Jeyavijayan (JV) Rajendran

Assistant Professor, Electrical and Computer Engineering, Texas A&M Univ.
Email: jv.rajendran@tamu.edu Webpage: cesg.tamu.edu/faculty/jv/
Address: 301 Wisenbaker Engineering Building, College Station, TX 77843, USA

Work Experience

- **Assistant Professor, Dept. of Electrical and Computer Eng., Texas A&M, Sep. 2017 – Present**
  - **Digital Integrated Circuit Design** – Fall 2017
  - **Hardware Security** – Spring 2018
- **Assistant Professor, Dept. of Electrical and Computer Eng., UT Dallas, Sep. 2015 – Aug. 2017**
  - **Introduction to Hardware Security** – Fall 2016
  - **VLSI Design** – Spring 2017 and Spring 2016
- **Summer Internships**
  - Research Associate, Intel Security Center of Excellence, Jun. 2012 – Aug. 2012
    Security validation of processors
  - Research Associate, Intelligent Infrastructure Labs, Hewlett Packard, Jun. 2011 – Aug. 2011
    Automated characterization of memristive devices
- **Teaching Assistant**
  - **Introduction to Trustworthy Hardware** – Spring 2010, Spring 2011, Spring 2013, Spring 2014
    Co-developed this course with Prof. Ramesh Karri.
    Duties: curriculum development, held weekly office and lab hours, and graded assignments and projects.
    The developed course material is now being used at more than five universities.
  - **Advanced Hardware Design** – Fall 2011, Fall 2012, Fall 2013, Fall 2014
    Duties: assisted in developing lecture notes and lab assignments, held weekly office and lab hours, and graded assignments and projects.
  - **Introduction to CMOS VLSI Design** – Spring 2011
    Duties: taught Cadence IC tools, held weekly office and lab hours, and graded assignments and exams.
  - **Embedded Systems** – Fall 2010
    Duties: taught assembly-level programming, held weekly office and lab hours, and graded assignments.
- **Research Assistant**, ECE Department, New York University, Aug. 2010 - 2015

Education

- **New York University**, New York, NY
  Ph.D. in Electrical Engineering, Jan. 2011 - Aug. 2015
  Advisor: Prof. Ramesh Karri; GPA: 3.98/4.0
  Google Scholar Citations: 2563; *h-index*: 27; *i-index*: 48 (as of 8/7/2018)
- **Polytechnic Institute of New York University**, New York, NY
  M.S. in Computer Engineering, Jan. 2009 - Jan. 2011
  Advisors: Prof. Ramesh Karri and Prof. Garrett S. Rose; GPA: 4.0/4.0
- **Anna University**, India.
  B.E. in Electronics and Communication Engineering, Aug. 2004 - May 2008; GPA: 87/100

Research Interests

Cybersecurity, VLSI, computer-aided design, computer architecture, and emerging technologies with emphasis on hardware security

Honors and Awards

- NSF CAREER Award, 2017
- ACM SIGDA Outstanding PhD Dissertation Award, 2016 (given at DAC'17)
- Alexander Hessel Award for the Best PhD Dissertation in Electrical Engineering at NYU, 2016

- **Best Student Paper Awards**
  - ACM Conference on Computer and Communications Security (CCS), 2013
  - IEEE Defect and Fault-Tolerance (DFT) Symposium, 2013
  - IEEE International Conference on VLSI Design, 2011
  - IEEE/ACM International Conference on Computerr-Aided Design(ICCAD), 2017 (nominated)
- **Student Research Competitions**
  - Most Popular Research Award, ACM Design Automation PhD Forum at DAC, 2014
  - Third place, ACM Student Research Competition - Grand Finals, 2013
  - Third place, ACM Student Research Competition for Design Automation at ICCAD, 2013
  - Third place, ACM Student Research Competition for Design Automation at DAC, 2012
  - Third place, IT security for next generation in Kaspersky American Cup, 2011
  - First place, CyberSecurity Awareness Week - Embedded Systems Challenge, 2009
- **Miscellaneous**
  - Most read paper in Springer Engineering (across all streams), 2016
  - Popular paper in IEEE Transactions on Computers, Nov. 2016
  - Service Recognition Award, Intel, 2012
  - Myron M. Rosenthal Award for Best M.S. Academic Achievement in ECE Department, NYU-Poly, 2011
  - Best Outgoing Student Award, 2008 (B.E.)
- **Students' and Mentees' honors**
  - Mr. Thomas Broadfoot, Ms. Danqing Liu, Ms. Lubaba Nahar, and Mr. Tarunesh Verma, Richard Newton Fellowship, 2016 and 2017
  - Mr. Thomas Broadfoot and Ms. Danqing Liue, selected for IEEE VTS Student Activities Program, 2016 and 2017
  - Mr. Tarunesh Verma, Undergraduate Research Award, 2016-2017
  - Mr. Reddy, Mr. Zhou, and Mr. Mahdi, Winners of CSAW Embedded Security Challenge, 2015 (co-advised)
  - Mr. Alvin Wei, Semifinalist, Intel's Nationwide Science Talent Search Competition, 2014

Grants

- *Physical-design techniques for secure split manufacturing*, National Science Foundation and Semiconductor Research Corporation, US $480,000, 2016-2019. Role: Lead PI
- *CAREER: Towards Provably-Secure Design of Integrated Circuits*, National Science Foundation, US $499,999, 2017-2022. Role: Sole PI
- *VeriSyn: Verification-guided Synthesis for Hardware Security*, Office of Naval Research, US $2,000,000, 2017-2021 (awarded) Role: Lead PI
- *ECLIPSE: Efficient Cross-Layered IP Protection SchemE*, Defense Advanced Research Project Agency, US $600,000, 2017-2019 (recommended). Role: PI

Publications

Book Chapters

B1. **J. Rajendran** and S. Garg, *Logic encryption*, a book chapter in "Hardware Protection through Obfuscation," edited by Domenic Forte, Swarup Bhunia, and Mark Tehranipoor, Springer, New York, Pages 71-88, 2017.

B2. S. Garg and **J. Rajendran**, *Split manufacturing*, a book chapter in "Hardware Protection through Obfuscation," edited by Domenic Forte, Swarup Bhunia, and Mark Tehranipoor, Springer, New York, Pages 243-262, 2017.

B3. **J. Rajendran**, O. Sinanoglu, and R. Karri *Physical Unclonable Functions and Intellectual Property Protection Techniques*, a book chapter in "Fundamentals of IP and SoC Security: Design, Verification and Debug," edited by Swarup Bhunia, Sandip Ray and Susmita Sur-Kolay, Springer, New York, Pages 199-222, 2017.

B4. R. Karri, **J. Rajendran,** and K. Rosenfeld, *Trojan Taxonomy*, a book chapter in "Hardware Security and Trust," edited by Mohammad Tehranipoor and Cliff Wang, Springer, New York, Pages 325-338, 2012.

Journals

J1. M. Yasin, B. Mazumdhar, O. Sinanoglu, and **J. Rajendran**, *Removal Attacks on Logic Locking and Camouflaging Techniques*, IEEE Transactions on Emerging Topics in Computing, Volume PP, Issue 99, 2017.

J2. M. Yasin, B. Mazumdhar, O. Sinanoglu, and **J. Rajendran**, *Testing the Trustworthiness of IC Testing: An Oracle-less Attack on IC Camouflaging*, IEEE Transactions on Information Forensics and Security, Volume PP, Issue 99, 2017.

J3. S. Ali, M. Ibrahim, **J. Rajendran**, O. Sinanoglu, and K. Chakrabarty, *Supply-Chain Security of Digital Microfluidic Biochips*, IEEE Computer Magazine, Volume 49, Issue 8, Pages 36-43, 2016.

J4. S. E. Zeltmann, N. Gupta, N. Tsoutsos, M. Maniatakos, **J. Rajendran**, and R. Karri, *Manufacturing and Security Challenges in 3D printing*, Journal of Materials, Volume 68, Issue 7, Pages 1872-1881, 2016 (Most read paper in Springer Engineering in 2016).

J5. **J. Rajendran**, O. Sinanoglu, and R. Karri, *Building Trustworthy Hardware Using Untrusted Components During High-Level Synthesis*, IEEE Transactions on Very Large Scale Integration Systems, Volume PP, Issue 99, Pages 1-14, 2016.

J6. M. Yasin, **J. Rajendran**, O. Sinanoglu, and R. Karri, *On Improving the Security of Logic Locking*, IEEE Transactions on Computer-Aided Design, Volume PP, Issue 99, Pages 1-1, 2015.

J7. **J. Rajendran**, A. Ali, O. Sinanoglu, and R. Karri, *Belling the CAD: Towards Security-Centric Electronic System Design*, IEEE Transactions on Computer-Aided Design, Volume 34, Issue 11, Pages 1266-1282, 2014.

J8. **J. Rajendran**, R. Karri, J. B. Wendt, M. Potkonjak, N. McDonald, G. S. Rose, and B. Wysocki, *Nano Meets Security: Exploring Nanoelectronic Devices for Security Applications*, Proceedings of the IEEE, Volume 103, Issue 5, Pages 829-849, 2015.

J9. **J. Rajendran**, R. Karri, and G.S. Rose, *Improving Tolerance to Variations in Memristor-based Applications Using Parallel Memristors*, IEEE Transactions on Computers, Volume 64, Issue 3, Pages 733-746, 2015.

J10. **J. Rajendran**, H. Zhang, C. Zhang, G.S. Rose, Y. Pino, O. Sinanoglu and R. Karri, *Fault Analysis-based Logic Encryption*, IEEE Transactions on Computers, Volume 64, Issue 2, Pages 410-424, 2015.

J11. C. Liu, **J. Rajendran**, C. Yang and R. Karri *Shielding Heterogeneous MPSoCs from Untrustworthy 3PIPs through Security-Driven Task Scheduling*, IEEE Transactions on Emerging Topics in Computing, Volume 2, Issue 4, Pages 461-472, 2014.

J12. **J. Rajendran**, O. Sinanoglu, and R. Karri, *Regaining Trust in VLSI Design: Design-for-Trust Techniques*, Proceedings of the IEEE, Volume 102, Issue 8, Pages 1266-1282, 2014.

J13. **J. Rajendran**, A. K. Kanuparthi, M. Zahran, S. Addepalli, G. Ormazabal, and R. Karri, *Securing processors against insider attacks: a circuit-microarchitecture co-design approach*, IEEE Design and Test Magazine, Volume 30, Issue 2, Pages 35-44, 2013.

J14. S. Kannan, **J. Rajendran**, O. Sinanoglu, and R. Karri, *Sneak Path Testing of Crossbar-based Non-volatile Random Access Memories*, IEEE Transactions on Nanotechnology, Volume 12, Issue 3, Pages 413-426, 2013.

J15. **J. Rajendran**, H. Manem, R. Karri and G.S. Rose, *An Energy-Efficient Memristive Threshold Logic Circuit*, IEEE Transactions on Computers, Volume 61, Issue 4, Pages 474-487, 2012.

J16. G.S. Rose, H. Manem, **J. Rajendran**, R. Karri and R. Pino, *Leveraging Memristive Systems in the Construction of Digital Logic Circuits*, Proceedings of the IEEE, Volume 100, Issue 6, Pages 2033-2049, 2012.

J17. H. Manem, **J. Rajendran** and G.S. Rose, *Design Considerations for Multi-Level CMOS/Nano Memristive Memory*, ACM Journal of Emerging Technologies in Computing, Volume 8, Issue 1, Pages 6:1-6:22, 2012.

J18. H. Manem, **J. Rajendran**, and G.S. Rose, *Stochastic Gradient Descent Inspired Training Technique for a CMOS/Nano Memristive Trainable Threshold Gate Array*, IEEE Transactions on Circuits and Systems-I, Volume 59, Issue 5, Pages 1051-1060, 2012.

J19. M. Tehranipoor, H. Salmani, X. Zhang, X. Wang, R. Karri, **J. Rajendran** and K. Rosenfeld, *Trustworthy Hardware: Trojan Detection and Design-for-Trust Challenges*, Computer Magazine, Volume 44, Issue 7, Pages 66-74, 2011.

J20. R. Karri, **J. Rajendran**, K. Rosenfeld and M. Tehranipoor, *Trustworthy Hardware: Identifying and Classifying Hardware Trojans*, Computer Magazine, Volume 43, Issue 10, Pages 39-46, 2010.

Conference Papers

C1. M. Zaman, A. Sengupta, D. Liu, O. Sinanoglu, Y. Makris, **J. Rajendran**, *Towards provably-secure performance locking,* accepted in the Proceedings of IEEE/ACM Design Automation and Test in Europe, 2018.

C2. Y. Wang, T. Cao, J. Hu, and **J. Rajendran**, *Front-End of Line Attacks in Split Manufacturing,* accepted in the Proceedings of IEEE/ACM International Conference on Computer-Aided Design, 2017.

C3. L. Feng, Y. Wang, W-K. Mak, **J. Rajendran**, J. Hu, *Making Split Fabrication Synergistically Secure and Manufacturable,* accepted in the Proceedings of IEEE/ACM International Conference on Computer-Aided Design, 2017.

C4. M. Yasin, A. Sengupta, M. Ashraf, M. Nabeel, **J. Rajendran**, and O. Sinanoglu, *Provably-secure Logic Locking: From Theory To Practice,* accepted at ACM Conference on Computer and Communications Security, 2017.

C5. M. Algappan, **J. Rajendran**, M. Doroslovacki, and G. Venkataramani, *DFS Covert Channels on Multi-Core Platforms,* accepted at IEEE Symposium on VLSI-SoC, 2017.

C6. M. Yasin, A. Sengupta, B. Schäfer, Y. Makris, O. Sinanoglu, **J. Rajendran**, *What to Lock?: Functional and Parametric Locking,* in the Proceedings of the ACM Great Lakes Symposium on VLSI, Pages 351-356, 2017.

C7. Y. Wang, P. Chang, J. Hu, and **J. Rajendran**, *Routing perturbation for enhanced security in split manufacturing*, in the Proceedings of IEEE Asia and South Pacific Design Automation Conference, Pages 605-610, 2017.

C8. M. Yasin, B. Mazumdhar, O. Sinanoglu, and **J. Rajendran**, *Security analysis of Anti-SAT,* in the Proceedings of IEEE Asia and South Pacific Design Automation Conference, Pages 342-247, 2017.

C9. Md. B. Majumder, M. Uddin, G. Rose, and **J. Rajendran**, *Sneak path enabled authentication for memristive crossbar memories*, in the Proceedings of IEEE Asian Hardware Oriented Security and Trust Symposium, 2016.

C10. C. Yang, B. Liu, W. Wen, M. Barnell, Q. Wu, H. Li, Y. Chen, and **J. Rajendran**, *Security of Neuromorphic Computing: Thwarting learning attacks using memristor's obsolescence effect*, in the Proceedings of IEEE International Conference on Computer-Aided Design, Pages 97:1-97:6, 2016.

C11. M. Yasin, B. Mazumdhar, O. Sinanoglu, and **J. Rajendran**, *CamoPerturb: Secure IC Camouflaging for Minterm Protection*, in the Proceedings of IEEE International Conference on Computer-Aided Design, Pages 29:1-29:8, 2016.

C12. M. Yasin, **J. Rajendran**, S. Saeed, and O. Sinanoglu, *Activation of Logic Encrypted Chips: Pre-Test or Post-Test?*, in the Proceedings of IEEE/ACM Design Automation and Test in Europe, Pages 139-144, 2016.

C13. M. Yasin, B. Mazumdhar, O. Sinanoglu, and **J. Rajendran**, *SARLock: Resisting SAT attacks on Logic encryption,* in the Proceedings of IEEE Symposium on Hardware Oriented Security and Trust, Pages 236-241, 2016.

C14. A. Kanuparthi, **J. Rajendran**, and R. Karri, *Controlling your control flow graph,* in the Proceedings of IEEE Symposium on Hardware Oriented Security and Trust, Pages 43-48, 2016.

C15. Y. Zhang, P. Chen, J. Hu, and **J. Rajendran**, *The Cat and Mouse in Split Manufacturing,* in the Proceedings of IEEE/ACM Design Automation Conference, Pages 165:1-165:6, 2016.

C16. J. Tang, R. Karri, and **J. Rajendran**, *Securing Pressure Measurements Using SensorPUFs,* in the Proceedings of IEEE International Symposium on Circuits and Systems, 2016.

C17. **J. Rajendran**, A. M. Dhandayuthapany, V. Vedula, and R. Karri, *Security Verification of 3rd Party Intellectual Property Cores for Information Leakage*, in the Proceedings of IEEE International Conference on VLSI Design, Pages 547-552, 2016.

C18. **J. Rajendran**, V. Vedula, and R. Karri, *Detecting Malicious Modifications of Data in Third-Party Intellectual Property Cores*, in the Proceedings of IEEE/ACM Design Automation Conference, Pages 112:1–112:6, 2015.

C19. D. Shahrjerdi, **J. Rajendran**, S. Garg, R. Karri, and F. Koushanfar, *Shielding and Securing Integrated Circuits using Sensors*, in the Proceedings of IEEE/ACM International Conference on Computer-Aided Design, Pages 170-174, 2014.

C20. D. Hoe, **J. Rajendran,** and R. Karri *Towards Secure Analog Designs: A Secure Sense Amplifier Using Memristors*, in the Proceedings of IEEE International Symposium on VLSI, Pages 516-521, 2014.

C21. A. Waksman, **J. Rajendran,** and S. Sethumadhavan *A Red Team/Blue Team Assessment of Functional Analysis Methods for Malicious Circuit Identification*, in the Proceedings of IEEE/ACM Design Automation Conference, Pages 1-4, 2014.

C22. **J. Rajendran**, M. Sam, O. Sinanoglu, and R. Karri, *Security Analysis of Integrated Circuit Camouflaging*, in the Proceedings of ACM Conference on Computer and Communications Security, Pages 709-720, 2013.

C23. M. Rostami, F. Koushanfar, **J. Rajendran** and R. Karri, *Hardware Security: Threat Models and Metrics*, in the Proceedings of IEEE Conference on Computer-Aided Design, Pages 819-823, 2013.

C24. C. Liu, **J. Rajendran**, C. Yang and R. Karri, *Shielding Heterogeneous MPSoCs from Untrustworthy 3PIPs through Security-Driven Task Scheduling*, in the Proceedings of IEEE Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems, Pages 101-106, 2013. **(Best Student Paper Award)**

C25. **J. Rajendran**, O. Sinanoglu, and R. Karri, *VLSI Testing based Security Metric for IC Camouflaging*, in the Proceedings of the IEEE International Test Conference, Pages 1-4, 2013.

C26. O. Sinanoglu, N. Karimi, **J. Rajendran**, R. Karri, Y. Jin, K. Huang, and Y. Makris, *Reconciling the IC Test and Security Dichotomy*, in the Proceedings of IEEE European Test Symposium, Pages 1-6, 2013.

C27. **J. Rajendran**, H. Zhang, O. Sinanoglu, and R. Karri, *High-Level Synthesis for Security and Trust*, in the Proceedings of the IEEE International On-Line Testing Symposium, Pages 232-233, 2013.

C28. 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*, in the Proceedings of IEEE VLSI Test Symposium, Pages 1-3, 2013.

C29. **J. Rajendran**, O. Sinanoglu, and R. Karri, *Is Split Manufacturing secure?,* in the Proceedings of the IEEE/ACM Design Automation and Test in Europe Conference, Pages 1259-1264, 2013.

C30. G. Rose, **J. Rajendran**, N. McDonald, R. Karri, M. Potkonjak, and B. Wysocki, *Hardware Security Strategies Exploiting Nanoelectronic Circuits*, in the Proceedings of IEEE/ACM Asia and South Pacific Design Automation Conference, Pages 368-372, 2013.

C31. S. Kannan, **J. Rajendran**, O. Sinanoglu, and R. Karri, *Sneak Path Testing of Memristor-based Memories*, in the Proceedings of IEEE International Conference on VLSI Design, Pages 386-391, 2013.

C32. **J. Rajendran**, G. S. Rose, R. Karri, and M. Potkonjak, *Nano-PPUF: A Memristor-based security primitive*, in the Proceedings of IEEE International Symposium on VLSI, Pages 84-87, 2012.

C33. **J. Rajendran**, Y. Pino, O. Sinanoglu, and R. Karri, *Security Analysis of Logic Obfuscation*, in the Proceedings of IEEE/ACM Design Automation Conference, Pages 83-89, 2012.

C34. **J. Rajendran**, Y. Pino, O. Sinanoglu, and R. Karri, *Logic encryption: A fault analysis perspective*, in the Proceedings of IEEE/ACM Design Automation and Test in Europe Conference, Pages 953-958, 2012.

C35. **J. Rajendran**, Y. Pino, O. Sinanoglu, and R. Karri, *Applying IC Testing Concepts to Secure ICs*, in the Proceedings of GOMACTECH, 2012.

C36. S. Kannan, **J. Rajendran**, O. Sinanoglu, and R. Karri, *Engineering Crossbar based Emerging Memory Technologies*, in the Proceedings of IEEE International Conference on Computer Design, Pages 478-479, 2012.

C37. **J. Rajendran**, V. Jyothi, and R. Karri, *Blue team red team approach to hardware trust assessment: The embedded systems challenge experience*, in the Proceedings of IEEE International Symposium on Computer Design, Pages 285-288, 2011.

C38. **J. Rajendran**, V.Jyothi, O.Sinanoglu, and R. Karri, *Design and analysis of ring oscillator based Design-for-Trust technique*, in the Proceedings of IEEE VLSI Test Symposium, Pages 105-110, 2011.

C39. **J. Rajendran**, R. Karri, and G.S. Rose, *Parallel Memristors: Improving Variation Tolerance in Memristive Digital Circuits*, in the Proceedings of IEEE International Symposium on Circuits and Systems, Pages 2241-2244, 2011.

C40. **J. Rajendran**, H. Manem, R. Karri and G.S. Rose, *An Approach to Tolerate Process Related Variations in Memristor-based Applications*, in the Proceedings of IEEE Symposium on VLSI Design, Pages 18-23, 2011. **(Best Student Paper Award)**

C41. **J. Rajendran**, H. Manem, R. Karri and G.S. Rose, *Memristor based Programmable Threshold Logic Array*, in the Proceedings of IEEE Symposium on Nanoscale Architectures, Pages 5-10, 2010.

C42. **J. Rajendran**, H. Borad, S. Mantravadi and R. Karri, *SLICED: Slide-based Concurrent Error Detection Technique for Symmetric Block Ciphers*, in the Proceedings of IEEE Symposium on Hardware Oriented Security and Trust, Pages 70-75, 2010.

C43. **J. Rajendran**, J. Jimenez, E. Gavas, V. Padman and R. Karri, *Towards a comprehensive and systematic classification of hardware Trojans*, in the Proceedings of IEEE Symposium on Circuits and Systems, Pages 1871-1874, 2010.

C44. **J. Rajendran**, H. Manem and G.S. Rose, *NDR based threshold logic fabric with memristive synapses*, in the Proceedings of IEEE-NANO, Pages 725-728, 2009.

C45. S. Chandrasekharan, **J. Rajendran** and A. Annamalai, *Data driven security alarm model for embedded applications*, in the Proceedings of IEEE International Conference on Computing, Communication and Networking, Pages 1-5, 2008.

Patents

P1. **J. Rajendran**, Y. Pino, O. Sinanoglu, and R. Karri, *Systems, processes, and computer-accessible medium for providing Logic Encryption utilizing Fault analysis*, U.S. Patent No. 9,081,929, issued July 14, 2015.

P2. V. Jyothi, R. Karri, **J. Rajendran**, and O. Sinanoglu, *Ring Oscillator Based Design-for-Trust*, U.S. Patent No. 9,081,991, issued July 15, 2015.

P3. **J. Rajendran**, A. M. Dhandayuthapany, V. Vedula and R. Karri, *System, Method And Computer-Accessible Medium For Security- verification of Third party intellectual property cores*, U.S. Patent pending, filed Dec. 2015.

P4. **J. Rajendran**, O. Sinanoglu and R. Karri, *System, Method And Computer-Accessible Medium For Fault Analysis Driven Selection Of Logic Gates To Be Camouflaged*, U.S. Patent pending, filed Sep. 2014.

P5. **J. Rajendran**, Y. Pino, R. Karri and O. Sinanoglu, *System, Method and Computer-Accessible Medium for Facilitating Logic Encryption*, U.S. Patent pending, filed Mar., 2014.

P6. **J. Rajendran**, O. Sinanoglu and R. Karri, *System, Method and Computer-Accessible Medium for Providing Secure Split Manufacturing*, U.S. Patent pending, filed Mar., 2014.

Mentoring Experience

- **PhD Dissertations**
  - Ms. Danqing Liu, Intellectual property protection (in progress)
  - Mr. Raymond Hung, Synthesis for hardware security (in progress)
  - Mr. Andrew Miller, Synthesis for hardware security (in progress)
- **M.S. Theses and Projects (at UT Dallas)**
  - Mr. Sai Marri, FPGA Security (in progress)
  - Mr. Songseok Choi, Hardware implementation of cryptographic algorithms (in progress)
- **M.S. Theses and Projects (at NYU)**
  - Mr. Zheng Wu, Security analysis of split manufacturing, 2014 (in progress)
  - Mr. Bozhi Liu, Side-channel attacks on ESL-generated designs, 2014 (in progress)
  - Mr. Aniket Sharma, Testability of RISC-V processor, 2014 (in progress)
  - Mr. Arunshankar Murugadhandayuthapany, Trojan detection in 3PIP designs, 2014 (in progress)
  - Mr. Aman Abdul Wahid Ali, Reverse engineering ESL-generated designs, 2014
  - Mr. Ilker Oztelcan, Characterization of camouflaged cells, 2013
  - Mr. Huan Zhang, Fault-analysis based logic encryption, 2012
  - Ms. Hetal Borad, Slide-based concurrent fault detection in AES, 2010
  - Mr. Xueyang Wang, Concurrent error detection in some SHA-3 candidates, 2010
  - Ms. Lakshmi Dondeti, Parity based concurrent error detection for Grain and Trivium, 2010
  - Mr. Minjie Xu, Concurrent error detection in some SHA-3 candidates, 2010
- **B.S. Theses and Projects (at UT Dallas)**
  - Mr. Victor Nguyen, Information-flow tracking, 2016
  - Mr. Tarunesh Verma, Secure hardware design, 2016
- **B.S. Theses and Projects (at NYU)**
  - Mr. Michael Sam, Design of camouflaged cells, 2013 (Winner, Best Student Paper Award at CCS, 2013)
  - Mr. Chi Zhang, Fault-analysis based logic encryption, 2012
- **High-school Projects**
  - Mr. Adrian Andreescu, Information-flow tracking, 2016
  - Mr. Derek Tsui, Camouflaging using dummy cells, 2014 (Stuyvesant High School)
  - Mr. Alvin Wei, A SAT-based tool for camouflaging, 2013 (Stuyvesant High School) (Semifinalist, Intel's Science Talent Search Competition, 2014)

Professional Activities

- **Program Committee Member**
  - IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), 2017 (Security track Co-chair)
  - IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2017
  - ACM Great Lakes Symposium on VLSI (GLSVLSI), 2017
  - IEEE International Conference on Consumer Electronics (ICCE), 2017

- IEEE International Conference on Computer Design (ICCD), 2017
- ACM Asian Symposium on Computer and Communications Security (Asia-CCS), 2017
- IEEE International Conference on Hardware-Oriented Security and Trust (HOST), 2016 and 2017
- IEEE International Conference on Computer Design (ICCD), 2016
- Applied Cryptography and Network Security (ACNS), 2016
- IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), 2016 and 2017
- IEEE International Conference on Compilers, Architectures, and Synthesis of Embedded Systems (CASES), 2016
- IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2014, 2016, and 2017
- ARO Workshop on Trustworthy Hardware, 2013 and 2014

- **Reviewing Activities**
  - **Journals:** Proceedings of the IEEE, IEEE Transactions on Computers, IEEE Transactions on Computer-Aided Design, IEEE Transactions on Very Large Scale Integration, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Circuits and Systems-II, IEEE Transactions on Nanotechnology, IEEE Design and Test Magazine, IEEE Transactions on Neural Networks and Learning Systems, IEEE Transactions on Reliability, IEEE Journal of Emerging and Selected Topics in Circuits and Systems, ACM Computing Surveys, ACM Journal of Emerging Technologies in Computing, ACM Transactions on Embedded Computing Systems, and Elsevier Journal of Parallel and Distributed Computing
  - **Conferences** (program committee/external/sub-reviewer): IEEE/ACM Design Automation Conference, IEEE/ACM International Conference on Computer-Aided Design, IEEE/ACM Design Automation and Test in Europe, IEEE International Test Conference, IEEE VLSI Test Symposium, IEEE European Test Symposium, IEEE Hardware Oriented Security and Trust, ACM Conference on Computer and Communications Security, IEEE International Conference on Computer Design, IEEE Symposium on Nanoscale Architectures, IEEE International Conference on Very Large Scale Integration, IEEE Defect and Fault Tolerance Symposium, IEEE International On-Line Test Symposium, IEEE Latin American Test Workshop, IEEE Design and Technology of Integrated Systems, IEEE Great Lakes Symposium on VLSI, and IEEE International Symposium on Circuits and Systems.
- **Workshop/Special sessions/Competition Organized**
  - **Hack@DAC**, DAC, 2017 (Co-founder)
    Hack@DAC is a red-team blue-team student competition for hardware security, co-located with DAC. More than 10 students from 5 universities have participated in the first edition, exposing vulnerabilities in electronic desigm automation tools.
  - **FOSTER**, 2017 (Co-founder)
    FOSTER is an NSF-sponsored workshop that brings representatives from the major stakeholders in the hardware security arena — government, industry, and academia — at a common venue. The FOSTER workshop seeks to define the roadmap and agenda for the next phase of hardware security research and identify concrete pathways for the transition to practice. More than 40 researchers from 25 organizations have participated in the first edition.
  - **Special session on cyber-physical system and security**, ASP-DAC, 2016
    This special session aims to expose hardware-related vulnerabilities in cyber-physical systems (CPSs). It brings together a wide-range of researchers to investigate questions such as "Is the current CPSs employed in critical infrastructure secure?"; "can an attacker exploit hardware properties to undermine the security of CPSs?" and "how do we build secure CPSs?"
  - **ARO Workshop on Trustworthy Hardware**, 2013 and 2014
    The workshop aims to identify new directions and challenges in critical aspects of IC and system security such as theoretical and conceptual foundations, synthesis, testing and verification, modeling and optimization, and case studies. The workshop was attended by 40 leading researchers in hardware security from industry and academia. Co-organized with Prof. Karri, Prof. Sinanoglu and Prof. Maniatakos.
    Duties: Procuring funding, designing the program, hosting the attendees, and chairing the sessions.
  - **Embedded Security Challenge (ESC)**, 2010 – 2014
    ESC (esc.isis.poly.edu) is a red-team blue-team student competition for hardware security. More than

100 students from 20 different universities have participated over the years. More than 100 benchmark designs for hardware Trojans and PUFs have been developed. ESC is funded by NSF, Intel, L3 Communications, Raytheon, and ARO. Participants have designed security primitives using emerging technologies (ESC 2014), designed a Trojan-infected hardware that evades a detection mechanism (ESC 2013), classified Trojan-free and Trojan-infected variants of a design (ESC 2012), attacked a processor using Trojans and designed physical unclonable functions (ESC 2011), and attacked a hardened design using Trojans (ESC 2010).

- **Special Session on emerging technology devices and security at IEEE GLSVLSI on VLSI, 2016**
  This special session has explored the security capabilities and threat in systems using emerging technology devices. It has brought together a wide-range of researchers to investigate questions such as "What are the security issues in emerging technology devices?"; "can we build effcient security primitives using these devices?" and "how can they support system security?"

- **Other services (Invited)**
  - Session chair at IEEE/ACM/EDAA Design Automation Conference, 2016
  - Session chair at IEEE International Conference on Hardware-Oriented Security and Trust (HOST), 2016
  - Session chair at IEEE Great-Lakes Symposium on VLSI (GLSVLSI), 2016
  - Session chair at IEEE VLSI Test Symposium, 2016
  - Session Chair at ARO Workshop on Trustworthy Hardware, 2013 and 2014
- **Professional Memberships**
  - Member, Institute of Electrical and Electronics Engineers (IEEE)
  - Member, Association of Computing Machinery (ACM)

Talks

- *Can we bell the CAD?*, US Department of Energy, 2017
- *Split Manufacturing*, Defense Microelectronic Activity, 2017
- *The evolution of logic locking*, Semiconductor Research Corporation, 2017
- *Can we bell the CAD?*, IEEE International Conference on System-on-Chip Design, 2016
- *Logic encryption*, DARPA Workshop on IP protection, 2016
- *Design approaches for trustworthy hardware from untrusted components*, Columbia Workshop on Hardware security, 2016
- *Trustworthy Integrated Circuit Design*, Texas A&M University, 2015
- *Trustworthy Integrated Circuit Design*, University of Southern California, 2015
- *Trustworthy Integrated Circuit Design*, University of Delaware, 2015
- *Trustworthy Integrated Circuit Design*, University of Pittsburgh, 2015
- *Trustworthy Integrated Circuit Design*, Pennsylvania State University, 2015
- *Trustworthy Integrated Circuit Design*, University of Texas at Dallas, 2015
- *Trustworthy Integrated Circuit Design*, University of Utah, 2015
- *Hardware Security and Trust Techniques for Low-Power Wireless Sensor SoC's*, Annual Review Meeting, Semiconductor Research Corporation, CMU, 2014
- *Reverse Engineering Integrated Circuits*, Security Summer School, New York University, 2014
- *Trustworthy Hardware Design*, SIGDA PhD forum, Design Automation Conference, 2014
- *Split Manufacturing – Panel Session*, IEEE VLSI Test Symposium, 2014
- *Design-for-Trust Techniques*, Security Summer School, New York University, 2013
- *Security Analysis of Logic Encryption*, Cisco Innovating Test Conference, 2013
- *Security Analysis of Logic Obfuscation*, Security Center of Excellence, Intel, 2012
- *Processor Encryption: Towards More Secure and Reliable Processors*, Kaspersky Cup Conference, 2011
- *Modeling a Memristor*, HP Labs, 2011
- **Conference Talks:** IEEE/ACM Design Automation Conference 2015, ACM Conference on Computer and Communications Security 2013, IEEE International Test Conference 2013, IEEE International On-Line Testing Symposium 2013, IEEE Design Automation and Test in Europe Conference 2013, IEEE/ACM Asia and South Pacific Design Automation Conference 2013, IEEE/ACM Design Automation Conference 2012, IEEE

International Symposium on Computer Design 2011, IEEE International Symposium on Circuits and Systems 2011, IEEE VLSI Test Symposium 2011, IEEE Symposium on VLSI Design 2011, IEEE Symposium on Hardware Oriented Security and Trust 2010, and IEEE Symposium on Nanoscale Architectures 2010

External Press

- Semiconductor Research Corp., *SRC Student Researchers Win Awards at DAC SIGDA Ph.D. Forum*, 2014
- eurekalert.org (AAAS), *NYU student cybersecurity researchers take honors at computer conferences*, 2013
- The National, *Confusion is the name of the game in outwitting microchip reverse engineers*, 2013
- New York University, *Hacking his way to the grand finals*, 2012
- Next Generation Communications, *Best Student Hardware Hackers and ID Protectors Win Trips to Compete in NYU-Poly Cyber Security Awareness Week*, 2011
- phys.org, *Beyond Watson: NYU-poly researchers create smarter circuits*, 2011
- IEEE Spectrum, *Creative Winners in Hardware Trojan Contest*, 2010
- redOrbit, *What Keeps NYU-Poly's Student Cyber Geniuses Awake Worrying?*, 2010
- Brooklyn Downtown star, *A Brooklyn lab's deviant magic*, 2010
- The Brooklyn Ink, *Hackers Converge in Brooklyn for NYU Computer Contest*, 2010
- GoMo News, *The Top 8 Ways to protect your smartphone*, 2010
- Mobile Blorge, *"White hat" students offer cellphone security tips*, 2010
- Ruters, *Brooklyn Transforms into Cyber Security Central as Student Hackers, Researchers and Professionals Compete in NYU-Poly Challenges*, 2010
- iPhoneapps.utilizer, *Found: Cyber Stars of the Future*, 2009