Personal information

First name / Surname	**Fatemeh Ganji**
Address	Worcester Polytechnic Institute (WPI) 100 Institute Road Worcester, MA 01609, USA
Telephone	(352) 294-3945
E-mail	fganji@wpi.edu
Webpage	https://www.wpi.edu/people/faculty/fganji

Research Interests

- Intellectual Property (IP) protection: Applications of Artificial Intelligence (AI) and cryptography for IP protection
- Applications of AI for hardware security: Counterfeit electronic component detection and avoidance, design and security assessment of Physically Unclonable Functions (PUFs), PCB and IC reverse and anti-reverse engineering.
- Chaos theory for cryptography: Design and evaluation of chaos-based hardware component
- Security and privacy in biometrics

Work experience

Dates	August 2020- Present
Position held	**Assistant Professor**
Main activities and responsibilities	Research: Security of AI hardware, AI for hardware security, Provably secure IP-protection methods
Name and address of employer	Cybersecurity and Electrical and Computer Engineering (ECE) Departments Worcester Polytechnic Institute (WPI) 100 Institute Road Worcester, MA 01609, USA https://www.wpi.edu/academics/departments/cybersecurity
Type of business	Academic research group
Dates	June 2018- August 2020
Position held	**Postdoctoral fellow**

Main activities and responsibilities	Research: application of machine learning techniques and chaos theory in hardware security and biometrics. ▪ Outstanding research results: development of a publicly accessible software for measuring the resistance of PUFs to machine learning attacks in a provable fashion: https://www.trust-hub.org/software ▪ Gained expertise in: biometrics in security and privacy-related applications, application of machine learning in counterfeit detection and reverse engineering, application of chaos theory in hardware security.
Name and address of employer	Prof. Domenic Forte Florida Institute for Cybersecurity Research, 601 Gale Lemerand Dr. P.O. Box 116550 Gainesville, FL 32611, USA https://fics.institute.ufl.edu
Type of business	Academic research group
Dates	May 2014- May 2018
Position held	**Research/ teaching assistant**
Main activities and responsibilities	Teaching activities: computer security (seminar), and cryptography (lecture). Research: vulnerability assessment of Physically Unclonable Functions (PUFs) through mathematical approaches, namely learning theory, and linear algebra. ▪ Outstanding research results: providing mathematical proofs of the vulnerability of arbiter PUFs, XOR arbiter PUFs, RO PUFs, and PUFs with no mathematical model (e.g., BR PUFs). ▪ Gained expertise in: theory of machine learning, lattice bases reduction attacks, Boolean analysis, and cryptography.
Name and address of employer	Prof. Dr. Jean-Pierre Seifert, Telecom Innovation Laboratories/ Technical University of Berlin Ernst-Reuter-Platz 7, 10587 Berlin, Germany http://sec.t-labs.tu-berlin.de
Type of business	University/ Research and innovation centre
Dates	June 2011- Feb 2014
Position held	**Research assistant**
Main activities and responsibilities	Research on energy efficiency in wireless local area networks (WLANs) ▪ Results: a novel switching on/off approach as a cornerstone of the energy efficiency strategies, contribution to the public deliverables, cooperation with several European institutes through, for instance, joint publications and mobility actions. ▪ Gained expertise in: computer networks, specifically, WLAN protocols, approaches towards green networking, working with and preparing experimental setups.

Name and address of employer	Prof. Dr. Adam Wolisz, Telecommunication Networks Group, / Technical University of Berlin Einsteinufer 25, FT 5, 10587 Berlin, Germany http://www.tkn.tu-berlin.de
Type of business	Academic research group
Dates	1 Sept 2007- 15 May 2011
Position held	**Wireless network Engineer**
Main activities and responsibilities	Design and optimization of wireless networks (UHF/VHF and microwave links), Project technical manager ▪ Gained expertise in: designing microwave, UHF and VHF links, national/ international standards used in the petroleum and natural gas industries.
Name and address of employer	F.Fardiss, Pars Telecom System Group No. 31, West Haghtalab St., Saadat Abad, Tehran, Iran http://parssaman.com/
Type of business	Consulting firm

Education and training

Dates	May 2014- August 2017
Title of qualification that will be awarded	**Doctor of Engineering (Dr.-Ing)** Thesis : On the learnability of physically unclonable functions Grade: Summa Cum Laude (with the highest distinction) Supervisor: Prof. Dr. J.P. Seifert
Name of the university	Technical University of Berlin
Dates	Sept 2008- Sept 2010
Title of qualification awarded	**Master of science (M.Sc) in telecommunication**
Name of the university	Malek Ashtar University of Technology
Dates	Sept 2001- Jan 2006
Title of qualification awarded	**Bachelor of Science (B.Sc) in electrical engineering**
Name of the university	K. N. Toosi University of Technology
PhD schools	▪ CROSSING winter school on quantum security ▪ TREND PhD school on green telecommunications

Awards and Honors

- BIMoS PhD Award 2018
- Nominated by Technical University of Berlin for ACM Doctoral Dissertation Award, 2018
- Nominated by Faculty IV (Electrical Engineering and Computer Science) of Technical University of Berlin for Marthe Vogt Award, 2018
- Received a Travel Grant for Lorentz Center, 2019
- Received a Travel Grant for Schloss Dagstuhl - NSF Support Grant
- Received a Travel Grant for the Financial Cryptography and Data Security Conference, 2018
- Received a Travel Grant for the Conference on Cryptographic Hardware and Embedded Systems, 2016
- Received a Travel Grant for the Conference on Cryptographic Hardware and Embedded Systems, 2015
- Received a Travel Grant for the ACM Conference on Computer and Communications Security, 2015

Professional Activities

Publications

Please see Annex 1 and my Google Scholar Citations profile: https://scholar.google.de/citations?user=jG6XBwIAAAAJ&hl=en&oi=ao

Selected talks

- Security of PUFs: Lessons Learned after Two Decades of Research, Tutorial, Conference on Cryptographic Hardware and Embedded Systems (CHES), 2019
- Lattice basis reduction attack against Physically Unclonable Functions, CrossFyre, 2015
- Dispelling the myth: cloning the Physically Unclonable Functions (PUFs), Krypto-Tag (10-11 Dec. 2015, ESCRYPT, Berlin)
- Assessment of the power saving potential in dense enterprise WLANs, 4th and 5th plenary meeting of TREND*

Reviewer for

- 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
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2020-2021)
- Transactions on Computers, IEEE
- Transaction on Mobile Computing, IEEE
- ACM Transactions on Privacy and Security
- Computer Communications, Elsevier
- Journal of Hardware and Systems Security, Springer

Technical Program Committee (TPC)	▪ Conference on Cryptographic Hardware and Embedded Systems (CHES), 2020-21 ▪ Design, Automation, and Test in Europe Conference (DATE), 2021 ▪ IEEE Symposium on Security and Privacy (S&P), 2020 (External reviewer) ▪ Conference on Security, Privacy and Applied Cryptography (SPACE), 2020 ▪ Field Programmable Logic and Applications (FPL), 2020 ▪ 8th International Workshop on Security Proofs for Embedded Systems (PROOFS), 2019-2020 ▪ 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
Supervision and Co-Supervision: Current students	▪ Ana Covic ▪ Sumaiya Shomaji ▪ Sreeja Chowdhury ▪ Rabin Yu Acharya
Supervision and Co-Supervision: Former students	▪ Sarah Amir ▪ Md Mahbub Alam ▪ Soroush M. Sohi ▪ Pascal Stauss ▪ Antonio Cavotta ▪ Abdulraouf Sawas
Guest Editor	▪ Co-editor of the report from Dagstuhl Seminar 16202 “Hardware Security”
Organizing activities	▪ Member of the organizing committee for 6th International Workshop on Constructive Side-Channel Analysis and Secure Design
Projects	▪ SISSDEN, https://sissden.eu/ ▪ TREND, http://www.fp7-trend.eu/
Academic memberships	▪ IEEE member since Jan. 2002 ▪ Member of IEEE Women in Engineering since Jan. 2008 ▪ Member of Berlin International Graduate School in Model and Simulation based Research (BIMoS) since Jun. 2015
Personal skills and competences	
Technical skills and competences	▪ Extensive knowledge of hardware security and machine learning theory. ▪ Good knowledge of cryptography ▪ Having teaching and peer-reviewing experiences.

Computer skills and competences	▪ Programming experience with Magma, MATLAB & Simulink (signal detection, time series analysis etc.), and engineering software such as Pathloss™ Program and RMW RF propagation simulation software. ▪ Having experience of working with experimental instruments, e.g., spectrum analyser, and network protocol analysers such as Wireshark, and Kismet.
Languages	▪ English (full professional proficiency) ▪ German (full professional proficiency) ▪ Persian (mother tongue)
Social skills and competences	Good skills of communication with partners/ colleagues developed through involvement in projects and activities
Organisational skills and competences	▪ Having experience of organizing small research groups ▪ Teaching experience

Annex 1. List of publications

Books

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

Journal Papers

[J1] F. Ganji, S. Tajik, Pascal Stauss, J.-P. Seifert, D. Forte, and M. Tehranipoor, "Rock'n' roll PUFs: Crafting Provably Secure PUFs from Less Secure Ones," Journal of Cryptographic Engineering, 2019.

[J2] F. Ganji, D. Forte, J.-P. Seifert, "PUFmeter: a Property Testing Tool for Assessing the Robustness of Physically Unclonable Functions to Machine Learning Attacks," IEEE Access, Vol.7, 2019.

[J3] F. Ganji, D. Forte, N. Asadizanjani, M. Tehranipoor, D. Woodard, "The Power of IC Reverse Engineering for Hardware Trust and Assurance," Electronic Device Failure Analysis (EDFA), May 2019.

[J4] F. Ganji, N. Karimian, D. Woodard, D. Forte, "Leave Adversaries in the Dark- BLOcKeR: Secure and Reliable Biometric Access Control", The Journal of the Homeland Defense and Security Information Analysis Center (HDIAC), Vol. 6, No. 1, Spring 2019.

[J5] F. Ganji, S. Tajik, F. Faessler, and J.-P. Seifert, "Having No Mathematical Model May Not Secure PUFs," Journal of Cryptographic Engineering, 2017.

[J6] F. Ganji, S. Tajik, and J.-P. Seifert, "PAC Learning of Arbiter PUFs," (extended version), Journal of Cryptographic Engineering, 2016.

[J7] F. Ganji, et al. "Greening the campus WLAN: energy-relevant usage and mobility patterns," Computer networks- Special issue on green communications, Vol.78, Elsevier, February 2014.

[J8] Ł. Budzisz, F. Ganji, G. Rizzo, M.A. Marsan, M. Meo, Y. Zhang, G. Koutitas, L. Tassiulas, S. Lambert, B. Lannoo, and M. Pickavet, "Dynamic Resource Provisioning for Energy Efficiency in Wireless Access Networks: a Survey and an Outlook," IEEE Communications Surveys and Tutorials, Vol.16, No.4, Fourth quarter 2014.

Conference and Workshop Papers

[C1] T. Krachenfels, F. Ganji, A. Moradi, S. Tajik, J.-P Seifert, "Real-world Snapshots vs. Theory: Questioning The T-probing Security Model, " accepted for IEEE Symposium on Security and Privacy, 2021.

[C2] R. Acharya, S. Chowdhury, F Ganji, and D. Forte, "Attack of the Genes: Finding Keys and Parameters of Locked Analog ICs Using Genetic Algorithm" accepted for IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), December 2020.

[C3] U. Botero, F. Ganji, N. Asadizanjani, D.Woodard, D. Forte, "Semi-Supervised Automated Layer Identification of X-ray Tomography Imaged PCBs", to appear IEEE International Conference on Physical Assurance and Inspection of Electronics (PAINE), December 2020.

[C4] P. Ghosh, U. Botero, F. Ganji, D. Woodard, RS Chakraborty, D. Forte, "Automated Detection and Localization of Counterfeit Chip Defects by Texture Analysis in Infrared (IR) Domain", to appear IEEE International Conference on Physical Assurance and Inspection of Electronics (PAINE), December 2020.

[C5] U. Botero, D. Koblah, DE Capecci, F. Ganji, N. Asadi, DL Woodard, D. Forte, "Automated Via Detection for PCB Reverse Engineering", to appear International Symposium for Testing and Failure Analysis (ISTFA), November 2020.

[C6] S. Chowdhury, F Ganji, D. Forte, "Low-Cost Remarked Counterfeit IC Detection Using LDO Regulators", accepted for IEEE International Symposium on Circuits and Systems (ISCAS), October 2020.

[C7] F. Ganji, S. Amir, S. Tajik, J.-P. Seifert, and D. Forte, "Pitfalls in Machine Learning-based Adversary Modeling for Hardware Systems," to appear in Proc. of Design, Automation and Test in Europe Conference and Exhibition, March 2020.

[C8] 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 Proc. of IEEE International Test Conference (ITC), November 2019.

[C9] S. Shomaji, F. Ganji, D. Woodard, and D. Forte, "Hierarchical Bloom Filter Framework for Security, Space-efficiency, and Rapid Query Handling in Biometric Systems," in Proc. of IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), September 2019.

[C10] M. Alam, S. Tajik, F. Ganji, M. Tehranipoor, D. Forte, "RAM-Jam: Remote Temperature and Voltage Fault Attack on FPGAs using Memory Collisions", in Proc. of Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), August 2019.

[C11] F. Ganji, S. Tajik, Pascal Stauss, J.-P. Seifert, D. Forte, and M. Tehranipoor, "Rock' n' roll PUFs: Crafting Provably Secure PUFs from Less Secure Ones," in Proc. of International Workshop on Security Proofs for Embedded Systems (PROOFS), August 2019.

[C12] P. Ghosh, F. Ganji, D. Forte, D. Woodard, RS Chakraborty, "Automated Framework for Unsupervised Counterfeit Integrated Circuit Detection by Physical Inspection," in Proc. of International Conference on Physical Assurance and Inspection of Electronics (PAINE), July 2019.

[C13] F. Ganji, S. Tajik, and J.-P. Seifert, "A Fourier Analysis Based Attack against Physically Unclonable Functions," in Proc. of Financial Cryptography and Data Security, 2018.

[C14] F. Ganji, S. Tajik, F. Faessler, and J.-P. Seifert, "Strong Machine Learning Attack against PUFs with No Mathematical Model," in Proc. of Conference on Cryptographic Hardware and Embedded Systems (CHES), 2016.

[C15] F. Ganji, S. Tajik, J.-P. Seifert, "Let Me Prove it to You: RO PUFs are Provably Learnable," in Proc. of International Conference on Information Security and Cryptology, 2015.

[C16] F. Ganji, J. Krämer, J. -P. Seifert, S. Tajik, "Lattice Basis Reduction Attack against Physically Unclonable Functions," in Proc. of ACM Conference on Computer and Communications Security, 2015.

[C17] F. Ganji, S. Tajik, J. -P. Seifert, "Why Attackers Win: On the Learnability of XOR Arbiter PUFs," in Proc. of Trust and Trustworthy Computing, 2015.

[C18] S. Tajik, H. Lohrke, F. Ganji, J. -P. Seifert, C. Boit, "Laser Fault Attack on Physically Unclonable Functions," in Proc. of Fault Diagnosis and Tolerance in Cryptography, 2015.

[C19] F. Ganji, A. Zubow, Ł. Budzisz, and A. Wolisz, "On detecting WLAN users communication attempts," in Proc. of IFIP Wireless and Mobile Networking Conference, May 2014.

[C20] F. Ganji, Ł. Budzisz , A. Wolisz, "Assessment of the Power Saving Potential in Dense Enterprise WLANs," in Proc. of 24th annual IEEE Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'13), London, Great Britain, September 2013.

[C21] F. Ganji, Ł. Budzisz, and A. Wolisz, "Assessment of the power saving potential in dense enterprise WLANs," TKN Group, TU Berlin, Tech. Rep. TKN-13-003, April 2013.

[C22] 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 Proc. of International Conference on Advanced Communication Technology (ICACT) 2010.

[C23] 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 Proc. of International Conference on Advanced Communication Technology (ICACT) 2010.

[C24] F. Samsami Khodadad and F. Ganji, M. R. Aref, "A Practical Approach for Coherent Signal Surveillance and Blind Parameter Assessment in Asynchronous DS-CDMA Systems in Multipath Channel," in Proc. of 18th Iranian Conference on Electrical Engineering (ICEE2010).

[C25] M. Hosseinnezhad and F. Ganji, "Low Complexity MMSE-based Channel Estimation Algorithm in Frequency Domain for Fixed Broadband Wireless Access System," in Proc. of 10th Annual IEEE Wireless and Microwave Technology Conference (WAMICON '09), 2009.

Informal Publications (Including Under-review Papers)

[I1] F. Ganji, and S. Tajik, "Physically Unclonable Functions and AI: Two Decades of Marriage," arXiv preprint arXiv:2008.11355, 2020.

[I2] S. Tajik, and F. Ganji, "Artificial Neural Networks and Fault Injection Attacks," arXiv preprint arXiv:2008.07072, 2020.

[I3] 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," arXiv preprint arXiv:2005.04344, 2020.

[I4] A. Covic, F. Ganji, and D. Forte, "Circuit Masking Schemes: New Hope for Backside Probing Countermeasures?," SRC TECHCON, 2020.

[I5] 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 Survey and Outlook from Image Analysis and Machine Learning Perspectives," arXiv preprint arXiv:2002.04210, 2020.

[I6] F. Ganji, "Composability of Machine-Learning Resistant PUFs – When Yao Fails -or- Can we build secure composite PUFs?," Secure Composition for Hardware Systems (Dagstuhl Seminar 19301). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019.

[I7] S.M. Sohi, F. Ganji, and J.P Seifert, "Recurrent Neural Networks for Enhancement of Signature-based Network Intrusion Detection Systems," arXiv preprint arXiv:1807.03212, 2018.

[I8] F. Ganji, S. Tajik, D. Forte, and J.-P. Seifert, "Blockchain-enabled Cryptographically-secure Hardware Obfuscation," Cryptology ePrint Archive: Report 2019/928.

Patents

[P1] S. Chowdhury, F. Ganji, N. Maghari and D. Forte, "Recycled Analog and Mixed Signal Chip Detection at Zero Cost Using LDO Degradation," Provisional Appl. No. 62/901,676, filed September 17, 2019, A&B Ref. 049648/534626, UF Ref. T17833US001

[P2] F. Ganji, S. Tajik, J.-P. Seifert, D. Forte, Mark M. Tehranipoor, "Hardness Amplification of Physically Unclonable Functions (PUFs)," Provisional Appl. No. 62/836,829, filed April 22, 2019, A&B Ref. 049648/529675, UF Ref. T17664