Curriculum Vitae of

Fatemeh Ganji

Assistant Professor
Electrical and Computer Engineering (ECE) Department
Worcester Polytechnic Institute (WPI)
100 Institute Road
Worcester, 01609-2280 MA
Email: fganji@wpi.edu

I. Education

2017 Doctor of Engineering (Dr.-Ing)- Electrical Engineering
Dissertation: On the learnability of physically unclonable functions
Grade: Summa Cum Laude (with the highest distinction)
Technische Universität Berlin, Germany

2010 Master of Science (M.Sc.)- Electrical Engineering
Malek Ashtar University of Technology, Iran

2006 Bachelor of Science (B.Sc.)- Electrical Engineering
K. N. Toosi University of Technology, Iran

II. Scholarship[1]

Total Citations (as per Google Scholar, Mar. 11, 2025): 1651
H-index (as per Google Scholar, Mar. 11, 2025): 22
Google Scholar Page: Link

A. Publications

Journals (peer-reviewed, published or in press)

[J20] M. Hashemi[WPI], D. Forte, and **F. Ganji**. Guardianmpc: Backdoor-resilient neural network computation. IEEE Access, 2025. [Impact factor: 3.9]

[J19] D. M. Mehta[WPI], M. Hashemi[WPI], D. Forte, S. Tajik, and **F. Ganji**. 1/0 shades of UC: Photonic side-channel analysis of universal circuits. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2024(3):574–602, 2024. [Impact factor: 3.5]

[J18] D. M. Mehta[WPI], M. Hashemi[WPI], D. S. Koblah, D. Forte, and **F. Ganji**. Bake it till you make it: Heat-induced leakage from masked neural networks. IACR Transactions on Cryptographic Hardware and Embedded System, 24(4):569–609, 2024. [Impact factor: 3.5]

[J17] M. Hasan, T. Hoque, **F. Ganji**, D. Woodard, D. Forte, and S. Shomaji. A resource efficient binary cnn implementation for enabling contactless iot authentication. Journal of Hardware and Systems Security, pages 1–14, 2024. [Impact factor: 1.2]

[1] Students, whose names are underlined, were/are mentored/supervised by F. Ganji. WPI's students are marked as Student[WPI]. Student$_{MQP}$[WPI] indicates that the student was part of an MQP team advised by F. Ganji.

[J16] D. S. Koblah, U. J. Botero, S. P. Costello, O. P. Dizon-Paradis, **F. Ganji**, D. L. Woodard, and D. Forte. A fast object detection-based framework for via modeling on pcb x-ray ct images. ACM Journal on Emerging Technologies in Computing Systems, 19(4):1–20, 2023. [Impact factor: 2.01]

[J15] R. Y. Acharya, **F. Ganji**, and D. Forte. Information theory-based evolution of neural networks for side-channel analysis. IACR Transactions on Cryptographic Hardware and Embedded Systems, pages 401–437, 2023. [Impact factor: 3.5]

[J14] T. Mosavirik[WPI], **F. Ganji**, P. Schaumont, and S. Tajik. Scatterverif: Verification of electronic boards using reflection response of power distribution network. ACM Journal on Emerging Technologies in Computing Systems (JETC), 2022. [Impact factor: 1.42]

[J13] D. S. Koblah, R. Y. Acharya, D. Capecci, O. P. Dizon-Paradis, S. Tajik, **F. Ganji**, D. L. Woodard, and D. Forte. A survey and perspective on artificial intelligence for security-aware electronic design automation. ACM Transactions on Design Automation of Electronic Systems (TODAES), 2022. [Impact factor: 1.74]

[J12] S. M. Sohi, J.-P. Seifert, and **F. Ganji**. Rnnids: Enhancing network intrusion detection systems through deep learning. Computers & Security, 102:102151, 2021. [Impact factor: 6.45]

[J11] S. Shomaji, Z. Guo, **F. Ganji**, N. Karimian, D. Woodard, and D. Forte. Blocker: A biometric locking paradigm for iot and the connected person. Journal of Hardware and Systems Security, 5(3):223–236, 2021. [Impact factor: 1.5]

[J10] S. Shomaji, P. Ghosh, **F. Ganji**, D. Woodard, and D. Forte. An analysis of enrollment and query attacks on hierarchical bloom filter-based biometric systems. IEEE Transactions on Information Forensics and Security, 16:5294–5309, 2021. [Impact factor: 7.178]

[J9] S. Chowdhury, A. Covic, R. Y. Acharya, S. Dupee, **F. Ganji**, and D. Forte. Physical security in the post-quantum era: A survey on side-channel analysis, random number generators, and physically unclonable functions. Journal of Cryptographic Engineering, pages 1–37, 2021. [Impact factor: 1.81]

[J8] U. J. Botero, R. Wilson, H. Lu, M. T. Rahman, M. A. Mallaiyan, **F. Ganji**, N. Asadizanjani, M. M. Tehranipoor, D. L. Woodard, and D. Forte. Hardware trust and assurance through reverse engineering: A tutorial and outlook from im- age analysis and machine learning perspectives. ACM Journal on Emerging Technologies in Computing Systems (JETC), 17(4):1–53, 2021. [Impact factor: 1.42]

[J7] **F. Ganji**, S. Tajik, P. Stauss, J.-P. Seifert, M. Tehranipoor, and D. Forte. Rock'n'roll pufs: Crafting provably secure pufs from less secure ones (extended version). Journal of Cryptographic Engineering, 2020. [Impact factor: 1.82]

[J6] S. Chowdhury, **F. Ganji**, and D. Forte. Recycled soc detection using ldo degradation. SN Computer Science, 1(6):1–21, 2020. [Impact factor: 1.31]

[J5] **F. Ganji**, D. Forte, and J.-P. Seifert. Pufmeter a property testing tool for assess- ing the robustness of physically unclonable functions to machine learning attacks. IEEE Access, 7:122513–122521, 2019. [Impact factor: 3.367]

[J4] **F. Ganji**, S. Tajik, F. Fäßler, and J.-P. Seifert. Having no mathematical model may not secure pufs. Journal of Cryptographic Engineering, 7(2):113–128, 2017. [impact factor: 1.61]

[J3] **F. Ganji**, S. Tajik, and J.-P. Seifert. Pac learning of arbiter pufs. Journal of Cryptographic Engineering, 6(3):249–258, 2016. [Impact factor: 1.81]

[J2] **F. Ganji**, Ł. Budzisz, F. G. Debele, N. Li, M. Meo, M. Ricca, Y. Zhang, and A. Wolisz. Greening campus wlans: Energy-relevant usage and mobility patterns. Computer Networks, 78:164–181, 2015. [Impact factor: 5.49]

[J1] Ł. Budzisz, **F. Ganji**, G. Rizzo, M. A. Marsan, M. Meo, Y. Zhang, G. Koutitas, L. Tassiulas, S. Lambert, B. Lannoo, et al. Dynamic resource provisioning for energy efficiency in wireless access networks: A survey and an outlook. IEEE Communications Surveys & Tutorials, 16(4):2259–2285, 2014. [Impact factor: 25.25]

Conference papers (peer-reviewed, published or in press)

[C34] M. Hashemi[WPI], S. Tajik, **F. Ganji**. Garblet: Multi-party Computation for Protecting Chiplet-based Systems, accepted for presentation at IEEE VLSI Test Symposium, 2025. [Acceptance rate: NA]

[C33] D. M. Mehta[WPI], T. Marcantonio[MQP][WPI], M. Hashemi[WPI], S. Karkache[MQP][WPI], D. Shanmugam, P. Schaumont, **F. Ganji**. SCAPEgoat: Side Channel Analusis Library, accepted for presentation at IEEE VLSI Test Symposium, 2025. [Acceptance rate: NA]

[C32] M. Hashemi[WPI], D. M. Mehta[WPI], K. Mitard[WPI], S. Tajik, and **F. Ganji**. FaultyGarble: Fault Attack on Secure Multiparty Neural Network Inference. Workshop on Fault Detection and Tolerance in Cryptography (FDTC), 2024. [Acceptance rate: NA]

[C31] M. Hashemi[WPI], D. Forte, and **F. Ganji**. Time is money, friend! Timing side-channel attack against garbled circuit constructions. International Conference on Applied Cryptography and Network Security, 2024. [Acceptance rate: 23%]

[C30] D. S. Koblah, D. M. Mehta[WPI], M. Hashemi[WPI], **F. Ganji**, and D. Forte. EDA workflow for optimization of robust model probing-compliant masked hardware gadgets. In GOMACTech, 2024. [Acceptance rate: NA]

[C29] D. S. Koblah, **F. Ganji**, D. Forte, and S. Tajik. Hardware moving target defenses against physical attacks: Design challenges and opportunities. In Proceedings of the 9th ACM Workshop on Moving Target Defense, pages 25–36, 2022. [Acceptance rate: NA]

[C28] M. Hashemi[WPI], S. Roy, **F. Ganji**, and D. Forte. Garbled EDA: Privacy preserving electronic design automation. In Proceedings of the 41st IEEE/ACM International Conference on Computer-Aided Design, pages 1–9, 2022. [Acceptance rate: 22.5%]

[C27] M. Hashemi[WPI], S. Roy, D. Forte, and **F. Ganji**. Hwgn2: Side-channel protected nns through secure and private function evaluation. In Security, Privacy, and Applied Cryptography Engineering: 12th International Conference, SPACE 2022, Jaipur, India, December 9–12, 2022, Proceedings, pages 225–248. Springer Nature Switzerland Cham, 2022. [Acceptance rate: 30%]

[C26] T. Krachenfels, **F. Ganji**, A. Moradi, S. Tajik, and J.-P. Seifert. Real-world snap- shots vs. theory: Questioning the t-probing security model. In 2021 IEEE Symposium on Security and Privacy (SP), pages 1955–1971. IEEE, 2021. [Acceptance rate: ~12.6%]

[C25] U. J. Botero, **F. Ganji**, D. L. Woodard, and D. Forte. Automated trace and copper plane extraction of x-ray tomography imaged pcbs. In 2021 IEEE Physical Assurance and Inspection of Electronics (PAINE), pages 1–8. IEEE, 2021. [Acceptance rate: ~35%]

[C24] R. Y. Acharya, N. F. Charlot, M. M. Alam, **F. Ganji**, D. Gauthier, and D. Forte. Chaogate parameter optimization using bayesian optimization and genetic algo- rithm. In International Symposium on Quality Electronic Design, 2021. [Acceptance rate: ~35%]

[C23] P. Ghosh, U. J. Botero, **F. Ganji**, D. Woodard, R. S. Chakraborty, and D. Forte. Automated detection and localization of counterfeit chip defects by texture analysis in infrared (ir) domain. In 2020 IEEE Physical Assurance and Inspection of Electronics (PAINE), pages 1–6. IEEE, 2020. [Acceptance rate: ~35%]

[C22] **F. Ganji**, S. Amir, S. Tajik, D. Forte, and J.-P. Seifert. Pitfalls in machine learning-based adversary modeling for hardware systems. In Design and Test European Conference, 2020. [Acceptance rate: ~36%]

[C21] S. Chowdhury, **F. Ganji**, and D. Forte. Low-cost remarked counterfeit ic detection using ldo regulators. In 2020 IEEE International Symposium on Circuits and Systems (ISCAS), pages 1–5. IEEE, 2020. [Acceptance rate: ~50%]

[C20] U. J. Botero, D. Koblah, D. E. Capecci, **F. Ganji**, N. Asadizanjani, D. L. Woodard, and D. Forte. Automated via detection for pcb reverse engineering. In ISTFA 2020, pages 157–171. ASM International, 2020. [Acceptance rate: NA]

[C19] U. J. Botero, **F. Ganji**, N. Asadizanjani, D. L. Woodard, and D. Forte. Semi- supervised automated layer identification of x-ray tomography imaged pcbs. In 2020 IEEE Physical Assurance and Inspection of Electronics (PAINE), pages 1–6. IEEE, 2020. [Acceptance rate: ~35%]

[C18] R. Y. Acharya, S. Chowdhury, F. Ganji, and D. Forte. Attack of the genes: Finding keys and parameters of locked analog ics using genetic algorithm. In 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pages 284–294. IEEE, 2020. [Acceptance rate: ~20%]

[C17] S. Shomaji, **F. Ganji**, D. Woodard, and D. Forte. Hierarchical bloom filter frame- work for security, space-efficiency, and rapid query handling in biometric systems. In 10th IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2019.

[C16] **F. Ganji**, D. Forte, N. Asadizanjani, M. Tehranipoor, and D. Woodard. The power of ic reverse engineering for hardware trust and assurance. Electronic Device Failure Analysis (EDFA), 2019.

[C15] S. Chowdhury, **F. Ganji**, T. Bryant, N. Maghari, and D. Forte. Recycled analog and mixed signal chip detection at zero cost using ldo degradation. In 2019 IEEE international test conference (ITC), pages 1–10. IEEE, 2019.

[C14] M. M. Alam, S. Tajik, **F. Ganji**, M. Tehranipoor, and D. Forte. Ram-jam: Remote temperature and voltage fault attack on fpgas using memory collisions. In 2019 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), pages 48– 55. IEEE, 2019.

[C13] **F. Ganji**, S. Tajik, and J.-P. Seifert. A fourier analysis based attack against physi- cally unclonable functions. In International Conference on Financial Cryptography and Data Security, pages 310–328. Springer, 2018.

[C12] **F. Ganji**, S. Tajik, and J.-P. Seifert. Let me prove it to you: Ro pufs are provably learnable. In Information Security and Cryptology-ICISC 2015: 18th International Conference, Seoul, South Korea, November 25-27, 2015, Revised Selected Papers 18, pages 345–358. Springer International Publishing, 2016.

[C11] **F. Ganji**, S. Tajik, F. Fäßler, and J.-P. Seifert. Strong machine learning attack against pufs with no mathematical model. In International Conference on Cryptographic Hardware and Embedded Systems, pages 391–411. Springer, Berlin, Heidelberg, 2016.

[C10] S. Tajik, H. Lohrke, **F. Ganji**, J.-P. Seifert, and C. Boit. Laser fault attack on physically unclonable functions. In 2015 workshop on fault diagnosis and tolerance in cryptography (FDTC), pages 85–96. IEEE, 2015.

[C9] **F. Ganji**, S. Tajik, and J.-P. Seifert. Why attackers win: on the learnability of xor arbiter pufs. In International Conference on Trust and Trustworthy Computing, pages 22–39. Springer, Cham, 2015.

[C8] **F. Ganji**, J. Krämer, J.-P. Seifert, and S. Tajik. Lattice basis reduction attack against physically unclonable functions. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pages 1070–1080, 2015.

[C7] **F. Ganji**, A. Zubow, Ł. Budzisz, and A. Wolisz. On detecting wlan users communication attempts. In 2014 7th IFIP Wireless and Mobile Networking Conference (WMNC), pages 1–8. IEEE, 2014.

[C6] M. Meo, Y. Zhang, Y. Hu, F. Idzikowski, Ł. Budzisz, **F. Ganji**, I. Haratcherev, A. Conte, A. Cianfrani, L. Chiaraviglio, et al. The trend experimental activities on "green" communication networks. In 2013 24th Tyrrhenian International Workshop on Digital Communications-Green ICT (TIWDC), pages 1–6. IEEE, 2013.

[C5] **F. Ganji**, Ł. Budzisz, and A. Wolisz. Assessment of the power saving potential in dense enterprise wlans. In 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pages 2835–2840. IEEE, 2013.

[C4] F. S. Khodadad, **F. Ganji**, A. Safaei, and F. S. Khodadad. A robust pn length estimation in down link low-snr ds-cdma multipath channels. In 2010 The 12th International Conference on Advanced Communication Technology (ICACT), vol- ume 2, pages 951–955. IEEE, 2010.

[C3] F. S. Khodadad, **F. Ganji**, and M. R. Aref. A practical approach for coherent signal surveillance and blind parameter assessment in asynchoronous ds-cdma systems in multipath channel. In 2010 18th Iranian Conference on Electrical Engineering, pages 305–310. IEEE, 2010.

[C2] **F. Ganji**, V. Tabatabavakili, F. S. Khodadad, M. Hosseinnezhad, and A. Safaei. A novel bem-based channel estimation algorithm for time variant uplink ofdma system. In 2010 The 12th International Conference on Advanced Communication Technology (ICACT), volume 2, pages 1289–1293. IEEE, 2010.

[C1] M. Hosseinnezhad and **F. Ganji**. Low complexity mmse based channel estimation algorithm in frequency domain for fixed broadband wireless access system. In 2009 IEEE 10th Annual Wireless and Microwave Technology Conference, pages 1–3. IEEE, 2009.

Book chapter

[BC3] **F. Ganji** and S. Tajik. Physically unclonable functions and ai. Security and Artificial Intelligence, pages 85–106, 2022. [Peer-reviewed]

[BC2] S. Tajik and **F. Ganji**. Artificial neural networks and fault injection attacks. Security and Artificial Intelligence, pages 72–84, 2022. [Peer-reviewed]

[BC1] A. Covic, S. Chowdhury, R. Y. Acharya, **F. Ganji**, and D. Forte. Post-quantum hardware security. In Emerging Topics in Hardware Security, page 199. Springer Nature, 2021.

Book

[B1] **F. Ganji**. On the Learnability of Physically Unclonable Functions. Springer, 2018.

B. Grants

The grants awarded on which I am PI or co-PI total $2,465,799 (without cost-share. $3,620,333 with cost-share). These grants are listed below:

	Funding Agency	Information
[A8]	Survival and Flourishing Fund's flexHEG grant	SPARTACUS: Secure, Private, and Tamper Resistant Technologies for AI Chips made in U.S. Performance period: 02/01/2025-01/31/2026 Amount awarded at WPI: $171,000, Total award amount: $233,000.
[A7]	Cisco Systems, Silicon Valley Community Foundation	Revisiting the IEEE P1735 Standard for In-house Semiconductor IP Protection Performance period: 03/15/2024- 03/15/2025 Amount awarded at WPI: $75,002, Total award amount: $92,502.
[A6]	National Science Foundation	POSE: Phase I: An Open-Source Approach to Measure and Analyze Embedded Systems Security Performance period: 07/01/2024- 06/01/2025 Amount awarded at WPI: $259,891, Total award amount: $299,891.
[A6]	Electric Power Research Institute	Title: ECHT: Electromagnetic and Thermal Testing for Hardware Verification Performance period: 9/20/2023- 6/30/2025 Amount awarded to WPI: $125,617, Total award amount: $125,617.
[A5]	Electric Power Research Institute	Title: Hardware Based Reference Signatures Phase 2 Performance period: 11/3/2022- 12/31/2023 Amount awarded to WPI: $171,629, Total award amount: $171,629.
[A4]	National Science Foundation	Title: ERI: Foundations of Machine Learning for Side-channel Analysis Performance period: 3/1/2022- 3/1/2025 Amount awarded to WPI: $194,726, Total award amount: $194,726.
[A3]	National Science Foundation	Title: MRI: Acquisition of High-Resolution Photon Emission/Laser Fault Injection Microscope with High-Performance Computers for Failure Analysis and Security Assessment of Electronic Systems Performance period: 08/15/2021- 08/15/2024

		Amount awarded to WPI: $360,608, Total award amount: $515,142.
[A2]	Massachusetts Technology Collaborative	Title: Toward a Globally Competitive Electronics Workforce Endowed with Next Generation CyberSecurity Technologies Performance period: February 2020- 09/30/2023. Amount awarded to WPI: $999,326, Total award amount: $1,999,326.
[A1]	Semiconductor Research Corporation	Title: IP Protection through Secure and Private Function Evaluation Performance period: 10/1/2020- 09/30/2023. Amount awarded to WPI: $108,000, Total award amount: $216,000.

C. Professional presentations

2025
- Presentation: "SNARKs for Private AI Monitoring," at the FlexHEG Builder Event in FAR.Labs (a collaborative AI safety research hub based in University of California, Berkeley), 2025.

2024
- Invited talk: "Should We Put Our Trust in the Implementation of MPC?" at the NIST Crypto Reading Club (https://csrc.nist.gov/presentations/2024/crclub-2024-10-02), 2024.
- Invited talk: "Boolean Analysis for Security Assessment of Physically Unclonable Functions" at the Women In Circuits Workshop on Hardware Security affiliated with IEEE European Solid-State Electronics Research Conference (https://www.esserc2024.org/w12-hardware-security), 2024.
- Presentation: "FaultyGarble: Fault Attack on Secure Multiparty Neural Network Inference" at the Workshop on Fault Detection and Tolerance in Cryptography (FDTC), 2024.
- Invited talk: "AI for Side-channel Analysis" at the Cisco Offensive Security Summit, 2024.
- Presentation: "Time is money, friend! Timing side-channel attack against garbled circuit constructions" at the 22nd International Conference on Applied Cryptography and Network Security (ACNS), 2024.
- Invited lecture: "Classic Rewind and Fast-forward to PQC: Lessons Learned from AI-assisted SCA" at DISTANT Training School affiliated with the annual Summer School on Real-world Crypto and Privacy (https://summerschool-croatia.cs.ru.nl/2024/DISTANT.html) , 2024.

2023
- Panelist on "WPI's Beyond These Towers: Data Science and AI in Our Lives (https://www.wpi.edu/news/calendar/events/beyond-these-towers-data-science-and-ai-our-lives), 2023.
- Presentation: "Information Theory-based Evolution of Neural Networks for Side-channel Analysis" at the annual Conference on Cryptographic Hardware and Embedded Systems (CHES), 2023.
- Panelist on "Crypto meets AI: AI and cryptanalysis" at GHTC (https://ghtcworkshop.tii.ae/2023/),
- affiliated event of the Crypto conference, 2023.

- Invited talk: "Side-Channel Protected NNs Through Secure and Private Function Evaluation" at the Workshop on Security for Custom Computing Machines (SCCM, https://sccm-workshop.github.io), 2023.

- Invited lecture: "From (Less Careful) Standardization of Intellectual Property Protection to Secure and Private Electronic Design Automation" at the annual Summer School on Real-world Crypto and Privacy (https://summerschool-croatia.cs.ru.nl/2023/), 2023.

2022

- Invited talk: "Neural Networks: predators and prey," Dagstuhl Seminar 22412-Intelligent Security: Is AI for Cybersecurity a Blessing or a Curse, October 9-14, 2022, Saarbrücken, Germany.

- Invited talk: "Neural Networks: predators and prey," WPI's Midsummer Workshop on Hardware Security, August 28-9, 2022, Worcester, USA.

- Invited talk: "Garbled EDA: Privacy-Preserving Electronic Design Automation," June 7, 2022, MITRE principal locations, Bedford, Massachusetts.

2021

- Keynote speech: "Machine Learning for Hardware Security: Standing on the Shoulders of Giants," at Artificial Intelligence in Hardware Security (AIHWS), June 21, 2021, Kamakura, Japan (Online) https://aihws2021.aisylab.com.

- Invited talk: "From Cryptography to Property Testing," Workshop on Artificial Intelligence and Cryptography (AICrypt), October 16, 2021, Zagreb, Croatia (Online) http://aicrypt.zemris.fer.hr.

- Invited panel: "Ask Me Anything III: Fatemeh Ganji", Cryptographic Hardware and Embedded Systems (CHES), 2021.

- Invited panel: "Women in Science: Challenges, Opportunities, and Motivations," as part of the Gender-Equality measures in SPP (Priority Program, Nano Security: From Nano-Electronics to Secure Systems).

- Invited talk "ML for Security of "things" and human beings" at the WPI's ECE Graduate Seminar.

D. Patents

[P4] D. J. Forte, D. Woodard, F. Ganji, and S. Shomaji. Biometric locking methods and systems for internet of things and the connected person, May 21, 2024. US Patent 11,989,273.

[P3] T. Mosavirik, F. Ganji, P. Schaumont, S .Tajik, P. Martyak, M. Thow. Methods for verifying integrity and authenticity of a printed circuit board, Aug. 17, 2023. WO Patent WO2023154395A1

[P2] F. Ganji, S. Tajik, J.-P. Seifert, D. Forte, and M. M. Tehranipoor. Hardness amplification of physical unclonable functions (pufs), Oct. 24, 2023. US Patent 11,799,673.

[P1] S. Chowdhury, F. Ganji, N. Maghari, and D. J. Forte. Detection of recycled integrated circuits and system-on-chips based on degradation of power supply rejection ratio, May 23, 2023. US Patent 11,657,405.

E. Scholarship in progress

Journals

[J1_Underreview] S. Nouraniboosjin[WPI] and **F. Ganji**. Too hot to be true: Temperature calibration for higher confidence in nn-assisted side-channel analysis. Cryptology ePrint Archive, Paper 2024/071, 2024. [Available Online] https://eprint.iacr.org/2024/071 [Accessed Feb. 10, 2025].

Conference papers

[C2_Underreview] A. Aysu, **F. Ganji**, T. Marcantonio, and P. Schaumont. An open-source ecosystem for implementation security testing. Cryptology ePrint Archive, 2024.

[C1_Underreview] R. Y. Acharya, L. L. Jeune, N. Mentens, **F. Ganji**, and D. Forte. Quantization-aware neural architectural search for intrusion detection. arXiv preprint arXiv:2311.04194, 2023. [Available Online] https://arxiv.org/abs/2311.04194 [Accessed Feb. 11, 2024].

F. Professional society memberships and offices

2008- Present Institute of Electrical and Electronics Engineers (IEEE)

2009- Present IEEE Women in Engineering

2013- Present IEEE Sustainable ICT Community

2015- Present International Association for Cryptologic Research (IACR)

2017- Present IEEE Computer Society Technical Committee on Security and Privacy

2019- Present Association for Computing Machinery (ACM)

G. Awards and honors

2024
- Media coverage: "Guardians of the Microchip" in the Fall 2024 WPI Journal.

2023
- ACM CCS 2023 Top Reviewer Award

2022
- Media coverage: "WPI Expands Cybersecurity Research With NSF-funded Microscope And High-performance Computers"
- NSF Engineering Research Initiation (ERI) Award

2021
- Media coverage: "Baker-Polito Administration Awards $1 Million to WPI for New Semiconductor Security Research Center"

2018
- BIMoS PhD Award
- Nominated by Technical University of Berlin for ACM Doctoral Dissertation Award
- Nominated by Faculty IV (Electrical Engineering and Computer Science) of Technical University of Berlin for Marthe Vogt Award
- Recognition of Ph.D. Degree with the Highest Distinction (Summa Cum Laude)

2016
- Runner-up papers for Conference on Cryptographic Hardware and Embedded Systems (CHES)

H. Editorial and referee activities

2024-2025
- Editorial Board member of "IACR Communications in Cryptology"

2023 ▪ Co-editor of a special issue on "Multi-tenant Computing Security Challenges and Solutions" for the Springer Journal of Hardware and Systems Security (HaSS)

2016 ▪ Co-editor of the report from Dagstuhl Seminar 16202 "Hardware Security"

III. Teaching

A. Teaching experience

Worcester Polytechnic Institute, MA, USA

2020-Present Assistant Professor

- ECE 2049- Embedded Computing in Engineering Design
- ECE 596- Graduate Seminars
- ECE 579-C- Applied Cryptography & Physical Attacks
- ECE 2305- Introduction to Communications and Networks
- ECE 2312- Discrete-Time Signal and System Analysis

University of Florida

2018 Postdoctoral Fellow

- Advanced Hardware Security and Trust (co-instructed with Prof. Dominic Forte)

Technische Universität Berlin, Germany

2015-2018
- Ph.D. Student and Postdoctoral Fellow
- Cryptography
- Computer Security Seminar (co-instructed with Prof. Jean-Pierre Seifert)

2011-2014 Graduate student- Electrical and Computer Engineering

- Seminar Network Technologies (co-instructed with Dr. Lukasz Budzisz)

K. N. Toosi University of Technology, Iran

2005 Junior Student- Electrical Engineering

- Teaching assistant: Signals and Systems

B. Teaching innovations at WPI

C25 ECE 2312- Discrete-Time Signal and System Analysis

- Post-lecture quizzes administrated and taken online in Canvas to encourage students to process what they learn and check their understanding.
- Introduction to pioneers with a minority background in relevant lectures, e.g., Ingrid Daubechies
- Setting up a separate course email account that TAs and the instructor can manage and answer students questions timely.
- Offering smaller, more frequent low-stakes assessments throughout the term to monitor student progress.
- Replaced larger assessments with a series of formative ones taken in the format of quizzes.

D24 ECE 2305- Introduction to Communications and Networks

- Introduction to pioneers with a minority background in relevant lectures, e.g., Mary Elizabeth Shannon (Moore)
- Using low-cost development boards to create demos to stimulate interest in students.
- Weekly quizzes taken online via Canvas to assess the course outcome more frequently with a lower grading load.
- Setting up a separate course email account that TAs and the instructor can manage, and answer students questions timely.

A23 ECE 2049- Embedded Computing in Engineering Design

- A competition was initiated to further engage the students in the course projects, where a team of three students was awarded development boards as prizes.

Fall 2022-2025 ECE 576- Applied Cryptography & Physical Attacks

- The format of the class is "flipped classroom" so that students study materials before class, then apply their learning during class.
- Applied the Think-pair-share strategy to keep the students engaged during online lectures. In this method students think individually, then discuss their ideas with a partner.
- Incorporating research component to offer first-hand experience for senior undergraduate and junior graduate students with no research experience.
- Designing a lecture on using research resource, academic honesty in research products, and making effective presentations.
- The students are offered a hands-on workshop to work with the most advanced equipment at Vernam Lab.

C. Undergraduate projects (MQPs, IQPs, Sufficiency projects) advised and co-advised at WPI

Topic: Automation of Photon Emission Analysis Pipeline for Cybersecurity

Year	#Students	Names	Primary advisor	Co-advisor
2024-2025	3	▪ Spencer Harding ▪ Keegan Kuhn ▪ Scott West	**Fatemeh Ganji**	---

Topic: Development of Open-source Educational Tools for Security Analysis of Integrated Circuits

Year	#Students	Names	Primary advisor	Co-advisor
2024-2025	2	▪ Nat Dynko (CS) ▪ Sharon Rose John Paul	**Fatemeh Ganji** Patrick Schaumont (ECE/CS)	---
2023-2024	2	▪ Samuel Karkache (CS) ▪ Trey Marcantonio		

Topic: Few-shot Machine Learning for Side-channel Analysis

Year	#Students	▪ Names	Primary advisor	Co-advisor
2021-2022	2	▪ Robert Brodin (CS) ▪ Wen Wu	**Fatemeh Ganji**	Craig Shue (CS)

Topic: Chaos or Noise? Characterization of Meta-stable Behavior of Bistable Rings

Year	#Students	▪ Names	Primary advisor	Co-advisor
2021-2022	2	▪ Isabel Herrero Estrada ▪ Victor Mercola	**Fatemeh Ganji**	Shahin Tajik (ECE)

D. Independent studies and directed research conducted at WPI

Spring 25 Topic: Efficient APIs for Side-channel Analysis
Alessandra Savio Serpes (CS/M.Sc.)

Topic: AI for Side-channel Analysis
Michael McInerney (CS/B.Sc.)

Fall 24 Topic: AI Inference Engines at the Edge

Anna Kelly (ECE/B.Sc.)

Spring 2024 Topic: Efficient Storage and Retrieval of Side-channel Data
Amit Virchandbhai Prajapati (DS/M.Sc.)

Summer 2022 Topic: Deep Learning for Side-channel Analysis
Venkatesh Mullur (RBE/B.Sc.)
Shivaram Srikanth (RBE/B.Sc.)

Spring 2021 Topic: Side-channel Analysis in Practice
Zhenyuan (Charlotte) Liu (ECE/Ph.D.)

E. Academic advising at WPI

Spring 2025
- 3 Ph.D. students: Mohammad Hashemi, Dev Mehta, Seyedmohammad Nouraniboosjin

Fall 2024
- 3 Ph.D. students: Mohammad Hashemi, Dev Mehta, Seyedmohammad Nouraniboosjin

Spring 2024
- 3 Ph.D. students: Mohammad Hashemi, Dev Mehta, Seyedmohammad Nouraniboosjin

Fall 2023
- 3 Ph.D. students: Mohammad Hashemi, Dev Mehta, Seyedmohammad Nouraniboosjin
- 1 M.Sc. student: Antonio Torres

Spring 2023
- 2 Ph.D. students: Mohammad Hashemi, Dev Mehta
  1 M.Sc. student: Victor Mercola

Fall 2022
- 2 Ph.D. students: Mohammad Hashemi, Dev Mehta
  1 M.Sc. student: Victor Mercola

Spring 2022
- 2 Ph.D. students: Mohammad Hashemi, Dev Mehta

Fall 2021
- 1 Ph.D.: Mohammad Hashemi

Number of advisees at WPI

	Primary Advisor	Graduate Advisor	Co-Advisor	Major 2 Advisor	Total Student Count
2024-2025	27	4	0	1	32
2023-2024	21	7	0	1	29
2022-2023	25	6	1	1	33
2021-2022	6	6	0	0	12
2020-2021	6	3	0	0	9

F. Mentoring

Fall 2021-Present
- External mentor in the program “Gender-equality measures in SPP (Priority Program, Nano Security: From Nano-Electronics to Secure Systems)”

Fall 2020-Present
- External mentor of 1 student with minority background

2021-2023
- External mentor of 2 students including 1 student with minority background

2020-2021
- External mentor of 4 students including 3 students with minority backgroun

IV. Services

A. Service to profession

Grant Reviewer

- NSF CSR Small Panelist: Privacy-preserving Technologies, 2024

Organization committee

- New England Hardware Security (NEHWS) Day workshop, 2021-2025
- Organizing the Open Tools, Interfaces and Metrics for Implementation Security Testing (OPTIMIST) workshop affiliated with CHES 2024

Conference chairing

- Session "Machine Learning" at Cryptographic Hardware and Embedded Systems (CHES), 2020, 2021, 2023, and 2024
- Session "Side Channel Metrics and Masking Schemes" at Cryptographic Hardware and Embedded Systems (CHES), 2022
- Design, Automation and Test in Europe Conference, 2021 (session ID: 5.2)
- "Session S5: AI, Vision & Robotics" at Field Programmable Logic and Applications (FPL) 2020

Technical Program Committee Member

- Program Track Co-Chair of Design, Automation and Test in Europe Conference (DATE), 2023-2025
- General Chair of New England Hardware Security (NEHWS), 2025
- Conference on Applied Cryptography and Network Security (ACNS), 2023-25
- Design, Automation and Test in Europe (DATE) Conference, 2021-2025
- Program Chair of New England Hardware Security (NEHWS), 2024
- Artificial Intelligence in Hardware Security (AIHWS), 2020-2024
- Conference on Cryptographic Hardware and Embedded Systems (CHES), 2020-2024
- ACM Conference on Computer and Communications Security (CCS), 2023
- International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS), 2023
- Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE), 2022-2023
- Attacks and Solutions in Hardware Security (ASHES), 2022-2023
- Top Picks in Hardware and Embedded Security, 2022
- Hardware and Architectural Support for Security and Privacy (HASP), 2021-2023
- Conference on Security, Privacy and Applied Cryptography (SPACE), 2021
- Field Programmable Logic and Applications (FPL), 2020
- 8th International Workshop on Security Proofs for Embedded Systems (PROOFS), 2019, 2020
- IEEE Symposium on Security and Privacy (S&P), 2020 (External reviewer)
- IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2018 (External reviewer)
- Student PC member of 38th IEEE Symposium on Security and Privacy, 2017

Reviewer for journals

- IACR Communications in Cryptology, IACR
- Journal of Cryptographic Engineering, Springer
- Journal of Hardware and Systems Security, Springer
- Security & Privacy (Journal), IEEE
- Transactions on Computers, IEEE
- Transactions on Computer-Aided Design of Integrated Circuits and Systems, IEEE
- Transactions on Circuits and Systems I: Regular Papers, IEEE
- Transactions on Circuits and Systems II: Express Briefs, IEEE
- Transactions on Information Forensics & Security, IEEE
- Transactions on Dependable and Secure Computing, IEEE
- Transactions on Embedded Computing Systems, IEEE

- Transactions on Emerging Topics in Computing, IEEE
- Transactions on Industrial Electronics, IEEE
- Transaction on Mobile Computing, IEEE
- Journal on Emerging and Selected Topics in Circuits and Systems, IEEE
- Transactions on Privacy and Security, ACM
- Journal on Emerging Technologies in Computing Systems, ACM
- Computer Communications, Elsevier
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2020-2024)

B. Service to departments and programs

2023-2024
- Chairing the Computer Engineering Curriculum Sub-committee
- Member of Diversity, Equity, Inclusion Committee
- Contribution to the development of new undergraduate program Bachelor's in Cyber Security

2022-2023
- Chairing the Computer Engineering Curriculum Sub-committee
- Member of Diversity, Equity, Inclusion Committee
- Participating as an advisee in the "Diversity, Equity, Inclusion Coffee Chat" held by the ECE Department

2021-2022
- Undergraduate Curriculum Ad Hoc Committee
- Member of Diversity, Equity, Inclusion Committee
- Member of Diversity, Equity, Inclusion Ad Hoc Committee

2020-2021
- Member of ECE Graduate Program Committee
- Contribution to the development of new graduate program Master's in Cyber Security

C. Service to the students

2025
- Ph.D. Committee member: Andrew Adiletta
- Recommendation letters for Ruoshui Tian (5 letter), Anna Kelly

2024
- ECE's MQP Provost Competition Committee member
- Recommendation letters for Victor Mercola (3 letters), Isabel Herrero Estrada (23 letters), Kelu Liu, William Folan, Dev Mehta, Mohammad Hashemi, Yashas Honnavalli, and Annalisa Allan.

2023
- ECE's MQP Provost Competition Committee member
- M.Sc. Thesis Committee member: Andrew Adiletta
- Ph.D. Committee member: Dillibabu Shanmugam
- Recommendation letters for: Jacob Nguyen, Arnav Sacheti,

2022
- Recommendation letters for: Zhenyuan (Charlotte) Liu

2021
- Ph.D. Committee member: Saad Islam

D. Service to the institute

2022-2023
- Panelist on "WPI's Beyond These Towers: Data Science & AI in Our Lives"