

Yier Jin

Endowed IoT Term Professor
Associate Professor
Department of Electrical and Computer Engineering
University of Florida, Gainesville, FL 32611
Phone: (352) 294-0401, **Email:** yier.jin@ece.ufl.edu
Home Page: <http://jin.ece.ufl.edu>

RESEARCH INTERESTS

- Internet of Things (IoT) and Cyber-Physical System (CPS) Design
- Trusted and resilient high-performance computing platforms
- Hardware-software co-design for system level security and protection
- Internet of Things (IoT) security
- Functional programming and proof writing for trusted IP cores
- Trustworthy SoC architecture

EDUCATION

Yale University, New Haven, Connecticut, USA
Ph.D. in Electrical Engineering, December 2012
Advisor: Yiorgos Makris
Thesis Title: “Trusted Integrated Circuits”

Zhejiang University, Hangzhou, China
M.S. in Electrical Engineering, June 2007
Advisors: Shiju Li, Xiaolang Yan and Haibin Shen
Thesis Title: “High Performance Finite Field Multipliers”
B.S. in Electrical Engineering, June 2005
Honors Graduate

PROFESSIONAL POSITIONS

Associate Professor 2017 - Present
Department of Electrical Engineering and Computer Science
University of Florida

Endowed IoT Term Professor 2017 - Present
The Warren B. Nelms Institute for the Connected World
Herbert Wertheim College of Engineering, University of Florida

Assistant Professor 2013 - 2017
Department of Electrical Engineering and Computer Science
University of Central Florida

Associate Partner 2014 - Present
Intel Collaborative Research Institute for Secure Computing

Cyber-Physical System Security Subcommittee Chair 2015 - 2016
IEEE Technical Committee on Cybernetics for Cyber-Physical Systems (CCPS)

Member 2015 - Present
Florida Institute for Cyber Security (FICS) at the University of Florida

Member 2016 - Present
VLSI Systems and Applications Technical Committee (VSA-TC),
IEEE Circuits and Systems Society (CASS)

Visiting Faculty Summer 2016, Summer 2017
AFRL Visiting Faculty Research Program

HONORS DISTINCTIONS

- **Best Paper Candidate**, Asian and South Pacific Design Automation Conference (ASP-DAC), 2018 (under selection)
- **Best Paper Candidate**, International Conference On Computer Aided Design (ICCAD), 2017 (under selection)
- **Endowed IoT Term Professorship**, University of Florida, 2017 - Present
- **Best Paper Award**, IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2017
- **Outstanding New Faculty Award**, ACM's Special Interest Group on Design Automation (SIGDA), 2017
- ACM Computing Reviews Notable Computing Books and Articles 2016, Hardware Category
- **Early CAREER Award**, Department of Energy (DoE), 2016
- **Best Paper Award**, Asian and South Pacific Design Automation Conference (ASP-DAC), 2016
- **First Place Award** (2011, 2016), **Second Place Award** (2008, 2013, 2014, 2015), **Third Place Award** (2009), New York University Cyber Security Awareness Week (CSAW) - Embedded System Challenge
- **Young Investigator Grant**, Southeastern Center for Electrical Engineering Education (SCEEE), 2015
- **Second Place Award**, CyberSEED IoT Security Challenge, University of Connecticut, 2015
- **Best Paper Award**, Design Automation Conference (DAC), 2015
- Travel Award, NSF-SRC-SIGDA-DAC Design Automation Summer School, 2009
- Honor Graduate, Zhejiang Provincial Institution of Higher Learning, The Educational Office of Zhejiang Province, China, 2005
- Excellent Graduate Award, Zhejiang University, 2005
- Undergraduate Scholarship, Zhejiang University, 2001–2005

PANELS

1. Hardware Security: Myth or Reality? *ACM/IEEE System Level Interconnect Prediction Workshop (SLIP)*, June 4, 2016
2. Hardware IP Protection Through Invasive and Non-Invasive Analysis, *IEEE Symposium on Hardware Oriented Security and Trust (HOST)*, May 5, 2016
3. Cyber Physical Systems Security: What Are the Challenges and Best Practices? *Florida Institute for Cybersecurity Research: Annual Conference on Cybersecurity*, February 9, 2016
4. ATARC Visionary Panel - Mobile Technology of the Future, *ATARC Federal Mobile Computing Summit*, August 12, 2015
5. Hacking Things: Security and Privacy Challenges in Internet of Things, *IEEE Conference on Communication and Network Security*, September 28, 2015

TUTORIALS

1. **Yier Jin**, "The The Emergence of Hardware Security," *IEEE International Conference on Data Science in Cyberspace (DSC)*, Shenzhen, China, June 2017.
2. Chip Hong Chang, and **Yier Jin**, "The Emergence of Hardware Oriented Security and Trust," *22nd Asia and South Pacific Design Automation Conference (ASP-DAC)*, Chiba, Japan, January 2017.
3. **Yier Jin**, "Introduction to Cyber-Physical System Security: From the Hardware Perspective," *8th IEEE International Workshop on Information Forensics and Security (WIFS)*, Abu Dhabi, UAE, December 2016.

4. **Yier Jin** and Ahmad-Reza Sadeghi, "IoT Security and Privacy Challenges and Solutions," *Embedded Systems Week (ESWEEK)*, Pittsburgh, PA, October 2016.

PUBLICATIONS

A. BOOK CHAPTER

1. Hiroto Yasuura, Chong-Min Kyung, Yongpan Liu, and Youn-Long Lin (Editors), "Smart Sensors at the IoT Frontier," Springer, 2017 (Orlando Arias, Kelvin Ly, and **Yier Jin**, "Security and Privacy in IoT Era")
2. S. Bhunia, S. Ray, and S. Sur-Kolay (Editors), "Fundamentals of IP and SoC Security - Design, Verification and Debug," Springer, 2017 (Xiaolong Guo, Raj Gautam Dutta, and **Yier Jin**, "Chapter 10. IP Trust Validation Using Proof-Carrying Hardware")
3. Prabhat Mishra, Swarup Bhunia, and Mark Tehranipoor (Editors), "Hardware IP Security and Trust," Springer, 2017 (Raj Gautam Dutta, Xiaolong Guo and **Yier Jin**, "Chapter 4. IP Trust: The Problem and Design/Validation-Based Solution")
4. Chip-Hong Chang, Miodrag Potkonjak (Editors), "Secure System Design and Trustable Computing," Springer, 2016 (**Yier Jin**, Dimitry Maliuk, Yiorgos Makris, "Chapter 7. Hardware Trojan Detection in Analog/RF Integrated Circuits")
5. Mark Tehranipoor, Cliff Wang (Editors), "Introduction to Hardware Security and Trust," Springer, 2011 (**Yier Jin**, Eric Love, Yiorgos Makris, "Chapter 16. Design for Hardware Trust")

B. JOURNAL PUBLICATIONS

1. Xiaolong Guo, Raj Gautam Dutta, Prabhat Mishra, and **Yier Jin**, "Automatic Code Converter Enhanced PCH Framework for SoC Trust Verification," *IEEE Transactions on Very Large Scale Integration System (TVLSI)*, vol. 25, no. 12, 2017.
2. Juan Wang, Hong Zhi, Yuhang Zhang, and **Yier Jin**, "Enabling Security-enhanced Attestation With Intel SGX for Remote Terminal and IoT," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, 2017. (to appear)
3. Jiaji He, Yiqiang Zhao, Xiaolong Guo, **Yier Jin**, "Hardware Trojan Detection through Chip-Free Electromagnetic Side-Channel Statistical Analysis," *IEEE Transactions on Very Large Scale Integration System (TVLSI)*, 2017. (to appear)
4. **Yier Jin**, Xiaolong Guo, Raj Gautam Dutta, Mohammad-Mahdi Bidmeshki, and Yiorgos Makris, "Data Secrecy Protection through Information Flow Tracking in Proof-Carrying Hardware IP (Part I: Framework Fundamentals)," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 12, no. 10, pp. 2416-2429, 2017.
5. Mohammad-Mahdi Bidmeshki, Xiaolong Guo, Raj Gautam Dutta, **Yier Jin**, and Yiorgos Makris, "Data Secrecy Protection through Information Flow Tracking in Proof-Carrying Hardware IP (Part II: Framework Automation)," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 12, no. 10, 2430-2443, 2017.
6. Yu Liu, **Yier Jin**, Aria Nosratinia, and Yiorgos Makris, "Silicon Demonstration of Hardware Trojan Design and Detection in Wireless Cryptographic ICs," *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, vol. 25, no. 4, pp. 1506-1519, 2017.
7. Jacob Wurm, **Yier Jin**, Yang Liu, Shiyang Hu, Kenneth Heffner, Fahim Rahman, and Mark Tehranipoor, "Introduction to Cyber-Physical System Security: A Cross-Layer Perspective," *IEEE Transactions on Multi-Scale Computing Systems (TMSCS)*, vol. 3, no. 3, pp. 215-227, 2017.
8. Travis Meade, Shaojie Zhang, and **Yier Jin**, "IP Protection Through Gate-Level Netlist Security Enhancement," *Integration, the VLSI Journal*, vol. 58, pp. 563-570, 2017.

9. Xiaolong Guo, Raj Gautam Dutta, and **Yier Jin**, “Eliminating the Hardware-Software Boundary: A Proof-Carrying Approach for Trust Evaluation on Computer Systems,” *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 12, no. 2, pp. 405-417, 2017.
10. Yu Bi, Kaveh Shamsi, Jiann-Shiun Yuan, **Yier Jin**, Michael Niemier, and X. Sharon Hu, “Tunnel FET Current Mode Logic for DPA-Resilient Circuit Designs,” *IEEE Transactions on Emerging Topics in Computing (TETC)*, vol. 5, no. 3, pp. 340-352, 2017.
11. Kan Xiao, Domenic Forte, **Yier Jin**, Ramesh Karri, Swarup Bhunia, and M. Tehranipoor, “Hardware Trojans: Lessons Learned After One Decade of Research,” *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 22, no. 1, pp. 6:1-6:23, 2016.
12. Sandip Ray, **Yier Jin**, and Arijit Raychowdhury, “The Changing Computing Paradigm with Internet of Things: A Tutorial Introduction,” *IEEE Design & Test (D&T)*, vol. 33, issue. 2, pp. 76-96, 2016.
13. Yu Bi, Kaveh Shamsi, Jiann-Shiun Yuan, Pierre-Emmanuel Gaillardon, Giovanni De Micheli, Xunzhao Yin, X. Sharon Hu, Michael Niemier, and **Yier Jin**, “Emerging Technology based Design of Primitives for Hardware Security,” *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 13, issue 1, pp. 3:1-3:19, 2016.
14. Orlando Arias, Jacob Wurm, Khoa Hoang, and **Yier Jin**, “Privacy and Security in Internet of Things and Wearable Devices,” *IEEE Transactions on Multi-Scale Computing Systems (TMSCS)*, vol. 1, issue 2, pp. 99-109, 2015.
15. **Yier Jin**, “Introduction to Hardware Security,” *Electronics*, vol. 4, issue. 4, pp. 763-784, 2015.
16. Yu Bi, Jiann-Shiun Yuan, and **Yier Jin**, “Beyond the Interconnections: Split Manufacturing in RF Designs,” *Electronics*, vol. 4, issue. 3, pp. 541-564, 2015.
17. Daniela Oliveira, Nicholas Wetzels, Max Bucci, Jesus Navarro, Dean Sullivan, and **Yier Jin**, “Hardware-Software Collaboration for Secure Coexistence with Kernel Extensions,” *ACM SIGAPP Applied Computing Review (ACR)*, vol. 14, no. 3, pp. 22-35, September 2014.
18. Eric Love, **Yier Jin**, and Yiorgos Makris, “Proof-Carrying Hardware Intellectual Property: A Pathway to Trusted Module Acquisition,” *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 7, no. 1, pp. 25-40, January 2012.
19. **Yier Jin**, and Yiorgos Makris, “Hardware Trojans in wireless cryptographic integrated circuits,” *IEEE Design & Test on Computers (D&T)*, vol. 27, pp. 10-25, 2010.
20. Haibin Shen, and **Yier Jin**, “Low Complexity Bit Parallel Multiplier for $GF(2^m)$ Generated by Equally-Spaced Trinomials,” *Information Processing Letters (IPL)*, vol. 107, no. 6, 2008, pp. 211-215.
21. **Yier Jin**, Haibin Shen, Huafeng Chen, and Xiaolang Yan, “Research of Fast Modular Multiplier for a Class of Finite Fields,” *Journal of Electronics (China)*, vol. 25, no. 4, 2008, pp. 482-487.

C. NEWSLETTER

1. **Yier Jin**, “Hardware Security: Past, Current, and Future,” *VLSI Circuits and Systems Letter*, vol. 1, no. 1, pp. 11-15, April 2015. (invited)
2. Dean Sullivan, **Yier Jin**, “What is Hardware-based Cybersecurity?” *ACM/SIGDA E-Newsletter*, vol. 45, no. 4, April 2015. (invited)

1. Tao Liu, Lei Jiang, **Yier Jin**, Gang Quan, and Wujie Wen, "PT-Spike: A Precise-Time-Dependent Single Spike Neuromorphic Architecture with Efficient Supervised Learning," *23rd Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2018. (to appear)
2. Qi Liu, Tao Liu, Zihao Liu, Yanzhi Wang, **Yier Jin**, and Wujie Wen, "Security Analysis and Enhancement of Model Compressed Deep Learning Systems under Adversarial Attacks," *23rd Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2018. (to appear)
3. Xiaolong Guo, Raj Gautam Dutta, Jiaji He, and **Yier Jin**, "PCH Framework for IP Runtime Security Verification," *Asian Hardware Oriented Security and Trust (AsianHOST)*, 2017. (to appear)
4. Zhen Ling, Kaizheng Liu, Yiling Xu, **Yier Jin**, and Xinwen Fu, "An End-to-End View of IoT Security and Privacy," *IEEE GLOBECOM*, 2017.
5. Tao Liu, Zihao Liu, Fuhong Lin, **Yier Jin**, Gang Quan, and Wujie Wen, "MT-Spike: A Multilayer Time-based Spiking Neuromorphic Architecture with Temporal Error Backpropagation," *International Conference On Computer Aided Design (ICCAD)*, 2017. (to appear)
6. Shaza Zeitouni, Ghada Dessouky, Orlando Arias, Dean Sullivan, Ahmad Ibrahim, **Yier Jin**, and Ahmad-Reza Sadeghi, "ATRIUM: Runtime Attestation Resilient Under Memory Attacks," *International Conference On Computer Aided Design (ICCAD)*, 2017. (to appear)
7. David Gens, Orlando Arias, Dean Sullivan, Christopher Liebchen, **Yier Jin**, and Ahmad-Reza Sadeghi, "LAZARUS: Practical Side-channel Resilient Kernel-Space Randomization," *International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2017. (to appear)
8. Orlando Arias, Dean Sullivan, and **Yier Jin**, "HA2lloc: Hardware-Assisted Secure Allocator," *Hardware and Architectural Support for Security and Privacy (HASP)*, 2017, pp. 8:1-8:7.
9. Travis Meade, Zheng Zhao, Shaojie Zhang, David Pan, and **Yier Jin**, "Revisit Sequential Logic Obfuscation: Attacks and Defenses," *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2017.
10. Kaveh Shamsi, Meng Li, Travis Meade, Zheng Zhao, David Z. Pan, and **Yier Jin**, "Cyclic Obfuscation for Creating SAT-Unresolvable Circuits," *GLSVLSI*, 2017, pp. 173-178.
11. Kaveh Shamsi, Meng Li, Travis Meade, Zheng Zhao, David Z. Pan, and **Yier Jin**, "Circuit Obfuscation and Oracle-guided Attacks: Who can Prevail?" *GLSVLSI*, 2017, pp. 357-362.
12. Raj Gautam Dutta, Xiaolong Guo, Teng Zhang, Kevin Kwiat, Charles Kamhoua, Laurent Njilla, and **Yier Jin**, "Estimation of Safe Sensor Measurements of Autonomous System Under Attack," *IEEE/ACM Design Automation Conference (DAC)*, 2017.
13. Kaveh Shamsi, Meng Li, Travis Meade, Zheng Zhao, David Z. Pan, and **Yier Jin**, "AppSAT: Approximately Deobfuscating Integrated Circuits," *IEEE Symposium on Hardware Oriented Security and Trust (HOST)*, 2017, pp. 46-51. **Best Paper Award**
14. Xiaolong Guo, Raj Gautam Dutta, and **Yier Jin**, "Proof-Carrying Hardware based IP Protection," *Government Microcircuit Applications and Critical Technology Conference (GOMACTech-17)*, 2017.
15. Raj Gautam Dutta, Xiaolong Guo, and **Yier Jin**, "Trusted Autonomous Systems under Sensor Attacks," *Government Microcircuit Applications and Critical Technology Conference (GOMACTech-17)*, 2017.

16. Nathalie Domingo, Bryan Pearson and **Yier Jin**, "Exploitations of Wireless Interfaces via Network Scanning," *International Conference on Computing, Networking and Communications (ICNC)*, 2017. (REU Site Paper)
17. Zihao Liu, Wujie Wen, Lei Jiang, **Yier Jin**, and Gang Quan, "A Statistical STT-RAM Retention Model for Fast Memory Subsystem Designs," *22nd Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2017.
18. Zhang Chen, Pingqiang Zhou, Tsung-Yi Ho, **Yier Jin**, "How Secure is Split Manufacturing in Preventing Hardware Trojan?" *IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, 2016.
19. Xiaolong Guo, Raj Gautam Dutta, Prabhat Mishra, and **Yier Jin**, "Automatic RTL-to-Formal Code Converter for IP Security Formal Verification," *17th International Workshop on Microprocessor and SOC Test and Verification (MTV)*, 2016.
20. Dean Sullivan, Orlando Arias, Ahmad-Reza Sadeghi, Lucas Davi, and **Yier Jin**, "Policy Agnostic Control-Flow Integrity," *Black Hat Europe*, 2016.
21. Kelvin Ly, Orlando Arias, Jacob Wurm, Khoa Hoang, Kaveh Shamsi, and **Yier Jin**, "Voting System Design Pitfalls: Vulnerability Analysis and Exploitation of a Model Platform," *IEEE International Conference on Computer Design (ICCD)*, 2016, pp. 149-152.
22. Travis Meade, Shaojie Zhang, Zheng Zhao, David Pan, and **Yier Jin**, "Gate-Level Netlist Reverse Engineering Tool Set for Functionality Recovery and Malicious Logic Detection," *International Symposium for Testing and Failure Analysis (ISTFA)*, 2016.
23. Raj Gautam Dutta, Xiaolong Guo, and **Yier Jin**, "Quantifying Trust in Autonomous System Under Uncertainties," 29th IEEE International System-on-Chip Conference (SOCC), 2016, pp. 362-367.
24. Meng Li, Kaveh Shamsi, Travis Meade, Zheng Zhao, Bei Yu, **Yier Jin**, and David Z. Pan, "Provably Secure Camouflaging Strategy for IC Protection," *International Conference On Computer Aided Design (ICCAD)*, 2016, pp. 28:1-28:8.
25. Kaveh Shamsi, Wujie Wen, and **Yier Jin**, "Hardware Security Challenges Beyond CMOS: Attacks and Remedies," *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2016, pp. 200-205.
26. Kelvin Ly and **Yier Jin**, "Security Challenges in CPS and IoT: from End-Node to the System," *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2016, pp. 63-68.
27. Kelvin Ly and **Yier Jin**, "Security Studies on Wearable Fitness Trackers," *38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 2016.
28. Dean Sullivan, Orlando Arias, Lucas Davi, Per Larsen, Ahmad-Reza Sadeghi, and **Yier Jin** "Strategy Without Tactics: Policy-Agnostic Hardware-Enhanced Control-Flow Integrity," *IEEE/ACM Design Automation Conference (DAC'16)*, 2016, pp. 83.2:1-6.
29. Nancy Cam-Winget, Ahmad-Reza Sadeghi, and **Yier Jin**, "Can IoT be Secured: Emerging Challenges in Connecting the Unconnected," *IEEE/ACM Design Automation Conference (DAC'16)*, 2016, pp. 71.3:1-6.
30. Adib Nahiyani, Domenic Forte, **Yier Jin**, Mark Tehranipoor, Xiao Kan, and Kun Yang, "Framework of Security Vulnerabilities in Finite State Machines," *IEEE/ACM Design Automation Conference (DAC'16)*, 2016, pp. 57.4:1-6.
31. Travis Meade, **Yier Jin**, Mark Tehranipoor, and Shaojie Zhang, "Gate-Level Netlist Reverse Engineering for Hardware Security: Control Logic Register Identification," *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2016, pp. 1334-1337.

32. Yu Bi, Kaveh Shamsi, Xunzhao Yin, Michael Niemier, Sharon Hu, and **Yier Jin**, "Enhancing Hardware Security with Emerging Transistor Technologies," *GLSVLSI*, 2016, pp. 305-310.
33. Xiaolong Guo, Raj Gautam Dutta, Prabhat Mishra, and **Yier Jin**, "Scalable SoC Trust Verification using Integrated Theorem Proving and Model Checking," *IEEE Symposium on Hardware Oriented Security and Trust (HOST)*, 2016, pp. 124-129.
34. Kaveh Shamsi and **Yier Jin**, "Security of Emerging Non-Volatile Memories: Attacks and Defenses," *IEEE VLSI Test Symposium (VTS)*, 2016.
35. Sandip Ray, Swarup Bhunia, **Yier Jin**, and Mark Tehranipoor, "[Extended Abstract] Security Validation in IoT Space," *IEEE VLSI Test Symposium (VTS)*, 2016.
36. Yu Bi, Kaveh Shamsi, Jiann-Shiun Yuan, Francois-Xavier Standaert, and **Yier Jin**, "Leverage Emerging Technologies For DPA-Resilient Block Cipher Design," *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, 2016, pp. 1538-1543.
37. An Chen, X. Sharon Hu, **Yier Jin**, Michael Niemier, Xunzhao Yin, "Using Emerging Technologies for Hardware Security Beyond PUFs," *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, 2016, pp. 1544-1549.
38. Travis Meade, Shaojie Zhang, and **Yier Jin**, "Netlist Reverse Engineering for High-Level Functionality Reconstruction," in *21st Asia and South Pacific Design Automation Conference (ASP-DAC 2016)*, 2016, pp. 655-660. **(Best Paper Award)**
39. Jacob Wurm, Orlando Arias, Khoa Hoang, Ahmad-Reza Sadeghi and **Yier Jin**, "Security analysis on consumer and industrial IoT Devices," in *21st Asia and South Pacific Design Automation Conference (ASP-DAC 2016)*, 2016, pp. 519-524.
40. Kaveh Shamsi, Pierre-Emmanuel Gaillardon, and **Yier Jin**, "Hardware Platform Protection Using Emerging Memory Technologies," *Government Microcircuit Applications and Critical Technology Conference (GOMACTech-16)*, 2016, pp. 21-24.
41. Travis Meade, Shaojie Zhang, Mark Tehranipoor, and **Yier Jin**, "A Comprehensive Netlist Reverse Engineering Toolset for IC Trust," *Government Microcircuit Applications and Critical Technology Conference (GOMACTech-16)*, 2016, pp. 281-284.
42. Yu Bi, Kaveh Shamsi, Jiann-Shiun Yuan, and **Yier Jin**, "More Than Moore in Security: Emerging Device based Low-Power Differentiate Power Analysis Countermeasures," *Government Microcircuit Applications and Critical Technology Conference (GOMACTech-16)*, 2016, pp. 467-470.
43. Kelvin Ly, Wei Sun, and **Yier Jin**, "Emerging Challenges in Cyber-Physical Systems: A Balance of Performance, Correctness, and Security," *IEEE Infocom CPSS Workshop*, 2016.
44. Sandip Ray, and **Yier Jin**, "Security Policy Enforcement in Modern SoC Designs," *International Conference On Computer Aided Design (ICCAD)*, 2015, pp. 345-350.
45. Xiaolong Guo, Raj Gautam Dutta, and **Yier Jin**, "Hierarchy-Preserving Formal Verification Methods for Pre-Silicon Security Assurance," *16th International Workshop on Microprocessor and SOC Test and Verification (MTV)*, 2015.
46. Kaveh Shamsi, Yu Bi, **Yier Jin**, Pierre-Emmanuel Gaillardon, Michael Niemier and X. Sharon Hu, "Reliable and High Performance STT-MRAM Architectures based on Controllable-Polarity Devices," *IEEE International Conference on Computer Design (ICCD)*, 2015, pp. 372-379.
47. Omar Nakhila, **Yier Jin**, and Cliff Zou, "Parallel Active Dictionary Attack on WPA2-PSK Wi-Fi Networks," *IEEE Military Communications Conference (MILCOM)*, 2015, pp. 665-670.

48. Yu Bi, Jiann-Shiun Yuan, and **Yier Jin**, "Split Manufacturing in Radio-Frequency Designs," *The 2015 International Conference on Security and Management (SAM)*, 2015, pp. 204-210.
49. Lucas Davi, Matthias Hanreich, Debayan Paul, Ahmad-Reza Sadeghi, Patrick Koerberl, Dean Sullivan, Orlando Arias, and **Yier Jin**, "HAFIX: Hardware-Assisted Flow Integrity Extension," *IEEE/ACM Design Automation Conference (DAC)*, 2015. **(Best Paper Award)**
50. Xiaolong Guo, Raj Gautam Dutta, **Yier Jin**, Farimah Farahmandi, and Prabhath Mishra, "Pre-Silicon Security Verification and Validation: A Formal Perspective," *IEEE/ACM Design Automation Conference (DAC)*, 2015.
51. Yang Liu, Shiyuan Hu, Jie Wu, Yiyu Shi, **Yier Jin**, Yu Hu, and Xiaowei Li, "Impact assessment of net metering on smart home cyberattack detection," *IEEE/ACM Design Automation Conference (DAC)*, 2015.
52. Charalambos Konstantinou, Michail Maniatakos, Fareena Saqib, Shiyuan Hu, Jim Plusquellic, and **Yier Jin**, "Cyber-Physical Systems: A Security Perspective," *European Test Symposium (ETS)*, 2015.
53. Jeff Biggers, Travis Meade, Shaojie Zhang, Youngok Pino, and **Yier Jin**, "Automated RTL Code Rebuilding through Netlist Analysis," *Government Microcircuit Applications and Critical Technology Conference (GOMACTech-15)*, 2015, pp. 155-158.
54. **Yier Jin**, "Innovative IoT Authentication Methods Leveraging Smart Sensors," *UCF Conference on Sensor Devices and Applications*, Oct 2015.
55. Ray Potter, **Yier Jin**, "Don't Touch That Dial: How Smart Thermostats Have Made Us Vulnerable," *RSA Conference*, 2015.
56. **Yier Jin**, "Security and Privacy in Internet of Things and Wearable Devices," *CHASE Conference on Secure/Trustworthy Systems and Supply Chain Assurance*, 2015.
57. Yu Bi, Pierre-Emmanuel Gaillardon, X. Sharon Hu, Michael Niemier, Jiann-Shiun Yuan, and **Yier Jin**, "Leveraging Emerging Technology for Hardware Security - Case Study on Silicon Nanowire FETs and Graphene SymFETs," *Asia Test Symposium (ATS)*, 2014, pp. 342-247.
58. **Yier Jin**, "Design-for-Security vs. Design-for-Testability: A Case Study on DFT Chain in Cryptographic Circuits," *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2014, pp. 19-24.
59. Dean Sullivan, Jeff Biggers, Guidong Zhu, Shaojie Zhang, and **Yier Jin**, "FIGHT-Metric: Functional Identification of Gate-Level Hardware Trustworthiness," *Design Automation Conference (DAC)*, 2014, pp. 173:1-173:4.
60. **Yier Jin**, and Dean Sullivan, "Real-Time Trust Evaluation in Integrated Circuits," *Design, Automation and Test in Europe Conference and Exhibition, (DATE)*, 2014.
61. **Yier Jin**, "EDA Tools Trust Evaluation through Security Property Proofs," *Design, Automation and Test in Europe Conference and Exhibition, (DATE)*, 2014.
62. **Yier Jin**, "Embedded System Security in Smart Consumer Electronics," *4th International Workshop on Trustworthy Embedded Devices (TrustedED 2014)*, 2014, pp. 59-59.
63. **Yier Jin**, Grant Hernandez, and Daniel Buentello, "Smart Nest Thermostat: A Smart Spy in Your Home," *Black Hat USA*, 2014.
64. **Yier Jin**, and Daniela Oliveira, "Trustworthy SoC Architecture with On-Demand Security Policies and HW-SW Cooperation," *5th Workshop on SoCs, Heterogeneous Architectures and Workloads (SHAW-5)*, 2014.
65. **Yier Jin**, and Yiorgos Makris, "A Proof-Carrying Based Framework for Trusted Microprocessor IP," *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, November 2013, pp. 824-829.

66. Yu Liu, **Yier Jin**, and Yiorgos Makris, "Hardware Trojans in Wireless Cryptographic ICs: Silicon Demonstration and Detection Method Evaluation," *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, November 2013, pp. 399-404.
67. **Yier Jin**, Dimitry Maliuk and Yiorgos Makris, "A Post-Deployment IC Trust Evaluation Architecture," *Proceedings of IEEE International On-Line Testing Symposium (IOLTS)*, July 2013, pp. 224-225. (invited)
68. **Yier Jin**, Bo Yang and Yiorgos Makris, "Cycle Accurate Information Assurance by Proof Carrying-Based Signal Sensitivity Tracing," *Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, June 2013, pp. 99-106.
69. Ozgur Sinanoglu, Naghmeh karimi, Jeyavijayan Rajendran, Ramesh Karri, **Yier Jin**, Dimitry Maliuk, Ke Huang, Yiorgos Makris, "Reconciling the IC Test and Security Dichotomy," *Proceedings of 18th IEEE European Test Symposium (ETS)*, May 2013, pp. 1-6.
70. **Yier Jin**, Michail Mihalidis and Yiorgos Makris, "Exposing Vulnerabilities of Untrusted Computing Platforms," *Proceedings of the IEEE International Conference on Computer Design (ICCD)*, 2012, pp. 131-134.
71. **Yier Jin**, and Yiorgos Makris, "Proof Carrying-Based Information Flow Tracking for Data Secrecy Protection and Hardware Trust," *Proceedings of VLSI Test Symposium (VTS)*, 2012, pp. 252-257.
72. **Yier Jin**, Dimitry Maliuk and Yiorgos Makris, "Post-Deployment Trust Evaluation in Wireless Cryptographic ICs," *Proceedings of the Design, Automation & Test in Europe (DATE)*, 2012, pp. 965-970.
73. **Yier Jin** and Yiorgos Makris, "PSCML: Pseudo-Static Current Mode Logic," *Proceedings of 18th IEEE International Conference on Electronics, Circuits, and Systems (ICECS)*, 2011, pp. 41-44.
74. **Yier Jin** and Yiorgos Makris, "Is Single Trojan Detection Scheme Enough?," *Proceedings of the IEEE International Conference on Computer Design (ICCD)*, 2011, pp. 305-308.
75. Eric Love, **Yier Jin** and Yiorgos Makris, "Enhancing Security via Provably Trustworthy Hardware Intellectual Property," *Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2011, pp. 12-17.
76. **Yier Jin** and Yiorgos Makris, "DFTT: Design-for-Trojan-Test," *Proceedings of 17th IEEE International Conference on Electronics, Circuits, and Systems (ICECS)*, 2010, pp. 1168-1171.
77. **Yier Jin**, Nathan Kupp and Yiorgos Makris, "Experiences in Hardware Trojan Design and Implementation," *Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2009, pp. 50-57.
78. **Yier Jin**, and Yiorgos Makris, "Hardware Trojan Detection Using Path Delay Fingerprint," *Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2008, pp. 51-57.
79. **Yier Jin**, and Haibin Shen, "Revisiting Scalable Modular Multiplication over $GF(2^m)$ for Elliptic Curve Cryptography," *Proceedings of 8th International Conference on Solid-State and Integrated Circuit Technology (ICSICT)*, 2006, pp. 2114-2117.
80. **Yier Jin**, Haibin Shen, and Rongquan You, "Implementation of SMS4 Block Cipher on FPGA," *Proceedings of International Conference on Communications and Networking in China (CHINACOM)*, 2006, pp. 1-4.
81. Haibin Shen, and **Yier Jin**, "Unbalanced Exponent Modular Reduction over Binary Field and Its Implementation," *Proceedings of International Conference on Innovative Computing, Information and Control (ICICIC)*, 2006, pp. 190-193.

82. Dawei Li, **Yier Jin**, Haibin Shen, and Xiaolang Yan, “Design of Random Number Generation Algorithm,” *Proceedings of International Conference on Computational Intelligence and Security (CIS)*, 2006, pp. 1287-1290.
83. Rongquan You, Haibin Shen, and **Yier Jin**, “Interconnect Estimation for Mesh-Based Reconfigurable Computing,” *Proceedings of The IFIP International Conference on Embedded and Ubiquitous Computing (EUC)*, LNCS 4096, 2006, pp. 766-775.

**INVITED
PRESENTATIONS**

- **SCx3 Cybersecurity Conference (keynote)**, Melbourne, FL November 2017
Title: “The Evolution of Hardware-Assisted Computing Systems for IoT”
- **Discover Financial Services**, Gainesville, FL October 2017
Title: “Security Enhanced Gateway for Multi-layer Smart Home IoT Payment System Protection” (Host: David Nelms)
- **Texas Instrument**, Dallas, TX July 2017
Title: “Security Challenges for SoC Designs in Internet of Things Era” (Host: Christy She)
- **IEEE International Workshop on Design Automation for Cyber-Physical Systems**, Austin, TX June 2017
Title: “Security and Privacy Challenges in Internet of Things” (Host: Xin Li)
- **Warren B. Nelms Institute for the Connected World (Opening Ceremony), University of Florida**, Gainesville, FL April 2017
Title: “Security and Privacy Challenges in Internet of Things” (Host: John Harris)
- **Notre Dame University**, Notre Dame, IN February 2017
Title: “Internet of Things Design and Security from a Cross-Layer Perspective” (Host: Sharon Hu)
- **Texas A & M University**, College Station, TX February 2017
Title: “Internet of Things Design and Security from a Cross-Layer Perspective” (Host: Alex Sprintson)
- **Cisco**, Gainesville, FL February 2017
Title: “Internet of Things (IoT): Design and Security” (Host: Yousef Iskander)
- **University of Florida**, Gainesville, FL January 2017
Title: “Internet of Things Design and Security from a Cross-Layer Perspective” (Host: William Eisenstadt)
- **Florida Security Workshop**, Tampa, FL December 2016
Title: “IoT Security Training Platforms for Professionals and Engineers” (Host: Simon Ou)
- **Florida Center of Cybersecurity**, Tampa, FL October 2016
Title: “Demonstration: Trusted CPS Platform Development”
- **University of George**, Athens, GA September 2016
Title: “IoT Security: From a Cross-Layer Perspective” (Host: Kang Li)
- **EDA Workshop**, Hong Kong, China August 2016
Title: “Arm-Race on Logic Obfuscation and IC Camouflaging for IP Protection” (Host: Zili Shao)
- **Air Force Research Lab (AFRL)**, Rome NY August 2016
Title: “Security Challenges in CPS and IoT: from End-Node to the System” (Host: Charles Kamhoua and Kevin Kwiatt)
- **Syracuse University**, Syracuse, NY July 2016
Title: “Security Vulnerability Database for IoT” (Host: Yanzhi Wang)
- **International Workshop on Hardware Security**, Beijing, China June 2016
Title: “Hardware’s Active Role in Cybersecurity” (Host: Xiaoxiao Wang)

- **University of Delaware**, Newark, DE May 2016
Title: “Introduction to Hardware Security: Past, Current and Future” (Host: Chengmo Yang)
- **The 4th Asia Workshop on Smart Sensor System (AWSSS 2016)**, Beijing, China March 2016
Title: “Security and Privacy in IoT Era: From Attack to Defense” (Host: Yongpan Liu)
- **FICS Annual Conference on Cybersecurity**, Gainesville, FL Feb 2016
Title: “IoT Security: From Hacking to Defense” (Host: Mark Tehranipoor and Patrick Traynor)
- **Cisco**, Gainesville, FL Dec 2015
Title: “Remote Assessment for IoT Security: Tools, Metrics, and Test Platforms” (Host: Bill Eklow)
- **National Institute of Standards and Technology (NIST)**, Gainesville, FL Dec 2015
Title: “Remote Assessment for IoT Security: Tools, Metrics, and Test Platforms” (Host: Donna Dodson)
- **University of Texas, San Antonio**, San Antonio, TX Nov 2015
Title: “Security and Privacy on IoT and Wearable Devices” (Host: Jianwei Niu)
- **ARO Workshop on Cryptography and Hardware Security for the Internet of Things**, College Park, MD Oct 2015
Title: “Case study on IoT Device Security and Privacy”
- **2015 China Internet Security Conference (Keynote Speech)**, Beijing, China Sep 2015
Title: “Smart vs. Security: IoT Security and Protections”
- **Notre Dame University**, Notre Dame, IN Sep 2015
Title: “Introduction to Hardware Security - Formal Methods, IoT Security, and Reverse Engineering” (Host: X. Sharon Hu)
- **NIST - Cybersecurity Innovation Forum**, Washington, DC Sep 2015
Title: “Hardware Trust and Integrity: The First Step Toward Securing Computer Systems” (Host: Andrew Regenscheid)
- **Cisco**, Gainesville, FL Sep 2015
Title: “IoT Security” (Host: Tony Jeffs)
- **National Security Campus**, Gainesville, FL Aug 2015
Title: “Introduction to Hardware Security - Formal Methods, IoT Security, and Reverse Engineering” (Host: Perry Tapp)
- **Honeywell - FICS**, Gainesville, FL Jun 2015
Title: “IoT/Hardware Security” (Host: Mark Tehranipoor)
- **Raytheon - FICS**, Gainesville, FL Jun 2015
Title: “Automated Functionality Rebuilding Through Netlist Reverse Engineering” (Host: Mark Tehranipoor)
- **Trustworthy Hardware Workshop** New York, NY Nov 2014
Title: “Computer System Protection through Run-time Hardware-Software Collaboration,” (Host: Ramesh Karri)
- **University of George**, Athens, GA Sep 2014
Title: “Computer System Protection through Hardware-Software Collaboration” (Host: Kang Li)
- **Pennsylvania State University**, State College, PA Sep 2014
Title: “Computer System Protection through Run-Time Hardware-Software Collaboration” (Host: Vijaykrishnan Narayanan)

- **University of Connecticut**, Storrs, CT Aug 2014
Title: “Embedded System Security in Smart Consumer Electronics: A Case Study on Google Nest Thermostat” (Host: Domenic Forte)
- **Information Sciences Institute/USC** Washington, D.C. May 2014
Title: “Security in Silicon - Challenges and Opportunities Ahead” (Host: Youngok Pino)
- **Intel Corp.** Hillsboro, OR Nov 2013
Title: “Proof-Carrying Based Trusted Embedded System Design and Secure SoC Integration” (Host: David Ott and Mukesh Ranjan)
- **Trustworthy Hardware Workshop** New York, NY Nov 2013
Title: “Trusted Embedded System Design Through the Unification of Trusted Third-Party Software Programs and Hardware IP Cores” (Host: Cliff Wang)
- **Northeastern University** Boston, MA Apr 2012
Title: “Trusted Integrated Circuits” (Host: Edmund Yeh)
- **University of New Mexico** Albuquerque, NM Apr 2012
Title: “Trusted Integrated Circuits” (Host: Nasir Ghani)
- **Stony Brook University** New York, NY Apr 2012
Title: “Trusted Integrated Circuits” (Host: Kenneth Short)
- **University of Maryland** College Park, MD Mar 2012
Title: “Trusted Integrated Circuits” (Host: Gang Qu)
- **George Mason University** Fairfax, VA Mar 2012
Title: “Trusted Integrated Circuits” (Host: Kris Gaj)
- **Illinois Institute of Technology** Chicago, IL Mar 2012
Title: “Trusted Integrated Circuits” (Host: Kui Ren)
- **Intel Corp.** Hillsboro, OR Jan 2012
Title: “Trusted Integrated Circuits and Proof Carrying-based Hardware Intellectual Property Protection” (Host: Dhinesh Manoharan)

RESEARCH FUNDING

- NSF / CNS, 1739736, “CPS: Medium: Security Certification of Autonomous Cyber-Physical Systems,” 2017 - 2021 (PI: Yier Jin, co-PI: Teng Zhang, \$830K)
- Department of Energy (DOE) Early Career Research Program, “Resilient and Robust High Performance Computing Platforms for Scientific Computing Integrity,” 2016 - 2021 (\$750K)
- NSF / CISE, 1704470, “SaTC: TTP: Medium: Collaborative: RESULTS: Reverse Engineering Solutions on Ubiquitous Logic for Trustworthiness and Security,” 2017 - 2020 (PI: Jia Di, co-PIs: Yier Jin, Shaojie Zhang, \$800K)
- NSF / DGE, 1723587, “SaTC: EDU: Online Digital Forensics Courses and Labs for Students and Professionals,” 2017 - 2019 (PI: Yier Jin, co-PI: Cliff Zou, \$300K)
- CISCO, “A Comprehensive Framework for IoT Security and Privacy Evaluation Through Quantitative Metric,” 2017 - 2019 (PI: Yier Jin, Co-PIs: Mark Tehranipoor, and Swarup Bhunia, \$220K)
- Army Research Office (ARO), “Bridging the Hardware-Software Gap: A Proof-Carrying Approach for Computer Systems Trust Evaluation,” 2016 - 2019 (\$330K)
- Florida Center for Cybersecurity (FC2) Collaborative Seed Grant Program, “Helmet: Deep Neural Network Protection Against Adversarial Attacks,” 2017 - 2018 (PI: Yier Jin, co-PI: Wujie Wen, \$50K)
- Semiconductor Research Corporation (SRC), “Framework for Automated and Systematic Security Assessment of Modern SoCs,” 2016 - 2018 (PI: Mark Tehranipoor, co-PIs: Swarup Bhunia, Domenic Forte, and Yier Jin, \$200K)

- Florida Center for Cybersecurity (FC2) Capacity Building Program, “Internet of Things Design and Security - An Online Course Development for Academia, Industry, and Government,” 2017 - 2018 (PI: Yier Jin, co-PI: Nasir Ghani, \$100K)
- NSF / EHR, 1643835, “Collaborative Research: Florida IT Pathways to Success (Flit-Path),” 2016 - 2021 (Cite PI: Mostafa Bassiouni, Cite co-PIs: Michael Georgiopoulos, Yier Jin, Mark Heinrich, Pamela Wisniewski, Fei Liu, and Boqing Gong, \$1.5M)
- NSF / CISE, CNS 1560302, “REU Site: Research Experiences in the Internet of Things,” 2016 - 2019 (PI: Damla Turgut, co-PI: Yier Jin, \$360K)
- NSF / EEC, 1611019, “RET Site: Collaborative Multidisciplinary Engineering Design Experiences for Teachers (CoMET),” 2016 - 2019 (PI: Hyoung Jin Cho, Co-PI: Damla Turgut, Senior Personnel: Yier Jin, Jihua Gou, Damian Dechev, Mingjie Lin, Woo Hyoung Lee, and Reza Abdolvand, \$595K)
- Florida Center for Cybersecurity (FC2) Collaborative Seed Grant Program, “Smart Grid Security Protection through Cross-Layer Approaches,” 2015 - 2017 (PI: Yier Jin, co-PI: Yao Liu, Cliff Zou, \$100K)
- CISCO, “Verification of IP Security and Trust,” 2016 - 2017 (PI: Prabhat Mishra, co-PI: Yier Jin, \$200K)
- Air Force Research Lab (AFRL), “Smart grid Security Protection through Cross-Layer Approaches - Thwarting Fault Injection Attacks,” 2016 (\$10K)
- NSF / CISE, CNS 1319105, “TWC: Small: Collaborative: Toward Trusted 3rd-Party Microprocessor Cores: A Proof Carrying Code Approach,” 2013 - 2017 (PI: Yier Jin, co-PI: Yiorgos Makris, \$450K) (REU Supplement \$32K)
- UCF In-House Award, “Trustworthiness Evaluation in Integrated Circuits,” 2015 - 2016, \$7.5K
- UCF COS/ORC SEED Grant, “SmartPhrog: A Responsive Low-Cost High-Performance Bioacoustic Solution Using the Raspberry Pi Single-Board Computer for Frog Population Monitoring,” 2015 - 2016 (PI: Anna Savage, co-PI: Shaojie Zhang, Yier Jin, \$36K)
- SCEEE/Woody Everett Research Initiation Grants, “Avalanche Effect in Cyber-Physical Systems Security Under Large-Scale Cyberattacks on Smart Devices,” 2015 - 2016 (\$32K)

TEACHING EXPERIENCE

Instructor for Courses Jul 2017 - Present
Electrical and Computer Engineering Department, University of Florida

- Undergraduate Course: EEL 4930 - Microprocessor II (aka IoT Design)

Instructor for Courses Dec 2012 - Present
Electrical and Computer Engineering Department, University of Central Florida

- Undergraduate Course: EEL 4742 - Embedded Systems
- Graduate Course: EEE 6347 - Trustworthy Hardware
- Graduate Course: EEE 5390C - Full Custom VLSI Design
- Undergraduate Course: EEE 4346C - Hardware Security and Trusted Circuit Design

Teaching Fellow Fall 2010, Fall 2008
School of Engineering and Applied Science, Yale University

- Graduate Course: EENG875 - Introduction to VLSI System Design

Teaching Fellow Spring 2010
School of Engineering and Applied Science, Yale University

- Undergraduate Course: EENG201b - Introduction to Computer Engineering

**CURRENT
PHD STUDENTS**

- Xiaolong Guo since Aug 2013
- Dean Sullivan since Jan 2014
- Raj Gautam Dutta since Aug 2014
- Kaveh Shamsi since Aug 2014
- Travis Meade (co-advised by Dr. Shaojie Zhang) since Aug 2014
- Orlando Arias since Aug 2016
- Kelvin Ly since Aug 2016

**CURRENT
UNDERGRAD**

- Jacob Hazelbaker
- Andrew Hughes

**CURRENT
HIGH SCHOOL
TEACHERS**

- Lauren Bracken (RET Teacher)
- James Ebbert (RET Teacher)
- Katherine Grady (RET Teacher)
- Jared Herretes (RET Teacher)
- Chad Hobby (RET Teacher)
- Junior Jn-Baptiste (RET Teacher)
- Kevin Scott (RET Teacher)
- Ronda Smucz (RET Teacher)
- Erika Trnka (RET Teacher)
- Jazmine Williams (RET Teacher)

**PREVIOUS
PHD STUDENTS**

- Travis Meade (co-advised by Dr. Shaojie Zhang)
- Yu Bi (co-advised by Dr. Peter Yuan)

**PREVIOUS
MS STUDENTS**

- Bo Hu
- Heather Lawrence

**PREVIOUS
UNDERGRAD**

- Alexis Drayton
- Coleman Rogers
- Jacob Wurm
- Khoa Hoang
- Kayshaunna Williams (REU Site Student)
- Bryan Pearson (REU Site Student)
- Nathalie Domingo (REU Site student)
- Thomas Louisville
- Andrew Mendoza
- Igor Prokopenko (Associate Information Security and Compliance Analyst at Publix Super Markets)
- Patrick Armengol (Graduate student at the Florida International University)
- Grant Hernandez (PhD student at the University of Florida)
- Dean Sullivan (PhD student at the University of Central Florida)
- Brandon Frazer (Associate electrical engineer at Mitsubishi Power Systems Americas)
- Ryan Dixon (Electrical engineer associate at Lockheed Martin)

- Victor Medina
- Danny Aybar
- Ritika Oswal
- Roland Anderson
- Richard Klimek
- Jeff Biggers
- Henry Chan

**INSTITUTIONAL
SERVICE**

- UF Semmoto Professor Search Committee Aug 2017 - Present
- UF Undergraduate EE Curriculum Committee Jul 2017 - Present
- UCF CpE Curriculum Oversight and Review Committee (CORC) May 2016 - Jun 2017
- UCF Cyber Cluster faculty search committee Sep 2015 - Jun 2017
- UCF Computer Engineering faculty search committee Oct 2014 - Jun 2016
- UCF ECE representative on the cybersecurity task force committee Aug 2014 - Jun 2017
- Faculty Library Representative for the Electrical and Computer Engineering Division of the Department of Electrical Engineering and Computer Science, University of Central Florida 2013 - 2017
- PhD Thesis Committee
 - Wei Liang (Advisor: Dr. Juin J. Liou and Dr. Kalpathy B. Sundaram)
 - Miao Meng (Advisor: Dr. Juin J. Liou and Dr. Kalpathy B. Sundaram)
 - Sirui Luo (Advisor: Dr. Juin J. Liou)
 - Zhixin Wang (Advisor: Dr. Juin J. Liou)
 - Jianling Yin (Advisor: Dr. Jun Wang)
 - Yunfeng Xi (Advisor: Dr. Juin J. Liou)
 - Jun Ding (Advisor: Dr. Nancy Hu)
 - Ruijun Wang (Advisor: Dr. Jun Wang)
 - Yu Bai (Advisor: Dr. Mingjie Lin)
 - Adithya Prakash (Advisor: Dr. Kalpathy B. Sundaram)

**PROFESSIONAL Associate Editor
SERVICE**

- Journal of Network and Information Security, Chinese (June 2017 - Present)
- Springer Journal of Hardware and System Security (June 2016 - Present)
- Integration, the VLSI Journal (June 2016 - Present)
- IET Cyber-Physical Systems: Theory & Applications (June 2016 - Present)
- IET Computers & Digital Techniques (March 2016 - Present)
- IEEE SMC Society Technical Committee on CCPS Newsletter (September 2015 - Present)

Guest Editor

- Springer Journal of Hardware and Systems Security. Special Issue on Secure and Trustworthy Computing Devices in the IoT Regime.
- IEEE Transactions on Multi-Scale Computing Systems. Special Issue/Section on Hardware/Software Cross-Layer Technologies for Trustworthy and Secure Computing.

Proposal Panelist/Reviewer

- Department of Energy (DoE), 2017
- Deutsche Forschungsgemeinschaft (German Research Foundation), 2016
- Department of Energy (DoE), 2016
- Department of Energy (DoE), Small Business Innovation Research (SBIR), 2016
- Foundation for Polish Science (FNP), 2016
- Florida Center of Cybersecurity (FC2) review panel, 2015, 2016
- CHIST-ERA review panel, 2016
- Ontario Research Fund - Research Excellence (ORF-RE), 2016

Conference/Workshop (Co-)Founder

- IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST)
- Internet of Things (IoT) and Automotive Security Workshop (IASW '17) affiliated to the IEEE International Symposium on Hardware Oriented Security and Trust (HOST '17)

Conference/Workshop (Co-)Chair

- IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST '16, '17)
- IEEE International Workshop on Design Automation for Cyber-Physical Systems (CPSDA), 2016, 2017
- Internet of Things (IoT) and Automotive Security Workshop (IASW '17), affiliated to the IEEE International Symposium on Hardware Oriented Security and Trust (HOST '17)
- Cyber-Physical Systems Security & Privacy Workshop (CPSSP '17), affiliated to the IEEE International Conference on Data Science in Cyberspace (IEEE DSC '17)
- SIGDA/DAC International Hardware Design Contest 2017
- IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2017)
- The First Florida Security Workshop, 2016
- Design Automation Summer School (DASS '16, '17)
- IEEE INFOCOM Workshop on Cross-Layer Cyber-Physical Systems Security (CPSS), 2016

Organizing Committee

- IEEE International Symposium on Hardware-Oriented Security and Trust (HOST '15, '16, '17, '18)
- Asia and South Pacific Design Automation Conference (ASP-DAC '17, '18)
- ICCAD Workshop on Design Automation for Analog and Mixed-Signal (AMS) Circuits 2017
- 36th IEEE International Conference on Consumer Electronics (ICCE '18)
- IEEE International Midwest Symposium on Circuits and Systems (MWSCAS '17)
- IEEE International Conference on Computer Design (ICCD '17)
- Security B-Sides Orlando, 2015, 2016.
- Asia Workshop on Smart Sensor System (AWSSS '16)
- International Symposium on VLSI Design and Test (VDATE '14)

Technical Program Committee

- The 27th International Conference on Computer Communication and Networks (ICCCN '18)
- ACM Student Research Competition at ICCAD (SRC@ICCAD '16, '17)
- The 30th International Conference on VLSI Design and 16th International Conference on Embedded Systems (VLSID '17, '18)
- The 18th International Symposium on Quality Electronic Design (ISQED '17, '18)
- Attack and Solutions in Hardware Security Co-located with ACM CCS (ASHES '17)
- IEEE International Symposium on Nanoelectronic and Information Systems (iNIS '15, '16, '17)
- IEEE International System-on-Chip Conference (SOCC '15, '16, '17)
- Smart Card Research and Advanced Application Conference (CARDIS '17)
- 12th EAI International Conference on Security and Privacy in Communication Networks (SecureComm '16, '17)
- International Test Conference (ITC '15, '16, '17)
- SIGDA PhD Forum at DAC 2016, 2017
- Hardware and Architectural support for Security and Privacy workshop (HASP '17)
- The 24th ACM Conference on Computer and Communications Security (CCS '17)
- The 1st International Test Conference in Asia (ITC-Asia '17)
- IEEE/ACM International Conference on Computer-Aided Design (ICCAD '17)
- The 1st International Workshop on Energy-Aware Computing and Communication (ECC) for Networked Cyber-Physical Systems (NCPS) '17
- The Fifth International Workshop on Security in Cloud Computing (AsiaCCS-SCC '17)
- Great Lake Symposium on VLSI (GLSVLSI '16, '17)
- International Workshop on Assured Cloud Computing and QoS Aware Big Data (WACC '17)
- IEEE Computer Society Annual Symposium on VLSI (ISVLSI '14, '15, '16, '17)
- ACM Asia Conference on Computer and Communications Security (ASIACCS '17)
- IEEE International Workshop on Information Forensics and Security (WIFS '16)
- International Conference on Communication and Network Security (ICCNS '16)
- Network and Distributed System Security Symposium (NDSS '16)
- International Verification and Security Workshop (IVSW '16)
- International Symposium for Testing and Failure Analysis (ISTFA '16)
- IEEE International Conference on Computer Design (ICCD '12, '15, '16)
- 37th IEEE Real-Time Systems Symposium (RTSS '16)
- 14th International Conference on Applied Cryptography and Network Security (ACNS '16)
- IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC '15, '16)
- Design Automation Conference (DAC '15, '16)
- The 28th Conference on VLSI Design and the 15th Conference on Embedded Systems (VLSI Design '16)
- Asia and South Pacific Design Automation Conference (ASP-DAC '16)
- The 13th International Conference on Information Technology (ICIT '14)

- The 23rd Asian Test Symposium (ATS '14)
- IEEE International Symposium on Hardware Oriented Security and Trust (HOST '14)
- IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT '12)