Curriculum Vitae of Yunsi Fei

Dept. of Electrical & Computer Engr.
Northeastern University
415 ISEC
360 Huntington Ave., Boston, MA 02115

E-mail: y.fei@northeastern.edu
Tel: 617-373-2039 (O)
Fax: 617-373-8970
URL: https://chest.coe.neu.edu

Employment History

10/2021 to current:	Associate Dean for Faculty Affairs, College of Engineering, Northeastern University, Boston, MA.
09/2019 to current:	Site Director, NSF IUCRC Center for Hardware and Embedded System Security and Trust (CHEST) Northeastern University
07/2017 to current:	Professor, Department of Electrical and Computer Engineering, Northeastern University, Boston, MA.
09/2017 – 04/2018:	Visiting Scientist, Secure Resilient System and Technology Group, MIT Lincoln Lab, Lexington, MA.
09/2011 – 06/2017:	Associate Professor, Department of Electrical and Computer Engineering, Northeastern University, Boston, MA.
08/2010 – 08/2011:	Associate Professor, Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT.
08/2004 – 08/2010:	Assistant Professor, Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT.

Research Areas

Hardware-oriented security and trust
Side-channel attack, protection, and evaluation
Integrated circuit and embedded system design automation
Secure and efficient computer architecture
Mobile computing and underwater sensor networks
Cyber-physical and machine learning systems

Professional Experience

1999-2004:	Research assistant, Princeton University, Princeton.
2002-2004:	Research visitor at NEC Labs America, Princeton, NJ.
1996-1999:	Research assistant, Tsinghua University, Beijing, China.

Education

Princeton University. PhD in Electrical Engineering. Completed in Aug. 2004.

- Dissertation: System-level energy analysis and optimization of embedded systems
- Advisor: Prof. Niraj K. Jha

Princeton University. Master of Arts in Electrical Engineering. May 2001.

Tsinghua University, China. Master of Science in Electronic Engineering, July 1999.

Tsinghua University, China. Bachelor of Science in Electronic Engineering, July 1997.

Awards

- **IEEE Fellow**, Class of 2026, for contributions in side-channel analysis, protection of computing accelerators, and robust security evaluation.
- **Northeastern University Outstanding PhD Student Award in Research,** Ruyi Ding, Apr. 2025.
- **Northeastern University College of Engineering Graduate External Award,** Ruyi Ding, Apr. 2024.
- **Best Poster Award,** the 3rd place, "Cross CPU-GPU Rowhammering Attacks," PhD student Yufei Wang, in New England Hardware Security Day 2025.
- **Distinguished Paper Award**, ACM Asia Conf. on Computer and Communications Security (AsiaCCS), "EMShepherd: Detecting Adversarial Samples via Side-channel Leakage," with PhD students Ruyi Ding, Cheng Gongye, and Siyue Wang, and Prof. A. Adam Ding. July 2023.
- **Best Poster award**, the 2nd place, "Software Power Side-channel Assisted Model Extraction of Deep Neural Networks," PhD student Xiang Zhang, in New England Hardware Security Day 2023.
- **Best Paper Award**, IEEE Great Lake Symposium on VLSI, "Protected ECC Still Leaks: A novel differential-bit side-channel power attack on ECDH and countermeasures," with PhD students Tianhong Xu and Cheng Gongye, May 2022.
- **Best Paper Award**, IEEE International Conference on Computer Design (ICCD), "Nacre: Durable, Secure and Energy-Efficient Non-Volatile Memory Utilizing Data Versioning," with PhD student Mohammad Tavana and Prof. David Kaeli, Nov. 2017.
- Dissertation Completion Fellowship of Northeastern University Office of the Provost, for Zhen Hang Jiang, May – Aug. 2019.
- Graduate Dissertation Research Grant of Northeastern University Office of the Provost, for Pei Luo, Jan. – Dec. 2017.
- Invited attendee for The Frontiers of Engineering Education (FOEE) Symposium, National Academy of Engineering, Sept. 2016.
- "Most Flag Points" award in MITRE Embedded Security Catch-the-Flag (eCTF) competition and 2nd place, advisor for a team of eight undergraduate students (Mitch Kucia, Alyssa Bezreh, Sam Sussman, Bryce Carter, Christopher Babroski, Xinhao Zhu, Chris Holtsnider, Ginamarie Spiridigliozzi), Apr. 2016.
- **Best Paper Award**, IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), with PhD student Yu Han, Oct. 2015.
- Northeastern University ReDI (Research and Development Initiatives) Cohort Challenge Participant, 2015 – 2016.
- College of Engineering Faculty Fellow, Northeastern University, 2015.
- **Best Cyber Security Solution** at *Advanced Cyber Security Center Annual Conference 2014.* "Scalable Open-source Side-channel Evaluation Platform for Cryptographic Devices", Neel Shah, Tushar Swamy, Harrison Dimmig, Yunsi Fei, and David Kaeli.
- NSF CAREER award, Trustworthy Computing Program, CNS, 2009
- Graduate Student Fellowship, Princeton Univ., 1999-2000
- Outstanding Graduate Students Fellowship, Tsinghua Univ., 1998
- Social Practice (summer internship) Scholarship, Tsinghua Univ., 1998
- Honored Graduate of Tsinghua University, 1997
- "12-9" Memorial Fellowship, Tsinghua Univ., 1995, 1996
- Distinguished Students Scholarship, Tsinghua Univ., 1992, 1993, 1994

Research Grants (External) – Summary: Have been on grants totaling $12.6 Million, my share amount is $6.5 Million, am the PI for $8.0 Million.

Active grants:

1. **Title: LP1: SPICE – Secure RISC-V Processor Design and Implementation as a Service**
   Agency: CHEST Industry Fund
   Term: 03/01/2025 − 8/31/2026
   Amount: $375,000
   Role: PI
2. **Title: Administration of CHEST I/UCRC Research Projects**
   Agency: CHEST Industry Fund
   Term: 01/01/2025 − 8/31/2026
   Amount: $100,000
   Role: PI
3. **Title: Fault Attacks on Post-Quantum Cryptography CRYSTAL-Kyber Implementations**
   Agency: CHEST Industry Fund
   Term: 07/01/2024 − 8/31/2025
   Amount: $70,000
   Role: PI
4. **Title: Cross-device and cross-leakage transfer learning based side-channel analysis**
   Agency: CHEST Industry Fund
   Term: 07/01/2024 − 8/31/2025
   Amount: $120,000
   Role: PI (share 60%, with Co-PI Adam Aidong Ding and Boyang Wang University of Cincinnati)
5. **Title: Ensuring confidentiality in fully analog neural system**
   Agency: CHEST Industry Fund
   Term: 07/01/2024 − 8/31/2025
   Amount: $75,000
   Role: Co-PI (share 30%)
6. **Title: Security Analysis of Post-Quantum Cryptography CRYSTAL-Kyber Implementations**
   Agency: CHEST Industry Fund
   Term: 07/01/2023 − 8/31/2025
   Amount: $100,000
   Role: PI
7. **Title: Chip Design and Fabrication for CHEST Projects**
   Agency: CHEST Industry Fund
   Term: 07/01/2023 − 8/31/2025
   Amount: $83,659
   Role: PI (60% share)
8. **Title: Cyber-hardening and cyber-security of additive manufacturing systems and devices**

Agency: Army Research Lab.
Term: 01/01/2023 − 12/31/2024
Amount: $156,228
Role: PI

9. **Title: EAGER: Side Channels Go Deep – Leveraging Deep Learning for Side-channel Analysis and Protection**
   Agency: National Science Foundation
   Term: 07/01/2022 − 06/30/2025
   Amount: $300,000
   Role: PI (Co-PI: Aidong Adam Ding)

10. **Title: RINGS: Internet of Things Resilience through Spectrum-Agile Circuits, Learning-Based Communications and Thermal Hardware Security**
    Agency: NSF
    Term: 05/01/2022 − 4/30/2025
    Amount: $999,996
    Role: Co-PI (PI: Marvin Onabajo, Co-PIs: Aatmesh Shrivastava, Francesco Restuccia)

11. **Title: SaTC: Core: Medium: Protecting Confidentiality and Integrity of Deep Neural Networks against Side-channel and Fault Attacks**
    Agency: National Science Foundation (NSF)
    Term: 10/01/2019 − 9/30/2025
    Amount: $1,224,000
    Role: PI (with Co-PIs Xue Lin and Thomas Wahl)

12. **Title: Phase I IUCRC Northeastern University: Center for Hardware and Embedded System Security and Trust (CHEST)**
    Agency: National Science Foundation (NSF)
    Term: 09/15/2019 − 08/31/2026
    Amount: $750,000
    Role: PI

Past grants:

1. **Title: Is ARM Trustzone trustable?**
   Agency: CHEST Industry Fund
   Term: 06/01/2021 − 12/31/2023 (Year 1 and Year 2)
   Amount: $105,000
   Role: PI
2. **Title: Secure RISC-V Design, Implementation, and Simulation (Year 2)**
   Agency: CHEST Industry Fund
   Term: 06/01/2021 − 6/30/2023
   Amount: $85,000
   Role: PI (Co-PI: David Kaeli)

3. **Title: Current sensing based on-chip Analog Trojan Detection Circuit Compatible with Design and Validation (Year 2)**
   Agency: CHEST Industry Fund
   Term: 06/01/2021 − 6/30/2023
   Amount: $75,000
   Role: Co-PI (PI: Aatmesh Shrivastava)

4. **Title: Persistent cache monitor to combat ransomware**
   Agency: CHEST Industry Fund
   Term: 06/01/2021 – 6/30/2023
   Amount: $100,000
   Role: PI (Co-PI: Adam Aidong Ding)

5. **Title: Secure Deep Learning on Edge Devices**
   Agency: ONR
   Term: 10/01/2021 – 9/30/2022
   Amount: $400,000
   Role: Co-PI (PI: Shelley Xue Lin, Co-PI: Xiaolin Xu)

6. **Title: Secure Design by RISC-V Framework (Year 1)**
   Agency: CHEST Industry Fund
   Term: 06/01/2020 – 12/31/2021
   Amount: $70,000
   Role: PI (Co-PI: David Kaeli)

7. **Title: Current sensing based on-chip Analog Trojan Detection Circuit Compatible with Chip Design and Validation Flow (Year 1)**
   Agency: CHEST Industry Fund
   Term: 06/01/2020 – 12/31/2021
   Amount: $50,000
   Role: Co-PI (with PI Aatmesh Shrivastava)

8. **Title: Side-channel vulnerabilities analysis of ADRF SOC**
   Company: Analog Devices
   Term: 08/01/2020 – 7/31/2021
   Amount: $30,000
   Role: single PI

9. **Title: Embedded ICS Security Modules**
   Agency: MIT Lincoln labs
   Term: 01/01/2019 – 12/31/2020
   Amount: $75,000
   Role: PI

10. **Title: Planning IUCRC Northeastern University: Center for Hardware and Embedded System Security and Trust (CHEST)**
    Agency: National Science Foundation (NSF)
    Term: 02/01/2018 – 01/31/2019
    Amount: $15,000
    Role: PI (center site director)

11. **Title: TWC: Medium: Automating Countermeasures and Security Evaluation against Software Side-channel Attacks**
    Agency: National Science Foundation (NSF), Secure and Trustworthy Cyberspace (SaTC)
    Term: 06/01/2016 – 05/31/2021
    Amount: $1,200,000
    Role: PI (my share: 45%, co-PI: Aidong Adam Ding (Math), Thomas Wahl (CCIS))

12. **Title: STARSS: Small: Side-channel Analysis and Resilience Targeting Accelerators**

Agency: National Science Foundation (NSF), Semiconductor Research Corporation (SRC), Secure and Trustworthy Cyberspace (SaTC) - STARSS
Term: 10/01/2016 − 09/30/2020
Amount: $450,000
Role: co-PI (my share: 50%, PI: David Kaeli)

13. **Title: Evaluating side-channel vulnerabilities of a SiOMetrics USB Token**
    Company: Analog Devices
    Term: 01/01/2018 – 6/30/2019
    Amount: $90,000
    Role: single PI

14. **Title: Embedded hardware-based security and side channel analysis**
    Company: Analog Devices
    Term: 11/01/2015 − 12/31/2016
    Amount: $20,000
    Role: single PI

15. **Title: Side-channel power analysis of security modules of ADSP-BF70x embedded processors**
    Company: Analog Devices
    Term: 08/01/2014 − 12/31/2016
    Amount: $20,000
    Role: single PI

16. **Title: MRI: Development of Northeastern University Marine Observatory NETwork (NU MONET)**
    Agency: National Science Foundation (NSF), Computer and Network Systems (CNS), Major Research Instrumentation (MRI)
    Term: 09/01/2014 − 08/31/2018
    Amount: $400,000 (NU additional 30% cost sharing $171,429).
    Role: co-PI (my share: 30%, PI: Stefano Basagni, other co-PI: Milicia Stojanovic, senior personnel: Mark Patterson)

17. **Title: MRI: Development of a Testbed for Side-Channel Analysis and Security Evaluation - TeSCASE**
    Agency: National Science Foundation (NSF), Computer and Network Systems (CNS), Major Research Instrumentation (MRI)
    Term: 10/01/2013 − 09/30/2018
    Amount: $500,000 (NU additional 30% cost sharing $214,286).
    Role: PI (my share: 50%, co-PIs: David Kaeli and Miriam Leeser, senior personnel: Adam A. Ding and Daniel Wichs)

18. **Title: TWC: Medium: Collaborative: A unified statistics-based framework for side-channel attack analysis and security evaluation of cryptosystems**
    Agency: National Science Foundation (NSF), Computer and Network Systems (CNS), Secure and Trustworthy Cyberspace (SaTC)
    Term: 07/01/2013 − 06/30/2017
    Amount: $798,057, with NU as the leading institute and NU's share of $522,102
    Role: PI (my share of the NU grant: 60%, co-PI: Adam A. Ding, WPI PI: Thomas Eisenbarth)

19. **Title: ARTS: Adaptive, RobusT, and Sustainable networking for undersea distributed sensor systems**
    Agency: Office of Naval Research (ONR)

Term: 10/01/2011 – 09/30/2015
Amount: $394,399
Role: single PI (Awarded to NU)

20. **Title: CAREER: Architectural enhancement and design methodologies for secure processing in embedded systems**
Agency: National Science Foundation (NSF), Computer and Network Systems (CNS)
Term: 09/01/2009 – 08/31/2014
Amount: $405,000 (UConn additional matching fund: $30,000)
Role: single PI (Awarded to UConn, $279,009 transferred in as a sub-award to NU)

21. **Title: ARTS: Adaptive, RobusT, and Sustainable networking for undersea distributed sensor systems**
Agency: Office of Naval Research (ONR)
Term: 06/01/2010 – 05/30/2014
Amount: $290,526
Role: single PI (Awarded to UConn, $137,646 transferred in as a sub-award to NU)

22. **Title: Graduate Assistance in Areas of National Needs (GAANN): Advanced Computer Security**
Agency: U.S. Department of Education
Term: 08/15/2009 – 08/14/2012 (Awarded to UConn)
Amount: $522,000
Role: co-PI (PI: John Chandy, other co-PIs: Mohammad Tehranipoor, Lei Wang, Zhijie Jerry Shi, Bing Wang, Alex Shvartsman, Aggelos Kiayias)

23. **Title: MRI: Development of instrumentation for an autonomous underwater sensor network system**
Agency: National Science Foundation (NSF), Major Research Instrumentation (MRI)
Term: 08/01/2008 – 07/31/2012 (Awarded to UConn)
Amount: $516, 000
Role: senior personnel

24. **Title: CRI: Developing a novel Infrastructure for underwater acoustic sensor networks**
Agency: National Science Foundation (NSF), Computing Research Infrastructure (CRI)
Term: 08/01/2007 – 07/31/2010 (Awarded to UConn)
Amount: $320, 000
Role: senior personnel

25. **Title: A multi-level/multi-faceted framework for energy-efficient application-specific instruction set processor synthesis**
Agency: National Science Foundation (NSF), Computing and Communication Foundation (CCF), Computing Processes and Artifacts (CPA)
Term: 04/01/2006 – 03/31/2011 (Awarded to UConn)
Amount: $275,000
Role: single PI

26. **Title: REU Site: Trustable Computing Systems Security Research and Education**
Agency: National Science Foundation, CNS - CISE - Research Experiences for Undergraduates Sites
Term: 06/01/2011 – 05/31/2014 (Awarded to UConn)
Amount: $350,000

Role: mentor (PI: John Chandy, other mentors: Aggelos Kiayias, Zhijie Jerry Shi, Mohammad Tehranipoor, Bing Wang, Lei Wang)

27. **Title: TUES Type I: Exploratory curriculum for trustable computing systems security education**
Agency: National Science Foundation, Division of Undergraduate Education
Term: 09/01/2011 – 08/31/2013 (Awarded to UConn)
Amount: $197,000
Role: co-PI (PI: John Chandy, other co-PIs: Zhijie Jerry Shi, Mohammad Tehranipoor, Lei Wang)

Research Grants (Internal)

1. UConn Intermediate Equipment Competition Grant, “Platform for Side-Channel Security Attack Analysis,” PI (with co-PIs: Mohammad Tehranipoor, Zhijie Jerry Shi, Aggelos Kiayias, Robert X. Gao, and Joseph McIsaac), $97,089, 2010-2011.
2. “Coordinated management of mobile computer systems: balancing Quality-of-Service (QoS) and energy efficiency,” UConn Research Foundation large grant, 06/01/2006-04/30/2008, single PI, $32,000.
3. Seed fund for UConn Underwater Sensor Networks Lab, contributed by UConn’s three departments (CSE, ECE, and EEP), School of Engineering, and BECAT center, co-PI (with Jun-hong Cui, Shengli Zhou, Zhijie Jerry Shi, and Bing Wang), $42,750.
4. UConn School of Engineering Dean’s commitment, 08/01/2006-06/30/2008, single PI, $20,000.

Publications (* indicates students/PostDocs advised by me)

Book Chapters:

B1. M. Vai, Y. Fei, and R. Khazan: Guest Editorial: Special Issue on Hardware Solutions for Cyber Security. J. Hardware and System Security (2019) 3(3).

B2. K. K. Raymond Choo, Y. Fei, Y. Xiang, and Y. Yu: Guest Editorial: Special Issue on Embedded Device Forensics and Security, ACM Transactions on Embedded Computing Systems (TECS) (Apr. 2017) 16 (2).

B3. T. Eisenbarth, Y. Fei, and D. Serpanos: Guest Editorial: Special Section on Embedded System Security. Embedded System Letters 7(1): 1-2 (2015).

B4. Y. Fei and *J. C. Martinez Santos, “Security in Embedded Systems.” In: M. Tehranipoor and C. Wang, Eds. *Introduction to Hardware Security and Trust*. New York: Springer, 2012.

Journal Publications:

Published/Accepted:

J1. J. Yang, T. Gourousis, M. Yan, *R. Ding, A. Mittal, M. Zhang, F. Restuccia, A. Shrivastava, Y. Fei, and M. Onabajo, “A low-power differential temperature sensor with chopped cascode transistors and switched-capacitor integration,” MDPI Electronics, Vol. 14, No. 12, June 2025.

J2. N. Mirchandani, *M. Sabbagh, Y. Fei, and A. Shrivastava, “A high-efficiency power obfuscation switched-capacitor DC-DC converter architecture,” *IEEE Trans. on Computer-aided Design of Integrated Circuits & Systems,* Vol. 43, No. 10, Oct. 2024.

J3. Y. Li, P. Zhao, *R. Ding, T. Zhou, Y. Fei, X. Xu, and X. Lin, “Neural architecture search for adversarial robustness via learnable pruning,” *Frontiers in High Performance Computing,* Vol. 2, Sept. 2024.

J4. A. Miittal, M. Zhang, T. Gourousis, *Z. Zhang, Y. Fei, M. Onabajoo, F. Restuccia, A. Shriivastava, “Sub-6-GHz Energy-Detection-Based Fast On-Chip Analog Spectrum Sensing With Learning-Driven Signal Classification,” IEEE Internet of Things J., Vol. 11, No. 14, July 2024.

J5. S. Maji, K. Lee, *C. Gongye, Y. Fei, and A. P. Chandrakasan, “An energy-efficient neural network accelerator with improved resilience against fault attacks,” *J. Solid State Circuits,* conditional accept with major revision, Jan. 2024.

J6. *Z. Zhang, A. Ding, and Y. Fei, “A guessing entropy-based framework for deep learning-assisted side-channel analysis,” *IEEE Trans. on Information Forensics and Security*, pp. 30183030, May 2023.

J7. T. Yang, A. Mittal, Y. Fei, and A. Shrivastava, “Large delay Analog Trojans: A silent fabrication-time attack exploiting analog modalities,” *IEEE Trans. on Very Large Scale Integration Systems,* vol. 29, no. 1, pp. 124-135, Jan. 2021.

J8. Mohammad Khavari Tavana, Yunsi Fei and David Kaeli, “Nacre: Durable, Secure and Energy-efficient Non-Volatile Memory Utilizing Data Versioning,” *IEEE Transactions on Emerging Technologies in Computing (TETC)*, Vol. 8, No. 4, pp. 897-906, Oct.-Dec. 2020.

J9. *Z. Zhang, A. A. Ding, and Y. Fei, “A fast and accurate guessing entropy estimation algorithm for full-key recovery,” *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES),* no. 2, Sept. 2020.

J10. *C. Luo, Y. Fei, A. Ding, and P. Closas, “Comprehensive Side-channel Power analysis of XTS-AES,” *Transactions on CAD (TCAD)*, Vol. 38, No. 12, pp. 2191-2220, Dec. 2019.

J11. *Z. H. Jiang, Y. Fei, and D. Kaeli, “Exploiting Bank Conflict based Side-channel Timing Leakage of GPUs,” *ACM Transaction on Architecture and Code Optimization (TACO),* Vol. 16, No. 4, Nov. 2019.

J12. *L. Zhang, A. Ding, Y. Fei, and *P. Luo, “Efficient nonprofiling 2nd-order power analysis on masked devices utilizing multiple leakage points,” *IEEE Trans. On Dependable & Secure Computing,* Vol. 16, No. 5, Sept. – Oct. 2019.

J13. *C. Luo, Y. Fei, and D. Kaeli, “Side-channel timing attack of RSA on a GPU,” *ACM Transaction on Architecture and Code Optimization (TACO)*, Vol. 16, No. 3, Aug. 2019.

J14. *C. Luo, Y. Fei, *L. Zhang, A. A. Ding, *P. Luo, S. Mukherjee, and D. Kaeli, “Power analysis attack of an AES GPU implementation,” *Springer. J. Hardware & System Security* (HASS)*,* Vol. 2, No. 1, pp. 69-82, Mar. 2018.

J15. *P. Luo, *K. Athanasiou, Y. Fei, and T. Wahl, “Algebraic fault analysis of SHA-3 under relaxed fault models,” *IEEE Trans. on Information Forensics and Security,* Vol. 13, No. 7, July 2018.

J16. *Y. Han and Y. Fei, “TARS: A traffic-adaptive receiver-synchronized medium access control protocol for underwater sensor networks”, *ACM Trans. On Sensor Networks* (TOSN), vol. 13(4), pp. 27:1-27:25, Dec. 2017.

J17. *B. Jiang and Y. Fei, “A PHEV power management cyber-physical system for on-road applications,” *IEEE Trans. On Vehicular Technology* (TVT), vol. 66, no. 7, pp. 5797-6807, July 2017.

J18. *B. Jiang and Y. Fei, "Vehicle speed prediction by two-level data driven models in vehicular networks," *IEEE Trans. On Intelligent Transportation Systems* (TITS), vol. 18, no. 7, pp. 1793-1801, July 2017.

J19. *P. Luo, Y. Fei, *L. Zhang, and A. A. Ding, "Differential fault analysis of SHA-3 under relaxed fault models," *Springer. J. Hardware & System Security* (HASS), vol. 1, no. 2, pp. 156-172, June 2017.

J20. *Y. Han and Y. Fei, "DAP-MAC: A delay-aware probability-based MAC protocol for underwater acoustic sensor networks," *Elsevier Ad Hoc Networks* (ADHOC), Vol. 48, pp. 80-92, Sept. 2016. (DOI: j0.1016/j.adhoc.2016.05.003)

J21. Y. Fei, A. A. Ding, *J. Lao and *L. Zhang, "A statistics-based success rate model for DPA and CPA," *Journal of Cryptographic Engineering* (JCE), vol. 5, no. 4, pp. 227-243, Nov. 2015. (DOI: 10.1007/s13389-015-0107-0.)

J22. *B. Jiang and Y. Fei, "Smart home in smart microgrid: A cost-effective energy ecosystem with intelligent hierarchical agents," *IEEE Trans. Smart Grid* (TSG), vol.6, no. 1, pp. 3-13, Jan. 2015.

J23. *J. C. Martinez-Santos and Y. Fei, "Leveraging speculative architectures for run-time program validation", ACM Trans. on Embedded Computing Systems (TECS), vol. 13, no. 1, Article No. 3, Aug. 2013. (doi:10.1145/2512456)

J24. *H. Lin and Y. Fei, "Resource sharing of pipelined custom hardware extension for energy-efficient application-specific instruction set processor design", *ACM Trans. on Design Automation of Electronic Systems* (TODAES), vol. 17, no. 4, Oct. 2012.

J25. *H. Lin, *T. Hu, and Y. Fei, "Utilizing custom registers in application-specific instruction set processors for register spill elimination", *ACM Trans. on Design Automation of Electronic Systems* (TODAES), vol. 17, no. 4, Oct. 2012.

J26. *X. Guan, Y. Fei, and *H. Lin, "Hierarchical design of an application-specific instruction set processor for high-throughput and scalable FFT processing," *IEEE Trans. on VLSI* (TVLSI), vol. 20, no. 3, pp. 551-563, Mar. 2012.

J27. *H. Lin, Y. Fei, *X. Guan, and Z. J. Shi, "Architectural enhancement and system software support for program code integrity monitoring in application-specific instruction set processors", *IEEE Trans. on VLSI* (TVLSI), vol. 18, no. 11, pp.1519-1532, Nov. 2010.

J28. *X. Guan and Y. Fei, "Register file partitioning and compiler support for reducing power consumption in embedded processors", *IEEE Trans. on VLSI* (TVLSI), vol. 18, no. 8, pp. 1248 – 1252, Aug. 2010.

J29. *T. Hu and Y. Fei, "QELAR: A Machine-learning-based adaptive routing protocol for energy-efficient and lifetime-extended underwater sensor networks", *IEEE Trans. on Mobile Computing* (TMC), vol. 9, no. 6, pp. 796 - 809, June 2010.

J30. *X. Guan and Y. Fei, "Reducing register file power consumption with RF partitioning and compiler support," *ACM Trans. on Design Automation of Electronic Systems* (TODAES), vol. 15, no. 3, May 2010.

J31. *H. Lin and Y. Fei, "Orchestrating horizontal parallelism and vertical instruction packing of programs to improve system overall efficiency", *IEEE Trans. on Computers* (TC), vol. 58, no. 9, pp. 1211-1220, Sept. 2009.

J32. Y. Fei, L. Zhong, and N. K. Jha, "An energy-aware framework for dynamic software management in mobile computing systems," *ACM Trans. on Embedded Computing Systems* (TECS), vol. 7, no. 3, Apr. 2008.

J33. Y. Fei, S. Ravi, A. Raghunathan, and N. K. Jha, “Energy-optimizing source code transformations for operating system driven embedded software,” *ACM Trans. on Embedded Computing Systems s* (TECS)*,* vol. 7, no. 1, Dec. 2007.

J34. Y. Fei and N. K. Jha, “Integrated functional partitioning and synthesis for low power distributed systems of systems-on-a-chip,” invited paper, Special Issue on Hardware-software Codesign for SOC in *Int. Journal Embedded Systems*, vol.1, no.1/2, pp. 2-13, 2005.

J35. J. Luo, L. Zhong, Y. Fei, and N. K. Jha, “Register binding based RTL power management for control-flow intensive designs,” *IEEE Trans. on Computer-aided Design of Integrated Circuits & Systems* (TCAD), vol. 23, no. 8, pp.1175-1183, Aug. 2004.

J36. Y. Fei, S. Ravi, A. Raghunathan, and N. K. Jha, “A hybrid energy estimation technique for extensible processors,” *IEEE Trans. on Computer-aided Design of Integrated Circuits & Systems* (TCAD), vol. 23, no. 5, pp. 652-664, May 2004.

J37. Y. Fei, H. Zhang, W. Dai, Y. Ye, Y. Guo, and B. Zhou, “Analysis on BER performance of OXC nodes with power equalization function module,” *Chinese Journal of Lasers*, vol. A28, no. 3, Mar. 2001.

J38. Y. Fei, W. Chen, H. Zhang, Y. Guo, and B. Zhou, “Analysis of power management in OXC node of WDM all-optical network,” *Electra Academia of Sinica*, vol. 28, no. 1, Jan. 2000.

J39. Y. Fei, X. Zheng, H. Zhang, Y. Guo, and B. Zhou, “A novel scheme of power equalization and power management in WDM all-optical networks,” *IEEE Photon. Technol. Lett*. (PTL), vol. 11, no. 9, pp.1189-1191, Sept.1999.

ePrint Archive:

J1. *Z. Jiang, Y. Fei, A. A. Ding, and T. Wahl, “Mempoline: Mitigating memory-based side0channel attacks through memory access obfuscation,” Cryptology ePrint Archive 2020/653 (https://eprint.iacr.org/2020/653).

J2. *L. Zhang, A. A. Ding, F. Durvaux, F.X.-Standaert, Y. Fei, “Towards sound and optimal leakage detection procedure,” Cryptology ePrint Archive 2017/287 (https://eprint.iacr.org/2017/287).

J3. *P. Luo, *C. Luo, Y. Fei, “System clock and power supply cross-checking for glitch detection,” Cryptology ePrint Archive 2016/968 (https://eprint.iacr.org/2016/968)

J4. *L. Zhang, A. A. Ding, Y. Fei, *Z. H. Jiang, “Statistical analysis for access-driven cache attacks against AES,” Cryptology ePrint Archive 2016/970 (https://eprint.iacr.org/2016/970).

J5. *P. Luo, *L. Zhang, Y. Fei, A.A. Ding, “An improvement of both security and reliability for Keccak implementations on smart card,” Cryptology ePrint Archive 2016/214 (https://eprint.iacr.org/2016/214).

J6. A. A. Ding, *L. Zhang, Y.Fei, and *P. Luo, “A statistical model for higher order DPA on masked devices,” Cryptology ePrint Archive 2014/433 (https://eprint.iacr.org/2014/433).

J7. Y. Fei, A. A. Ding, *J. Lao and *L. Zhang, “A statistics-based fundamental model for side-channel attack analysis,” Cryptology ePrint Archive 2014/152 (https://eprint.iacr.org/2014/152).

Conferences and Workshops:

C1. *R. Ding, *T. Xu, X. Shen, A. A. Ding, and Y. Fei, “MoEcho: Exploiting side-channel attacks to compromise user privacy in mixture-of-experts LLMs,” *ACM Conf. on Computer and Communications Security* (CCS), Oct. 2025.

C2. *T. Xu, A. A. Ding, and Y. Fei, “EXAM: Exploiting exclusive system-level cache in Apple M-series SoCs for enhanced cache occupancy attacks,” *ACM Asia Conf. on Computer and Communications Security* (AsiaCCS), Aug. 2025.

C3. *R. Ding, *T. Xu, A. A. Ding, and Y. Fei, “Graph in the Vault: Protecting edge GNN inference with trusted execution environment,” *IEEE/ACM Proc. Design Automation Conf.* (DAC)*,* June 2025.

C4. *R. Ding, *C. Gongye, *Davis Ranney, A. A. Ding, and Y. Fei, “MACPruning: Dynamic Operation Pruning to Mitigate Side-Channel DNN Model Extraction,” *IEEE Int. Conf. on Hardware-oriented Security and Trust* (HOST), May 2025.

C5. L. Reichling, R. Evans, M. Ninan, P. Mai, B. Wang, Y. Fei, and J. Emmert, “MicroPower: Micro Neural Networks for Side-Channel Attacks,” *IEEE Int. Conf. on Hardware-oriented Security and Trust* (HOST), May 2025.

C6. *X. Zhang, *Z. Zhang, A. A. Ding, and Y. Fei, “AccessShadow: Leveraging adversarial samples to counter deep learning-assisted cache timing attacks,” *IEEE Int. Conf. on Hardware-oriented Security and Trust* (HOST), May 2025.

C7. *Davis Ranney, *Yufei Wang, A. A. Ding, and Y. Fei, “USBSnoop – Revealing devices activities via USB congestions,” *IEEE Int. Conf. on Hardware-oriented Security and Trust* (HOST), May 2025.

C8. *R. Ding, T. Zhou, L. Su, A. A. Ding, X. Xu, and Y. Fei, “Probe-Me-Not: Protecting Pre-trained Encoders from Malicious Probing,” *Network and Distributed System Security Symp. (NDSS),* Feb. 2025.

C9. S. Duan, *R. Ding, J. He, A. A. Ding, Y. Fei, and X. Xu, “GraphCroc: Cross-correlation autoencoder for graph structural reconstruction,” NeurIPS, Dec. 2024.

C10. *R. Ding, L. Su, A. A. Ding, and Y. Fei, “Non-transferrable pruning,” *European Conf. on Computer Vision*, Oct. 2024.

C11. *T. Xu, A. A. Ding, and Y. Fei, “TrustZoneTunnel: A Cross-world Pattern History Table-based Microarchitectural Side-channel Attack,” *IEEE Int. Conf. on Hardware-oriented Security and Trust* (HOST), May 2024.

C12. *C. Gongye and Y. Fei, “One flip away from chaos: Unraveling single points of failure in quantized DNNs,” *IEEE Int. Conf. on Hardware-oriented Security and Trust* (HOST), May 2024.

C13. *C. Gongye, Y. Luo, X. Xu, and Y.Fei, “Side-Channel-Assisted Reverse-Engineering of Encrypted DNN Hardware Accelerator IP and Attack Surface Exploration,” *IEEE. Int. Symp. Security & Privacy* (S&P), May 2024.

C14. *X. Zhang, A. A. Ding, and Y.Fei, “Deep-learning Model Extraction through Software-based Power Side-channel,” accepted for publication in *ACM/IEEE Int. Conf. Computer-aided Design (ICCAD*), Nov. 2023.

C15. *R. Ding, S. Duan, X. Xu, and Y.Fei, “VertexSerum: Poisoning graph neural networks for link inference,” *IEEE/CVF Int. Conf. on Computer Vision* (ICCV), pp. 4532-4541, Oct. 2023.

C16. S. Maji, K. Lee, *C. Gongye, Y. Fei, and A. P. Chandrakasan, “An energy-efficient neural network accelerator with improved protections against fault-attacks,” *ESSCIRC IEEE European Solid State Circuits Conf.,* pp. 233-236, Sept. 2023.

C17. T. Gourousis, *Z. Zhang, M. Yan, M. Zhang, A. Mittal, A. Shrivastava, F. Restuccia, Y. Fei, and M. Onabajo, “Identification of stealthy hardware Trojans through on-chip sensing and an autoencoder-based machine learning algorithm,” IEEE Int. Midwest Symp. on Circuits and Systems (MWSCAS), Aug. 2023.

C18. *C. Gongye, Y. Luo, X. Xu, and Y. Fei, "HammerDodger: A Lightweight Defense Framework against RowHammer Attack on DNNs," *Proc. Design Automation Conf.* (DAC), July 2023.

C19. [**Distinghuished Paper Award]** *R. Ding, *C. Gongye, S. Wang, A. A. Ding, and Y. Fei, "EMShepherd: Detecting adversarial examples via side-channel leakage," *AsiaCCS,* July 2023.

C20. [**Best Paper Award]** *T. Xu, *C. Gongye, and Y. Fei, "Protected ECC still leaks: A novel differential-bit side-channel power attack on ECDH and countermeasures," *Proc. Great Lake Symp. on VLSI,* June 2022.

C21. *X. Zhang, *Z. Zhang, *R. Ding, *C. Gongye, A. A. Ding, and Y. Fei, "Ran$Net: An anti-ransomware methodology based on cache monitoring and deep learning," *Proc. Great Lake Symp. On VLSI,* June 2022.

C22. Y. Luo, S. Duan, *C. Gongye, Y. Fei, and X. Xu, "NNReArch: A Tensor program scheduling framework against neural network architecture reverse engineering," *IEEE Int. Symp. On Field-Programmable Custom Computing Machines (*FCCM), May 2022.

C23. M. Abedi, T. Yang, Y. Fei, and A. Shrivastava, "High-precision nano-amp current sensor and obfuscation based analog Trojan detection circuit," *IEEE Int. Symp. on Circuits & Systems* (ISCAS), May 2022.

C24. [**Best Paper Candidate]** *R. Ding, *Z. Zhang, *X. Zhang, *C. Gongye, Y. Fei, and A. A. Ding, "A Cross-Platform Cache Timing Attack Framework via Deep Learning," *Proc. Design Automation & Test in Europe* (DATE), Mar. 2022.

C25. *Konstantinos Athanasiou, Thomas Wahl, Aidong Adam Ding, and Yunsi Fei, "Masking Feedforward Neural Networks against Power Analysis Attacks," Proc. on Privacy Enhancing Technologies (PoPETs), no.4, 2022.

C26. Y. Luo#, *C. Gongye#, Y. Fei, and X. Xu, "DeepStrike: Remotely-Guided Fault Injection Attacks on DNN Accelerator in Cloud-FPGA," *IEEE/ACM Design Automation Conf.* (DAC), Dec. 2021*. (*acceptance rate 23%; #: equal contributor).

C27. *M. Sabbagh, Y. Fei, and D. Kaeli, "GPU overdrive fault attacks on neural networks," *ACM/IEEE Int. Conf. Computer-aided Design (ICCAD),* Nov. 2021. *(*acceptance rate 23.5%).

C28. S. Wang, P. Zhao, X. Wang, S. Chin, T. Wahl, Y. Fei, Q. Chen, and X. Lin, "Intrinsic examples: Robust fingerprinting of deep neural networks," British Machine Vision Conf., Nov. 2021.

C29. *Amel Nestor Docena, Thomas Wahl, Trevor Pearce and Yunsi Fei, "Sensitive Samples Revisited: Detecting Neural Network Attacks Using Constraint Solvers," *Int. Symp. on Symbolic Computing in Software Science (SCSS), Sept. 2021.*

C30. *M. Sabbagh, Y. Fei, and D. Kaeli, "Overdrive fault attacks on GPUs," IEEE/IFIP Int. Conf. on Dependable Systems and Networks, June. 2021.

C31. *M. Sabbagh, Y. Fei, and D. Kaeli, *"*Secure Speculative Execution via RISC-V Open Hardware Design," The Fifth Workshop on Computer Architecture Research with RISC-V (CARRV), June 2021.

C32. *G. Knipe, *D. Rodriguez, Y. Fei, and D. Kaeli, "RISC-V Microarchitecture Simulation State Enumeration," The Fifth Workshop on Computer Architecture Research with RISC-V (CARRV), June 2021.

C33. J. Ahn, C. Jin, J. Kim, M. Rhu. Y. Fei, D. Kaeli, and J. Kim, "Trident: A hybrid correlation-collision GPU cache timing attack for AES key recovery," *IEEE Int. Symp. High Performance Computer Architecture (HPCA)*, Feb. 2021 (acceptance rate 63/258 =24.4%).

C34. E. Karimi, Y. Fei, and D. Kaeli, "Hardware/software obfuscation against timing side-channel attack on a GPU", *IEEE Int. Symp. Hardware Oriented Security & Trust (HOST),* Dec. 2020.

C35. *Cheng Gongye, Hongjia Li, *Xiang Zhang, *Majid Sabbagh, Geng Yuan, Xue Lin, Thomas Wahl, and Yunsi Fei, "New Passive and Active Attacks on Deep Neural Networks in Medical Applications," special session paper, *ACM/IEEE Int. Conf. Computer-aided Design (ICCAD),* Nov. 2020.

C36. Yukui Luo, *Cheng Gongye, Shaolei Ren, Yunsi Fei and Xiaolin Xu, "Stealthy-Shutdown: Practical Remote Power Attacks in Multi-Tenant FPGAs," *IEEE Int. Conf. Computer Design (ICCD)*, Oct. 2020.

C37. Yunsi Fei, Guang Gong, *Cheng Gongye, Kalikinkar Mandal, Raghvendra Rohit, *Tianhong Xu, Yunjie Yi, and Nusa Zidaric, "Correlation Power Analysis and Higher-order Masking Implementation of WAG," *Selected Areas in Cryptography (SAC)*, Oct. 2020.

C38. Nikita Mirchandani, Nasim Shafiee, Yunsi Fei, and Aatmesh Shrivastava, "An Ultra-Low Power and Lower Area Current-Mode Based Physically Unclonable Function with Less Than 100nW Power Consumption and a Native Instability of 0.6875% for IoT Applications," *IEEE Int. Midwest Symp. On Circuits & Systems, Aug. 2020.*

C39. *M. Sabbagh, Y. Fei, and D. Kaeli, "A novel GPU overdrive fault attack," *ACM/IEEE Design Automation Conf. (DAC)*, July 2020.

C40. *C. Gongye, Y. Fei, and T. Wahl, "Reverse engineering deep neural networks using floating-point side channel," *ACM/IEEE Design Automation Conf. (DAC)*, July 2020.

C41. *Konstantinos Athanasiou, Thomas Wahl, A. Adam Ding and Yunsi Fei, "Automatic detection and repair of transition-based leakage in software binaries," *Conf. on Verified Software: Theories, Tools, and Experiments,* July 2020.

C42. *M. Sabbagh, *C. Gongye, Y. Fei, and Y. Wang, "Evaluating fault resilience of compressed deep neural networks," invited paper, *IEEE Int. Conf. Embedded Software and Systems (ICESS)*, June 2019.

C43. P. Zhao, S. Wang, *C. Gongye, Y. Wang, Y. Fei, and X. Lin, "Fault sneaking attack: A stealthy framework for misleading deep neural networks," *IEEE Design Automation Conf. (DAC),* June 2019. (acceptance rate: ~25%).

C44. E. Karimi, *Z.H. Jiang, D. Kaeli, and Y. Fei, "A timing side-channel attack on a mobile GPU," *IEEE Int. Conf. Computer Design* (ICCD), Oct. 2018 (acceptance rate: 29%).

C45. *M. Sabbagh, Y. Fei, T. Wahl, and A. Ding, "SCADET: A side-channel attack detection tool for tracking Prime+Probe," *ACM Int. Conf. Computer-aided Design (*ICCAD), Nov. 2018. (acceptance rate: 24%)

C46. *C. Luo, Y. Fei, and D. Kaeli, "Effective simple-power analysis attacks of Elliptic Curve Cryptography on embedded systems," *ACM Int. Conf. Computer-aided Design (*ICCAD), Nov. 2018. (acceptance rate: 24%)

C47. [**Best Paper Candidate]** *C. Luo, Y. Fei, and D. Kaeli, "GPU acceleration of RSA is vulnerable to side-channel timing attacks," *ACM Int. Conf. Computer-aided Design (*ICCAD), Nov. 2018. (acceptance rate: 24%)

C48. A. Adam Ding, *L. Zhang, F. Durvaux, F-X. Standaert, and Y. Fei, "Toward sound and optimal leakage detection procedure," *Smart Card Research and Advanced Application Conference (*CARDIS), Nov. 2017.

C49. *Z. Jiang and Y. Fei, "A novel cache bank timing attack", *ACM Int. Conf. Computer-Aided Design* (ICCAD), Nov. 2017. (acceptance rate: ~20%)

C50. *Pei Luo, *Konstantinos Anthansiou, *Liwei Zhang, *Zhen Jiang, Yunsi Fei, A. Adam Ding and Thomas Wahl, “Compiler-assisted Threshold Implementation Design,” *IEEE Int. Conf. on Computer Design* (ICCD), Nov. 2017.

C51. **[Best Paper Award]** Mohammad Khavari Tavana, Yunsi Fei and David Kaeli, “Nacre: Durable, Secure and Energy-efficient Non-Volatile Memory Utilizing Data Versioning,” *IEEE Int. Conf. on Computer Design* (ICCD), Nov. 2017.

C52. *Z. Jiang, Y. Fei, and D. R. Kaeli, “A novel side-channel timing attack on GPUs”, *ACM Great Lake Symposium on VLSI* (GLSVLSI), May 2017. (acceptance rate: 24%)

C53. *C. Luo, Y. Fei, and A. A. Ding, “Side-channel power analysis of XTS-AES,” *IEEE Proc. Design Automation & Test in Europe* (DATE), 2017. (acceptance rate: 24%)

C54. *P. Luo, *K. Athanasiou, Y. Fei, and T. Wahl, “Algebraic fault analysis of SHA-3,” *IEEE Proc. Design Automation & Test in Europe* (DATE), 2017. (acceptance rate: 24%)

C55. Y. M. Aval, *Y. Han, A. Tu, S. Basagni, M. Stojanovic, and Y. Fei, “Testbed-based performance evaluation of handshake-free MAC protocols for underwater acoustic sensor networks,” *MTS/IEEE Proc. Oceans,* Sept. 2016.

C56. *P. Luo, Y. Fei, *L. Zhang, and A. A. Ding, “Differential fault analysis of SHA3-224 and SHA3-256,” *Int. WkShp on Fault Diagnosis and Tolerance in Cryptography* (FDTC), Aug. 2016.

C57. *Y. Han, Y. Fei, and A. A. Ding, “A Stochastic MAC Protocol with Randomized Power Control for Underwater Sensor Networks”, *IEEE International Conference on Sensing, Communication and Networking* (SECON), June 2016. (acceptance rate: 26%)

C58. *P. Luo, C. Li, and Y. Fei, “Concurrent error detection for reliable SHA-3 design,” *ACM Great Lake Symp. on VLSI* (GLSVLSI), May 2016. (acceptance rate: 28%)

C59. *Z. Jiang, Y. Fei, and D. R. Kaeli, “A complete key recovery timing attack on a GPU,” *Int. Symp. High Performance Computer Architecture* (HPCA), Mar. 2016. (acceptance rate: 22%)

C60. *L. Zhang, A. A. Ding, Y. Fei, and *P. Luo, “A Unified metric for quantifying information leakage of cryptographic devices under power analysis attacks,” *AsiaCrypt*, Nov.-Dec. 2015. (acceptance rate: 25%)

C61. *C. Luo, Y. Fei, *P. Luo, S. Mukherjee, and D. Kaeli, “Side-channel power analysis of a GPU AES implementation”, *Int. Conf. Computer Design* (ICCD), Oct. 2015. (acceptance rate: 19.8%)

C62. **[Best Paper Award]** *Y. Han and Y. Fei, “TARS: A traffic-adaptive receiver-synchronized MAC protocol for underwater sensor networks,” *Int. Symp. on Modeling, Analysis and Simulation of Computer and Telecommunication Systems* (MASCOTS), Oct. 2015. (acceptance rate: 18.8%)

C63. X. Fang, M. Leeser, Y. Fei, and *P. Luo, “Leakage evaluation on power balance countermeasure against side-channel attack on FPGAs,” *IEEE High Performance Extreme Computing Conf.* (HPEC), Sept. 2015.

C64. *P. Luo, *L. Zhang, Y. Fei, and A.A. Ding "Towards secure cryptographic software implementation against side-channel power analysis attacks", *Int. Conf. on Application-specific Systems, Architectures, and Processors* (ASAP), July 2015 (acceptance rate: 37.6%).

C65. X. Fang, Y. Fei, and M. Leeser, “Balance power leakage to fight against side-channel analysis at gate level in FPGAs”, *Int. Conf. on Application-specific Systems, Architectures, and Processors* (ASAP), July 2015. (2-page poster) (acceptance rate: 51.7%)

C66. *P. Luo, Y. Fei, *X. Fang, A. Adam Ding, D. R. Kaeli, and M. Leeser, "Side-channel analysis of MAC-Keccak hardware implementations," in *Wkshp on Hardware and Architectural Support for Security & Privacy* (HASP), in conjunction with *Int. Symp. Computer Architecture*, June 2015.

C67. *B. Jiang and Y. Fei, "Traffic and Vehicle Speed Prediction with Neural Network and Hidden Markov Model in Vehicular Networks," *Proc. IEEE Intelligent Vehicles Symp.* (IV), June 2015.

C68. *L. Zhang, A. A. Ding, Y. Fei, and *P. Luo, "Efficient 2nd-order power analysis on masked devices utilizing multiple leakage," *Proc. IEEE Int. Symp. on Hardware Oriented Security & Trust* (HOST), May 2015 (acceptance rate: 24%).

C69. *Y. Han and Y. Fei, "DAP-MAC: A delay-aware probability-based MAC protocol for underwater sensor networks", *Int. Conf. Networking and Communications*, *Wireless Ad Hoc and Sensor Networks Symposium* (ICNC-WAHS), Feb. 2015 (acceptance rate: 22.5%).

C70. *P. Luo, Y. Fei, X. Fang, A. A. Ding, M. Leeser, and D. R. Kaeli, "Power analysis attack on hardware implementation of MAC-Keccak on FPGAs," *Proc. Int. Conf. on Reconfigurable Computing and FPGAs* (ReConfig), Dec. 2014.

C71. *P. Luo, Y. Fei, *L. Zhang, and A. A. Ding, "Side-channel power analysis of different protection schemes against fault attacks on AES," *Proc. Int. Conf. on Reconfigurable Computing and FPGAs* (ReConfig), Dec. 2014.

C72. *M. Shafaei and Y. Fei, "HiTS: A high-throughput memory scheduling scheme to mitigate denial-of-service attacks in multi-core systems," *Int. Symp. On Computer Architecture and High Performance Computing (*SBAC-PAD), Oct. 2014. (acceptance rate: 32%)

C73. A. A. Ding, *L. Zhang, Y. Fei, *P. Luo, "A statistical model for multivariate DPA on masked devices," *Int. Wkshp on Cryptographic Hardware and Embedded Systems (*CHES), pp. 147-169, Sept. 2014. (acceptance rate: 26%)

C74. *T. Swamy, *N. Shah, *P. Luo, Y. Fei, and D. Kaeli, "Scalable and efficient implementation of correlation power analysis using Graphic Processing Units (GPUs)," in *Wkshp on Hardware and Architectural Support for Security & Privacy* (HASP), in conjunction with *Int. Symp. Computer Architecture*, June 2014.

C75. *J. Martinez Santos and Y. Fei, "HATI: Hardware assisted thread isolation for concurrent C/C++ programs," IPDPS Workshops 2014: 322-331.

C76. *B. Jiang and Y. Fei, "On-road PHEV Power Management with Hierarchical Strategies in Vehicular Network," *IEEE Intelligent Vehicles Symposium* (IV), June 2014.

C77. *J. C. Martinez Santos and Y. Fei, "Micro-architectural support for metadata coherence in multi-core dynamic information flow tracking," in *Wkshp on Hardware and Architectural Support for Security & Privacy* (HASP), in conjunction with *Int. Symp. Computer Architecture*, June 2013.

C78. *T. Hu and Y. Fei, "An adaptive routing protocol based on connectivity prediction for underwater disruption tolerant networks," in *IEEE Global Communications Conf.* (GlobeCom), Dec. 2013 (acceptance rate: 37%).

C79. *T. Hu and Y. Fei, "DSH-MAC: Medium access control based on decoupled and suppressed handshaking for long-delay underwater acoustic sensor networks", in *IEEE Conf. Local Computer Networks* (LCN), Oct. 2013. (acceptance rate: 26.4%)

C80. *B. Jiang and Y. Fei, "Decentralized scheduling of PEV on-street parking and charging for smart grid reactive power compensation", *IEEE PES Innovative Smart Grid Technologies Conf.* (ISGTC), Feb. 2013.

C81. *J. C. Martinez Santos and Y. Fei, “Designing and implementing a malicious 8051 processor,” Proc. IEEE Int. Symp. on Defect and Fault Tolerance in VLSI & Nanotechnology Systems (DFT), Hardware Security Session on Capture the Chip, Oct. 2012.

C82. *J. C. Martinez Santos, Y. Fei, and Z. J. Shi, “Static secure page allocation for light-weight dynamic information flow tracking,” *Int. Conf. on Compilers, Architecture & Synthesis for Embedded Systems* (CASES)*,* Oct. 2012 . (acceptance rate: 30.0%).

C83. Y. Fei, *Q. Luo, and A. A. Ding, “A statistical model for DPA with novel algorithmic confusion analysis,” *Proc. Int. Wksp on Cryptographic Hardware & Embedded Systems* (CHES)*,* Sept. *2012*. (acceptance rate: 27%)

C84. *T. Hu and Y. Fei, “MURAO: A multi-level routing protocol for acoustic-optical hybrid underwater sensor networks,” *Proc. IEEE Communication Society Conf. on Sensor, Mesh & Ad Hoc Communications & Networks* (SECON)*,* June 2012. (acceptance rate: 31.1%)

C85. *X. Guan and Y. Fei, “Adaptive extended min-sum algorithm for nonbinary LDPC decoding,” *IEEE Global Communications Conf.* (GlobeCom)*,* Dec. 2011 (acceptance rate: 36.6%).

C86. *B. Jiang and Y. Fei, “Dynamic residential demand response and distributed generation management in smart microgrid with hierarchical agents,” in *Proc. Int. Conf. on Smart Grid & Clean Energy Technologies* (ICSGCET)*,* Sept. 2011.

C87. *Q. Luo and Y. Fei, “Algorithmic collision analysis of evaluating cryptographic systems and side-channel attacks,” in *Proc. IEEE Int. Symp. on Hardware Oriented Security & Trust* (HOST)*,* June 2011 (acceptance rate: 31%).

C88. *T. Hu and Y. Fei, “An adaptive and energy-efficient routing protocol based on machine learning for underwater delay tolerant networks,” *Proc. ACM/IEEE Int. Symp. on Modeling, Analysis, and Simulation of Computer & Telecommunication Systems* (MASCOTS)*,* Aug. 2010 (acceptance rate: 51%).

C89. *H. Lin and Y. Fei, “Exploring custom instruction synthesis for application-specific instruction set processors with multiple design objectives,” *IEEE Int. Symp. on Low Power Electronics & Design* (ISLPED)*,* Aug. 2010 (acceptance rate: 34%).

C90. *H. Lin and Y. Fei, “A novel multi-objective instruction synthesis flow for application-specific instruction set processors,” *Proc. ACM Great Lakes Symposium on VLSI* (GLSVLSI)*,* May 2010 (acceptance rate: 34%).

C91. J.-H. Cui, P. Xie, H. Yan, *T. Hu, Z. Shi, Y. Fei, S. Zhou, Z. Zhou, and Z. Peng, “AQUA-SIM: An NS-2 based simulator for underwater sensor networks,” *Proc. MTS/IEEE Oceans,* Oct. 2009.

C92. *H. Lin and Y. Fei, “Resource sharing of pipelined custom hardware extension for energy-efficient application-specific instruction set processor”, *Proc. IEEE Int. Conf. on Computer Design* (ICCD)*,* Oct. 2009 (acceptance rate: 34%).

C93. *J. C. Martinez Santos, Y. Fei, and Z. J. Shi, “PIFT: Efficient dynamic information flow tracking using secure page allocation,” *Proc. IEEE Embedded Systems Week/Workshop on Embedded Systems Security* (WESS)*,* Oct. 2009.

C94. *X. Guan, Y. Fei, and *H. Lin, “A hierarchical design of application-specific instruction set processor for high-throughput FFT”, in *Proc. IEEE Int. Symp. Circuits & Systems* (ISCAS), May 2009 (acceptance rate: ~40%).

C95. *X. Guan, *H. Lin, and Y. Fei, “Design of an application-specific instruction set processor for high-throughput and scalable FFT”, in *Proc. IEEE Design Automation & Test in Europe Conf.* (DATE)*,* Apr. 2009 (acceptance rate: 23.4%).

C96. H. Yan, Z. J. Shi, and Y. Fei, "Efficient implementation of Elliptic Curve Cryptography on DSP for underwater sensor networks," in *WkShp on Optimizations for DSP & Embedded Systems,* Mar. 2009.

C97. *T. Hu and Y. Fei, "QELAR: A Q-learning-based energy-efficient and lifetime-aware routing protocol for underwater sensor networks", in *Proc. IEEE Int. Performance Computing & Communications Conf.* (IPCCC)*,* Dec. 2008 (acceptance rate: 29.8%).

C98. *J. C. Martinez Santos and Y. Fei, "Leveraging speculative architectures for run-time program validation", in *Proc. IEEE Int. Conf. Computer Design* (ICCD), Oct. 2008 (acceptance rate: 34%).

C99. *X. Guan and Y. Fei, "Reducing register file power consumption through partitioning and compiler support", in *Proc. IEEE Int. Conf. Application-specific Systems, Architectures & Processors* (ASAP), July 2008 (acceptance rate: 31.8%).

C100. V. Kundeti, Y. Fei, and S. Rajasekaran, "An efficient digital circuit for implementing sequence alignment algorithm in an extended processor", in *Proc. IEEE Int. Conf. Application-specific Systems, Architectures & Processors* (ASAP), July 2008 (acceptance rate: 31.8%).

C101. *H. Lin, G. Sun, Y. Fei, Y. Xie, and A. Sivasubramaniam, "Thermal-aware design considerations for application-specific instruction set processor," in *Proc. IEEE Symp. on Application Specific Processors* (SASP), pp. 63-68, June, 2008 (acceptance rate: ~25%).

C102. *H. Lin and Y. Fei, "Harnessing horizontal parallelism and vertical instruction packing of programs to improve system overall efficiency," in *Proc. IEEE Design Automation & Test in Europe Conf.* (DATE), pp. 758-763, Mar. 2008 (acceptance rate: 23.6%).

C103. *H. Lin, Y. Fei, *X. Guan, and Z. J. Shi, "Compiler-assisted architectural support for program code integrity monitoring in application-specific instruction set processors," in *Proc. IEEE Int. Conf. Computer Design* (ICCD), pp. 187-193, Oct. 2007 (acceptance rate: 21%).

C104. Y. Fei, *H. D. Lin, and *X. Guan, "A hardware/software cooperative approach for reducing memory traffic in application-specific instruction set processors," in *Proc. IEEE Int. Midwest Symposium on Circuits & Systems* (MWSCAS)*,* pp. 1269 -1272, Aug. 2007.

C105. Y. Fei and Z. Shi, "Microarchitectural support for program code integrity monitoring in application-specific instruction set processors," in *Proc. IEEE Design Automation & Test in Europe Conf.* (DATE), pp. 815—820, Apr. 2007 (acceptance rate: 22%).

C106. *H. Lin and Y. Fei, "Utilizing custom registers in application-specific instruction set processors for register spills elimination," in *Proc. ACM Great Lakes Symposium on VLSI* (GLSVLSI)*,* pp. 323-328, Mar. 2007 (acceptance rate: 10.5% for full paper).

C107. Y. Fei, L. Zhong, and N. K. Jha, "An energy-aware framework for coordinated dynamic software management in mobile computers," in *Proc. ACM/IEEE Int. Symp. on Modeling, Analysis, and Simulation of Computer & Telecommunication Systems* (MASCOTS), pp. 306-317, Oct. 2004 (acceptance rate: 39%).

C108. Y. Fei, S. Ravi, A. Raghunathan, and N. K. Jha, "Energy-optimizing source code transformations for OS-driven embedded software," in *Proc. IEEE International Conference on VLSI Design* (ICVLSI), pp. 261-266, Jan. 2004 (acceptance rate: 36%).

C109. W. Wang, T. K. Tan, J. Luo, Y. Fei, L. Shang, K. S. Vallerio, L. Zhong, A. Raghunathan, and N. K. Jha, "A comprehensive high-level synthesis system for control-flow intensive behaviors," in *Proc. IEEE Great Lakes Symposium on VLSI* (GLSVLSI), April 2003 (acceptance rate: 12.5% for full paper).

*C110.*Y. Fei, S. Ravi, A. Raghunathan, and N. K. Jha, “Energy estimation for extensible processors,” in *Proc. IEEE Design Automation & Test in Europe Conference* (DATE), pp. 682-687, Mar. 2003 (acceptance rate: 25.8%).

*C111.*L. Zhong, J. Luo, Y. Fei, and N. K. Jha, “Register binding based power management for high-level synthesis of control-flow intensive behaviors,” in *Proc. IEEE Int. Conf. Computer Design* (ICCD), pp. 391-394, Sept. 2002 (acceptance rate: 27.2%).

*C112.*Y. Fei and N. K. Jha, “Functional partitioning for low-power distributed systems of systems-on-a-chip,” in *Proc. IEEE Asia South Pacific Design Automation Conference (*ASP-DAC)*,* pp. 274-281, Jan. 2002 (acceptance rate: 42%).

*C113.*W. Chen, Y. Fei, L. Zong, Z. Xu, H. Zhang, and B. Zhou, “Reconfigurable all optical add/drop multiplexer with dynamic gain control Function,” in *SPIE Proceedings: Photonic’ 98, Fiber Optic Components and Optical Communication*, vol. 3552, pp. 98-102, Oct. 1998.

*C114.*W. Chen, H. Zhang, Y. Fei, L. Zhong, Y. Guo, and B. Zhou, “The same source crosstalk in the WDM dynamic all-optical cross-connects,” in *SPIE Proceedings: Photonic’ 98, Fiber Optic Components and Optical Communication*, Oct. 1998.

Patents

- Y. Fei and Z. H. Jiang, “Methods and Systems for Protecting against Memory-based Side-channel Attacks,” US Patent 12,177,328, 2024.
- Y. Fei and H. Lin, “System and methods to improve efficiency of VLIW processors,” US 20110022821 A1, application.

Tutorials

- “Protecting confidentiality and integrity of deep neural networks against side-channel and fault attacks,” IEEE International Symposium on Hardware-oriented Security and Trust (HOST), Dec. 7th, 2020.
- “New passive and active attacks on deep neural networks in medical applications,” Session 3D: Hardware/software codesign for machine learning in medicine, ACM/IEEE International Conference on Computer Aided Design of Integrated Circuits, Nov. 2nd, 2020.

Invited Talks

- Invited talk, Chinese University of Hong Kong, “Side-channel for AI Security: Foe or Friend?” Sept. 2025.
- Invited distinguished speech, NSF-India MeitY (Ministry of Electronics and Information Technology) joint-workshop, “Physical Side-channel for Hardware Security: Foe or Friend?” Nov. 2-3, 2023.
- Schmidt Family Distinguished Speaker, Computer Science Department of William Mary College, “Side-channel for security: Foe or Friend?” Oct. 2, 2023.
- Guest lecture for MIT EECS 6.888 – Secure Hardware Design, “DisruptNet: Integrity Breach of Deep Neural Networks,” Apr. 25th, 2022.
- Invited talk, “DisruptNet: Integrity Breach of Deep Neural Networks,” National Microelectronics Security Training (MEST) Center Webinar, Florida Institute of Cybersecurity (FICS), Mar. 16th, 2022.
- Special Security Panel, “Cybersecurity: Current, tomorrow, and beyond”, ICCD, Oct. 26, 2021
- Invited talk, “Security vulnerabilities of deep neural network execution,” ESWEEK 2021 TRAIN (Trustable and Reliable AI Accelerator Design) workshop. Oct. 14th, 2021

- Invited talk, “Discovering security vulnerabilities of GPU acceleration,” Nvidia, Apr. 6th 2021.
- Invited talk, “Side-channel attacks on DNNs and DNNs for side-channel attacks,” MITRE, Mar. 12, 2021.
- Invited talk, “Looking into the brains of robotics,” Empowering girls in engineering and robotics workshop, Penn State College Park, Mar. 27, 2021, the EngineerGirl Ambassador program for elementary and middle school girls, sponsored by National Academy of Engineering.
- Invited talk, “Security vulnerabilities of deep neural networks execution”, Chinese Institute of Engineers – Greater New York Chapter, Oct. 18th, 2020
- Invited talk, “Evaluating fault resilience of compressed deep neural networks,” IEEE International Conference on High Performance Extreme Computing Conference (HPEC), Sept. 26th, 2019.
- Invited to attend Dagstuhl seminar 19301 “Secure Composition for Hardware Systems”, July 22- 26, 2019.
- “Root of Untrust – Hardware Security”, panelist for the Workshop on Computer Architecture Research Direction (CARD) in International Symposium on Computer Architecture (ISCA), June 23rd, 2019.
- NXP, “Side-channel attacks: Cyber defense and offense,” Online technical seminar, Nov. 20, 2018.
- MassTech Cybersecurity Forum, “Root of untrust – hardware security,” Boston, MA, Sept. 27th, 2018.
- Nvidia, “Discovering side-channel vulnerabilities of accelerators,” San Jose, CA, July 23rd, 2018.
- Google, “Side-channel attacks: Cyber offense and defense,” San Jose, CA, July 23rd, 2018.
- US National Security Agency, Cyber Command, “Side-channel attacks: Cyber offense and defense,” Fort George G. Meade, MD, May 18th, 2018.
- Organizer for NSF Workshop on Side and Cover Channel in Computer Systems, Mar. 22-23, 2018.
- MIT Lincoln Labs, “Towards secure processor against information leakage,” Lexington, MA. Apr. 2nd, 2018.
- MIT Lincoln Labs, “Hardware-oriented Security: Side-Channel Analysis, Protection, Evaluation, and Testbed,” Lexington, MA. Mar. 9th, 2017.
- SRC T3S PI meeting, “Side-channel Analysis and Resilience Targeting Accelerators,” Arlington, VA, Jan. 11, 2017.
- University of Waterloo, “Identifying and exploiting timing side channels in GPUs,” Waterloo, CA, Jan. 5th, 2017.
- MITRE corporation, “Hardware-oriented Security: Side-Channel Analysis, Protection, Evaluation, and Testbed,” Bedford, MA, Oct. 11, 2016.
- Analog Devices Inc. Invited Seminar, “Hardware-oriented Security: Side-Channel Analysis, Protection, Evaluation, and Testbed,” Norwood, MA, Aug. 31, 2016.
- EMC Inc. Technical Talk, “Hardware-oriented Security: Attacks, Protection, and Security Evaluation,” Hopkinton, MA, Oct. 27, 2015
- Draper Research Labs, “Hardware-oriented Security: Attacks, Protection, and Security Evaluation,” Cambridge, MA, Oct. 13, 2015.
- MIT Lincoln Lab, “The chip whispers – side channel attack analysis and modeling”, Lexington, MA, Oct. 29, 2013.
- IEEE High Performance and Extreme Computing Conference, “Quantifying side-channel leakage with novel algorithmic confusion analysis”, Sept. 12, 2013.

- Department of Electronics and Information Engineering, Huazhong University of Science and Technology, China, July 14th, 2012.
- Department of Electrical and Computer Engineering, Tufts University, "Improving energy efficiency and security of embedded systems and mobile networks", May 10th, 2011.
- Department of Electrical and Computer Engineering, Northeastern University, "Improving energy efficiency and security of embedded systems and mobile networks", March 18th, 2011.
- Department of Electrical and Computer Engineering Seminar (invited), Worcester Polytechnic University, "Hardware/software Codesign Approach for Dynamic Information Flow Tracking," Apr. 29th, 2011.
- Army Research Office Special Workshop on Hardware Assurance (invited), "Hardware/software Codesign Approach for Dynamic Information Flow Tracking," Apr. 11-12th, 2011.
- Army Research Office Special Workshop on Hardware Assurance (invited), "Architectural Enhancement and System Software Support for Run-time Code/Data Integrity Monitoring in Embedded Processors," Aug. 14th, 2009.
- Department of Electrical and Computer Engineering, Boston University, "Machine-Learning-based Adaptive Network Design for Lifetime Extension in Underwater Sensor Networks," Apr. 13th, 2009.
- Microsoft Research Asia seminar, "Energy and Security Conscious Embedded Systems for Mobile and Sensor Network Applications", June 7th, 2007.
- Intel China Research Center, Beijing, China, "Exploring Application-specific Instruction Set Processors for Security and Reliability Enhancement," May 29th, 2007.
- University of Colorado, Boulder, Department of Electrical and Computer Engineering seminar, Apr. 2006.
- Tsinghua University, Department of Electronic Engineering seminar, June 30th, 2005.
- Intel China Research Center, Beijing, China, "Energy-Efficient Adaptable Computing: From Extensible Processor to Tunable Application," June 29th, 2005.
- Naval Underwater Warfare Center, New Port, US, Technical Presentation Series seminar, June 10th, 2005.
- Brown University, Computer Engineering seminar, May 3rd, 2005.
- University of Connecticut, Department of Electrical and Computer Engineering colloquium, Nov. 19th, 2004.
- Yale University, Department of Electrical and Computer Engineering seminar, Apr. 2004.
- Boston University, Department of Electrical and Computer Engineering seminar, Apr. 2004.
- University of Maryland, College Park, Department of Electrical and Computer Engineering seminar, Mar. 2004.
- University of Connecticut, Department of Electrical and Computer Engineering seminar, Mar. 2004.
- University of California, Santa Cruz, Department of Computer Engineering seminar, Feb. 2004.
- IBM Research Austin Center, invited talk, Feb. 2004.

Teaching Activities (Summary: taught two graduate-level course and two undergraduate-level courses at NU, taught five courses at UConn)

Electrical and Computer Engineering Department, Northeastern University

- Fall 2025/2024/2023/2022, Spring 2019/2020/2021: Undergraduate-level course "Computer Hardware and System Security" (New Course EECE 5699)
- Fall 12,13,14,15,16/Spring13,14: Undergraduate-level course "Computer Architecture and Organization"
- Fall 2018,2019/Spring 2013,2014,2016,2017: Graduate-level course "Computer Hardware Security" (New Course EECE 7390)
- Fall 11/Spring 12: Undergraduate-level course "Computer Architecture for Computer Scientists"

Electrical and Computer Engineering Department, University of Connecticut

- Fall 05: Undergraduate-level course "Electrical and Computer Engineering Principles"
- Spring 05-11: Undergraduate-level course "Digital Systems Design" (New Course)
- Spring 11: Undergraduate-level lab "Microprocessor Application Lab" (New Course)
- Fall 04/06/07/08/10: Graduate-level course "Advanced VLSI Design" (New Course)
- Fall 07/Spring 08: Graduate-level seminar course (New Course)

Advised Students and Research Fellows (Summary: graduated 17 PhDs, 7 NU MS, and mentored 2 post-docs. Supervised tens of undergraduate REUs)

- Current PhD students (4):
  1. Yashaswini Markaram, expected to graduate in 2029.
  2. Yufei Wang, expected to graduate in Aug. 2028.
  3. Davis Ranney, expected to graduate in Aug. 2027.
  4. Tianhong Xu, expected to graduate in Aug. 2026.

- PostDoc fellows:
  1. **Dr. Saion Roy** (PhD: University of Illinois Urbana Champion), Sept. 2024 - .
  2. **Dr. Zhiming Zhang** (PhD: University of New Hampshire), Oct. 1st 2021 – Sept. 2022, first job: Qualcom Inc.
  3. **Dr. Qiasi Luo** (Completed on Dec. 31st, 2011, first job: Marvell Technologies Inc.)
- PhD alumni (in reverse chronological order of graduation) and their First/Current Affiliation:
  1. **Ruyi Ding** (Dissertation defense: Apr. 21, 2025)

     Dissertation title: *Towards Robust and Secure Deep Learning: From Training through Deployment to Interference*

     First job: Assistant Professor, Louisiana State University
  2. **Xiang Zhang** (Dissertation defense: Nov. 19th, 2024)

     Dissertation title: *Confidentiality and Privacy-preserving: Intertwining Deep Learning and Side-channel Analysis.*
  3. **Cheng Gongye** (Proposal defense: June 2, 2023; dissertation defense: Dec. 4th, 2023)

     Dissertation title: *Hardware Security Vulnerabilities in Deep Neural Networks and Mitigation*

     First job: Nvidia Inc. (Santa Clara, CA)

4. **Ziyue Zhang** (co-advised with Prof. A. Aidong Ding), dissertation defense: Nov. 27, 2023.

   Dissertation title: *Advanced deep learning-assisted side-channel attack framework and transfer learning.* ***(Won the NU Math Department Outstanding Dissertation Award)***

   First job: Meta Inc.
5. **Elmira Karimi** (advisor: Prof. David Kaeli), Proposal defense: June 8th, 2021; dissertation defense: Apr. 29, 2022.
   Dissertation title: *Exploring high performance sparse operation on GPUs*
   First job: Philips
6. **Konstantinos Athanasiou**, PhD (co-advised with Prof. Thomas Wahl), graduated in Dec. 2021.

   Dissertation title: Application and Analysis of Masking Countermeasures in Software
   First job: Mathworks, MA
7. **Majid Sabbagh**, PhD (Dissertation defense: June 22nd, 2021; Proposal defense: Dec.16th, 2020).

   Dissertation title: *The perils of shared computing: A hardware security perspective*

   Current job: Google Inc., Santa Clara, CA
8. **Saoni Mukherjee**, PhD (co-advised with Prof. David Kaeli) (Dissertation defense: April 13, 2020; proposal defense: April 2019)
   Dissertation title: *A Power Modeling Approach to Protect GPUs from Side Channel Attacks*
   Current job: Dell EMC, MA
9. **Zhen Hang Jiang**, PhD Aug. 2019 (Dissertation defense: July 29, 2019; proposal defense: Oct. 31, 2018)
   Dissertation title: *Memory-based Side-channel Attacks and Countermeasures*
   Current job: Facebook, WA (Research Staff Member)
10. **Chao Luo**, PhD May 2019 (Dissertation defense: Jan. 12, 2019; proposal defense: Dec. 3, 2018)
    Dissertation title: *Novel Side-Channel Attacks on Emerging Cryptographic Algorithms and Computing Systems*
    Current job: MathWorks, MA (Senior Software Engineer)
11. **Pei Luo**, PhD Aug. 2017 (Dissertation defense: July 31st, 2017; proposal defense: Feb. 2nd, 2017)
    Dissertation title: *Side-channel Security Analysis and Protection of SHA-3*
    Current job: Intel Research Lab, Santa Clara, CA (Technical Staff).
12. **Liwei Zhang**, PhD co-advised with Prof. Adam Aidong Ding (Dissertation defense: Apr. 20, 2017)
    Dissertation title: *Statistical Analysis of Side-channel Attacks and Countermeasures*
    Current job: Staples, MA
13. **Yu Han**, PhD (Dissertation defense: June 22nd, 2016; proposal defense: Jan. 28th, 2016)
    Dissertation title: *Stochastic Medium Access Control for Underwater Acoustic Sensor Networks*
    Current job: Akamai, Cambridge, MA

14. **Bingnan Jiang,** PhD (Dissertation defense: Aug. 11th, 2015; proposal defense: Nov. 13th, 2014)
    Dissertation title: *Optimization and Management of Cyber-physical Systems – Smart Grid and Plug-in Hybrid Electric Vehicles*
    Currently with ACT Lakewood, CO (Operations Research Scientist).
15. **Juan Carlos Martinez Santos**, PhD (LASPAU grantee, dissertation defense: July 26th, 2013, proposal defense: June 5th, 2012;)
    Dissertation title: *Architectural Support for Software Security*
    Currently Associate Professor of ECE, Universidad Tecnologica de Bolivar, Colombia
16. **Xuan Guan,** PhD (Dissertation defense: Apr. 25th, 2011, proposal defense: Aug. 25th, 2010;)
    Dissertation title: *Application-specific instruction set processor design for data-intensive applications*
    Currently Intel lab, Santa Clara, CA
17. **Hai Lin**, PhD (Dissertation defense: Apr. 28th, 2011; proposal defense: Dec. 3rd, 2009)
    Dissertation title: *Multi-objective application-specific instruction set processor design: Towards high performance, energy-efficient, and secure embedded systems*
    Currently at AMD, TX

- MS alumni
    1. **Derek Rodriguez**, Electrical and Computer Engineering MS graduated in Aug. 2023)

       Dissertation title: Using Simulation to Measure Speculative Windows in RISC-V Microarchitectures
    2. **Tianhong Xu,** Electrical and Computer Engineering MS (Apr. 22, 2021)

       Dissertation title: A novel simple power analysis (SPA) attack against Elliptic Curve Cryptography (ECC)
    3. **Amel Docena,** Khoury Computer Science MS (Apr. 2020)

       Dissertation title: Systematic analysis of Deep Neural Networks: Retrieving Sensitive Samples via SMT Solving
    4. **Rasit Mete Esrefoglu**, cybersecurity MS (Jan. 2020),

       Dissertation title: *ARMs Race: Exploiting Branch Prediction Microarchitecture and Speculative Execution on ARMv7*

       First job: Akamai Inc.
    5. **Ritesh Gupta,** MS (May 2019)
    6. **Haofan Shi**, MS (May 2017)
    7. **Tiansi Hu,** MS (completed June. 8th, 2012)
       Dissertation title: *Adaptive, Robust, and Energy-efficient Protocols for Underwater Wireless Sensor Networks*
       Currently with Cadence, CA
- Undergraduate alumni: 2024 summer REU: Grace Li (Khoury), 2024 Spring REU: James Brennan and Charlie Bershatsky, 2023 summer REU: Steven Qie (UIUC), 2021 summer REU: Jack Leightcap, 2017 summer REU: Amit Deliwala, Gregory Chan, Tomas Hoang, Timothy Wong, Colleen Finnegan (2017), Harrison Dimmig, Ryan Pitcher (2016 sumer), Louie Liu, Neel Shah (2015), Tushar Swamy (2015), Ang Shen

(2014), Claude J. Manville (graduated in 2010), Jeff Wroten (supported by NSF REU program, graduated in 2006), Kolawole Ladoja (NSF REU, graduated in 2007), Brian Outlaw (graduated in 2011), Gustavo K. Contreras (spring 2011), Owen Search (NSF REU summer 2011), Karl Severin (NSF REU summer 2011)

- High School Students:
  1. Northeastern University Young Scholar Program, June-July 2020. Jessica Liao (Andover High School), Faraz Iqbal (Franklin High School)

Professional Service

- Session lead for "hardware security of emerging computing systems," NSF SaTC PI Meeting, Sept. 4-5, 2024.
- Track chair for "Algorithms and Computing for Hardware Security", IEEE Int. Conf. on Computer-aided Design (ICCAD), 2024, 2025
- Track chair for "Algorithms and Tools for Hardware Security", IEEE Int. Conf. on Computer-aided Design (ICCAD), 2023.
- TPC member for CCS 2025, USENIX Security 2022, HOST 2021.
- ACM SIGDA Outstanding New Faculty Award Committee, 2021
- ACM Transactions on Embedded Computing Editor-in-Chief Search Committee, 2019
- IEEE Senior Member (2019)
- Guest editor, IEEE Journal on Emerging Technologies in Computing Systems, Hardware Security, 2020-2021.
- Associate Editor, ACM Transactions on Architecture and Code Optimization (TACO), 2020-.
- Associate Editor, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES) 2020.
- General co-chair, International Conference on Cryptographic Hardware and Embedded Systems (CHES) 2019.
- Panelist, Workshop on Computer Architecture Research Direction (CARD), International Symposium on Computer Architecture (ISCA), June 23, 2019.
- Track chair for "Hardware Security II: Attack and Defense", Design Automation Conference (DAC), 2021.
- Track chair for "Hardware Security II: Attack and Defense", Design Automation Conference (DAC), 2020.
- Track chair for 1.4 Embedded Software and Security, International Conference on Computer Aided Design (ICCAD), Nov. 2018.
- Organizer, Workshop on Side-channel and Covert Channel in Computer Systems, NSF, Mar. 2018
- Associate Editor, Springer International Journal on Hardware and System Security (HASS), 2017-.
- Associate Editor, ACM Transaction on Embedded Computing Systems, 2014-2020.
- Guest Editor, Special Issue on Side-channel and Fault Attacks, Springer International Journal of Parallel Programming, with Rosario Cammarota (Intel) and Patrick Schaumont (Virginia Tech.), 2017 – 2019.
- Guest Editor, Springer Journal of Hardware and System Security Special Issue on Hardware Solutions for Cyber Security (HSCS), 2017-2019 (with Michael Vai and Roger I. Khazan – MIT Lincoln labs)
- Guest Editor, ACM Transaction on Embedded Computing Systems Special Issue on Embedded Device Forensics and Security (EDFS), 2015-2016 (with Raymond Choo (UT San Antonio), Yang Xiang (Deakin University, Australia), and Yu Yu (Shanghai Jiaotong University)).

- Associate Editor, IEEE Embedded System Letter, Special Issue on Embedded System Security, 2014. (with Dimitrios Serpanos (Univ. Patras) and Thomas Eisenbarth (WPI))
- Editorial Board Member, Journal of Low Power Electronics. 2010-
- Co-chair for Boston Area Computer Architecture (BARC) workshop, 2016.
- Co-chair of Technical Program Committee for 8th ACM Workshop on Embedded System Security (WESS) 2013, Montreal.
- Chair for IEEE Connecticut Section Women-in-Engineering Affinity group (2006-2011)
- Panelist for National Science Foundation: CISE Secure and Trustworthy Cyberspace (SaTC), 2014, 2016, 2018, 2019, 2020, 2022; CISE IUCRC (2022); CCF Exploiting Parallelism and Scalability (XPS), 2013; Cyber-enabled Sustainability Science and Engineering (CyberSEES), 2013; CNS Trustworthy Computing, 2009; CCF Computing Processes and Artifacts (CPA), 2006
- Reviewer for Army Research Office Young Investigator Program, 2010
- TPC member:
  - IEEE International Symposium on High Performance Computer Architecture (HPCA), 2018
  - IEEE Design Automation Conference (DAC), 2020 (Track Chair), 2019, 2018, 2017
  - IEEE/ACM International Conference on Computer-aided Design (ICCAD), 2019 (Track Chair), 2018, 2017, 2016
  - IEEE International Workshop on Hardware Oriented Security and Trust (HOST), 2018, 2017, 2012, 2010, 2009
  - IEEE International Symposium on Computer Architecture (ISCA), 2013
  - IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS), 2012
  - IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC), 2009
  - IEEE International Conference on Embedded Software and Systems (ICESS), 2009
  - IEEE International Symposium on Application Specific Processors (SASP), 2010, 2009, 2008
  - IEEE International Parallel and Distributed Processing Symposium (IPDPS), 2008
  - IFIP/IEEE International Conference on Very Large Scale Integrated Circuits (VLSI-SOC), 2008, 2007 (Session Chair)
  - ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED), 2008, 2007
  - International Symposium on Circuits & Systems (ISCAS) 2009, 2008, 2007, 2006
  - Annual Boston Area Computer Architecture Workshop, 2007 (Session chair)
  - International Conference on Communication, Circuits, & Systems, 2006.
  - International Conference on Communication & Networking in China 2006.
- Reviewer for
  - Journal of Cryptology
  - ACM Transactions on Design Automation of Electronic Systems (TODAES)
  - ACM Transactions on Architectures and Code Optimizations (TACO)
  - IEEE Transactions on Computer-aided Design of Integrated Circuits and Systems (TCAD)
  - IEEE Transactions on Circuits and Systems (TCAS-II)
  - IEEE Transactions on Computers (TC)
  - IEEE Transactions on Aerospace and Electronic Systems (TAES)
  - IEEE Transactions on Very Large Scale Integration Systems (TVLSI)

- ACM/IEEE International Conference on Compilers, Architecture, and Synthesis of Embedded Systems (CASES)
- ACM/IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)
- IEEE Design Automation Conference (DAC)
- IEEE International Conference on VLSI Design (ICVLSI)
- IEEE Asia South Pacific Design Automation Conference (ASP-DAC)

Institutional Service

At Northeastern University (2011-)

- Department of Electrical and Computer Engineering Tenure and Promotion Committee, Dec. 2020 – Dec. 2021.
- Department of Electrical and Computer Engineering advisory vision committee, Oct. 2020 – Dec. 2021.
- Department of Electrical and Computer Engineering faculty council, chair, 2019-2021.
- Department of Electrical and Computer Engineering faculty hiring committee, 2018-2019.
- Department of Electrical and Computer Engineering graduate affair committee (GAC), 2016 – 2017.
- Teaching assignment coordinator for the ECE Computer Engineering group, 2016 – 2017.
- Northeastern University ReDI (Research and Development Initiatives) Cohort Challenge 2015-2016
- Department of Electrical and Computer Engineering Search Committee for Cyber-Human Systems, Nov. 2015-2016
- Department of Electrical and Computer Engineering Search Committee for Academic Specialists, Feb. 2015
- Department of Electrical and Computer Engineering hiring committee, 2014 - 2015
- College of Engineering Research Advancement Planning Committee, 2014 - 2015
- Department of Electrical and Computer Engineering Search Committee for Neuro Cyber-Human Systems, Nov. 2014 – May 2015
- Department of Electrical and Computer Engineering Search Committee for Academic Specialists, July 2014
- Department of Electrical and Computer Engineering Tenure and Promotion Committee (consists of six faculty members by election), 2012 - 2015
- Department of Electrical and Computer Engineering Undergraduate Study Committee (USC), 2012 - 2014
- Faculty search committee for interdisciplinary position on security between MIE and ECE departments, 2012-2013
- College of Engineering First Year Engineering Redesign (FYER) Committee (2011)

At University of Connecticut (2004-2011)

- UConn ECE Department Colloquium Coordinator (2008 - 2011)
- Faculty advisor for IEEE UConn chapter (2005 - 2008)
- Faculty search committee member of UConn ECE department (2004 - 2005, 2005 - 2006)
- Evaluation committee member of UConn ECE senior design projects (2004 - current)

- Mentor for UConn ECE NSF REU (Research Experience for Undergraduates) program

PhD course at Princeton University (1999-2004)

- Committee member of ACSSPU (Association of Chinese Students and Scholars of Princeton Univ.) (1999-2000)

Synergistic Activities

- Participated in developing a low-power behavioral synthesis tool commercialized by a company *Alternative System Concept,* 2002-2003.

Member of Dissertation Committee

Gordon Fellow Master Students (Northeastern)

- Daniel Hullihen, *AMD Improving Delta Color Compression (DCC)*, Dec. 14th, 2015 (Advisor: David Kaeli)
- Jason Harland, *EMC Global Hardware Engineering Firmware Validation and Qualification Transformation,* Aug. 7th, 2012, (Advisor: David Kaeli)

PhD Students (after joined Northeastern)

- Yukui Luo (Advisor: XIaolin Xu, dissertation defense: Aug. 8 2023)
  Dissertation title: Securing FPGA as a shared cloud-computing resource: Threats and Mitigations
- Siyue Wang (Advisor: Xue Lin, proposal defense: May 13th 2020)
  Dissertation title: Towards robust and secure deep learning models and beyond
- Pu Zhao (Advisor: Xue Lin, proposal defense: Dec. 9th 2020, dissertation defense: Aug. 10, 2021)
  Dissertation title: Towards Robust Image Classification with Deep learning and Real-Time DNN Inference on Mobile
- Haohao Liao (Advisor: Catherine Gebotsy, University of Waterloo, dissertation defense: Feb. 04, 2020)
  Dissertation title: Electromagnetic Fault Injection on Two Microcontrollers: Methodology, Fault Model, Attack, and Countermeasures
- Zhengyu Yang (Advisor: Ningfang Mi, proposal defense: Jan 22, 2018, dissertation defense: July 30, 2018)
  Dissertation title: Flash-based Storage Management in Cloud Computing Datacenter Infrastructures
- Navid Farazmand (Advisor: David Kaeli, proposal defense: Dec. 5th, 2016, dissertation defense: Mar. 14th, 2018)
  Dissertation title: Dynamic voltage and frequency scaling for 3D graphics applications on the state-of-the-art mobile GPUs
- Akshay Lahiry (Advisor: David Kaeli, proposal defense: Dec. 20, 2017, dissertation defense: Aug. 8, 2018)
  Dissertation title: Exploring Compression in the GPU Memory Hierarchy for Graphics and Computer
- Mohammad Khavari Tavana (Advisor: David Kaeli, proposal defense: Sept. 15, 2017, dissertation defense: Mar. 28, 2018)
  Dissertation title: *Architectural Support for Design Dependable Non-volatile Main Memories*

- Gangqiang Yang (Advisor: Guang Gong and Mark Aagaard, Department of Electrical and Computer Engineering, University of Waterloo. Dissertation defense date: Jan. 5th, 2017)
  Dissertation title: *Optimized Hardware Implementations of Lightweight Cryptography*
- Nasibeh Teimouri (Advisor: Gunar Schirner, proposal defense: Sept. 29, 2016, dissertation defense: Nov. 29, 2017)
  Dissertation title: *Improving Scalability of Chip-Multiprocessors with Many Accelerators*
- Amir Kavian Ziabari (Advisor: David Kaeli, proposal defense: July 15th, 2016, dissertation defense: Dec. 2nd, 2016)
  Dissertation title: *Reducing the global memory inefficiencies in GPU-based systems*
- Xin Fang (Advisor: Miriam Leeser and Stratis Ioannidis, proposal defense: Oct. 31, 2016, dissertation defense: Aug. 21, 2017)
  Dissertation title: *Privacy Preserving Computations Accelerated using FPGA Overlays*
- Yi Yao (Advisor: Ningfang Mi, Proposal defense: Feb. 6th, 2015, dissertation defense: Aug. 11th. 2015)
  Dissertation title: *Resource management in large-scale data processing platforms*
- Steven Olivieri (Advisor: Alexander M Wyglinski, (WPI ECE), Dissertation defense: Jan. 26th, 2015)
  Dissertation title: *An investigation of security in near-field communications*
- Jennifer Mankin (Advisor: David Kaeli, Dissertation defense: Sept. 26, 2013)
  Dissertation title: Classification of malware persistence mechanisms using low-artifact disk instrumentation
- Masoud Zamani (Advisor: Medhi Tehoori, Proposal defense: Dec. 7th 2012, Dissertation defense: Apr. 2nd, 2013)
  Dissertation title: *Robust design techniques for emerging technologies of computing*
- Ayse Yilmazer (Advisor: David Kaeli, Proposal defense: July 16th, 2013, Dissertation defense: Dec. 5, 2013)
  Dissertation title: *HQL: A Scalable Synchronization Mechanism for GPUs*
- Jenny Mankin (Advisor: David Kaeli, Proposal defense: Oct. 17th, 2012, Dissertation defense: Sept. 26, 2013)
  Dissertation title: *Malware analysis and classification through low-artifact disk instrumentation*

PhD Students (UConn)

- Weiguo Tang (Major Advisor: Lei Wang, Proposal defense: Dec. 14th, 2010)
- Jeremy Lee (Major Advisor: Mohammad Tehranipoor, Dissertation defense: Dec. 17th, 2010)
- Junxia Ma (Major Advisor: Mohammad Tehranipoor, Dissertation defense: Dec. 10th, 2010)
- Ke Peng (Major Advisor: Mohammad Tehranipoor, Dissertation defense: Dec. 9th, 2010)
- Xiaoxiao Wang (Major Advisor: Mohammad Tehranipoor, Dissertation defense: Dec. 9th, 2010)
- Summit Narayan (Major Advisor: John Chandy, Dissertation defense: June 17th, 2010)
- Nisar Ahmed (Major Advisor: Mohammad Tehranipoor, Dissertation defense: Sept. 2007)

MS Students (Northeastern)

- Amel Nesto Docena (Advisor: Thomas Wahl, Thesis defense: Apr. 23, 2020)
  Thesis title: Retrieving sensitive samples through SMT solving.
- Trinayan Baruah (advisor: David Kaeli, Thesis defense: Dec. 13, 2017)
  Thesis title: Energy Efficient Execution of Heterogeneous Applications

- Chenyan Liu (Advisor: Gunar Schirner, Thesis defense: Aug. 21st, 2014))
- Xin Fang (Advisor: Miriam Leeser, Thesis defense: July 30th, 2013)
  Thesis title: *Variable precision floating point reciprocal, divider, and square root for major FPGA vendors*
- David Kusinsky (Advisor: Miriam Leeser, Thesis defense: Apr. 4th, 2013)
  Thesis title: *FPGA-based hyperspectral covariance coprocessor for size, weight, and power constraint platforms*
- Anoop R. (Advisor: Ningfang Mi, project presentation: Nov. 27th, 2012)
- Jun Li (Advisor: Ningfang Mi, project presentation: Aug. 16, 2012)
  Project title: *Auction-based resource management of Amazon spot instances*

MS Students (UConn)

- Anuradharthi Thiruvenkata Ramani (Major Advisor: John Chandy, Dissertation Defense: Apr. 1st, 2009)