Qiaoyan Yu

Contact Information

Kingsbury W215, 33 Academic Way, Durham, NH 03824 qiaoyan.yu@unh.edu

Research Expertise

- Hardware security with special emphasis on Trojan detection/mitigation, side-channel (power) analysis attack, and three-dimensional (3D) integrated circuit (IC) security, FPGA security;
- Cybersecurity with special emphasis on Internet-of-Things (IoT), embedded systems, communication protocol interface;
- Approximate computing systems, machine learning, artificial neural network;
- Error control coding and fault-tolerant on-chip communication;
- Cyber-physical system with special emphasis on automobile security.

Education

University of Rochester, Rochester, NY

Ph.D., Electrical Engineering, May 2011

- Thesis Topic: *Transient and Permanent Error Management for Networks-on-Chip*
- Advisor: Paul Ampadu, Ph.D.

M.S., Electrical Engineering, May 2007

Zhejiang University, Hangzhou, China

M.S., Information Science & Electronic Engineering, March 2005

Xidian University, Hangzhou, China

B.S., Telecommunications Engineering, July 2002

Work Experience

Professor July 2021 to Present

Department of Electrical and Computer Engineering,
University of New Hampshire

- Research interests: hardware security, cybersecurity, approximate computing, Internet-of-Things, edge device and network security for advanced manufacturing, embedded systems, cyber-physical system, hardware reliability, VLSI fault tolerance.
- Teaching interests: Cybersecurity, Hardware Security, Sensor Network for Advanced Manufacturing, Embedded Systems, Digital Systems, VLSI Design.

Associate Professor June 2017 to June 2021

Department of Electrical and Computer Engineering,
University of New Hampshire

- Research interests: hardware security with special emphasis on hardware Trojan detection and mitigation, three-dimensional integrated circuits (3D ICs) security, side-channel analysis attack, security primitive design, embedded system security, cybersecurity, approximate computing, cyber-physical system, Networks-on-Chip, hardware reliability, VLSI fault tolerance.
- Teaching interests: Digital Systems, VLSI Design, Hardware Security and Trust I &II, Embedded Microprocessor based Design.

Assistant Professor August 2011 to May 2017

Department of Electrical and Computer Engineering,
University of New Hampshire

- Research interests: cyber-physical system, hardware security, security primitive design, error control for Networks-on-Chip, fault-tolerance for many-core systems, flexible organic transistors and emerging nanoelectronics
- Taught courses: Computer Organization, Introduction to Digital Systems, Electronic Design II, Digital Systems, Junior Lab I & II, Introduction to VLSI, Reliable VLSI Designs, Robust IC Design and Verification, Hardware Security and Trust I

Postdoctoral Scholar May 2011 to July 2011

Department of Electrical and Computer Engineering,
University of Rochester
Research project: Error control for Networks-on-Chip

Research Assistant August 2006 to May 2011

Department of Electrical and Computer Engineering,
University of Rochester
Supervisor: Paul Ampadu, Ph.D.
Research projects: Reliable backend integrated hybrid photonic-electronic Networks-on-Chip, dual-layer cooperative error control for nanoscale Networks-on-Chip, ballistic deflection transistor, simulation, device and circuit designs, leakage management techniques for nanoscale CMOS memories

Internship June 2008 to August 2008

Supercomputer Center, University of California, San Diego,
Research project: development fo a flexible and parallel simulator for Networks-on-Chip with error control mechanisms (Sponsored by NSF Cyber-Infrastructure Experience for Graduate Students CIEG)

Teaching Assistant August 2005 to July 2006

Department of Electrical and Computer Engineering,
University of Rochester
Courses: Electromagnetic Waves; Computer Organization

Research Assistant September 2002 to March 2005

Information Science & Electronic Engineering,
Zhejiang University
Research project: implementation of 16-bit fixed-point digital signal processor (DSP)

Professional Distinctions, Awards, and Honors

Honors and Best Paper/Dissertation/Poster Awards

- Best Poster Award, Texas Analog Center of Excellence 2018
- National Science Foundation CAREER Award 2017
- Faculty Development Award, University of New Hampshire 2012, 2017
- Best Poster Award, IEEE Computer Society Annual Symposium on VLSI 2016
- Best Student Paper Finalist, Intl. Midwest Symp. on Circuits and Systems 2015
- Nominated for an Outstanding Dissertation Award in engineering and applied sciences, University of Rochester 2011
- Best Ph.D. Dissertation Award in the ECE Department, University of Rochester 2011
- Best Paper Finalist, 5th ACM/IEEE Intl. Symp. on Networks-on-Chip 2011

- Best Student Paper, 7th Intl. Conf. on Solid-State and Integrated-Circuit Technology 2004

Teaching Awards

- Nominee of the TechWomen|TechGirls Educator of the Year 2018, New Hampshire
- Excellence in Teaching Award, College of Engineering and Physical Sciences, University of New Hampshire 2015

Mentor for Student Competitions

- Mentor for the 3rd place winner in the competition of Embedded Security Challenge at Cyber Security Awareness Week (CSAW) 2015, 2016, 2017
- Mentor for the Finalist in the competition of Embedded Security Challenge at Cyber Security Awareness Week (CSAW) 2014, 2018, 2019, 2020, 2021

Fellowships

- Air Force Visiting Faculty Research Program (VFRP) Fellowship 2017
- CSAW Summer Faculty Research and Training Fellowship 2014
- NSF Cyber-Infrastructure Experiences for Graduate Students (CIEG) 2008

Travel Awards

- USENIX Security Symposium 2016
- NSF CISE CAREER Workshop 2014

RESEARCH GRANTS (TOTAL FUNDING: $1,359,113)

G1. National Science Foundation (NSF), "RII Track-2 FEC: HealthWear+: Converging Smart Textile Wearables, AI, and IoT-security for Human Health," $1,657,620, Period: 06/01/2022-05/31/2026, Co-PI: Qiaoyan Yu, PI: Kunal Mankodiya (University of Rhode Island), Co-PI: Edward Sazonov (University of Alabama). (Pending)

G2. National Science Foundation (NSF), "Building a NHCyberSEE Laboratory for Hands-on Experience Oriented Cybersecurity Education," $499,634, Period: 05/02/2022-05/01/2025, PI: Qiaoyan Yu, Co-PI: Dongpeng Xu, Diliang Chen, and Hong Jin. (Pending)

G3. National Science Foundation (NSF), "IUCRC Planning Grant University of New Hampshire: Center for Digital Factory Innovations (CDFI)," $20,000, Period: 06/2021-05/2022, Senior Personal: Qiaoyan Yu, PI: Nicholas Kirsch. (Current)

G4. FY2021 CoRE Interdisciplinary Working Group, "Developing a Cybersecurity Assessment Testbed for Advanced Manufacturing," $15,000, Period: 09/01/2021-08/31/2022, PI: Qiaoyan Yu, Co-PI: Diliang Chen, Edward Song, John Roth, Dongpeng Xu, and Hong Jin. (Current)

G5. National Science Foundation (NSF), "SaTC:CORE:Small: Towards Securing the Hardware and Software for Approximate Computing Systems," No. 2022279, $499,988, Period: 09/01/2020-08/31/2023, PI: Qiaoyan Yu, Co-PI: Dongpeng Xu. (Current)

G6. National Science Foundation, CAREER Award Supplement for WISE Workshop, No. 2019391, $17,800, Period: 02/28/2020 - 02/27/2021, PI: Qiaoyan Yu. (Current)

G7. National Science Foundation, CAREER Award REU Supplement, No. 1934277, $16,000, Period: 05/28/2019 - 05/27/2021, PI: Qiaoyan Yu (Current)

G8. National Science Foundation (NSF)/Semiconductor Research Corporation(SRC), No. 1717130, "SaTC: STARSS: Small: Collaborative: Managing Hardware Security in Three-Dimensional Integrated Circuits," $235,000, Period: 10/01/2017-09/30/2022, Lead PI: Qiaoyan Yu. (Completed)

G9. National Science Foundation CAREER Award, No. 1652474, "CAREER: Proactive Defense Methods for Chip Integrity and Security," $485,827, Period: 04/15/2017-02/28/2022, PI: Qiaoyan Yu. (Current)

G10. Weapons Neutron Research Facility (WNR) at LANSCE, User facility request proposal, Proposal Number: NS-2013-5176-F, "Investigating Single- and Multiple-Event Transients in Integrated Circuits", 11/23/2013, Approved to use the facility, PI: Qiaoyan Yu. 24-hour experimental work was allocated. No support fund is available in addition to the facility use time.

G11. Weapons Neutron Research Facility (WNR) at LANSCE, User facility request proposal, Proposal Number: NS-2014-6457-A, "Investigating Single- and Multiple-Event Transients in Integrated Circuits (cont.)", 04/22/2014, Approved to use the facility, PI: Qiaoyan Yu.

G12. NSF-Center for High-rate Nanomanufacturing (CHN) at UNH, "Exploiting All-Inkjet-Printed Flexible Transistors to Design Emerging Low-Cost and High-Fabrication-Rate Logic Circuits", $82,301, Period: 12/01/2012-11/30/2013. PI: Qiaoyan Yu. (Completed)

G13. NSF Research Experience for Undergraduates (REU), $15,197.00, Period: 06/01/2013-08/30/2014, PI: Qiaoyan Yu. (Completed)

Books and Book Chapters (Total: 8)

B1. **Q. Yu**, S. Sunkavilli, and Z. Zhang, "FPGA Security: Security Threats from Untrusted FPGA CAD Toolchain," in Book *Electronic Design for AI, IoT and Hardware Securityic Design*, Ali Iranmanesh(Ed), Springer Press, Sept. 2022.

B2. **Q. Yu**, P. Yellu, and L. Buell, "Towards Securing Approximate Computing Systems: Security Threats and Attack Mitigation, " in Book *Approximate Computing,* W. Liu and F. Lombardi (Eds), Springer Press, 2022.

B3. **Q. Yu**, Z. Zhang and J. Dofe, "Proactive Defense Against Security Threats on IoT Hardware," in Book *Modeling and Design of Secure Internet of Things,* C. A. Kamhoua, L. Njilla, A. Kott, and S. Shetty (Eds), Wiley-IEEE Press, March 2020.

B4. **Q. Yu**, J. Dofe, Z. Zhang, and S. Kramer, "Hardware Obfuscation Methods for Hardware Trojan Prevent/Detection," in Book *The Hardware Trojan War: Attacks, Myths, and Defenses,* Swarup Bhunia and Mark M. Tehranipoor (Eds), ISBN 978-3-319-68511-3, Springer Press, Jan. 2018.

B5. **Q. Yu**, J. Dofe, Y. Zhang, and J. Frey, "Hardware Hardening Approaches using Obfuscation, Encryption and Camouflaging," in Book *Hardware IP Security and Trust,* P. Mishra, S. Bhunia, and M. Tehranipoor (Eds), Springer Press, Dec. 2016.

B6. P. Ampadu, **Q. Yu**, and B. Fu, "Reliable Networks-on-Chip Design for Sustainable Computing Systems," in Book *Design Technologies for Green and Sustainable Computing Systems,* P. Pande, A. Ganguly, K. Chakrabarty (Eds), Springer Press, 2013, pp 23-57.

B7. **Q. Yu** and P. Ampadu,"Transient and Permanent Error Control For Networks-On-Chip," ISBN 978-1-4614-0961-8, Springer Press, New York, 2011.

B8. P. Ampadu, B. Fu, D. Wolpert and **Q. Yu**, "Adaptive Voltage Control for Energy-efficient NoC Links," in Book *Low-Power Networks on Chip*, C. Silvano, M. Lajolo, G. Palermo (Eds), Springer Press, 2011, pp. 45-69.

Refereed Journal Publications (Total: 25)

J1. *P. Yellu, and and **Q. Yu**,"Securing Approximate Computing Systems via Obfuscating Approximate-Precise Boundary," IEEE Trans. on Computer-Aided Design of Integrated. Circuits and Systems. https://doi:10.1109/TCAD.2022.3168261.

J2. *M. R. Monjur, J. Heacock, J. Calzadillas, R. Sun, Md S. Mahmud, J. Roth, K. Mankodiya, E. Sazonov, and **Q. Yu**,"Hardware Security in Sensor and its Networks," Frontiers in Sensors, vol. 2, Feb. 2022. https://doi:10.3389/fsens.2022.850056

J3. *P. Yellu, L. Buell, M. Mark, M. Kinsy, D. Xu, and **Q. Yu**, "Security Threat Analyses and Attack Models for Approximate Computing Systems: From Hardware and Micro-Architecture Perspectives," ACM Trans. Des. Autom. Electron. Syst. 26, 4, Article 32 (February 2021), 31 pages. https://doi.org/10.1145/3442380

J4. A. Miele, **Q. Yu**, and M. K. Michael, "Guest Editorial: Reliability-aware Design and Analysis Methods for Digital Systems: from Gate to System Level," in IEEE Transactions on Emerging Topics in Computing, vol. 8, pp. 561-563, July-Sept. 2020.

J5. *Z. Zhang, J. Dofe, P. Yellu and **Q. Yu**, "Comprehensive Analysis on Hardware Trojans in 3D ICs: Characterization and Experimental Impact Assessment," Springer Nature Computer Science, Issue 1, Article number 233, pp. 1-13, July 2020, DOI: 10.1007/s42979-020-00220-0.

J6. *Z. Zhang, J. Dofe, and **Q. Yu**, "Improving Power Analysis Attack Resistance using Intrinsic Noise in 3D ICs," Integration, the VLSI Journal, vol. 73, pp. 30-42, July 2020.

J7. Y. Zhang, Z. Pan, P. Wang, D. Ding, and **Q. Yu**, "A 0.1-pJ/b and ACF <0.04 Multiple-valued PUF for Chip Identification Using Bit-line Sharing Strategy in 65nm CMOS," IEEE Trans. on Very Large Scale Integr. (VLSI) Syst., vol. 27, no. 5, pp. 1043-1052, Mar. 2019.

J8. *Z. Zhang[1] and **Q. Yu**, "Towards Energy-Efficient and Secure Computing Systems," Journal of Low Power Electronics and Applications, vol. 8, no. 4, pp. 1-15, Nov. 2018.

J9. *Z. Zhang, L. Njilla, C. Kamhoua, and **Q. Yu**, "Thwarting Security Threats From Malicious FPGA Tools With Novel FPGA-Oriented Moving Target Defense," IEEE Trans. on Very Large Scale Integr. (VLSI) Syst., vol. 27, no. 3, pp. 665-678, Nov. 2018.

J10. L. Bu, J. Dofe, **Q. Yu**, and M. Kinsy, "SRASA: a Generalized Theoretical Framework for Security and Reliability Analysis in Computing Systems," Journal of Hardware and Systems Security, pp. 1-19, Sept. 2018.

J11. Y. Zhang, D. Ding, P. Zhao, P. Wang, and **Q. Yu**, "An ultra-low power multiplier using multi-valued adiabatic logic in 65nm CMOS process," Microelectronics Journal, vol. 78, pp. 26-34, 2018.

J12. C. Yan, J. Dofe, S. Kontak, **Q. Yu**, and E. Salman, "Hardware-Efficient Logic Camouflaging for Monolithic 3D ICs," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 37, no. 2, pp. 799-803, 2018.

J13. *J. Dofe, and **Q. Yu**, "Novel Dynamic State-Deflection Method for Gate-Level Netlist Obfuscation," IEEE Trans. on Computer-Aided Design of Integrated. Circuits and Systems, vol. 37, no. 2, pp. 273-285, Feb. 2018.

[1]The first author with * is Q. Yu's student.

J14. *J. Frey and **Q. Yu**, "A Hardened Network-on-Chip Design using Runtime Hardware Trojan Mitigation Methods," Integration, the VLSI Journal, 56(117), pp. 15-31, July 2016.

J15. *J. Dofe, H. Pahlevanzadeh, and **Q. Yu**, "A Comprehensive FPGA-based Assessment on Fault-Resistant AES against Correlation Power Analysis Attack," Journal of Electronics Testing: Theory and Applications, vol. 32, no. 5, pp. 611-624, Oct. 2016.

J16. K. Wu, P. Liu, W. Wang, **Q. Yu**, and Y. Jiang, "PSS4: Four-Phase Shifted Sinusoid Symbol Signaling for High Speed IO Interconnects," Computers and Electrical Engineering - Journal – Elsevier, 51(C), pp. 104-117, 2016.

J17. *J. Dofe, J. Frey, H. Pahlevanzadeh and **Q. Yu**, "Strengthening SIMON Implementation against Intelligent Fault Attacks," IEEE Embedded System Letters, vol. 7, no. 4, pp. 113-117, Dec. 2015.

J18. *H. Pahlevanzadeh and **Q. Yu**, "A New Analytical Model of SET Latching Probability for Circuits Experiencing Single- or Multiple-Cycle Single-Event Transients," Journal of Electronic Testing: Theory and Applications, vol. 30, no. 5, pp. 595-609, Sept. 2014.

J19. *W. Danesh, J. Dofe, and **Q. Yu**, "Efficient hardware Trojan detection with differential cascade voltage switch logic," VLSI Design, vol. 2014, Article ID 652187, 11 pages, May 2014.

J20. **Q. Yu**, M. Zhang and P. Ampadu, "Addressing Network-On-Chip Router Errors with Inherent Information Redundancy," ACM Trans. on Embedded Computing Syst.-Special Issue on On-Chip and Off-Chip Network Archit. vol. 12, no. 4, Article No.105, Jun. 2013.

J21. **Q. Yu** and P. Ampadu, "Dual-Layer Adaptive Error Control for Network-On-Chip Links," IEEE Trans. on Very Large Scale Integr. (VLSI) Syst., vol. 20, no.7, pp. 1304-1317, July 2012.

J22. **Q. Yu** and P. Ampadu, "A Dual-Layer Method for Transient and Permanent Error Co-Management in NoC Links," IEEE Trans. on Circuit and Systems II-Express Briefs, vol. 58, no. 1, pp. 36-40, Jan. 2011.

J23. **Q. Yu** and P. Ampadu,"A Flexible Parallel Simulator for Networks-On-Chip with Error Control," IEEE Trans. on Computer-Aided Design of Integrated Circuits and Syst. (TCAD), vol. 29, no. 1, pp. 103-116, Jan. 2010.

J24. **Q. Yu** and P. Ampadu, "Adaptive Error Control for Nanometer Scale NoC Links," IET Computers & Digital Techniques-Special Issue on Advances in Nanoelectronics Circuits and Syst., vol. 3, no. 6, pp. 643-659, Nov. 2009.

J25. D. Huo, **Q. Yu**, D. Wolpert and P. Ampadu, "A Simulator for Ballistic Nanostructures in a 2-D Electron Gas," ACM J. on Emerging Technologies in Computing Syst. (JETC), vol. 5, no. 1, Article 5, Jan. 2009.

Peer-reviewed Conference Publications (Total: 62)

C1. *M. R. Monjur, J. Calzadillas, M. Kajol, and **Q. Yu**, "Hardware Security in Advanced Manufacturing," in Proc. Proc. Great Lakes Symposium on VLSI (GLSVLSI'22), Apr. 2022.

C2. *S. Sunkavilli, and **Q. Yu**, "Security Threats and Countermeasure Deployment Using Partial Reconfiguration in FPGA CAD Tools," to appear in Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST'22), June 2022.

C3. *M. R. Monjur, J. Calzadillas, J. Heacock, and **Q. Yu**, "Challenges of Securing Low-Power LoRaWAN Devices Deployed in Advanced Manufacturing, " in Proc. International Symposium on Quality Electronic Design (ISQED'22), pp. 263, Apr. 2022.

C4. M. R. Monjur, J. Heacock, R. Sun, and **Q. Yu**, "An Attack Analysis Framework for LoRaWAN Applied Advanced Manufacturing," in Proc. IEEE International Symposium on Technologies for Homeland Security, Nov. 2021. DOI: 10.1109/HST53381.2021.9619

C5. *S. Sunkavilli, Z. Zhang, and **Q. Yu**, "New Security Threats on FPGAs: From FPGA Design Tools Perspective," Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI'21), pp. 278-283, July 2021.

C6. *Z. Zhang, I. Miketic, E. Salman, and **Q. Yu**, "Towards Enhancing Power-Analysis Attack Resilience for Logic Locking Techniques," Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI'21), pp. 132-137, July 2021.

C7. D. Xu, B. Liu, W. Feng, J. Ming, J. Li, Q. Zheng, and **Q. Yu**, "Boosting SMT Solver Performance on Mixed-Bitwise-Arithmetic Expressions," in Proc. The 42nd ACM SIG-PLAN Conference on Programming Language Design and Implementation (PLDI), Virtual Event, pp. 651–664, June 20–26, 2021.

C8. *Z. Zhang, I. Miketic, E. Salman, and **Q. Yu**, "Assessing Correlation Power Analysis (CPA) Attack Resilience of Transistor-Level Logic Locking," in Proc. Great Lakes Symposium on VLSI (GLSVLSI'21), pp. 415-420, June 2021.

C9. *S. Sunkavilli, Z. Zhang, and **Q. Yu**, "Analysis of Attack Surfaces and Practical Attack Examples in Open Source FPGA CAD Tools," in Proc. International Symposium on Quality Electronic Design (ISQED'21), pp. 504-509, April 2021.

C10. *M. S. Wara, and **Q. Yu**, "New Replay Attacks on Zigbee Devices for Internet-of-Things (IoT) Applications, " in Proc. 16th IEEE International Conference on Embedded Software and Systems (ICESS'20), pp. 1-6, Dec. 2020.

C11. *Z. Zhang, and **Q. Yu**, "FTAI: Frequency-based Trojan-Activity Identification Method for 3D Integrated Circuits," in Proc. IEEE International Midwest Symposium on Circuits and Systems (MWSCAS'20), pp. 281-284, Aug. 2020 (Invited Paper).

C12. *M. R. Monjur, S. Sunkavilli, and **Q. Yu**, "ADobf: Obfuscated Detection Method against Analog Trojans on I2C Master-Slave Interface," in Proc. IEEE International Midwest Symposium on Circuits and Systems (MWSCAS'20), pp. 1064-1067, Aug. 2020 (Invited Paper).

C13. *P. Yellu, Z. Zhang, D. Xu, and **Q. Yu**, "Blurring Boundaries: A New Way to Secure Approximate Computing Systems," in Proc. Great Lakes Symposium on VLSI (GLSVLSI'20), Sept. 2020. DOI:10.1145/3386263.3407593.

C14. *P. Yellu, and **Q. Yu**, "Can We Securely Use Approximate Computing?", in Proc. Intl. Symp. on Circuits and Syst. (ISCAS 2020), Oct. 2020.

C15. *Z. Zhang, and **Q. Yu**, "Invariance Checking based Trojan Detection Method for Three-Dimensional Integrated Circuits" in Proc. Intl. Symp. on Circuits and Syst. (ISCAS 2020), Oct. 2020.

C16. *P. Yellu, M. R. Monjur, T. Kammerer, D. Xu, and **Q. Yu**, "Security Threats and Countermeasures for Approximate Arithmetic Computing," in Proc. Asia and South Pacific Design Automation Conference (ASP-DAC) 2020, pp. 259-264, Jan. 2020.

C17. J. Wang, Y. Zhang, P. Wang, Z. Luan, X. Xue, X. Zeng, and **Q. Yu**, "An Orthogonal Algorithm for Key Management in Hardware Obfuscation," in Proc. Asian Hardware Oriented Security and Trust Symposium (AsianHOST) 2019. DOI: 10.1109/AsianHOST47458.2019.9006703.

C18. *P. Yellu, Z. Zhang, M. M. R. Monjur, R. Abeysinghe, and **Q. Yu**, "Emerging Applications of 3D Integration and Approximate Computing in High-Performance Computing Systems: Unique Security Vulnerabilities," in Proc. 2019 IEEE High Performance Extreme Computing Conference, pp. 1-7, Sept. 2019.

C19. *Z. Zhang, and **Q. Yu**, "Modeling Hardware Trojan in 3D ICs," in Proc. ISVLSI IEEE Computer Society Annual Symposium on VLSI (ISVLSI'19), July 2019. DOI: 10.1109/ISVLSI.2019.00093.

C20. *P. Yellu, N. Boskov , M. Kinsy, and **Q. Yu**, "Security Threats on Approximate Computing Systems," in Proc. Great Lakes Symposium on VLSI (GLSVLSI'19), pp. 387-392, May 2019.

C21. *Z. Zhang, J. Dofe, and **Q. Yu**, "A Survey on Energy Efficiency Techniques for Secure Computing Systems," in Proc. the 9th international GREEN and sustainable computing conference, pp.1-6, Oct. 2018.

C22. *Z. Zhang, and **Q. Yu**, "Exploiting Principle of Moving Target Defense to Secure FPGA Systems," in Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI'18), pp. 393-398, Jul. 2018.

C23. *Z. Zhang, and **Q. Yu**, "Investigating Reliability and Security of Integrated Circuits and Systems," in Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI'18), pp. 106-177, Jul. 2018.

C24. *J. Dofe, and **Q. Yu**, "Exploiting PDN Noise to Thwart Correlation Power Analysis Attacks in 3D ICs," in Proc. 20th ACM/IEEE System Level Interconnect Prediction 2018 workshop, pp. 1-5, Jun. 2018.

C25. *Z. Zhang, **Q. Yu**, L. Njilla, and C. Kamhoua, "FPGA-Oriented Moving Target Defense against Security Threats from Malicious FPGA Tools," in Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST'18), pp. 163-166, May 2018.

C26. *Z. Zhang, L. Njilla, C. Kamhoua, K. Kwiat, and **Q. Yu**, "Securing FPGA-based Obsolete Component Replacement for Legacy Systems," in Proc. International Symposium on Quality Electronic Design (ISQED'18), pp. 401-406, Mar. 2018.

C27. **Q. Yu**, Z. Zhang, and J. Dofe, "Exploiting Hardware Obfuscation Methods to Prevent and Detect Hardware Trojans," in Proc. IEEE International Midwest Symposium on Circuits and Systems (MWSCAS'17), Aug. 2017. (Invited Paper) DOI: 10.1109/MWSCAS.2017.8053049

C28. *J. Dofe, P. Gu, D. Stow, **Q. Yu**, E. Kursun, and Y. Xie, "Security Threats and Countermeasures in Three-Dimensional Integrated Circuits," in Proc. Great Lakes Symposium on VLSI (GLSVLSI'17), pp. 321-326, May 2017.

C29. *J. Dofe, Z. Zhang, **Q. Yu**, C. Yan, and E. Salman, "Impact of Power Distribution Network on Power Analysis Attacks in Three-Dimensional Integrated Circuits," in Proc. Great Lakes Symposium on VLSI (GLSVLSI'17), pp. 327-332, May 2017.

C30. *M. R. Ansari, T. Miller, C. She, and **Q. Yu**, "A Low-Cost Masquerade Attack Detection Method for Secure Controller Area Network in Automobiles," in Proc. International Symposium on Circuits and Syst. (ISCAS'17), pp 2178-2181, May 2017.

C31. *S. Kramer, Z. Zhang, J. Dofe, and **Q. Yu**, "Mitigating Control Flow Attacks in Embedded Systems with Novel Built-in Secure Register Bank," in Proc. Great Lakes Symposium on VLSI (GLSVLSI'17), pp. 483-486, May 2017.

C32. *J. Dofe, and **Q. Yu**, "Security Vulnerabilities of Three-Dimensional Integrated Circuits," in Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST'17), May 2017. DOI: 10.1109/HST.2017.7951820

C33. *J. Dofe, C. Yan, S. Kontak, E. Salman, and **Q. Yu**, "Transistor-Level Camouflaged Logic Locking Method for Monolithic 3D IC Security," in Proc. Asian Hardware Security and Trust Symposium (AsianHOST'16), pp. 1-6, Dec. 2016.

C34. *M. R. Ansari, T. Miller, and **Q. Yu**, "Prototype Demonstration of Secure Control Area Network (CAN) against Masquerade and Replay Attacks," in Proc. Hardware Demon Session in IEEE International Symposium on Hardware Oriented Security and Trust (HOST'16), pp. xviii, May 2016.

C35. *J. Dofe, Y. Zhang, and **Q. Yu**, "DSD: A Dynamic State-Deflection Method for Gate-Level Netlist Obfuscation," in Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI'16), pp.565-570, Jul. 2016. (Best Poster Award)

C36. *J. Dofe, **Q. Yu**, H. Zhang, and E. Salman, "Hardware Security Threats and Potential Countermeasures in Emerging 3D ICs," in Proc. Great Lakes Symposium on VLSI (GLSVLSI'16), pp. 69-74, May 2016.

C37. *J. Dofe, J. Frey, and **Q. Yu**, "Hardware Security Assurance in Emerging IoT Applications," in Proc. Intl. Symp. on Circuits and Syst. (ISCAS'16), pp. 2050-2053, May 2016. (Invited Paper)

C38. *H. Pahlevanzadeh, J. Dofe, and **Q. Yu**, "Assessing CPA Resistance of AES with Different Fault Tolerance Mechanisms," in Proc. the 21st Asia and South Pacific Design Automation Conference (ASP-DAC'16), pp. 661-666, Jan. 2016.

C39. *M. R. Ansari, S. Yu, and **Q. Yu**, "IntelliCAN: Attack-Resilient Controller Area Network (CAN) for Secure Automobiles," in Proc. 17th IEEE Symposium Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT'15), pp. 234-237, Oct. 2015.

C40. *J. Dofe, J. Frey, Patrick Nsengiyumva, and **Q. Yu**, "Investigating Power Characteristics of Memristor-based Logic Gates and Their Applications in a Security Primitive," in Proc. IEEE International Midwest Symposium on Circuits and Systems (MWSCAS'15), pp. 409-4012, Aug. 2015.

C41. *J. Frey, and **Q. Yu**, "Exploiting State Obfuscation to Detect Hardware Trojans in NoC Network Interfaces," in Proc. IEEE International Midwest Symposium on Circuits and Systems (MWSCAS'15), pp. 827-830, Aug. 2015. (Best Student Paper Finalist)

C42. *P. Nsengiyumva, and **Q. Yu**, "Investigation of Single Event Upsets in Dynamic Logic Based Flip-Flops," in Proc. Intl. Symp. on Circuits and Syst. (ISCAS'15), pp. 818-821, May 2015.

C43. *J. Dofe, C. Reed, N. Zhang, and **Q. Yu**, "Fault-Tolerant Methods for a New Lightweight Cipher SIMON," in Proc. International Symposium on Quality Electronic Design (ISQED'15), pp. 460-464, May 2015.

C44. *K. Wu, H. Pahlevanzadeh, P. Liu, **Q. Yu**, "A New Fault Injection Method for Evaluation of Combining SEU and SET Effects on Circuit Reliability," in Proc. Intl. Symp. on Circuits and Syst. (ISCAS'14), pp. 602-605, Jun. 2014.

C45. *H. Pahlevanzadeh and **Q. Yu**, "Systematic Analyses for Latching Probability of Single-Event Transients," in Proc. International Symposium on Quality Electronic Design (ISQED'14), pp. 442-449, Mar. 2014.

C46. **Q. Yu** and J. Frey, "Exploiting Error Control Approaches for Hardware Trojans on Network-on-Chip Links," in Proc. 16th IEEE Symp. Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT'13), pp. 266-271, Oct. 2013.

C47. **Q. Yu** and D. Stock, "Collaborative Error Control Method for Sequential Logic Circuits," in Proc. Intl. Symp. on Circuits and Syst. (ISCAS'13), pp. 785-788, May 2013.

C48. *T. Zhang and **Q. Yu**, "A Fully Integrated Video Digital-To-Analog Converter with Minimized Gain Error," in Proc. Intl. Symp. on Circuits and Syst. (ISCAS'13), pp. 837-840, May 2013.

C49. K. Wu, P. Liu and **Q. Yu**, "A Novel Energy-Efficient Serializer Design Method for Gigascale Systems," in Proc. Intl. Symp. on Circuits and Syst. (ISCAS'13), pp. 1978-1981, May 2013.

C50. **Q. Yu** and P. Ampadu, "Transient Error Management for Partially Adaptive Router in Network-On-Chip (NoC)," in Proc. Intl. Symp. on Circuits and Syst. (ISCAS'12), pp. 1672-1675, May 2012.

C51. M. Zhang, **Q. Yu** and P. Ampadu, "Fine-Grained Splitting Methods to Address Permanent Errors in Network-On-Chip Links," in Proc. Intl. Symp. on Circuits and Syst. (ISCAS'12), pp. 2717-2720, May 2012.

C52. **Q. Yu**, J. Cano, J. Flich and P. Ampadu, "Transient and Permanent Error Control for High-End Multiprocessor Systems-On-Chip," in Proc. 6th ACM/IEEE International Symposium on Networks-on-Chip (NoCS'12), pp. 169-176, May 2012.

C53. **Q. Yu**, M. Zhang and P. Ampadu, "Exploiting Inherent Information Redundancy to Manage Transient Errors in NoC Routing Arbitration," in Proc. 5th ACM/IEEE International Symposium on Networks-on-Chip (NoCS'11), pp. 105-112, May 2011.

C54. **Q. Yu**, M. Zhang and P. Ampadu, "A Comprehensive Networks-On-Chip Simulator for Error Control Explorations," in Proc. 5th ACM/IEEE Intl. Symp. on Networks-on-Chip (NoCS'11), pp. 263-264, May 2011.

C55. **Q. Yu** and P. Ampadu, "Transient and Permanent Error Co-Management Method for Reliable Networks-On-Chip," in Proc. 4th ACM/IEEE Intl. Symp. on Networks-on-Chip (NoCS'10), pp. 145-154, May 2010.

C56. **Q. Yu**, B. Zhang, Y. Li and P. Ampadu, "Error Control Integration Scheme for Reliable NoC," in Proc. 2010 IEEE Intl. Symp. on Circuit and Syst. (ISCAS'10), pp. 3893-3896, May 2010.

C57. **Q. Yu** and P. Ampadu, "Dual-Layer Cooperative Error Control for A Reliable Nanoscale NoC," in Proc. 24th IEEE Intl. Symp. on Defect and Fault Tolerance in VLSI Sys. (DFT'09), pp. 431-439, Oct. 2009.

C58. **Q. Yu** and P. Ampadu, "Adaptive Error Control for NoC Switch-To-Switch Links in a Variable Noise Environment," in Proc. 23rd IEEE Intl. Symp. on Defect and Fault Tolerance in VLSI Sys. (DFT'08), pp. 352-360, Oct. 2008.

C59. **Q. Yu** and P. Ampadu, "Configurable Error Correction for Multi-Wire Errors in Switch-to-Switch SoC Links," in Proc. 21st Annual IEEE Intl. SoC Conf. (SoCC'08), pp. 71-74, Sept. 2008.

C60. **Q. Yu** and P. Ampadu, "Adaptive Error Control for Reliable Systems-On-Chip," in Proc. Intl. Symp. on Circuits and Syst. (ISCAS'08), pp. 832-835, May 2008.

C61. D. Huo, **Q. Yu** and P. Ampadu, "A Ballistic Nanoelectronic Device Simulator," in Proc. Intl. Symp. on Nanoscale Architectures (NanoArch'07), pp. 38-45, Oct. 2007.

C62. B. Fu, **Q. Yu**, and P. Ampadu, "Energy-Delay Minimization in Nanoscale Domino Logic," in Proc. 16th Great Lakes Symp. on VLSI (GLSVLSI'06), pp. 316-319, Apr. 2006.

C63. **Q. Yu**, P. Liu, Q. Yao and K. Chen, "A Functional Verification Method for Pipelined DSP," in Proc. 7th IEEE Intl. Conf. on Solid-State and Integrated-Circuit Technology, vol. 3, pp. 2055-2058, Oct. 2004. (Best Student Paper)

Poster Presentations (Total: 3)

C1. *P. Yellu, and **Q. Yu**, "APB Concealing: New Obfuscation Method for Securing Approximate Computing Systems," WIP in DAC 2021.

C2. *P. Yellu, L. Buell, and **Q. Yu**, "Blurring Boundaries: A New Way to Secure Approximate Computing Systems," Poster Session in New England Hardware Security Day 2021, [Online]: http://vernam.wpi.edu/nehws21/program/

C3. *P. Yellu, L. Buell, and **Q. Yu**, "WiP: Systematic Attack Models for Approximate Computing Systems," in Hardware and Architectural Support for Security and Privacy (HASP) 2020.

Invited Talks (Total: 28)

T1. Q. Yu, May 2022, "Proactive Defense Methods for Hardware-Oriented Security," Future of Moving Data Summit— Network Measurement, Performance and Tuning, NH, USA.

T2. Q. Yu, Mar. 2022, "Blurring Boundaries: A New Method for Securing Approximate Computing Systems," University of Delaware, DE, USA.

T3. Q. Yu, Mar. 2021, "Towards Securing Approximate Computing Systems ", Villanova University, PA, USA.

T4. Q. Yu, Mar. 2021, "Hardware Security in Three Dimensional (3D) Integrated Circuits and Systems", NYU, NY, USA.

T5. Q. Yu, Oct. 2020, "Hardware Security—The Root of Trust," National Cyber Security Awareness Month (NCSAM).

T6. Q. Yu, Oct. 2020, "Hardware Security in Three-Dimensional Integrated Circuits and Systems," ISCAS2020 Tutorial.

T7. Q. Yu, June 2020, "Exploiting Principles of Moving Target Defense to Address FPGA Security Threats," Intel.

T8. Q. Yu, June 2020, "Managing Hardware Security in Three Dimensional Integrated Circuits," Hardware Security e-Workshop, Semiconductor Research Corporation (SRC).

T9. Q. Yu, Feb. 2019, "Proactive Defense Methods for Integrated Circuits & Systems Security," University of Georgia, GA, USA.

T10. Q. Yu, Feb. 2019, "Assuring the Root of Trust for Internet-of-Things (IoTs)," George Mason University, VA, USA.

T11. Q. Yu, Nov. 2018, "Towards Securing 2D and 3D Integrated Circuits and Systems," MIT Lincoln Laboratory, MA, USA.

T12. Q. Yu, May 2018, "A Whitebox Introduction to Fault Attacks," HOST2018 Tutorial.

T13. Q. Yu, Feb. 2018, "Proactive Defense Methods for Integrated Circuits & Systems Security," Virginia Tech., VA, USA.

T14. Q. Yu, Oct. 2017, "Multi-Layer Design Obfuscation Methods for Hardware Security," Clarkson University, NY, USA.

T15. Q. Yu, Aug. 2017, "Proactive Defense Methods for Chip Integrity and Security," Tokyo University, Japan.

T16. Q. Yu, Aug. 2017, "Proactive Defense Methods for Chip Integrity and Security," Asia and South Pacific Design Automation Conference EDA Workshop, Japan.

T17. Q. Yu, Aug. 2017, "Countermeasures against Security Threats on Integrated Circuits and Systems," Shanghai Jiao Tong University, Shanghai, China.

T18. Q. Yu, Aug. 2017, "Addressing Security Threats on Integrated Circuits," Zhejiang University, Hangzhou, China.

T19. Q. Yu, Jul. 2017,"Proactive Defense Methods for Integrated Circuits and Systems," MITRE, Bedford, MA, USA.

T20. Q. Yu, Jun. 2017, "Towards Securing 2D and 3D Integrated Circuits (ICs)," Air Force Research Laboratory, Cyber Assurance Branch, Rome, NY, USA.

T21. Q. Yu, Apr. 2017, "Design Obfuscation Methods for Securing 2D and 3D Integrated Circuits," Worcester Polytechnic Institute, MA, USA.

T22. Q. Yu, Dec. 2016, "Gate-level Design Obfuscation Methods for Secure Circuits and Systems," National Tsing Hua University, Hsinchu, Taiwan.

T23. Q. Yu, Nov. 2016, "Managing Security for 2D and 3D Integrated Circuits (ICs)," University of Delaware, DE, USA.

T24. Q. Yu, Jun. 2016, "Design Obfuscation Methods for 2D and 3D Integrated Circuits (ICs)," Charles Stark Draper Laboratory, MA, USA.

T25. Q. Yu, Jun. 2016, "Hardware Design Obfuscation Methods against Active and Passive Hardware Attacks," CHASE Conference on Secure/Trustworthy Systems and Supply Chain Assurance, University of Connecticut, CT, USA.

T26. Q. Yu, Aug. 2015, "Hardware Trojan Detection in Networks-on-Chip," Asia and South Pacific Design Automation Conference EDA Workshop, Taiwan.

T27. Q. Yu, Aug. 2015, "Hardware Security and Trust," Invited Talk, Ningbo University, Ningbo, China.

T28. Q. Yu, Jan. 2013, "Energy-efficient and Reliable Many-core Systems," Hangzhou Dianzi University, Hangzhou, China.

T29. Q. Yu, Jan. 2013, "Reliable VLSI Design," Ningbo University, Ningbo, China.

T30. Q. Yu, Nov. 2012, "Reliability Management for Energy-efficient Hybrid Many-core Systems," Oak Ridge National Laboratory, Oak Ridge, TN, USA.

Professional Service

Director

- Center for for Hardware Assurance, Attack-Resilient Network, Embedded Systems & Sensor Network Security (HARNESS) 2019-present

Co-founder

- Workshop for Women in Hardware and Systems Security (WISE) 2017-present

Editor Service

- Associate Editor for Integration, the Journal of VLSI 2013-present
- Associate Editor for Microelectronics Journal- Elsevier 2012-2017
- Guest Editor for IEEE Transactions on Emerging Topics in Computing, Special Issue on Reliability-aware Design and Analysis Methods for Digital Systems: from Gate to System Level 2017
- Guest Editor for VLSI Design-Hindawi, Special Issue on Advanced VLSI Architecture Design for Emerging Digital Systems 2014

Conference/Workshop Organization

- Track Chair for the track "Energy-Efficient, Reliable VLSI Systems (ERS)" in 7th IEEE International Symposium on Smart Electronics Systems (iSES) 2021
- Track Chair for the track "Hardware and Cyber Security" in IEEE International Midwest Symposium on Circuits and Systems 2018, 2020
- Track Chair for the track "System Design and Security" in IEEE Computer Society Annual Symposium on VLSI (ISVLSI) 2018
- Vice-chair for the "Security Track" in Asia and South Pacific Design Automation Conference (ASP-DAC) 2018
- General Co-chair for IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems 2017
- Program Co-chair for IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems 2016
- Publicity Chair for IEEE International Hardware-Oriented Security and Trust Symposium (HOST) 2017-2019
- Publicity Chair for IEEE Asian Hardware-Oriented Security and Trust Symposium (AsianHOST) 2017-2019
- Publication Chair for IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems 2012-2015
- Session Chairs for ISCAS'12, ISCAS'13, ASP-DAC'14, HOST'15, HOST'16, AsianHOST'16, GLSVLSI'16, GLSVLSI'17, MWSCAS'17, DAC'20

Technical Program Committee

- IEEE Microelectronics Design & Test Symposium 2021
- Hardware and Architectural Support for Security and Privacy (HASP) 2020
- Top Picks in Hardware and Embedded Security 2019, 2020
- The 33rd ACM International Conference on Supercomputing (ICS '19) 2019
- First International Workshop on Heterogeneous Computation in Specific Domain Accelerations 2019
- IEEE Computer Society Annual Symposium on VLSI (ISVLSI) 2018-2022
- Design Automation Conference (DAC), Track SEC2. 2017-2019
- IEEE Hardware-Oriented Security and Trust Symp. (HOST) 2017-2019, 2021
- Great Lakes Symposium on VLSI (GLSVLSI) 2016-Present
- International Symposium on Circuits and Syst. (ISCAS) 2012-Present
- IEEE International Midwest Symposium on Circuits and Systems 2018-Present
- IEEE Asian Hardware-Oriented Security and Trust Symp. (AsianHOST) 2016-2020

- IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT) 2013-2018
- Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC) 2017, 2018
- EEE International Conference on Computer Design (ICCD) 2016, 2017
- Asia and South Pacific Design Automation Conference (ASP-DAC) 2015, 2017
- IEEE International Symposium on Embedded Multicore System-on-Chip 2013

Reviewer for Journals

- Proceedings of the IEEE
- IEEE Transactions on Information Forensics & Security
- IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems
- IEEE Transactions on Very Large Scale Integration Systems
- IEEE Transactions on Circuits and Systems Part II: Express Briefs
- IEEE Transactions on Reliability
- IEEE Transactions on Dependable and Secure Computing
- IEEE Transactions on Computers
- IEEE Design & Test of Computers
- ACM Journal on Emerging Technologies in Computing Systems
- ACM Transactions on Embedded Computing Systems (TECS)
- ACM Transactions on Design Automation of Electronic Systems (TODAES)
- Embedded Systems Letter
- Integration, the Journal of VLSI
- Journal of Hardware and System Security - Springer

Reviewer for Panels

- NSF Graduate Research Fellowship Program Panel, 2014
- NSF CSR panel, 2017
- NSF SaTC panel, 2018
- NSF SaTC panel, 2018
- NSF SaTC panel, 2019
- NSF SaTC panel, 2021

Student Mentoring

Current PhD Students

- Pruthvy Yellu (Expected May 2023)
- Sandeep Sunkavilli (Expected May 2024)
- Mohammad Mezanur Monjur (Expected May 2025)
- Mashrafi Alam Kajol (Expected May 2026)

PhD Alumnus

- Zhiming Zhang (September 2021)
  Dissertation title: A Comprehensive Study of the Hardware Trojan and Side-Channel Analysis Attacks in Three-Dimensional (3D) Integrated Circuits (ICs)
  Current position: Postdoc Scholar, Northeastern University

- Jaya Dofe (September 2018)
  Dissertation title: Novel Hardware Defense Mechanisms for 2D and 3D Integrated Circuits to Thwart Security Attacks
  Current position: Tenure-track Assistant Professor, California State University at Fullerton

- Hoda Pahlevanzadeh (December 2016)
  Dissertation title: Assessing and Improving the Reliability and Security of Circuits Affected by Natural and Intentional Faults
  Current position: Adjunct Professor, University of New Hampshire

Master Alumni

- Mohammad Shafeul Wara (September 2021)
  Current Position: Analog Product Engineer-II, Microchip Technology Inc.
- Mezanur Rahman Monjur (September 2020)
  Current Position: PhD student, University of New Hampshire
  Dissertation title: Internet-of-Things (IoT) Security Threats: Attacks on Communication Interface
- Zhiming Zhang (May 2018)
  Current position: Ph.D. student at University of New Hampshire
  Dissertation Title: Securing FPGA Systems with Moving Target Defense Mechanisms
- Chenghua She (September 2017)
  Current position: Associate Firmware Engineer, Vicor Corporation
- Mohammad Raashid Ansari (September 2016)
  Current position: Senior Research Engineer, Qualcomm
  Dissertation title: Low-Cost Approaches to Detect Masquerade and Replay Attacks on Automotive Controller Area Network
- Jonathan Frey (May 2016)
  Current position: Senior Member of the Technical Staff, Charles Stark Draper Laboratory in Cambridge, MA
  Dissertation title: Mitigation of Hardware Trojan Attacks on Networks-on-Chip
- Jaya Dofe (May 2015)
  Current position: Tenure-track Assistant Professor, California State University at Fullerton
  Dissertation title: Hardware Attack Detection and Prevention for Chip Security
- Patrick Nsengiyumva (May 2015)
  Current position: Electrical Design & Radiation Effects Engineer, Boeing
  Dissertation title: Investigating Single-Event Upsets in Static and Dynamic Registers
- Jiawei Zhong (December 2014)
  Current job position: Senior Quality Engineer, MathWorks.
  Dissertation title: Network Interface Design for Network On Chip

Undergraduate Research

- Joshua Calzadillas, Fall 2021
  LoRaWAN Security
- Joseph Heacock, Summer 2021
  LoRaWAN Security
- David Wallace, Spring 2020
  Fuzzing Theory Application in Side-Channel Attacks
- Landon Buell, Spring, Summer 2020
  Approximate Computing in Conventional Neural Network
- Timothy Kammerer, 2019 Summer
  Countermeasure against Security Threats in Embedded Systems
- Ranuli Abeysinghe, 2019 Summer
  Security Threats in Hash Function
- Sean Kramer, 2016-2017
  Managing security for embedded systems
- William Melanson, 2015-2016
  An Approach to Attack the Weakened Cryptographic Security of an Election System
- Casey Liss, 2015-2016
  Hardware Implementation and Analysis of the Hash Function Keccak-256 for IoT Based Application
- Jonathan Frey, 2013-2014
  Hardware Trojan Detection: De-Trigger and Correction Schemes for Networks-on-Chip

- Rory O'Brien, 2013-2014
  Radiation effects on Integrated Circuits
- Bridget Sullivan, Summer 2013
  Flexible electronic device modeling
- Jeffery Cahill, 2012-2013
  FSAE Race Car
- Drew Stock, 2012-2013
  Soft error injection tool and simulation