Qiaoyan Yu

Contact Information

Email: qiaoyan.yu@unh.edu
Homepage: https://sites.usnh.edu/qyu
Google Scholar: https://tinyurl.com/am3zsk2c
ORCID: https://orcid.org/0000-0002-7232-8529

Key Achievements

- Research Grant $2,278,296
- Publications: 8 book/book chapters, 30 journals, 86 IEEE/ACM peer-reviewed conference papers
- 47 invited talks (5 keynotes)
- Program Director at NSF CISE/CNS/SaTC Program
- Founder of WHiSPerS: Wearable Health Monitoring Sensors for Privacy and Security; HWiQ Workshop: Hardware Security in the Era of Quantum Computing & Post-Quantum Cryptography; Workshop for Women in Hardware and Systems Security (WISE)
- General chair for ITC-Asia'26, DFTS'17, and 2024 edition of Top Picks in Hardware and Embedded Security; track chair for ISVLSI, ASP-DAC, and MWSCAS; publicity chair for HOST, AsianHOST, and ICESS, technical committee member for top-tier conferences: CCS, EMBS, DATE, DAC, FDTC, ICCD, HASP, ISVLSI, ISCAS, AsianHOST, GLSVLSI, DFT, SOCC, MDTS, ICS.
- Associate editors and guest editors for several journals

Research Expertise

- Microelectronics security with special emphasis on hardware Trojan, side-channel analysis attack, and three-dimensional integrated circuit security, FPGA security;
- In-Sensor Computing for wearable health monitoring systems;
- Approximate computing systems and their application in energy-efficient and privacy-preserving Machine Learning (ML) and Artificial Intelligence (AI);
- Quantum computing with special emphasis on quantum sensing and noise analysis and mitigation;
- Cybersecurity with special emphasis on Internet-of-Things (IoT), embedded systems, communication protocol interface;
- Sustainable system design, error control coding, and fault-tolerant on-chip communication;
- Cyber-physical system with special emphasis on automobile security.

Education

University of New Hampshire, Durham, NH

Master of Business Administration (MBA), May 2025

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, Xi'an, China

B.S., Telecommunications Engineering, July 2002

Work Experience

Program Director June 2024 to present

Secure and Trustworthy Cyberspace (SaTC)
Division of Computer and Network Systems (CISE/CNS)
U.S. National Science Foundation

Expert August 2023 to June 2024

Secure and Trustworthy Cyberspace (SaTC)
Division of Computer and Network Systems (CISE/CNS)
U.S. National Science Foundation

Professor July 2021 to Present

Department of Electrical and Computer Engineering,
University of New Hampshire

- Research interests: quantum computing, in-sensor computing, microelectronics security, cybersecurity, FPGA security, embedded systems security, 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: Emerging computing systems, quantum security, ML/AI accelerators and applications, Embedded Systems, Microelectronic Security, Fault Tolerance, Cybersecurity, Sensor Network for Advanced Manufacturing, 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 of 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 Paper Award Finalist, ASP-DAC 2025
- Best Lightning Talk, Wearable Health monitoring Sensors for Privacy and Security Symposium 2025
- Best Poster Award, GLSVLSI 2024 2024
- Best Poster Award, The 5th Workshop for Women in Hardware and Systems Security 2022
- 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

- The Royal Society Wolfson Visiting Fellowship 2026
- 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 PI's Share: $2,278,296)

G1. National Institutes of Health (NIH), New Hampshire IDeA Network of Biomedical Research Excellence (NH-INBRE), AW002111, 08/25/2025-06/30/2026, $75,349, PI: Dean Sullivan, Co-PI: Qiaoyan Yu, Wei Lu.

G2. National Science Foundation (NSF), Graduate Research Fellowship Program, "A Secure FPGA Architecture for CRYSTALS-Kyber and CRYSTALS-Dilithium: Side-Channel Resistance and Quantum Resilience," Period 09/01/2025-08/31/2028, $159,000, Thesis Advisor: Qiaoyan Yu. Graduate Student: Gabbie MacNeil.

G3. National Science Foundation (NSF), Intergovernmental Personnel Award, Period 06/17/2024-06/16/2026, No. 2432347, $451,032, PI: Qiaoyan Yu

G4. National Science Foundation (NSF), "Building a NHCyberSEE Laboratory for Hands-on Experience Oriented Cybersecurity Education," No. 2154606, $399,999, Period: 07/15/2022-06/30/2025, PI: Qiaoyan Yu, Co-PI: Dongpeng Xu, Diliang Chen, and Hong Jin.

G5. National Science Foundation (NSF), "IUCRC Planning Grant University of New Hampshire: Center for Digital Factory Innovations (CDFI)," No. 2113841, $20,000, Period: 06/2021-05/2022, Senior Personnel: Qiaoyan Yu, PI: Nicholas Kirsch.

G6. 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.

G7. 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.

G8. National Science Foundation (NSF), CAREER Award Supplement for WISE Workshop, No. 2019391, $17,800, Period: 02/28/2020-02/27/2021, PI: Qiaoyan Yu.

G9. National Science Foundation, CAREER Award REU Supplement, No. 1934277, $16,000, Period: 05/28/2019 - 05/27/2021, PI: Qiaoyan Yu

G10. National Science Foundation CAREER Award, "CAREER: Proactive Defense Methods for Chip Integrity and Security," No. 1652474, $485,827, Period: 04/15/2017-02/28/2023, PI: Qiaoyan Yu.

G11. National Science Foundation (NSF)/Semiconductor Research Corporation(SRC), "SaTC: STARSS: Small: Collaborative: Managing Hardware Security in Three-Dimensional Integrated Circuits," No. 1717130, $235,000, Period: 10/01/2017-09/30/2022, Lead PI: Qiaoyan Yu.

G12. 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.

G13. 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.

G14. 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.

G15. NSF Research Experience for Undergraduates (REU), $15,197, Period: 06/01/2013-08/30/2014, PI: Qiaoyan Yu.

PATENT (TOTAL:1)

T1. Qiaoyan Yu and Wei lu, "Systems and Methods for Privacy-Preserved Nonverbal and Verbal Vocalization-Based Pain-level Classification," Provisional Application (pending).

BOOKS AND BOOK CHAPTERS (TOTAL: 8)

B1. S. Sunkavilli*, Z. Zhang and **Qiaoyan Yu**, "FPGA Security: Security Threats from Untrusted FPGA CAD Toolchain," in Book *Electronic Design for AI, IoT and Hardware Security IC Design*, Ali Iranmanesh(Ed), Springer Press, pp. 551-574, Jan. 2023.

B2. **Qiaoyan 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), ISBN 978-3-030-98347-5, Springer Press, 2022. DOI: 10.1007/978-3-030-98347-5_14

B3. **Qiaoyan 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. **Qiaoyan 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. **Qiaoyan 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, **Qiaoyan 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. **Qiaoyan 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 **Qiaoyan 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: 31)

J1. Wei Lu, Ornella Lucresse Soh, Issa Traoré, Isaac Woungang, Marcelo L. Brocardo, Eric Brown, and **Qiaoyan Yu**,"XAPT: eXplainable Anomaly-driven Prediction of Threat Stages in APT Campaigns," IEEE Access (under review)

J2. *S. Sunkavilli, Mashrafi Alam Kajol, and **Qiaoyan Yu**, "S^{2}FAM: Signal-Slowdown-based Fault Attack Mitigation Method for Secure Multi-tenant FPGA," ACM Journal on Emerging Technologies in Computing Systems, Volume 21, Issue 3, Article No.: 8, pp. 1-25. https://doi.org/10.1145/3756013

J3. *S. Sunkavilli, N. Chennagouni, and **Qiaoyan Yu**, "A New Dynamic Countermeasure to Strengthen Design Obfuscation in FPGAs," ACM Transactions on Design Automation of Electronic Systems, Vol. 30, No. 3, Article No.: 37, pp. 1-25. https://doi.org/10.1145/3716502

J4. *P. Yellu, N. Chennagouni, and **Qiaoyan Yu**, "INEAD: Intermediate Node Evaluation-based Attack Detection for Secure Approximate Computing Systems," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 43, No. 3, March 2024, pp 716–727. https://doi.org/10.1109/TCAD.2023.3328826

J5. *Mashrafi Alam Kajol, Mohammad Mezanur Rahman Monjur, and Qiaoyan Yu, "A Circuit-Level Solution for Secure Temperature Sensor," Sensors 2023, 23(12), 5685; https://doi.org/10.3390/s23125685.

J6. *M. R. Monjur, J. Calzadillas, and **Qiaoyan Yu**,"Hardware Security Risks and Threat Analyses in Advanced Manufacturing Industry," ACM Transactions on Design Automation of Electronic Systems, June 2023. https://doi.org/10.1145/3603502.

J7. *P. Yellu, and **Qiaoyan Yu**,"Securing Approximate Computing Systems via Obfuscating Approximate-Precise Boundary," IEEE Trans. on Computer-Aided Design of Integrated. Circuits and Systems, April 2022. https://doi:10.1109/TCAD.2022.3168261.

J8. *M. R. Monjur, J. Heacock, J. Calzadillas, R. Sun, Md S. Mahmud, J. Roth, K. Mankodiya, E. Sazonov, and **Qiaoyan Yu**,"Hardware Security in Sensor and its Networks," Frontiers in Sensors, vol. 2, Feb. 2022.

J9. *P. Yellu, L. Buell, M. Mark, M. Kinsy, D. Xu, and **Qiaoyan Yu**, "Security Threat Analyses and Attack Models for Approximate Computing Systems: From Hardware and Micro-Architecture Perspectives," ACM Transactions on Design Automation of Electronic Systems, 26, 4, Article 32 (February 2021), 31 pages.

J10. A. Miele, **Qiaoyan 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.

J11. *Z. Zhang, J. Dofe, P. Yellu and **Qiaoyan 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.

J12. *Z. Zhang, J. Dofe, and **Qiaoyan Yu**, "Improving Power Analysis Attack Resistance using Intrinsic Noise in 3D ICs," Integration, the VLSI Journal, vol. 73, pp. 30-42, July 2020.

J13. Y. Zhang, Z. Pan, P. Wang, D. Ding, and **Qiaoyan 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.

J14. *Z. Zhang[1] and **Qiaoyan Yu**, "Towards Energy-Efficient and Secure Computing Systems," Journal of Low Power Electronics and Applications, vol. 8, no. 4, pp. 1-15, Nov. 2018.

J15. *Z. Zhang, L. Njilla, C. Kamhoua, and **Qiaoyan 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.

J16. L. Bu, J. Dofe, **Qiaoyan 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.

J17. Y. Zhang, D. Ding, P. Zhao, P. Wang, and **Qiaoyan Yu**, "An ultra-low power multiplier using multi-valued adiabatic logic in 65 nm CMOS process," Microelectronics Journal, vol. 78, pp. 26-34, 2018.

J18. C. Yan, J. Dofe, S. Kontak, **Qiaoyan 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.

J19. *J. Dofe, and **Qiaoyan 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.

J20. *J. Frey and **Qiaoyan Yu**, "A Hardened Network-on-Chip Design using Runtime Hardware Trojan Mitigation Methods," Integration, the VLSI Journal, 56(117), pp. 15-31, July 2016.

J21. *J. Dofe, H. Pahlevanzadeh, and **Qiaoyan 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.

J22. K. Wu, P. Liu, W. Wang, **Qiaoyan 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.

J23. *J. Dofe, J. Frey, H. Pahlevanzadeh and **Qiaoyan Yu**, "Strengthening SIMON Implementation against Intelligent Fault Attacks," IEEE Embedded System Letters, vol. 7, no. 4, pp. 113-117, Dec. 2015.

J24. *H. Pahlevanzadeh and **Qiaoyan 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.

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

J25. *W. Danesh, J. Dofe, and **Qiaoyan Yu**, "Efficient hardware Trojan detection with differential cascade voltage switch logic," VLSI Design, vol. 2014, Article ID 652187, 11 pages, May 2014.

J26. **Qiaoyan 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.

J27. **Qiaoyan 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.

J28. **Qiaoyan 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.

J29. **Qiaoyan 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.

J30. **Qiaoyan 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.

J31. D. Huo, **Qiaoyan 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: 88)

C1. *Gabrielle MacNeil, Sounak Bhowmik and Himanshu Thapliyal, and **Qiaoyan Yu**, "Circuit-Level Mitigation of Decoherence in Quantum Sensors," to appear in GOMACTech'26.

C2. *Mashrafi Kajol, Nishanth Chennagouni, O. Sami Saydjari, Tao Wei, and **Qiaoyan Yu**, "In-Sensor Computing System Architecture for AI-based Rapid Decision-Making Applications," to appear in GOMACTech'26.

C3. *Nishanth Chennagouni, Sandeep Sunkavilli, Wei Lu, and **Qiaoyan Yu**, "Feature-Approximation-based Privacy Preservation for Wearable Sensing Systems," to appear in Proc. Asia and South Pacific Design Automation Conference (ASP-DAC'26), Jan. 2026. (**Best Paper Award Finalist**)

C4. *Julia Liu and **Qiaoyan Yu**, "Melody-Centric Cryptography: A Human-Centered Framework for Symmetric Key Generation," in Proc. 2025 IEEE MIT Undergraduate Research Technology Conference (URTC), Oct. 2025.

C5. *Gabrielle MacNeil, Sandeep Sunkavilli, and **Qiaoyan Yu**, "Authenticating Quantum Circuits Through Localized Noise Fingerprints," in Proc. ACM QSec: Quantum Security and Privacy Workshop, co-located with CCS'25, Oct. 2025.

C6. *Mashrafi Kajol. Wei Lu, and **Qiaoyan Yu**, "Security Under the Lens: Vulnerabilities in In-Sensor Computing Systems," to appear in International Conference on Computer-Aided Design (ICCAD'25), Oct. 2025. (Invited Paper)

C7. *Mashrafi Kajol, Md Abdullah Al Rumon, Shehjar Sadhu, Suparna Veeturi, Dharma Rane, Dhaval Solanki, Kunal Mankodiya, Wei Lu, and **Qiaoyan Yu**, "Invisible Leaks: Covert Channel Exploitation in In-Sensor Computing System," in Proc.of Great Lakes Symposium on VLSI (GLSVLSI'25), pp. 397-398, June 2025.

C8. *Mashrafi Kajol, Nishanth Chennagouni, and **Qiaoyan Yu**, "Security Challenges Toward In-Sensor Computing Systems," in Proc. of Great Lakes Symposium on VLSI (GLSVLSI'25), pp. 41-48, June 2025.

C9. *Mashrafi Kajol, Sandeep Sunkavilli, and **Qiaoyan Yu**, "An On-chip Sensor Placement Strategy For Mitigation Framework Against Voltage-Drop Attack," in Proc. Proc. International Symposium on Circuits and Syst. (ISCAS'25), May 2025.

C10. Naiqian Zhang, Dongpeng Xu, Jiang Ming, Jun Xu, and **Qiaoyan Yu**, "SoK: Inspecting Virtual Machine Diversification Inside Virtualization Obfuscation," in Proc. IEEE S&P 2025.

C11. *Nishanth Chennagouni, Eric Brown, Wei Lu, and **Qiaoyan Yu**, "Bio-FDApx: Biometric-Feature-Driven Approximation for Real-time Health Monitoring Systems, " in The 9th Workshop on Approximate Computing (AxC2024), Oct. 31 2024.

C12. *Nishanth Chennagouni, and **Qiaoyan Yu**, "Optimizing Wearable Sensors with Multi-Feature Approximate Computing," in Proc. The 7th Intl. Conf. on Wireless Intelligent, and Distributed Environment for Communication (WIDECOM'24), Oct. 2024.

C13. *Mohammad Monjur and **Qiaoyan Yu**, "Advanced Continuous-Time Convolution Framework for Security Assurance in Wireless Sensor Networks," in Proc. Great Lakes Symposium on VLSI (GLSVLSI'24), June 2024.

C14. *Nishanth Chennagouni, Mashrafi Kajol, Diliang Chen, Dongpeng Xu, and **Qiaoyan Yu**, "Feature-driven Approximate Computing for Wearable Health-Monitoring Systems," in Proc. Great Lakes Symposium on VLSI (GLSVLSI'24), June 2024.

C15. Mohammad Monjur* and **Qiaoyan Yu**, "CTC: Continuous-Time Convolution based Multi-Attack Detection for Sensor Networks," in Proc. 2024 IEEE International Symposium on Circuits and Systems (ISCAS'24), May 2024.

C16. **Qiaoyan Yu**, Sandeep Sunkavilli, Mashrafi Alam Kajol, Mohammad Monjur, Nishanth Chennagouni, Diliang Chen and Karen Jin"Hands-on Project Oriented Cybersecurity Education for High School Students," in Proc. 2024 IEEE Integrated STEM Education Conference (ISEC), pp. 1-6, March 2024.

C17. *Mohammad Monjur and **Qiaoyan Yu**, "Continuous Time Convolution Based Trust Verification for Wireless Microelectronics," in Proc. GOMACTech 2024, March 2024.

C18. *Nishanth Chennagoun, Mohammad Monjur, Wei Lu, and **Qiaoyan Yu**, "A Hybrid Neural Network for Simultaneous Multi-Attack Detection in Sensor Networks," in Proc. Asian Hardware Security and Trust Symposium (AsianHOST'23), Dec. 2023.

C19. *M. A. Kajol, S. Sunkavilli, and **Qiaoyan Yu**, "AHD-LAM: A New Mitigation Method against Voltage-Drop Attacks in Multi-tenant FPGAs," in Proc. Asian Hardware Security and Trust Symposium (AsianHOST'23), Dec. 2023.

C20. Brandon Peddle, W. Lu, and **Qiaoyan Yu**, "Detecting DDoS Attacks in IoMT Networks Through Machine Learning Based Classification," in Proc. 2023 International Conference on Wireless Intelligent and Distributed Environment for Communication (WIDECOM'23).

C21. *M. A. Kajol and **Qiaoyan Yu**, "Attack-Resilient Temperature Sensor Design," in Proc. Intl. Symp. on Circuits and Syst. (ISCAS 2023), June 2023.

C22. **Qiaoyan Yu**, D. Sullivan, D. Chen, D. Xu, K. Jin, and J. Calzadillas, "WIP: Interdisciplinary Teaching via Hands-on Practice in Cybersecurity," in Proc. 13th IEEE Integrated STEM Education Conference, March 2023.

C23. D. Chen, N. Ghoreishi, F. Olugbon, S. Ansah, M.C. Huang, and **Qiaoyan Yu**, "Optimal pressure sensor locations in smart insoles for heel-strike and toe-off detection," in Proc. IEEE Biomedical Circuits and Systems Conference (BioCAS'22), pp. 458-461, Oct. 2022.

C24. *P. Yellu, N. Chennagouni, and **Qiaoyan Yu**, "Leveraging Intermediate Node Evaluation to Secure Approximate Computing for AI Applications," in Proc. the 21st IEEE Symposium on Technologies for Homeland Security, pp. 1-8, Nov. 2022. DOI: 10.1109/HST56032.2022.10025430.

C25. *S. Sunkavilli, N. Chennagouni, and **Qiaoyan Yu**, "DPReDO: Dynamic Partial Reconfiguration enabled Design Obfuscation for FPGA Security," in Proc. The IEEE International System-on-Chip Conference (SOCC'22), Sept. 2022. DOI:10.1109/SOCC56010.2022.9908070

C26. *M. R. Monjur, J. Calzadillas, M. Kajol, and **Qiaoyan Yu**, "Hardware Security in Advanced Manufacturing," in Proc. Great Lakes Symposium on VLSI (GLSVLSI'22), pp. 469-474, Apr. 2022.

C27. *S. Sunkavilli, and **Qiaoyan Yu**, "Security Threats and Countermeasure Deployment Using Partial Reconfiguration in FPGA CAD Tools," in Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST'22), pp. 33-36, June 2022. DOI: 10.1109/HOST54066.2022.9839731.

C28. *M. R. Monjur, J. Calzadillas, J. Heacock, and **Qiaoyan Yu**, "Challenges of Securing Low-Power LoRaWAN Devices Deployed in Advanced Manufacturing, " in Proc. International Symposium on Quality Electronic Design (ISQED'22), Apr. 2022. DOI:10.1109/ISQED54688.2022.9806290.

C29. *M. R. Monjur, J. Heacock, R. Sun, and **Qiaoyan Yu**, "An Attack Analysis Framework for LoRaWAN Applied Advanced Manufacturing," in Proc. IEEE International Symposium on Technologies for Homeland Security, pp. 1-7, Nov. 2021. DOI: 10.1109/HST53381.2021.9619847.

C30. *S. Sunkavilli, Z. Zhang, and **Qiaoyan 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.

C31. *Z. Zhang, I. Miketic, E. Salman, and **Qiaoyan 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.

C32. D. Xu, B. Liu, W. Feng, J. Ming, J. Li, Q. Zheng, and **Qiaoyan 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.

C33. *Z. Zhang, I. Miketic, E. Salman, and **Qiaoyan 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.

C34. *S. Sunkavilli, Z. Zhang, and **Qiaoyan 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.

C35. *M. S. Wara, and **Qiaoyan 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.

C36. *Z. Zhang, and **Qiaoyan 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).

C37. *M. R. Monjur, S. Sunkavilli, and **Qiaoyan 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).

C38. *P. Yellu, Z. Zhang, D. Xu, and **Qiaoyan 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.

C39. *P. Yellu, and **Qiaoyan Yu**, "Can We Securely Use Approximate Computing?", in Proc. Intl. Symp. on Circuits and Syst. (ISCAS 2020), Oct. 2020.

C40. *Z. Zhang, and **Qiaoyan Yu**, "Invariance Checking based Trojan Detection Method for Three-Dimensional Integrated Circuits" in Proc. Intl. Symp. on Circuits and Syst. (ISCAS 2020), Oct. 2020.

C41. *P. Yellu, M. R. Monjur, T. Kammerer, D. Xu, and **Qiaoyan 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.

C42. J. Wang, Y. Zhang, P. Wang, Z. Luan, X. Xue, X. Zeng, and **Qiaoyan 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.

C43. *P. Yellu, Z. Zhang, M. M. R. Monjur, R. Abeysinghe, and **Qiaoyan 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.

C44. *Z. Zhang, and **Qiaoyan 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.

C45. *P. Yellu, N. Boskov , M. Kinsy, and **Qiaoyan Yu**, "Security Threats on Approximate Computing Systems," in Proc. Great Lakes Symposium on VLSI (GLSVLSI'19), pp. 387-392, May 2019.

C46. *Z. Zhang, J. Dofe, and **Qiaoyan 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.

C47. *Z. Zhang, and **Qiaoyan 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.

C48. *Z. Zhang, and **Qiaoyan 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.

C49. *J. Dofe, and **Qiaoyan 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.

C50. *Z. Zhang, **Qiaoyan 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.

C51. *Z. Zhang, L. Njilla, C. Kamhoua, K. Kwiat, and **Qiaoyan 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.

C52. **Qiaoyan 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

C53. *J. Dofe, P. Gu, D. Stow, **Qiaoyan 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.

C54. *J. Dofe, Z. Zhang, **Qiaoyan 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.

C55. *M. R. Ansari, T. Miller, C. She, and **Qiaoyan 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.

C56. *S. Kramer, Z. Zhang, J. Dofe, and **Qiaoyan 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.

C57. *J. Dofe, and **Qiaoyan 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

C58. *J. Dofe, C. Yan, S. Kontak, E. Salman, and **Qiaoyan 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.

C59. *M. R. Ansari, T. Miller, and **Qiaoyan 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.

C60. *J. Dofe, Y. Zhang, and **Qiaoyan 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)

C61. *J. Dofe, **Qiaoyan 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.

C62. *J. Dofe, J. Frey, and **Qiaoyan 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)

C63. *H. Pahlevanzadeh, J. Dofe, and **Qiaoyan 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.

C64. *M. R. Ansari, S. Yu, and **Qiaoyan 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.

C65. *J. Dofe, J. Frey, Patrick Nsengiyumva, and **Qiaoyan 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.

C66. *J. Frey, and **Qiaoyan 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)

C67. *P. Nsengiyumva, and **Qiaoyan 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.

C68. *J. Dofe, C. Reed, N. Zhang, and **Qiaoyan 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.

C69. *K. Wu, H. Pahlevanzadeh, P. Liu, **Qiaoyan 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.

C70. *H. Pahlevanzadeh and **Qiaoyan 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.

C71. **Qiaoyan 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.

C72. **Qiaoyan 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.

C73. *T. Zhang and **Qiaoyan 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.

C74. K. Wu, P. Liu and **Qiaoyan 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.

C75. **Qiaoyan 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.

C76. M. Zhang, **Qiaoyan 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.

C77. **Qiaoyan 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.

C78. **Qiaoyan 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.

C79. **Qiaoyan 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.

C80. **Qiaoyan 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.

C81. **Qiaoyan 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.

C82. **Qiaoyan 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.

C83. **Qiaoyan 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.

C84. **Qiaoyan 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.

C85. **Qiaoyan 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.

C86. D. Huo, **Qiaoyan Yu** and P. Ampadu, "A Ballistic Nanoelectronic Device Simulator," in Proc. Intl. Symp. on Nanoscale Architectures (NanoArch'07), pp. 38-45, Oct. 2007.

C87. B. Fu, **Qiaoyan 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.

C88. **Qiaoyan 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: 20)

P1. Nishanth Chennagouni, Sandeep Sunkavilli, Wei Lu, and **Qiaoyan Yu**, "FAxC: Exploiting Feature Approximation for Privacy Preservation in Human Activity Recognition," Design Automation Conference (DAC'25), June 2025.

P2. Nishanth Chennagouni, Sandeep Sunkavilli, and **Qiaoyan Yu**,"FAxC: Exploiting Feature Approximation for Privacy Preservation in Human Activity Recognition," Wearable Health monitoring Sensors for Privacy and Security (WHiSPers) Symposium, March 2025.

P3. Mashrafi Kajol, Nishanth Chennagouni, and **Qiaoyan Yu**, "Security Challenges Towards In-Sensor Computing," Wearable Health monitoring Sensors for Privacy and Security (WHiSPers) Symposium, March 2025.

P4. Mashrafi Kajol, Nishanth Chennagouni, Andrew Lu, Wei Lu, Dean Sullivan, and **Qiaoyan Yu**, "Leveraging In-Sensor Computing to Preserve Privacy in Remote Health Monitoring," The Network and Distributed System Security (NDSS) Symposium 2025, San Diego, CA, February 2025.

P5. Nishanth Chennagouni, Sandeep Sunkavilli, and **Qiaoyan Yu**, "MFDApx: Multi-Feature Driven Approximate Computing for Wearable Sensing Systems," in IEEE-EMBS International Conference on Body Sensor Networks, Oct. 2024.

P6. Mohammad Monjur and **Qiaoyan Yu**, "Advanced Continuous-Time Convolution Framework for Security Assurance in Wireless Sensor Networks," in Great Lakes Symposium on VLSI (GLSVLSI'24), June 2024. (Best Poster Award)

P7. Mashrafi Alam Kajol, Sandeep Sunkavilli, and **Qiaoyan Yu**, "Voltage-Drop Attack Mitigation in Multi-Tenant FPGA Environments," Poster Session in New England Hardware Security Day 2024, April 2024.

P8. Sandeep Sunkavilli, Nishanth Chennagouni and **Qiaoyan Yu**, "Dynamic Attack Resilience for New FPGA Use Model," Poster Session in New England Hardware Security Day 2024, April 2024.

P9. Nishanth Chennagouni, Mohammad Monjur, Wei Lu, and **Qiaoyan Yu**, "A Hybrid Neural Network for Simultaneous Multi-Attack Detection in Sensor Network," Poster Session in New England Hardware Security Day 2024, April 2024.

P10. Sandeep Sunkavilli, Mashrafi Alam Kajol, and **Qiaoyan Yu**, "Dynamic Mitigation of Multiple and Persistent Voltage Attacks on Multi-tenant FPGA," GoMACTECH, March 2024.

P11. S. Sunkavilli and **Qiaoyan Yu**, "DPReDO: A Post Deployment Dynamic Countermeasure to Strengthen Design Obfuscation for FPGA Accelerators," New England Hardware Security Day, Boston, April 2023.

P12. Mohammad Monjur, and **Qiaoyan Yu**, "Multiple Physical Attacks in Sensor Network," DEPSCoR Day 2023.

P13. Sandeep Sunkavilli, and **Qiaoyan Yu**, "Dynamic Attack Resilience for New FPGA Use Model," DEPSCoR Day 2023.

P14. M. Monjur, J. Heacock and **Qiaoyan Yu**, "Analysis of Security Vulnerability of LoRaWAN Applied in Advanced Manufacturing," 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2022.

P15. M. Monjur and **Qiaoyan Yu**, "Security Risks and Challenges for Low-power Edge devices in Advanced Manufacturing," 2022 New England Hardware Security Workshop Day.

P16. P. Yellu, and **Qiaoyan Yu**, "APB Concealing: New Obfuscation Method for Securing Approximate Computing Systems," WIP in DAC 2021.

P17. P. Yellu, L. Buell, and **Qiaoyan 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/

P18. P. Yellu, L. Buell, and **Qiaoyan Yu**, "WiP: Systematic Attack Models for Approximate Computing Systems," in Hardware and Architectural Support for Security and Privacy (HASP) 2020.

P19. S. Sunkavilli and **Qiaoyan Yu**, "Security from CAD Tools Perspective for Using Dynamic Partial Reconfiguration in On premise and Off premise FPGAS," 2022 New England Hardware Security Workshop Day.

P20. J. Dofe, Y. Zhang, and **Qiaoyan 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)

Invited Talks (Total: 47)

T1. Qiaoyan Yu, Dec 4-5, 2025, **Visionary Talk** "New Frontiers in Hardware and Systems Security," The Nelms Annual IoT Conference, Gainesville, FL, USA.

T2. Qiaoyan Yu, June 22, 2025, **Keynote** "Standardizing Attack Model for Hardware Security Community," Workshop on Hardware Attack Artifacts, Analysis, and Metrics (WHAAAM), co-located with DAC 2025, San Francisco, CA, USA.

T3. Qiaoyan Yu, June 22, 2025, "Mitigating Voltage-Drop Attacks through Intelligent On-Chip Sensor Utilization," The 3rd AI/CAD for Hardware Security Workshop (AICAD4Sec 2025), co-located with DAC 2025, San Francisco, CA, USA.

T4. Qiaoyan Yu, May 20, 2025, **Keynote** "Research and Education Opportunities in NSF SaTC Programs," The 34th Microelectronics Design and Test Symposium (IEEE MDTS 2025), Albany, New York, USA.

T5. Qiaoyan Yu, May 30, 2025, "Biometric-Feature-Driven Approximation (Bio-FDApx) for Wearable Health Monitoring Systems," Queen's University, Belfast, United Kingdom (UK).

T6. Qiaoyan Yu, Mar. 2025, " Check it & Track it–Cybersecurity Hands-on Projects for High School Students," ISEC'25 Workshop: Robotics, AI, and Cybersecurity Research and Education for Pre-University Communities, Princeton, NJ, USA.

T7. Qiaoyan Yu, Jan. 2025, "Hardware Security–The Root of Trust in Cybersecurity," Dartmouth College, Hanover, NH, USA.

T8. Qiaoyan Yu, Nov. 2024, **Keynote** "Opportunities in NSF to Support Women's Participation in STEM," Workshop for Women in Hardware and Systems Security, IBM Thomas J. Watson Research Center, New York, USA.

T9. Qiaoyan Yu, Oct. 2024, **Visionary Talk** "NSF Proposal Preparation and Helpful Hints," ACM CCS 2024 DEI Workshop, Salt Lake City, Utah, USA.

T10. Qiaoyan Yu, Oct. 2024, **Keynote** "Research and Education Opportunities in NSF SaTC Programs," Quantum Computer Cybersecurity Symposium, Yale University, New Haven, CT, USA.

T11. Qiaoyan Yu, Aug. 2024, **Keynote** "Research and Education Opportunities in NSF CNS Program, " 1st Symposium on Emerging Topics in Networks, Systems, and Cybersecurity, Hoboken, NJ, USA.

T12. Qiaoyan Yu, April 2024, "Hardware Security in The Era of Machine Learning," Virginia Tech, VT, USA.

T13. Qiaoyan Yu, May 2023, "Hardware Security in The Era of Machine Learning," 2023 IEEE Microelectronics Design and Test Symposium, Albany, NY, USA.

T14. Qiaoyan Yu, Apr. 2023, "Building Security into Integrated Circuits and Systems," Arizona State University, Tempe, AZ, USA.

T15. Qiaoyan Yu, Nov. 2022, "Hardware Security and Its Implication in Practical Applications," University of Arkansas, Fayetteville, AR, USA.

T16. Qiaoyan Yu, Oct. 2022, "Introduction to Approximate Computing," University of Maine, Orono, ME, USA.

T17. Qiaoyan Yu, Oct. 2022, "Security Challenges in Advanced Manufacturing," Cybersecurity Awareness Month, University of New Hampshire, Durham, NH, USA.

T18. Qiaoyan Yu, May 2022, "Proactive Defense Methods for Hardware-Oriented Security," Future of Moving Data Summit— Network Measurement, Performance and Tuning, NH, USA.

T19. Qiaoyan Yu, Mar. 2022, "Blurring Boundaries: A New Method for Securing Approximate Computing Systems," University of Delaware, DE, USA.

T20. Qiaoyan Yu, Mar. 2021, "Towards Securing Approximate Computing Systems ", Villanova University, PA, USA.

T21. Qiaoyan Yu, Mar. 2021, "Hardware Security in Three Dimensional (3D) Integrated Circuits and Systems", NYU, NY, USA.

T22. Qiaoyan Yu, Oct. 2020, "Hardware Security—The Root of Trust," National Cyber Security Awareness Month (NCSAM).

T23. Qiaoyan Yu, Oct. 2020, "Hardware Security in Three-Dimensional Integrated Circuits and Systems," ISCAS2020 Tutorial.

T24. Qiaoyan Yu, June 2020, "Exploiting Principles of Moving Target Defense to Address FPGA Security Threats," Intel.

T25. Qiaoyan Yu, June 2020, "Managing Hardware Security in Three Dimensional Integrated Circuits," Hardware Security e-Workshop, Semiconductor Research Corporation (SRC).

T26. Qiaoyan Yu, Feb. 2019, "Proactive Defense Methods for Integrated Circuits & Systems Security," University of Georgia, GA, USA.

T27. Qiaoyan Yu, Feb. 2019, "Assuring the Root of Trust for Internet-of-Things (IoTs)," George Mason University, VA, USA.

T28. Qiaoyan Yu, Nov. 2018, "Towards Securing 2D and 3D Integrated Circuits and Systems," MIT Lincoln Laboratory, MA, USA.

T29. Qiaoyan Yu, May 2018, "A Whitebox Introduction to Fault Attacks," HOST2018 Tutorial.

T30. Qiaoyan Yu, Feb. 2018, "Proactive Defense Methods for Integrated Circuits & Systems Security," Virginia Tech., VA, USA.

T31. Qiaoyan Yu, Oct. 2017, "Multi-Layer Design Obfuscation Methods for Hardware Security," Clarkson University, NY, USA.

T32. Qiaoyan Yu, Aug. 2017, "Proactive Defense Methods for Chip Integrity and Security," Tokyo University, Japan.

T33. Qiaoyan Yu, Aug. 2017, "Proactive Defense Methods for Chip Integrity and Security," Asia and South Pacific Design Automation Conference EDA Workshop, Japan.

T34. Qiaoyan Yu, Aug. 2017, "Countermeasures against Security Threats on Integrated Circuits and Systems," Shanghai Jiao Tong University, Shanghai, China.

T35. Qiaoyan Yu, Aug. 2017, "Addressing Security Threats on Integrated Circuits," Zhejiang University, Hangzhou, China.

T36. Qiaoyan Yu, Jul. 2017,"Proactive Defense Methods for Integrated Circuits and Systems," MITRE, Bedford, MA, USA.

T37. Qiaoyan Yu, Jun. 2017, "Towards Securing 2D and 3D Integrated Circuits (ICs)," Air Force Research Laboratory, Cyber Assurance Branch, Rome, NY, USA.

T38. Qiaoyan Yu, Apr. 2017, "Design Obfuscation Methods for Securing 2D and 3D Integrated Circuits," Worcester Polytechnic Institute, MA, USA.

T39. Qiaoyan Yu, Dec. 2016, "Gate-level Design Obfuscation Methods for Secure Circuits and Systems," National Tsing Hua University, Hsinchu, Taiwan.

T40. Qiaoyan Yu, Nov. 2016, "Managing Security for 2D and 3D Integrated Circuits (ICs)," University of Delaware, DE, USA.

T41. Qiaoyan Yu, Jun. 2016, "Design Obfuscation Methods for 2D and 3D Integrated Circuits (ICs)," Charles Stark Draper Laboratory, MA, USA.

T42. Qiaoyan 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.

T43. Qiaoyan Yu, Aug. 2015, "Hardware Trojan Detection in Networks-on-Chip," Asia and South Pacific Design Automation Conference EDA Workshop, Taiwan.

T44. Qiaoyan Yu, Aug. 2015, "Hardware Security and Trust," Invited Talk, Ningbo University, Ningbo, China.

T45. Qiaoyan Yu, Jan. 2013, "Energy-efficient and Reliable Many-core Systems," Hangzhou Dianzi University, Hangzhou, China.

T46. Qiaoyan Yu, Jan. 2013, "Reliable VLSI Design," Ningbo University, Ningbo, China.

T47. Qiaoyan Yu, Nov. 2012, "Reliability Management for Energy-efficient Hybrid Many-core Systems," Oak Ridge National Laboratory, Oak Ridge, TN, USA.

Professional Service

Program Director

- Division of Computer and Network Systems (CNS), Computer and Information Science and Engineering (CISE), National Science Foundation, 2024-present

Founder

- WHiSPerS: Wearable Health monitoring Sensors for Privacy and Security Symposium 2025
- HWiQ Workshop: Hardware Security in the Era of Quantum Computing & Post-Quantum Cryptography 2025, 2026
- WISE Workshop: Workshop for Women in Hardware and Systems Security 2017-present

Education Chair

- Educational Activities in New Hampshire State 2023-present

Panel Service

- CAD For Assurance: Hardware IP Security In The Age of Heterogeneous Integration, Oct. 2024
- ICCAD Sushi Workshop, Oct. 2024
- GLSVLSI, June 13, 2024
- ISVLSI, July, 2024
- NH Aspirations in Computing Award Celebration Day, May 13, 2023

Editor Service

- Associate Editor of the IEEE Trans. on Circuits and Systems - I: Regular Papers 2024-present
- Associate Editor of Integration, the Journal of VLSI 2013-present
- Associate Editor of Microelectronics Journal- Elsevier 2012-2017
- Guest Editor of 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 of VLSI Design-Hindawi, Special Issue on Advanced VLSI Architecture Design for Emerging Digital Systems 2014

Conference/Workshop Organization

- General Co-chair, IEEE International Test Conference in Asia (ITC-Asia) 2026
- General Co-chair, "Top Picks in Hardware and Embedded Security 2023," 2023
- 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-present
- 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 Engineering in Medicine and Biology Society (EMBS) 2025
- The ACM Conference on Computer and Communications Security (CCS) 2025
- Design, Automation, and Test in Europe (DATE) 2024
- IEEE Microelectronics Design & Test Symposium 2021-Present
- Hardware and Architectural Support for Security and Privacy (HASP) 2020
- Top Picks in Hardware and Embedded Security 2019, 2020, 2023
- 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-present
- 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
- IEEE 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 SaTC panel, 2022, 2023
- 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

- Gabrielle MacNeil (Expected May 2029)

- Mashrafi Alam Kajol (Expected May 2027)
- Nishanth Goud Chennagouni (Expected May 2027)
- Mohammad Mezanur Monjur (Expected May 2026)

PhD Alumnus

- Sandeep Sunkavilli (May 2025)
  Dissertation title: Dynamic Defense Strategies for FPGA Security
  Current position: Lecturer, University of New Hampshire
- Pruthvy Yellu (September 2023)
  Dissertation title: Securing Approximate Computing Systems
  Current position: Logic Design Engineer, Teradyne.
- 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: Senior Engineer, Qualcomm
- 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

Master Alumni

- Mohammad Shafeul Wara (September 2021)
  Current Position: Senior Engineer I-Product, 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)
  Backend Software Engineer, TikTok

Dissertation title: Network Interface Design for Network On Chip

Undergraduate Research

- Andre Boufama, Summer 2023
  Overpass Oasis: Bridging Nature with Innovation, Concept
- Hao Zhang, Fall 2022
  Camera-based Sensing System Security
- Joshua Calzadillas, Fall 2021, Summer 2022
  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