Counterfeit Detection", *International Symposium for Testing and Failure Analysis (ISTFA)*, November 2015.

C75. N. Asadizanjanizanjani, S. Shahbazmohamadi, M. Tehranipoor, **D. Forte** "Non-destructive PCB Reverse Engineering Using X-ray Micro Computed Tomography", *International Symposium for Testing and Failure Analysis (ISTFA)*, November 2015.

C76. B. Shakya, U. Guin, M. Tehranipoor, **D. Forte**, "Performance Optimization for On-Chip Sensors to Detect Recycled ICs," *IEEE International Conference on Computer Design (ICCD)*, October 2015.

C77. M. T. Rahman, **D. Forte**, F. Rahman, M. Tehranipoor, "A Pair Selection Algorithm for Robust RO-PUF Against Environmental Variations and Aging," *IEEE International Conference on Computer Design (ICCD)*, October 2015.

C78. S. Chen, J. Chen, **D. Forte**, J. Di, M. Tehranipoor, L. Wang, "Chip-level Anti-reverse Engineering using Transformable Interconnects," *IEEE Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, October 2015.

C79. K. Yang, **D. Forte**, M.Tehranipoor, "ReSC: RFID-enabled Supply Chain Management and Traceability for Network Devices," *11th Workshop on RFID Security (RFIDSec 2015)*, June 2015.

C80. Z. Guo, J. Di, M. Tehranipoor, **D. Forte**, "Investigation of Obfuscation-based Anti-Reverse Engineering for Printed Circuit Boards," *Design Automation Conference (DAC) 2015*, June 2015.

C81. K. Xiao, **D. Forte**, M. Tehranipoor, "Efficient and Secure Split Manufacturing via Obfuscated Built-In Self-Authentication," *Hardware-Oriented Security and Trust (HOST) 2015*, May 2015. [**HOST 2015 Best Paper Award**]

C82. N. Karimian, F. Tehranipoor, M.T. Rahman, **D. Forte**, "Genetic Algorithm for Hardware Trojan Detection with Ring Oscillator Network (RON)" *IEEE International Conference on Technologies for Homeland Security (HST)*, April 2015.

C83. K. Yang, **D. Forte**, M. Tehranipoor, "An RFID-based Technology for Electronic Component and System Counterfeit Detection and Traceability" *IEEE International Conference on Technologies for Homeland Security (HST)*, April 2015.

C84. A. Hosey, M.T. Rahman, K. Xiao, **D. Forte**, M. Tehranipoor, "Advanced Analysis of Cell Stability for Reliable SRAM PUF," *IEEE Asian Test Symposium (ATS)*, November 2014.

C85. S. Shahbazmohamadi, **D. Forte**, M. Tehranipoor, "Advanced Physical Inspection Methods for Counterfeit Detection", *International Symposium for Testing and Failure Analysis (ISTFA)*, November 2014.

C86. M.T. Rahman, **D. Forte**, Q. Shi, G. Contreras, M. Tehranipoor, "CSST: Preventing Distribution of Unlicensed and Rejected ICs by Untrusted Foundry and Assembly," *IEEE Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, October 2014.

C87. H. Dogan, **D. Forte**, M. Tehranipoor, "Aging Analysis for Recycled FPGA Detection," *IEEE Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, October 2014.

C88. U. Guin, X. Zhang, **D. Forte**, M. Tehranipoor, "Low-cost On-Chip Structures for Combating Die and IC Recycling," *Design Automation Conference (DAC)*, June 2014.

C89. M.T. Rahman, K. Xiao, X. Zhang, **D. Forte**, Z. Shi, M. Tehranipoor, "TI-TRNG: Technology Independent True Random Number Generator," *Design Automation Conference (DAC)*, June 2014.

C90. M.T. Rahman, **D. Forte**, Q. Shi, G. Contreras, M. Tehranipoor, "CSST: An Efficient Secure Split-Test for Preventing IC Piracy," *IEEE North Atlantic Test Workshop (NATW)*, May 2014

C91. K. Xiao, M.T. Rahman, **D. Forte**, M. Su, Y. Huang, M.Tehranipoor, "Bit Selection Algorithm Suitable for High-Volume Production of SRAM-PUF," *Hardware-Oriented Security and Trust (HOST)*, May 2014.

C92. C. Bao, **D. Forte**, A. Srivastava, "On Application of One-class SVM to Reverse Engineering-Based Hardware Trojan Detection", in *International Symposium on Quality Electronic Design (ISQED)*, March 2014.

C93. M.T. Rahman, **D. Forte**, J. Fahrny, M. Tehranipoor, "ARO-PUF: An Aging-Resistant Ring Oscillator PUF Design", *Design, Automation, and Test in Europe (DATE)*, March 2014.

C94. U. Guin, **D. Forte**, M. Tehranipoor, "Anti-Counterfeit Techniques: From Design to Resign", *Microprocessor Test and Verification (MTV)*, December 2013.

C95. **D. Forte**, C. Bao, A. Srivastava, "Temperature Tracking: An Innovative Run-Time Approach for Hardware Trojan Detection", *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, November 2013.

C96. **D. Forte** and A. Srivastava, "Manipulating Manufacturing Variations for Better Silicon-Based Physically Unclonable Functions", *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, August 2012.

C97. **D. Forte** and A. Srivastava, "On Improving the Uniqueness of Silicon-Based Physically Unclonable Functions Via Optical Proximity Correction", *Design Automation Conference (DAC)*, June 2012. **[DAC-2012 Best Paper Nomination]**

C98. **D. Forte** and A. Srivastava, "Adaptable Architectures for Distributed Visual Target Tracking", *IEEE International Conference on Computer Design (ICCD)*, October 2011.

C99. **D. Forte** and A. Srivastava, "Energy-Aware and Quality-Scalable Data Placement and Retrieval for Disks in Video Server Environments", *IEEE International Conference on Computer Design (ICCD)*, October 2011.

C100. **D. Forte** and A. Srivastava, "Energy-aware video storage and retrieval in server environments," *International Green Computing Conference and Workshops (IGCC)*, July 2011.

C101. **D. Forte** and A. Srivastava, "Resource-aware architectures for particle filter based visual target tracking," *International Green Computing Conference and Workshops (IGCC)*, July 2011.

C102. **D. Forte** and A. Srivastava, "Adaptable video compression and transmission using lossy and workload balancing techniques", *NASA/ESA Conference on Adaptive Hardware and Systems (AHS)*, June 2011. **[Awarded AHS-2011 Best Student Paper]**

C103. **D. Forte** and A. Srivastava, "Energy-aware video coding of multiple views via workload balancing", *NASA/ESA Conference on Adaptive Hardware and Systems (AHS)*, June 2011.

C104. **D. Forte** and A. Srivastava, "Energy and Thermal-Aware Video Coding via Encoder/Decoder Workload Balancing", *International Symposium on Low Power Electronics and Design (ISLPED)*, August 2010.

C105. **D. Forte** and A. Srivastava, "Thermal-Aware Sensor Scheduling for Distributed Estimation", *International Conference on Distributed Computing in Sensor Systems (DCOSS)*, June 2010.

Non-Refereed Conference and Journal Papers

NR1. S. Roy, M. Hashemi, F. Ganji, **D. Forte**, "Active IC Metering Protocol Security Revisited and Enhanced with Oblivious Transfer", to appear *SRC TECHCON*, September 2022.

NR2. J. Schubeck, D. Koblah, U. Botero, **D. Forte**, "A Comprehensive Taxonomy of PCB Defects", in *GOMACTech*, March 2022.

NR3. J. Bellay, **D. Forte**, R. Martin, C. Taylor, "Hardware Vulnerability Description, Sharing and Reporting: Challenges and Opportunities", in *GOMACTech*, March 2021.

NR4. DS Koblah, UJ Botero, F. Ganji, D. Woodard, **D. Forte**, "Via Modeling on X-Ray Images of Printed Circuit Boards Through Deep Learning", in *GOMACTech*, March 2021.

NR5. A. Covic, F. Ganji, **D. Forte**, "Circuit Masking Schemes: New Hope for Backside Probing Countermeasures?", in *SRC TECHCON*, September 2020.

NR6. M. Gao, H. Wang, M. Tehranipoor, **D. Forte**, "iPROBE V2: Internal Shielding-based Countermeasures against Both Back-side and Front-side Probing Attacks", in *SRC TECHCON*, September 2020.

NR7. U.J. Botero, N. Asadizanjani, D. Woodard, **D. Forte**, "A Framework for Automated Alignment & Layer Identification of X-Ray Tomography Imaged PCBs", in *GOMACTech*, March 2020.

NR8. **D. Forte**, S. Bhunia, R. Karri, J. Plusquellic, M. Tehranipoor, "IEEE International Symposium on Hardware Oriented Security and Trust (HOST): Past, Present, and Future", *IEEE International Test Conference (ITC)*, November 2019.

NR9. R. Wilson, N. Asadizanjani, **D. Forte**, D. Woodard, "First Auto-Magnifier Platform for Hardware Assurance and Reverse Engineering Integrated Circuits ", *Microscopy & Microanalysis (M&M)*, August 2019.

NR10. F. Ganji, **D. Forte**, N. Asadizanjanizanjani, M. Tehranipoor, D. Woodard, "The Power of IC Reverse Engineering for Hardware Trust and Assurance", *Electronic Device Failure Analysis (EDFA)*, May 2019.

NR11. F. Ganji, N. Karimian, D. Woodard, **D. Forte**, "Leave Adversaries in the Dark- BLOcKeR: Secure and Reliable Biometric Access Control", *The Journal of the Homeland Defense and Security Information Analysis Center (HDIAC)*, Vol. 6, No. 1, Spring 2019.

NR12. A. Stern, K. Yang, J. Vosatka, A. Duncan, J. Park, **D. Forte**, M. Tehranipoor, "RASC: Enabling Remote Access to Side-Channels for Mission Critical Systems", in *GOMACTech*, March 2019.

NR13. H. Wang, Q. Shi, N. Asadizanjani, **D. Forte**, M. Tehranipoor, "A Physical Design Flow against Front-side Probing Attacks by Internal Shielding", in *SRC TECHCON*, September 2018.

NR14. E.L. Principe, N. Asadizanjani, **D. Forte**, M. Tehranipoor, M. DiBattista, R. Chivas, S. Silverman, N. Piche, M. Marsh, J. Mastovich, "Steps Toward Computational Guided Deprocessing of Integrated Circuits" in *GOMACTech*, March 2018.

NR15. D. Capecci, G. Contreras, **D. Forte**, M.Tehranipoor, S. Bhunia, "Automated SoC Security from Design to Fabrication" in *GOMACTech*, March 2018.

NR16. S. Baireddy, U.J. Botero, N. Asadizanjani, M.Tehranipoor, D. Woodard, **D. Forte**, "Automated Detection of Counterfeit IC Defects Using Image Processing" in *GOMACTech*, March 2018.

NR17. U.J. Botero, M.Tehranipoor, **D. Forte**, "Downgrade: A Framework for Obsolescence Handling through Backwards Compatibility" in *GOMACTech*, March 2018.

NR18. E.L. Principe, N. Asadizanjani, **D. Forte**, M. Tehranipoor, R. Chivas, M. DiBattista, S. Silverman, "Plasma FIB Deprocessing of Integrated Circuits from the Backside", *Electronic Device Failure Analysis (EDFA)*, Vol. 19, No. 4, November 2017.

NR19. Z. Guo, M. Tehranipoor, **D. Forte**, "Memory-based Counterfeit IC Detection Framework", in *SRC TECHCON*, September 2017.

NR20. Q. Shi, N. Asadizanjanizanjani, **D. Forte**, M.Tehranipoor, "Layout-based Microprobing Vulnerability Assessment for Security Critical Applications," in *GOMACTech*, March 2017.

NR21. M. T. Rahman, **D. Forte**, and M. Tehranipoor, "SRAM Inspired Design and Optimization for Developing Robust Security Primitives," in *SRC TECHCON*, September 2016. [**Awarded Best in Session**]

NR22. M. M. Alam, N. Asadizanjanizanjani, M.Tehranipoor, **D. Forte**, "The Impact of X-ray Tomography on the Reliability of FPGAs " in *GOMACTech*, March 2016.

NR23. Z. Guo, N. Karimian, M. Tehranipoor, **D. Forte**, "Biometric Based Human-to-Device (H2D) Authentication", in *GOMACTech*, March 2016.

NR24. N. Asadizanjanizanjani, S. Shahbazmohamadi, **D. Forte**, M. Tehranipoor, "Nondestructive X-ray Tomography Based Bond Pull and Ball Shear Analysis" in *GOMACTech*, March 2016.

NR25. M. T. Rahman, **D. Forte**, and M. Tehranipoor, "Robust SRAM-PUF: Cell Stability Analysis and Novel Bit-Selection Algorithm," in *SRC TECHCON*, September 2015.

NR26. M.T. Rahman, A. Hosey, F. Rahman, **D. Forte**, M. Tehranipoor, "RePa: A Pair Selection Algorithm for Reliable Keys from RO-based PUF" in *GOMACTech*, March 2015.

NR27. H. Dogan, **D. Forte**, M. Tehranipoor, "Aging Analysis for Recycled FPGA Detection" in *GOMACTech*, March 2015.

NR28. N. Asadizanjanizanjani, S. E. Quadir, S. Shahbazmohamadi, M. Tehranipoor, **D. Forte**, "Rapid Nondestructive Reverse Engineering of Printed Circuit Boards by High Resolution X-ray Tomography" in *GOMACTech*, March 2015.

NR29. U. Guin, **D. Forte**, M. Tehranipoor, "Low-cost On-Chip Structures for Combatting Die and IC Recycling," in *GOMACTech*, March 2014.

NR30. K. Xiao, M.T. Rahman, **D. Forte**, M. Tehranipoor, "Low-cost Analysis for Identification of Mass-Produced Electronic Devices," in *GOMACTech*, March 2014.

NR31. U. Guin, **D. Forte**, D. DiMase, M. Tehranipoor, "Counterfeit IC Detection: Test Method Selection Considering Test Time, Cost, and Tier Level Risks," in *GOMACTech*, March 2014.

PATENTS

Pt1. M. Tehranipoor, A. Nahiyan, **D. Forte**. *Hardware Trojan Detection Through Information Flow Security Verification*, granted on March 8, 2022.

Pt2. D. Woodard, R. Wilson, N. Asadizanjani, **D. Forte**. *Histogram-based Auto Segmentation: A Novel Approach to Segmenting Integrated Circuit Structures from SEM Images*, granted on March 8, 2022.

Pt3. M. Tehranipoor, **D. Forte**, F. Farahmandi, A. Nahiyan, F. Rahman, MS Rahman. *Protecting Obfuscated Circuits Against Attacks That Utilize Test Infrastructures*, granted on January 11, 2022.

Pt4. D. Woodard, R. Wilson, N. Asadizanjani, **D. Forte**. *Method and Apparatus for Automatic Extraction of Standard Cells to Generate a Standard Cell Candidate Library*, granted on October 26, 2021.

Pt5. M. Tehranipoor, H. Wang, Q. Shi, H. Shen, **D. Forte**. *Prevention of Front-side Probing Attacks*, granted on August 10, 2021.

Pt6. B. Shakya, H. Shen, M. Tehranipoor, **D. Forte**. *Covert Gates To Protect Gate-Level Semiconductors*, granted on July 6, 2021.

Pt7. M. Tehranipoor, **D. Forte**, B. Shakya, N. Asadizanjanizanjani, *Circuit Edit and Obfuscation for Trusted Chip Fabrication*, granted on June 8, 2021.

Pt8. **D. Forte**, S. Chowdhury, F. Ganji, N. Maghari. *Detection Of Recycled Integrated Circuits And System-On-Chips Based On Degradation Of Power Supply Rejection Ratio*, published on March 18, 2021.

Pt9. M. Tehranipoor, K. Yang, H. Shen, U. Botero, **D. Forte**. *Cross-Registration For Unclonable Chipless RFID Tags*, granted on February 23, 2021.

Pt10. M. Tehranipoor, A. Nahiyan, J. Park, **D. Forte**. *CAD Framework for Power Side-channel Vulnerability Assessment*, published on January 28, 2021.

Pt11. **D. Forte**, H. Shen, N. Asadizanjani, M. Tehranipoor. *Nanopyramid: An Optical Scrambler Against Probing Attacks*, published on August 6, 2020.

Pt12. M. Tehranipoor, **D. Forte**, N. Asadizanjanizanjani, Q. Shi, *Layout-Driven Method to Assess Vulnerability of ICs To Microprobing Attacks*, granted on February 25, 2020.

Pt13. M. Tehranipoor, U. Guin, **D. Forte**, *A Comprehensive Framework for Protecting Intellectual Property in Semiconductor Industry*, published on May 30, 2019

Pt14. S. Bhunia, H. Shen, M. Tehranipoor, **D. Forte**, N. Asadizanjanizanjani, *Vanishing Via for Hardware IP Protection from Reverse Engineering*, granted on May 7 2019.

Pt15. M. Tehranipoor, H. Shen, K. Yang, **D. Forte**, *Unclonable Environmentally-sensitive Chipless RFID Tag with a Plurality of Slot Resonators*, granted on January 15, 2019.

## Project Sponsors and Grants

**Total: $48,341,850; Total Share: $8,478,530; Total as PI: $5,709,032**

CG1. *AFRL*: "MEST Phase 2," Co-PI, 07/19/21 - 07/19/25

CG2. *NSF*: "Collaborative: SaTC: CORE: Small: ERADICATOR: Techniques for Laser Assisted Side-Channel Attack Monitor and Response," Co-PI, 06/15/22 - 05/31/25

CG3. *NSF*: "SaTC: TTP: Medium: I-C-U: AI-Enabled Recovery and Assurance of Semiconductor IP from SEM Images," Co-PI, 04/07/22 - 03/31/25

CG4. *AFOSR*: "CYAN: Enabling Cyber Defense in Analog and Mixed Signal Domain," Co-PI, 08/16/2022 - 05/14/2024

CG5. *DARPA*: "ABIL - Automatic Implementation of Secure Silicon (AISS) by Industry Leaders," Co-PI, 05/01/2020 -04/30/2024

CG6. *SRC*: "IP Protection through Secure and Private Function Evaluation," PI, 10/1/2020 -09/30/2023

CG7. *NSF*: "CCRI: ENS: Enhancement of Trust-Hub, a Web-based Portal to support the Cybersecurity Research Community," Co-PI, 07/15/2020 - 06/30/2023

CG8. *ONR*: "On-Chip Intelligent Sensor based Real-Time Analog Trojan Detection Framework for Microprocessor Trustworthiness," PI, 05/15/2019 - 05/14/2023

CG9. *NSF*: "CAREER: Transformative Approaches for Hardware Obfuscation Protection, Attacks, and Assessment," PI, 06/01/17 - 05/31/23

CG10. *ARO*: "SWIFT: A Signature-enabled Wireless Infrastructure for Forensics, Tracking, and Locking of Electronic Systems," PI, 02/01/2019 - 04/30/2023

CG11. *AFRL*: "Trusted Silicon Stratus (TSS) Vulnerability Risk Assessment & Mitigation (V-RAM)," Co-PI, 03/04/2020 - 03/04/2023

CG12. *AFRL*: "STAMP: A Holistic Backward/Forward Trust Framework for Protecting Microelectronics Throughout Lifecycle," Co-PI, 09/14/2020 - 12/18/2023

CG13. *AFOSR*: "Development of Universal Security Theory for Evaluation and Design of Nanoscale Devices," Co-PI, 07/01/14 - 12/31/2022

CG14. *Intel*: "Security-Aware FSM Design Flow for Identifying and Mitigating Fault Attacks," PI, 12/03/2019 - 10/31/2022

CG15. *AFRL*: "Hardware Vulnerability Ontology and Database for the Trusted Silicon Stratus," PI, 07/23/2020 - 08/24/2022

CG16. *NSF*: "SaTC: STARSS: Small: iPROBE: - An Internal Shielding Approach for Protecting against Frontside and Backside Probing Attacks," PI, 08/15/17 - 7/31/2022

CG17. *NSF*: "SaTC: EDU: PHIKS - PHysical Inspection and attacKs on electronicS," Co-PI, 06/01/18 - 07/31/2022

CG18. *US AMC*: "Protection for Critical Technology: Pre-Silicon Security Verification and Backside Protection Schemes for Microelectronic Devices," Co-PI, 12/13/2019 - 08/01/2022

CG19. *AFRL*: "STV Phase 3 - Trust and Assurance of Microelectronics (TAME)," Co-PI, 05/15/2020 - 05/31/2022

CG20. *AFRL*: "AutoBoM Phase 2 - Trust and Assurance of Microelectronics (TAME)," Co-PI, 05/15/2020 - 05/31/2022

CG21. *DARPA*: "Hardware IP Protection through Provably Secure State-Space Obfuscation," Co-PI, 02/21/18 - 03/08/2022

CG22. *DARPA*: "ARCHS: Automated Rule Checking for Hardware Security," Co-PI, 03/03/2020 - 12/31/2021

CG23. *DoE*: "Model Based PCB Attestation," PI, 02/17/2021 - 08/31/2021

CG24. *FL DOE*: "Embry-Riddle - Center for Aerospace Resilience," Co-PI, 11/20/2020 - 07/31/2021

CG25. *NSF*: "NSF Student Travel Grant for 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)," PI, 12/15/2019 - 03/31/2021

CG26. *NSF*: "SaTC: STARSS: Design of Low-Cost Memory-Based Security Primitives and Techniques for High-Volume Products," Co-PI, 10/01/14 - 09/30/20

CG27. *SRC*: "SaTC: STARSS: Small: iPROBE: - An Internal Shielding Approach for Protecting against Frontside and Backside Probing Attacks," PI, 08/15/17 - 09/03/20

CG28. *Air Force*: "2D/3D Data Collection of PCB Surface Mount Components for Automated Bill of Material Generation," Co-PI, 07/01/2019 - 08/15/2020

CG29. *ARO*: "Human-to-Device (H2D): A Novel Anti-tampering Mechanism for DOD Applications Driven by Cardiovascular Biometric and Obfuscation," PI, 04/01/16 - 07/15/2020

CG30. *Cisco*: "BRAND: A Basic Framework for PCB Reverse Engineering, Analysis, and Defect Diagnosis," Co-PI, 05/08/2018 - 06/07/2020

CG31. *NSF*: "Combating Counterfeit Analog and Mixed Signal ICs with Lightweight Embedded Mechanisms and Innovative Electrical Tests ," PI, 06/01/16 - 05/31/2020

CG32. *Honeywell*: "Test Vehicle Design for HT Detection Validation," Co-PI, 06/09/17 - 02/01/20

CG33. *NIST*: "Utilizing NIST Entropy as a Service and Chaotic Circuits for Management of Electronics Supply Chain," PI, 09/01/16 - 12/31/2019

CG34. *Cisco*: "FORTISv2.0: Establishing Forward Trust for Protecting IPs and ICs in Todays Complex Supply Chain," PI, 07/06/17 - 08/05/19

CG35. *Cisco*: "An Integrative Approach to Secure IC Design through Obfuscation and Authentication," Co-PI, 01/01/16 - 06/30/19

CG36. *NSF*: "CI-EN: Trust-Hub: Development of Benchmarks, Metrics, and Validation Platforms for Hardware Security, and a Web-based Dissemination Portal," Co-PI, 05/01/15 - 06/30/19

CG37. *SRC*: "Framework for Automated and Systematic Security Assessment of Modern SoCs," Co-PI, 12/01/16 - 11/30/18

CG38. *Cisco*: "FORTIS: Establishing Forward Trust for Protecting IPs and ICs in Todays Complex Supply Chain," PI, 04/06/16 - 09/30/18

CG39. *SRC*: "SaTC: STARSS: Design of Low-Cost Memory-Based Security Primitives and Techniques for High-Volume Products," Co-PI, 10/01/14 - 01/31/18

CG40. *NSF*: "SHF:Small:GOALI: Advanced Physical Inspection of Counterfeit Integrated Circuits," PI, 08/01/14 - 07/31/17

CG41. *SRC*: "Security Rule Check: A Comprehensive Framework for Evaluating Security of Integrated Circuits," Co-PI, 01/01/15 - 12/31/16

CG42. *ARO*: "STIR: Scientific Exploration of Cyber-Driven Dynamic, Distributed Big Data Forensics Systems," Co-PI, 04/01/16 - 12/31/16

CG43. *Comcast*: "Novel Innovative RFID-enabled Supply Chain Management and Traceability for Comcast Products," Co-PI, 01/01/15 - 12/31/15

CG44. *Comcast*: "Novel Set-top Box Personalization and Content Restriction Enabled by User Photoplethysmosgraph (PPG)," PI, 01/01/15 - 12/31/15

CG45. *MDA*: "CDC: Counterfeit Defect Characterization of Recycled Electronic Components," Co-PI, 01/01/14 - 12/31/15

CG46. *Honeywell*: "CPD: Counterfeit Parts Defect Characterization," PI, 01/01/14 - 12/31/15

CG47. *Synokey*: "Design of Robust SRAM PUF," Co-PI, 06/01/13 - 05/31/14

Equipment Acquisition Grants

**Total: $2,530,422; Total Share: N/A; Total as PI: N/A**

EG1. *NSF*: "MRI:Acquisition of a High Resolution Photon Emission/Electro-Optical Microscope," Co-PI, 10/01/17 - 09/30/20

EG2. *ONR (DURIP)*: "Nano-probing Integrated Circuits for Physical Attacks and Hardware Security Assessment," Co-PI, 07/16/18 - 07/15/19

EG3. *ARO (DURIP)*: "Security Validation of Integrated Circuits by Detailed Parameter Analysis Using Probe Station," Co-PI, 04/27/17 - 04/26/18

EG4. *AFOSR (DURIP)*: "Precise Nano-Fabrication and Advanced Circuit Edit Using Helium Ion Beam for Hardware Security and Trust," Co-PI, 09/15/16 - 09/14/17

Equipment Acquisition Gifts

**Total: $2,454,230; Total Share: N/A; Total as PI: N/A**

G1. *Tektronix*: Suite of Oscilloscopes, Logic Analyzers, Function/Waveform Generators, Spectrum/Power Analyzers, Power Supplies, and Digital Multimeters

G2. *TESCAN*: FERA-3 GMH Xe-Plasma FIB with Integrated Schottky FESEM, LYRA-3 XMH Ga LIMIS FIB with Integrated Schottky FESEM, SKYSCAN 2211 MultiScale X-ray Nano-CT System

## Advisees

*Past Post-doctoral Fellows and Research Scientists [Title and Current Affiliation]*[1]

Navid Asadizanjani$^{\star}$ [Assistant Professor, University of Florida], Xiaolin Xu$^{\star}$ [Assistant Professor, Northeastern University], Jungmin Park$^{\star\dagger}$ [Research Assistant Professor, University of Florida], Qihang Shi$^{\star}$ [Post Doc, Tsinghua University] Haoting Shen$^{\star}$ [Assistant Professor, University of Nevada at Reno], Fatemah Ganji [Assistant Professor, Worcester Polytechnic Institute], Shahin Tajik$^{\star}$ [Assistant Professor, Worcester Polytechnic Institute], Farhaan Fowze [Nvidia]

*Current PhD*

Rabin Acharya, David Koblah, Pallabi Ghosh, Yunkai Bai, Minyan Gao, Tasnuva Farheen, Jiaming Wu, Steffi Roy, Sourav Roy

*Past PhD [Current Affiliation]*

*University of Florida:* Zimu Guo [Micron Technology], Bicky Shakya [Qualcomm], Mahbub Alam [Intel], Sreeja Chowdhury [Ansys], Sumaiya (Joyti) Shomaji [Assistant Professor, University of Kansas], Ulbert (Joey) Botero [MIT Lincoln Laboratory], Sarah Amir [Qualcomm], Muhtadi (Zaki) Choudhury [TBD]
*University of Connecticut:* Nima Karimian [Assistant Professor, West Virginia University]

*Current MS*

Ryan Holzhausen

*Past MS*

*University of Florida:* Ana Covic, Yunkai Bai, Bicky Shakya, Rahul Vittal, Janani Prakash, Tirth Atul Ray
*University of Connecticut:* Nima Karimianbahnemiri

*Current Undergrad*

JinHong Chen, Luis de la Mata, Alyssa Caples, Jeffrey Douglas Earle Shim-Francis, Edward Zhang, Gabriel Hernandez

*Past Visting MS (Institution)*

Pallabi Ghosh (IIT Kharagpur)

*Past Undergrad*

Kevin Ferreira, Giovanni Ferioli, Joshua Ryals, Bryce Herrera, Justin Schubeck, Nicholas Sileo, Michael Levin, Carl Simpron, Christopher Kelton, Benjamin Goldstein, Abby Pham, Gerard Avecilla, Brandon Wand, Spencer Dupee, James Mashburn, David Koblah, Sriram Baireddy, Jackson Carroll, Julia Merino-Calleja, Andrew Stern, Nathan Dunn$^{\star}$, Somtochukwu Okwuosah, Alison Hosey, Jacquelyn Khadijah-Hajdu$^{\star}$, Wesley Stevens$^{\star}$, Ryan Nesbit$^{\star}$, Dan Guerrera$^{\star}$, Shane Tobey$^{\star}$, Kasim Ward$^{\star}$, Carl DiFrederico$^{\star}$, Anthony Schend$^{\star}$, Michael Vetri$^{\star}$, Tyler Rich$^{\star}$

## Professional Activities

*Editorial Activities*

Associate Editor, Journal of Cryptographic Engineering (JCEN), 2021–present
Associate Editor, ACM Journal on Emerging Technologies in Computing (JETC), 2020–present
Associate Editor, Springer Journal of Hardware and System Security (HaSS), 2016–present
Guest Editor, ACM Journal on Emerging Technologies in Computing (JETC) Special Issue on "Emerging Challenges and Solutions in Hardware Security", 2020
Guest Editor, Springer Journal of Hardware and System Security (HaSS) Special Issue on "Hardware Reverse Engineering and Obfuscation", 2018
Guest Editor, IEEE Computer Special Issue on "Supply Chain Security for Cyber-Infrastructure", 2016

*Conference Organizing Committee and Track Chair*

[1] Note: $\star$ and $\dagger$ indicate co-advised by Mark Tehranipoor and Swarup Bhunia respectively

Steering Committee Member, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2020–present
Co-Program Chair, Workshop on Attacks and Solutions in Hardware Security (ASHES), 2022
Registration Chair, IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2021
Publicity and Industry Liaison Chair, Workshop on Attacks and Solutions in Hardware Security (ASHES), 2021
Track Chair, IFIP/IEEE International Conference on Very large Scale Integration (VLSI-SoC), 2021
General Chair, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2020
Publicity Chair, Workshop on Attacks and Solutions in Hardware Security (ASHES), 2020
Program Chair, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2019
Publicity Chair, IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2019
Publicity Chair, Workshop on Attacks and Solutions in Hardware Security (ASHES), 2019
Vice Program Chair, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2018
Reverse Engineering Track Chair, International Symposium for Testing and Failure Analysis (ISTFA), 2018
Publicity Chair, Workshop on Attacks and Solutions in Hardware Security (ASHES), 2018
Publicity Chair, IEEE Asian Hardware-Oriented Security and Trust Symposium (AsianHOST), 2016–2018
Program Co-Chair, International Verification and Security Workshop (IVSW), 2017
Tutorial Chair, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2017
Poster Chair, FICS Research Annual Conference on Cybersecurity, 2017
Reverse Engineering Track Chair, International Symposium for Testing and Failure Analysis (ISTFA), 2016
Publicity Chair, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2015, 2016
Hardware Security Challenge Co-Chair, CSI Cybersecurity, Education & Diversity Challenge Week (CyberSEED), 2014

*Program Committee (PC) and Review Boards*

*2023:* Hardwear.io USA, USENIX Security Symposium

*2022:* ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED), Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Great Lakes Symposium on VLSI (GLSVLSI), Hardwear.io USA, Hardwear.io NL, International Conference on Security, Privacy and Applied Cryptographic Engineering (SPACE), International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), USENIX Security Symposium, Workshop on Attacks and Solutions in Hardware Security (ASHES)

*2021:* Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Great Lakes Symposium on VLSI (GLSVLSI), IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), International Conference on Security, Privacy and Applied Cryptographic Engineering (SPACE), International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), Smart Card Research and Advanced Application Conference (CARDIS)

*2020:* Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Great Lakes Symposium on VLSI (GLSVLSI), IEEE International Conference on Physical Attacks and Inspection on Electronics (PAINE), International Conference on Security, Privacy and Applied Cryptographic Engineering (SPACE), International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), Smart Card Research and Advanced Application Conference (CARDIS), Workshop on Attacks and Solutions in Hardware Security (ASHES)

*2019:* Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Great Lakes Symposium on VLSI (GLSVLSI), IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Interna-

tional Conference on Physical Attacks and Inspection on Electronics (PAINE), Smart Card Research and Advanced Application Conference (CARDIS), Workshop on Attacks and Solutions in Hardware Security (ASHES)

*2018:* Asian Hardware Oriented Security and Trust Symposium (AsianHOST), DAC PhD Forum, Great Lakes Symposium on VLSI (GLSVLSI), International Symposium on Quality Electronic Design (ISQED), IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), ASM International Symposium for Testing and Failure Analysis (ISTFA), International Test Conference (ITC), International Workshop on Physical Attacks and Inspection on Electronics (PAINE), Network and Distributed System Security Symposium (NDSS), Smart Card Research and Advanced Application Conference (CARDIS), Workshop on Attacks and Solutions in Hardware Security (ASHES)

*2017:* Asian Hardware Oriented Security and Trust Symposium (AsianHOST), DAC PhD Forum, Great Lakes Symposium on VLSI (GLSVLSI), International Conference on Computer-Aided Design (ICCAD), IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), International Symposium on Quality Electronic Design (ISQED), International Test Conference (ITC), Network and Distributed System Security Symposium (NDSS), Smart Card Research and Advanced Application Conference (CARDIS), Workshop on Attacks and Solutions in Hardware Security (ASHES)

*2016:* Asian Hardware Oriented Security and Trust Symposium (AsianHOST), Design Automation Conference (DAC), DAC PhD Forum, IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), International Conference on Computer-Aided Design (ICCAD), International Symposium on Quality Electronic Design (ISQED), ASM International Symposium for Testing and Failure Analysis (ISTFA)

*2015:* Design Automation Conference (DAC), International Conference on Computer-Aided Design (ICCAD), International Conference on Computer Design (ICCD), IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), International Test Conference (ITC), International Symposium on Quality Electronic Design (ISQED), Workshop on Embedded Systems Security (WESS)

*2014:* IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), TRUDEVICE Workshop on Test and Fault Tolerance for Secure Devices, Workshop on Embedded Systems Security (WESS)

*2013:* Workshop on Embedded Systems Security (WESS)

*Working Groups*

*2020–present:* Test Article Development Working Group, Member
*2020–present:* Hardware CWE Special Interest Group (HW CWE SIG), Member
*2018–present:* IEEE P1735 Working Group, Member
*2018–2019:* TAME Hardware Assurance and Weakness Collaboration and Sharing (HAWCS) Working Group (intially called Hardware Vulnerability Database), Scribe and Member

*Professional Memberships*

*2018–present:* ACM, Member
*2019–present:* IEEE, Senior Member
*2019–present:* IEEE Reliability Society, Member
*2018–present:* IEEE Circuits and Systems Society, Member
*2021–present:* Sigma Xi, Member

*Proposal Panelist/ Ad-Hoc Reviewer*

*2021:* National Science Foundation (NSF), Army Research Office (ARO)
*2020:* National Science Foundation (NSF), Army Research Office (ARO)
*2019:* National Science Foundation (NSF)
*2018:* National Science Foundation (NSF), Critical Infrastructure Resilience Institute (CIRI)
*2017:* American Association for the Advancement of Science (AAAS), Army Research Office (ARO)
*2016:* National Science Foundation (NSF)

*Reviewer for*

*ACM Computing Surveys*
*ACM Journal on Emerging Technologies in Computing Systems (JETC)*
*ACM Transactions on Design Automation of Electronic Systems (TODAES)*
*ACM Transactions on Privacy and Security (TOPS)*
*Biomedical Engineering/Biomedizinische Technik (BMT)*
*IEEE Access*
*IEEE Communications Letters*
*IEEE Design & Test (D&T)*
*IEEE Internet of Things Magazine*
*IEEE Journal of Solid-State Circuits (JSSC)*
*IEEE Journal on Emerging and Selected Topics in Circuits and Systems (JETCAS)*
*IEEE Transactions on Biomedical Engineering (TBME)*
*IEEE Transactions on Biometrics, Behavior, and Identity Science (T-BIOM)*
*IEEE Transactions on Circuits and Systems I (TCAS1)*
*IEEE Transactions on Circuits and Systems II (TCAS2)*
*IEEE Transactions on Computer-Aided Design of Integrated Circuits (TCAD)*
*IEEE Transactions on Computers*
*IEEE Transactions on Embedded Computing Systems (TECS)*
*IEEE Transactions on Emerging Topics in Computing (TETC)*
*IEEE Transactions on Industrial Electronics (TIE)*
*IEEE Transactions on Information Forensics and Security (TIFS)*
*IEEE Transactions on Multi-Scale Computing Systems (TMSCS)*
*IEEE Transactions on Nanotechnology (TNANO)*
*IEEE Transactions on Dependable and Secure Computing (TDSC)*
*IEEE Transactions on VLSI Systems (TVLSI)*
*IET Computers & Digital Techniques*
*Image and Vision Computing*
*Integration, the VLSI Journal*
*Journal of Cryptographic Engineering (JCEN)*
*Journal of Electronic Testing: Theory and Applications (JETTA)*
*Microelectronics Reliability*
*Nature Communications*
*Nature Electronics*
*Neurocomputing*
*Sensors*

*University Appointments and Service*

**University of Florida, ECE Department**, Gainesville, Fl

Reviewer, 2016 UF Opportunity Seed Fund Concept Paper, December 2015

*College Appointments and Service*

**University of Florida, ECE Department**, Gainesville, Fl

Associate Director, Florida Institute for National Security, Fall 2022 – present
Ad hoc substitute for Prof. David Arnold, HWCOE Research Advisory Council (RAC), 2021 – 2022
Panelist, HWCOE Early Career Stage Investigator Workshop, April 2022
Red team participant, HWCOE Internal NSF CAREER Review Process, July 2019
Speaker, HWCOE Early Career Stage Investigator Workshop, February 2018

*Departmental Appointments and Service*

**University of Florida, ECE Department**, Gainesville, Fl

Faculty Search Committee, AY 2021 – 2022
Graduate Recruiting & Admissions Committee (GRAC), 2015 – 2021
EEL 4930 Programming for EE 2 ABET Course Committee, 2020 – 2022
Chair, Computer Engineering Subcommittee on Undergraduate EE Programming, Spring 2019 – Fall 2020

EEE 3000 Intro to ECE ABET Course Committee, 2018 – 2020
Faculty Search Committee, AY 2017 – 2018
EEL 4242 Power Electronics 1 ABET Course Committee, 2017 – 2019
EEE 4404 Mixed Signal IC Testing I ABET Course Committee, 2016 – 2019
EEE 4310 Digital Integrated Circuits ABET Course Committee, 2015 – 2019
EEL 3111 Circuits 1 ABET Course Committee, 2015 – 2017

**University of Connecticut, ECE Department**, Storrs, CT

Department Judge- First Annual Graduate Poster Competition, 2015
Course and Curriculum Committee, AY 2014-2015

*Invited Keynotes, Talks, and Webinars (39)*

**Silicon Valley Cybersecurity Conference (SVCC)**, Virtual Keynote — August 2022
Title: "Microelectronics Supply Chain Revisited: Lessons Learned and Promising New Directions"

**Microelectronics Reliability and Qualification Workshop**, Virtual — February 2022
Title: "Security Never Sleeps: Why Hardware Needs to be Protected from Design Through Resign"

**IIT Kharagpur Distinguished Lecture Series on Cyber Security**, Virtual — November 2021
Title: "Hardware Security and Assurance: The Power of Reverse Engineering"

**OhioU EECS Seminar Series**, Virtual — October 2021
Title: "Hardware Security and Assurance: The Power of Reverse Engineering"

**IEEE Computer Society Oregon Chapter**, Virtual — October 2021
Title: "Hardware Security and Assurance: The Power of Reverse Engineering"

**ROLLCAGE Strategy Meeting - Vehicle Security**, , Virtual — October 2021
Title: "Advances in Deep Learning and Bloom Filters for Cyber Defense"

**WPI ECE Graduate Seminar Lecture**, Virtual — September 2021
Title: "Hardware Obfuscation: A Critical Outlook on its Security and Potential Applications"

**CALCE/SMTA Counterfeit Parts and Materials Symposium**, Virtual — August 2021
Title: "Closing the Gaps in Counterfeit Chip Detection and Avoidance for Good"

**KCNSC Cross-Consortia All-Hands Meeting**, Virtual — July 2021
Title: "Model-Assisted PCB Attestation (MPA)"

**Society for Electronic Transactions and Security (SETS)**, Virtual — July 2021
Title: "Hardware Security and Assurance: The Power of Reverse Engineering"

**Hardwear.io**, Virtual — July 2021
Title: "Trust but Verify: Hardware Assurance in Globalized Supply Chain through Reverse Engineering"

**MEST Center Webinar**, Zoom — September 2020
Title: "Counterfeit Detection: Electrical/Logical Test Techniques"

**Department of Defense (DoD)**, Teleconference — March 2020
Title: "Software/Firmware Security: Is that Good Enough?"

**ANSYS**, WebEx — February 2020
Title: "Leveraging Side Channels and Computer Design Automation (CAD) for Security"

**MEST Center Webinar**, Zoom — December 2019
Title: "Introduction to Hardware Obfuscation"

**University of Arkansas**, Fayetteville, AR — October 2019
Title: "Hardware Security Assessment and Mitigation from Device to SoC"

**Intel Tech Sharing Forum**, WebEx — September 2019
Title: "Hardware Security Assessment and Mitigation from Device to SoC"

**Intel Security Conference (iSecCon)**, Haifa, Israel — June 2019
Title: "Security-aware FSM Design Flow for Identifying and Mitigating Vulnerabilities to Fault Attacks"

**IEEE Custom Integrated Circuits Conference**, Austin, TX — April 2019

Title: "State-of-the-Art and Challenges in Design-for-Anti-Counterfeit"

**GRC Technology Transfer e-Workshop**, WebEx April 2019
Title: "iPROBEv1.0: CAD/EDA for Low Cost Protection Against Frontside Probing Attacks"

**ECASE-Army Symposium**, Adelphi, MD April 2019
Title: "SWIFT: A Signature-enabled Wireless Infrastructure for Forensics, Tracking, and Locking of Electronic Systems"

**NXP Semiconductors**, Chandler, AZ Oct. 2018
Title: "CAD Assessment and Flow for Protection Against Chip Editing and Probing"

**NSWC Crane**, Crane, IN Aug. 2018
Title: "Trusted and Assured Microelectronics: Solutions and Challenges Ahead"

**Trust and Assurance Model Teleconference**, Zoom July 2018
Title: "FORTIS: Establishing Forward Trust for Protecting IPs and ICs in Today's Complex Supply Chain"

**CIA Summer Symposium**, McLean, VA June 2018
Title: "Biometrics Research at the University of Florida"

**ITEA 2018 Cybersecurity Workshop**, Fort Walton Beach, FL March 2018
Title: "Hardware for Cyber (H4C): A Suite of Electronic System Protections from Nano to System Levels"

**CIA Tech Exchange on Trust & Validation of Electronics**, Chantilly, VA Feb. 2018
Title: "Trust & Validation of Electronics at FICS Research"

**Cisco Research Center System & Platform Security Summit**, San Jose, CA Dec. 2017
Title: "Teardown and Recommendations for IEEE Standard for Protecting Electronic-Design Intellectual Property"

**International Test Conference (ITC) 2017**, Fort Worth, TX Nov. 2017
Title: "Upgrade/Downgrade: A Perspective on Challenges and Opportunities in Overcoming the Legacy System Issue"

**AsianHOST 2017**, Beijing, China Oct. 2017
Title: "Security of the Internet of Things: New Frontiers"

**GRC Technology Transfer e-Workshop**, WebEx July 2016
Title: "Design of Low-Cost Memory-Based Security Primitives and Techniques for High-Volume Products"

**Workshop on Cyber Science, Biometrics and Digital Forensics**, Miami, FL Nov. 2015
Title: "Biometrics Meets Hardware Security"

**Northrop Grumman Lunch N Learn**, Baltimore, MD Nov. 2015
Title: "New Directions in Hardware Security and Supply Chain Assurance"

**Workshop on Cryptography and Hardware Security for the IoT**, College Park, MD Oct. 2015
Title: "Hardware Security Challenges and Solutions in the IoT Era"

**University of Florida**, Gainesville, FL March 2015
Title: "Hardware-based Primitives for System Authentication and Protection"

**Design, Automation & Test in Europe (DATE)**, Dresden, DE March 2014
Title: "Protocol Attacks on Advanced PUF Protocols and Countermeasures"

**University of South Florida**, Tampa, FL March 2013
Title: "Towards Comprehensive Solutions for Hardware Security"

**Raytheon BBN Technologies**, Columbia, MD March 2013
Title: "Towards Comprehensive Solutions for Hardware Security"

**University of Connecticut**, Storrs, CT Feb. 2013
Title: "Towards Comprehensive Solutions for Hardware Security"

*Campus and Departmental Talks (9)*

**UF Eta Kappa Nu (HKN) Speaker Series**, Gainesville, FL Nov. 2020
Title: "Introduction to FICS Research"

**UF Eta Kappa Nu (HKN) Speaker Series**, Gainesville, FL Oct. 2019
Title: "Introduction to FICS Research"

**Early Stage Investigator Workshop**, Gainesville, FL Feb. 2018
Title: "Navigating the Early Stage Investigator Proposal Process"

**Forum on Trusted and Assured MicroElectronics (TAME)**, Gainesville, FL Nov. 2017
Title: "Emerging Solutions for Trusted and Assured Microelectronics"

**UF Eta Kappa Nu (HKN) Speaker Series**, Gainesville, FL Nov. 2017
Title: "Introduction to FICS Research"

**FICS Annual Conference on Cybersecurity**, Gainesville, FL Feb. 2016
Title: "Human-to-Device Authentication"

**CHASE Conference on Secure/Trustworthy Systems and Supply Chain Assurance**, Storrs, CT April 2015
Title: "Anti-reverse Engineering with Human-to-Device Authentication"

**CHASE Workshop on Secure/Trustworthy Systems and Supply Chain Assurance**, Storrs, CT April 2014
Title: "Design of Robust SRAM PUFs"

**University of Connecticut (ECE Seminar Series)**, Storrs, CT Dec. 2013
Title: "Trojan and Counterfeit Detection for Secure and Trustworthy Hardware"

*Invited Panel and Roundtable Discussions (13)*

Panelist, **Hardwear.io USA**, Santa Clara, CA June 2022
Title: "Ecosystem-level Challenges and Trends to Resolving Hardware Security Vulnerabilites"

Panelist, **HWCOE Early Career Stage Investigator Workshop**, Gainesville FL April 2022
Title: "Young Investigator/Faculty Award/Program and Early Career Research Program (YIP/YFA/ECRP) Panel"

Panelist, **IEEE AsianHOST 2020**, Zoom Dec. 2020
Title: "AI for Hardware Security: Boon or Bane"

Organizer, **IEEE HOST**, ON24 Webcast July 2020
Title: "How Can Hardware Security Contribute to the Fight Against COVID-19 and to Post Pandemic Life?"

Panelist, **University of Maryland**, College Park, MD Nov. 2018
Title: "11th Annual ECEGSA Roundtable on Academic Careers"

Panelist, **IEEE International Workshop on Physical Attacks And Inspection On Electronics (PAINE)**, San Francisco, CA June 2018
Title: "Crossroad Between Physical Inspection and Hardware Security"

Co-Lead, **TAME Forum Breakout Session 3**, McLean, VA May 2018
Title: "National Technology Roadmap for Trusted and Assured Microelectronics"

Moderator and Organizer, **HOST 2018 Visionary Panel**, McLean, VA May 2018
Title: "Future of HOST: What to Expect in the Next Decade?"

Panelist, **IEEE-HKN Student Leadership Conference**, Gainesville, FL April 2018
Title: "Life of a Research Professor"

Panelist, **EGN6933 - ENG FACULTY DEV**, Gainesville, FL Jan. 2018
Title: "How to Get a Faculty Job"

Panelist, **Trusted Microelectronics Special Topic: Field Programmable Gate Array (FPGA) Assurance**, McLean, VA March 2017
Title: "FPGA Security Research Panel"

Moderator, **Dagstuhl Seminar 16202**, Wadern, Germany May 2016
Title: "PUFs and Security Components"

Panelist, **University of Maryland**, College Park, MD Oct. 2013
Title: "6th Annual ECEGSA Roundtable on Academic Careers"

*Tutorials and Training Sessions (7)*

**International Symposium on Circuits and Systems (ISCAS)** May 2022
Title: "IC Security and Assurance: Counterfeit IC Detection and Avoidance"
Presenter: D. Forte

**The National MicroElectronics Security Training Center (MEST)** May 2020
Title: "Logic Locking Hands-on Training"
Presenter: D. Forte

**Conference on Cryptographic Hardware and Embedded Systems (CHES) 2018** Sept. 2018
Title: "Counterfeit Integrated Circuits: Threats, Detection, and Avoidance"
Presenters: D. Forte and R.S. Chakraborty

**International Test Conference (ITC) 2016** Nov.2015
Title: "Test Opportunities and Challenges for Secure Hardware and Verifying Trust in Integrated Circuits"
Presenters: D. Forte and S. Bhunia

**International Test Conference (ITC) 2015** Oct. 2015
Title: "Test Opportunities and Challenges for Secure Hardware and Verifying Trust in Integrated Circuits"
Presenters: M. Tehranipoor and D. Forte

**Design Automation and Test in Europe (DATE) 2014** March 2014
Title: "All You Need to Know About Hardware Trojans and Counterfeit ICs"
Presenters: M. Tehranipoor and D. Forte

**IEEE Conference on VLSI 2013** Jan. 2014
Title: "All You Need to Know About Hardware Trojans and Counterfeit ICs"
Presenters: M. Tehranipoor and D. Forte

## Teaching Experience

**University of Florida, ECE Department**, Gainesville, FL

*Instructor*

- EEL4310/5322: Digital Integrated Circuits Design/ VLSI Circuits and Technology S'17–22
- EEE6742 (Formerly EEL6935): Advanced Hardware Security and Trust F'16–18, F'20–21

*Co-Instructor*

- EEL4930/5934: Introduction to Hardware Security and Trust S'16

**University of Connecticut, ECE Department**, Storrs, CT

*Instructor*

- ECE3421: VLSI Design and Simulation S'15
- ECE2001W: Electrical Circuits F'13–14
- ECE6095-005: Hardware Trojan Detection and Prevention S'14

*Guest Lecturer*

- ECE4451/5451: Introduction to Hardware Security and Trust F'14

**University of Maryland, ECE Department**, College Park, MD

*Co-instructor*

- ENEE759T: Digital VLSI Design, Technology & Tools S'13

*Teaching Assistant*

- ENEE644: Computer-Aided Design of Digital System S'10
- ENEE350: Computer Organization F'07, S'07
- ENEE446: Digital Computer Design F'07
- ENEE241: Numerical Techniques in Engineering F'06

Note: 'F' and 'S' denote Fall and Spring respectively.

*Mentor*

- Teaching Assistant Training and Development (TATD) 2010–2011, 2011–2012

## Citizenship Status

U. S. Citizen