NADER SEHATBAKHSH

Los Angeles, CA 90095
Contact: (+1)4044262998 ⋄ nsehat@ucla.edu
Homepage: https://ssysarch.ee.ucla.edu/nader/

WORK EXPERIENCE

Assistant Professor, University of California, Los Angeles *June 2020 - Current*
Electrical and Computer Engineering (ECE) Department, Samueli School of Engineering.

EDUCATION

Georgia Institute of Technology *Atlanta, GA, USA*
PhD Computer Science *Aug. 2014 - May 2020*
Thesis Title: *"Leveraging Side-Channel Signals for Security and Trust"*
Advisors: Milos Prvulovic and Alenka Zajic.

Georgia Institute of Technology *Atlanta, GA, USA*
M.Sc. Electrical Engineering *Aug. 2014 - Dec. 2017*

University of Tehran *Tehran, Iran*
B.Sc. Electrical Engineering *Sept. 2009 - Jun. 2014*

SELECTED HONORS AND AWARDS

- **NSF CAREER Award**, 2024.
- **Cisco Research Award**, 2022.
- **Jumior Faculty Fellow Award**, 2021.
- **Best Paper Award**, 49th IEEE/ACM Symposium on Microarchitecture (MICRO-49), 2016.
- **Best Paper Nominee**, 26th IEEE International Symposium on High-Performance Computer Architecture (HPCA-26), 2020.
- **IEEE Micro Top Picks Honorable Mention**, 2018.
- **Featured Paper**, in the March 2020 issue of IEEE Transactions on Computers.
- **Second Best Demo Award**, IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2017.
- **Best Student Paper Award**, IEEE Region 8 Student Paper Contest, 2014.

SELECTED PUBLICATIONS

(For the full list please refer to my Google Scholar Page.)

Conferences:

C19. [MobiCom'24] *"LightPure: Realtime Adversarial Image Purification for Mobile Devices Using Diffusion Models."*
Hossein Khalili, Seongbin Park, Vincent Li, Brandan Bright, Ali Payani, Ramana Rao Kompella and **Nader Sehatbakhsh**.
The 30th ACM Annual International Conference On Mobile Computing And Networking (MobiCom).

C18. [**GLSVLSI'24**] *"SCRIPT: A Multi-Objective Routing Framework for Securing Chiplet Systems against Distributed DoS Attacks."*
Ebadollah Taheri, Pooya Aghanoury, Sudeep Pasricha, Mahdi Nikdast, and **Nader Sehatbakhsh**.
IEEE Great Lakes Symposium on VLSI (GLSVLSI).

C17. [**MobiSys'24**] *"RefreshChannels: Exploiting Dynamic Refresh Rate Switching for Mobile Device Attacks."*
Gaofeng Dong, Jason Wu, Julian De Gortari Briseno, Akash Deep Singh, Justin Feng, Ankur Sarker, **Nader Sehatbakhsh**, and Mani Srivastava.
The 22nd ACM International Conference on Mobile Systems, Applications, and Services (MobiSys).

C16. [**SafeThings'24**] *"Unleash the Power: Non-Invasive On-Chip Malware Detection in Heterogeneous IoT Systems by Leveraging Side-Channels."*
Fatemeh Arkannezhad, Pooya Aghanoury, Justin Feng, Hossein Khalili, and **Nader Sehatbakhsh**.
IEEE/ACM Workshop on the Internet of Safe Things.

C15. [**SafeThings'24**] *"Virtual Keymysteries Unveiled: Detecting Keystrokes in VR with External Side-Channels."*
Hossein Khalili, Alexander Chen, Theodoros Papaiakovou, Timothy Jacques, Hao-Jen Chien, Changwei Liu, Aolin Ding, Amin Hass,Saman Zonouz, and **Nader Sehatbakhsh**.
IEEE/ACM Workshop on the Internet of Safe Things.

C14. [**NDSS'23**] *"IDA: Hybrid Attestation with Support for Interrupts and TOCTOU."*
Fatemeh Arkannezhad, Justin Feng, and **Nader Sehatbakhsh**.
The Network and Distributed System Security (NDSS) Symposium.

C13. [**DAC'23**] *"Hybrid Obfuscation of Chiplet-Based Systems."*
Yousef Safari, Pooya Aghanouri, Subu Iyer, **Nader Sehatbakhsh**, and Boris Vaisband.
The 60th Annual Design Automation Conference (DAC).

C12. [**IMWUT/UbiComp'23**] *"Fingerprinting IoT Devices Using Latent Physical Side-Channels."*
Justin Feng, Tianyi Zhao, Shamik Sarkar, Dominic Konrad, Timothy Jacques, Danijela Cabric, and **Nader Sehatbakhsh**.
Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT).

C11. [**ECTC'23**] *"Secure and Scalable Key Management for Waferscale Heterogeneous Integration."*
Yousef Safari, Pooya Aghanouri, Subu Iyer, and **Nader Sehatbakhsh**.
The 73rd Electronic Components and Technology Conference (ECTC).

C10. [**MobiCom'23**] *"Enc^2:Privacy-Preserving Inference for Tiny IoTs via Encoding and Encryption."*
Hao-Jen Chien, Hossein Khalili, Amin Hass, and **Nader Sehatbakhsh**.
The 29th Annual International Conference On Mobile Computing And Networking (MobiCom).

C9. [**IPSN'23**] *"Everything has its Bad Side and Good Side: Turning Processors to Low Overhead Radios Using Side-Channels."*
Justin Feng, Timothy Jacques, Omid Abari, and **Nader Sehatbakhsh**.
The 22nd International Conference on Information Processing in Sensor Networks (IPSN).

C8. [**HPCA'20**] *"A New Side-Channel Vulnerability on Modern Computers by Exploiting Electromagnetic Emanations from the Power Management Unit."*
Nader Sehatbakhsh, Berkay Yilmaz, Alenka Zajic, and Milos Prvulovic.
In Proceedings of the 26th IEEE International Symposium on High-Performance Computer Architecture

(HPCA-26).
Acceptance Rate: 19.3%.

C7. [**HPCA'20**] *"EMSim: A Microarchitecture-Level Simulation Tool for Modeling Electromagnetic Side-Channel Signals."*
Nader Sehatbakhsh, Berkay Yilmaz, Alenka Zajic, and Milos Prvulovic.
In Proceedings of the 26th IEEE International Symposium on High-Performance Computer Architecture (HPCA-26).
Acceptance Rate: 19.3%.
HPCA Best Paper Nominee.

C6. [**MICRO'19**] *"EMMA: Hardware/Software Attestation Framework for Embedded Systems Using Electromagnetic Signals."*
Nader Sehatbakhsh, Alireza Nazari, Haider Khan, Alenka Zajic, and Milos Prvulovic.
In Proceedings of the 52nd IEEE/ACM International Symposium on Microarchitecture (MICRO-52).
Acceptance Rate: 21%.

C5. [**AAAI-FSS'19**] *"Security and Privacy Considerations for Machine Learning Models Deployed in the Government and Public Sector."*
Nader Sehatbakhsh, Ellie Daw, Onur Savas, Amin Hassanzadeh, Ian McCulloh.
In Proceedings of the AAAI Conference on Artificial Intelligence, Fall Symposium Series (AAAI-FSS'19).

C4. [**HOST'18**] *"Syndrome: Spectral Analysis for Anomaly Detection on Medical IoT and Embedded Devices."*
Nader Sehatbakhsh, Monjur Alam, Alireza Nazari, Alenka Zajic, and Milos Prvulovic.
In Proceedings of the 11th International Symposium on Hardware-Oriented Security and Trust (HOST'18).
Acceptance Rate: 19%.
Second Best Demo Award.

C3. [**ISCA'17**] *"EDDIE: EM-Based Detection of Deviations in Program Execution."*
Alireza Nazari, **Nader Sehatbakhsh** (*same contribution*), Monjur Alam, Alenka Zajic, and Milos Prvulovic.
In Proceedings of the 44th International Symposium on Computer Architecture (ISCA'17).
Acceptance Rate: 16%.
Micro Top Picks Honorable Mention.

C2. [**MICRO'16**] *"Spectral Profiling: Observer-Effect-Free Profiling by Monitoring EM Emanations."*
Nader Sehatbakhsh, Alireza Nazari, Alenka Zajic, and Milos Prvulovic.
In Proceedings of the 49th IEEE/ACM International Symposium on Microarchitecture (MICRO-49).
Acceptance Rate: 21%.
MICRO Best Paper Award.

C1. [**DTIS'14**] *"FPGA Implementation of Genetic Algorithm for Dynamic Filter-Bank-Based Multi-carrier Systems."*
Nader Sehatbakhsh Mohammad Aliasgari, and Sied Mehdi Fakhraie.
In Proceedings of the 8th IEEE International Conference on Design and Technologies in Nanoscale Era (DTIS'14).
Acceptance Rate: 29%.
Best Student Paper Award.

Journals:

J7. [**IEEE Computer Architecture Letters**] *"Simulating Our Way to Safer Software: A Tale of Integrating Microarchitecture Simulation and Leakage Estimation Modeling."*
Justin Feng, Fatemeh Arkannezhad, Christopher Ryu, Enoch Huang, Siddhant Gupta, and **Nader Sehatbakhsh**.
10.1109/LCA.2023.3303913 (2024).

J6. [**IEEE Journal of IoT**] *"Context-Aware Hybrid Encoding for Privacy-Preserving Computation in IoT Devices."*
Hossein Khalili, Hao-Jen Chien, Amin Hass, and **Nader Sehatbakhsh**.
DOI: 10.1109/JIOT.2023.3288523 (2023).

J5. [**IEEE Transactions on Computers**] *"REMOTE: Robust External Malware Detection Framework by Using Electromagnetic Signals."*
Nader Sehatbakhsh, Alireza Nazari, Monjur Alam, Frank Werner, Yuanda Zhu, Alenka Zajic, and Milos Prvulovic.
DOI: 10.1109/TC.2019.2945767 (2019).
Featured Paper in March 2020 issue.

J4. [**IEEE Transactions on Dependable and Secure Computing**] *"IDEA: Intrusion Detection through Electromagnetic-Signal Analysis for Critical Embedded and Cyber-Physical Systems."*
Haider Khan, **Nader Sehatbakhsh**, Luong N. Nguyen, Robert Callan, Arie Yeredor, Milos Prvulovic, and Alenka Zajic.
DOI: 10.1109/TDSC.2019.2932736 (2019).

J3. [**IEEE Transactions on Information Forensics and Security**] *"Communication Model and Capacity Limits of Covert Channels Created by Software Activities."*
Berkay Yilmaz, **Nader Sehatbakhsh**, Milos Prvulovic, and Alenka Zajic.
DOI: 10.1109/TIFS.2019.2952265 (2019).

J2. [**Journal of Hardware and Systems Security (HASS)**] *"Malware Detection in Embedded Systems using Neural Network Model for Electromagnetic Side-Channel Signals."*
Haider Khan, **Nader Sehatbakhsh**, Luong N. Nguyen, Milos Prvulovic, and Alenka Zajic.
DOI: 10.1007/s41635-019-00074-w (2019).

J1. [**IEEE Transactions on Antenna and Propagations**] *"A Directive Antenna Based on Conducting Disks for Detecting Unintentional EM Emissions at Large Distances."*
Prateek Juyal, Sinan Adibeli, **Nader Sehatbakhsh**, and Alenka Zajic.
DOI: 10.1109/TAP.2018.2870370 (2018).

FUNDING

(**Total Amount:** $2,560,508.)

- Sole-PI, ***NSF***, My Share: $599,856
  "CAREER:Integrating Microarchitecture Simulation and Side-Channel Leakage Modeling for Safer Software", 2024-2029.
- Co-PI, ***NSF***, My Share: $629,001
  "Collaborative Research: SaTC: CORE: Medium: Security and Robustness for Intermittent Computing Using Cross-Layer Post-CMOS Approaches", 2024-2027.
- Sole-PI, ***NSF***, My Share: $599,856
  "CSR: Small: Leveraging Physical Side-Channels for Good", 2024-2027.

- Co-PI, ***NSF***, My Share: $399,971
  "Collaborative Research: SaTC: CORE: Medium: Security and Robustness for Intermittent Computing Using Cross-Layer Post-CMOS Approaches", 2024-2027.
- PI, ***NSF***, My Share: $399,563
  "Collaborative Research: CNS Core: Medium: IoCT: System Mechanisms for Enabling an Internet of Collaborative Things", 2022-2025.
- Sole-PI, ***Cisco***, My Share: $150,000
  "Trustworthy and Private Deep Learning by Leveraging New Lightweight Diffusion Purification Methods", 2022-2023.
- Co-PI, ***IARPA***, My Share: $232,117
  "Smart AI-enabled Future-proof Engine for Guarding againstUnauthorized and Anomalous RF Radiation (SAFEGUARD)," 2020-2022.
- Sole-PI, ***Accenture***, My Share: $100,000
  "Privacy-Preserving ML through Adversarial Feature Learning (AFL)", 2022 (Gift).
- Sole-PI, ***Anthony Lai Foundation***, My Share: $50,000
  "Junior Faculty Fellow", 2021 (Gift).

TEACHING

(For the full list and materials please refer to my Teaching page.)

- *ECE-M116/CS-M151* Computer Architecture Systems,
  Undergrad (250+ Students), UCLA. Winter'21, Fall'22, Fall'23, Fa'24.
- *ECE-209AS* (*Permanent number:* **202C**) Secure and Trustworthy Edge Computing Systems (New Course)
  Graduate (70+ Students), UCLA. Spring'21, Winter'22, Spring'23, Winter'24.
- *ECE-188* Secure Computer Systems (New Course)
  Undergrad (40+ Students), UCLA. Spring'22, Winter'23
- *ECE-209AS* Secure and Advanced Computer Architecture (New Course)
  Graduate (50+ Students), UCLA. Spring'24.

STUDENTS

PhD:

- Justin Feng, 2021-
- Pooya Aghanouri, 2022-
- Fatemeh Arkannezhad, 2023-
- Hossein Khalili, 2024-
- Dao Dian Xiao, 2025-
- Fan Zhang, 2025-
- Reza Sajadiany, 2025-

MS:

- Vincent Li, 2023-2024
- Shashank Balla, 2020-2021

Undergraduate:

- Seongbin Kim, 2023-2025
- Steve Zang, 2023-2025
- Brandan Bright, 2024-
- Timothy Jacques, 2022-2024
- Enoch Huang, 2022-2024
- Siddhant Gupta, 2021-2024
- Dominic Konrad, 2022-2023
- Brandon Lou, 2021-2023
- Robert Chang, 2020-2021
- David Karalli, 2020-2021
- Sanjana Sarda, 2020-2021.

SERVICE

University Committee Service:

1- *PhD Thesis Committee*:

- Tamjid Al Rahat, ECE, 2024.
- Tianmu Li, ECE, 2023.
- Wenhao Yu, ECE, 2022.
- Chandrakanth Choppa, ECE, 2022.
- Chenkai Ling, ECE, 2022.
- Weikang Qiao, ECE, 2020.

2- *PhD Prelim Committee*:

- Youngseung Jeon (twice) ECE, 2024.
- George Krafakis, ECE, 2024.
- Kunlin Cai, ECE, 2024.
- Anwesha Chattoraj, ECE, 2024.
- Zicheng He, ECE, 2023.
- William Shand, ECE, 2023.
- Arkaprova Ray, ECE, 2022.
- Yuwen Jia, ECE, 2022.
- Kshitiz Tyagi , ECE, 2022.
- Alexander Graening, ECE, 2022.
- Zeyu Wang, ECE, 2022.
- Gaofeng Dong, ECE, 2021.

- Kenny Chen, ECE, 2021.
- Kia Karbasi, ECE, 2021.

3- *MS Thesis Committee*:

- JINGXUAN ZHU, ECE, 2023.
- Julian de Gortari, ECE, 2020.

4- *Other Service Committee*:

- ECE Department Website Review Ad-Hoc Committee, 2020-

Program Committee:

- *CCS*, 2024-
- *NDSS*, 2024-
- *SenSys*, 2023-2024.
- *IoTDI*, 2023-2024.
- *MICRO*, 2021-2023, 2024-
- *ISCA*, 2021-2023.
- *CASES*, 2021-
- *ICCAD*, 2022-
- *ICCPS*, 2021.
- *ICCD*, 2020-2023.
- *HASP*, 2020.
- *DAC*, 2020.

Journal Reviewer:

- *ACM Journal on Emerging Technologies in Computing Systems*
- *IEEE Transactions on Dependable and Secure Computing*
- *IEEE Transactions on Information Forensics and Security*
- *IEEE Transactions on Circuits and Systems I*
- *IEEE Transactions on Computers*

Organizing Committee:

- *Lightning Talk Chair, ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2024*

TALKS, PANELS, AND PRESENTATIONS

- Speaker, "Internet of Collaborative Things" *Dagstuhl Seminar Series*, Wadern, Germany, 7/24.
- Speaker, "Can Chiplet Integration Enhance Security?" *IEEE DAC Workshop - Chiplet-based Heterogeneous Integration and CO-design (CHICO)*, San Francisco, CA, 7/24.

- Speaker, "Can Chiplet Integration Enhance Security?" *IEEE Computer Society Distinguished Talk Series*, Portland, OR, 5/24.
- Panelist, *CHIPS R&D National Advanced Packaging Manufacturing Program (NAPMP) Advanced Packaging Summit*, San Jose, CA, 4/24.
- Speaker, "Leveraging Side-Channels for Good," *BAE Systems Invited Talk*, Boston, MA, 9/23.
- Speaker, "Privacy-Preserving Machine Learning for IoT Device," *Accenture Distinguished Research Speaker Series*, San Francisco, CA, 8/23.
- Speaker, "Chiplet Integration Security Considerations," *Intel Distinguished Speaker Series*, Portland, OR, 7/23.
- Tutorial, "Privacy-Preserving Machine Learning," *Crypto Summer School*, Croatia, 7/23.
- Speaker, "Designing Simulation Tools for Side-Channel Modeling," *Florida Atlantic University (FAU), ECE Department*, Miami, FL, 4/23.
- Speaker, "Protecting Privacy in Collaborative Edge-Cloud Systems," *University of California, Riverside, ECE Department*, Riverside, CA, 11/22.
- Speaker, "Adversarial Represnation Learning for IoT Devices," *Google Visiting Faculty Talks*, Venice, CA, 2/22.
- Speaker, "Hardware and Supply Chain Security in the Era of Advanced Heterogenous Integration," *Microelectronics Packaging and Test Engineering Council (MEPTEC) Supply-Chain Security Workshop*, Remote, 4/21.
- Speaker, "Leveraging Analog-Domain Side-Channel Signals for Security," Accenture Cyber-Fusion Center, Washington D.C., 7/19.
- Speaker, "Software Attestation for Embedded Systems Using Electromagnetic Signals," *DARPA review meeting*, Atlanta, GA, 8/18.
- Speaker, "Robust External Malware Detection Framework by Using Electromagnetic Signals," *DARPA review meeting.* Atlanta, GA, 8/17.