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 *July 2020 – Present*
Department of Electrical and Computer Engineering, Samueli School of Engineering.

EDUCATION

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

Georgia Institute of Technology *Atlanta, GA, USA*
M.S. in Electrical and Computer Engineering *Aug. 2014 – Dec. 2017*

University of Tehran *Tehran, Iran*
B.S. in Electrical Engineering *Sept. 2009 – Jun. 2014*

SELECTED HONORS AND AWARDS

- **DARPA MTO Pitch Day Award**, one of only eight academic awardees nationwide; awarded $400,000 in research funding, 2025.
- **NSF CAREER Award**, 2024.
- **Industry Research Awards**, competitive research funding, gifts, and cloud/API credits from *Amazon*, *Cisco*, *OpenAI*, *Accenture*, and *DENSO*, totaling approximately *$700,000*, 2022–2026.
- **Best Reviewer Award**, Network and Distributed System Security Symposium (NDSS), 2025.
- **Best Paper Nominee**, IEEE International Symposium on High-Performance Computer Architecture (HPCA), 2020.
- **IEEE Micro Top Picks Honorable Mention**, selected among the most influential computer architecture papers of the year, 2018.
- **Best Paper Award**, IEEE/ACM International Symposium on Microarchitecture (MICRO), 2016.

RESEARCH FUNDING

Total Funding: $3,319,791

Principal Investigator on **12 externally funded research projects**, including **8 sole-PI awards**, demonstrating a sustained record of independent research funding totaling more than **$3.3 million**. Research support has been secured from the National Science Foundation (NSF), Defense Advanced Research Projects Agency (DARPA), Intelligence Advanced Research Projects Activity (IARPA), Department of Energy (DOE), and industry partners including Cisco, Accenture, and DENSO.

- **Sole-PI**, *DENSO International America, Inc.* My Share: $130,000
  "DDI: Dynamic Data Integrity," 2026–2027.
- **Sole-PI**, *DARPA MTO* My Share: $400,000
  "High-Performance Ambient Resilient Processing for Intermittent Environments (HARPIE)," 2025–2026.

- **Sole-PI**, *NSF* My Share: $637,515
  "CAREER: Integrating Microarchitecture Simulation and Side-Channel Leakage Modeling for Safer Software," 2024–2029.
- **Sole-PI**, *NSF* My Share: $599,856
  "CSR: Small: Leveraging Physical Side-Channels for Good," 2024–2027.
- **Sole-PI**, *DENSO International America, Inc.* My Share: $100,000
  "Lightweight Attestation for Real-Time, Resource-Efficient Inter-Device Collaboration," 2025–2026.
- **Co-PI**, *DOE* My Share: $120,769
  "Secure Smart Manufacturing Solution for Small and Medium Manufacturers," 2024–2025.
- **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.
- **Co-PI**, *NSF* My Share: $399,563
  "Collaborative Research: CNS Core: Medium: IoCT: System Mechanisms for Enabling an Internet of Collaborative Things," 2022–2026.
- **Sole-PI**, *Cisco* My Share: $150,000
  "Trustworthy and Private Deep Learning by Leveraging Lightweight Diffusion Purification Methods," 2022–2023.
- **Co-PI**, *IARPA* My Share: $232,117
  "Smart AI-Enabled Future-Proof Engine for Guarding Against Unauthorized and Anomalous RF Radiation (SAFEGUARD)," 2020–2022.
- **Sole-PI**, *Accenture* My Share: $100,000
  "Privacy-Preserving Machine Learning through Adversarial Feature Learning (AFL)," 2022.
- **Sole-PI**, *UCLA Junior Faculty Fellow* My Share: $50,000
  "Secure Computation, Sensing, and Actuation for Enabling Trustworthy Space IaaS," 2021.

SELECTED PUBLICATIONS

My research lies at the intersection of embedded systems, computer architecture, and hardware security, with a primary focus on the security and privacy of emerging computing platforms. The work can be broadly categorized into two complementary thrusts: **(i) secure hardware and computer architectures**, including secure chiplet design and side-channel analysis; and **(ii) secure and efficient embedded systems**, with an emphasis on trustworthy computing and the security and privacy of tiny machine-learning-based connected devices. The publications below highlight representative contributions from each research thrust since joining UCLA. A complete publication list is available on my Google Scholar profile.

Thrust 1: Secure Hardware and Computer Architectures:

- **[DAC'26a]** *"WINNER: A Wireless In-Vivo/Ex-Vivo Runtime Analyzer for Intermittent Computing."*
  Justin Feng, Arman Roohi, and **Nader Sehatbakhsh**.
  Proceedings of the 63rd Annual ACM/IEEE Design Automation Conference, 2026.
- **[NDSS'26]** *"XR Devices Send WiFi Packets When They Should Not: Cross-Building Keylogging Attacks via Non-Cooperative Wireless Sensing."*
  Christopher Vattheuer, Justin Feng, Hossein Khalili, **Nader Sehatbakhsh**, and Omid Abari.
  Proceedings of the Network and Distributed System Security Symposium, 2026.
- **[DAC'26b]** *"Orbitbrain: Secure and Reliable Chiplet Architecture for Space Edge AI and Orbital Data Centers."*

Farshad Firouzi, Abhishek Moitra, Soheil Salehi, Matthew Marinella, **Nader Sehatbakhsh**, and Krishnendu Chakrabarty.
Proceedings of the 63rd Annual ACM/IEEE Design Automation Conference, 2026.

- **[ISQED'26]** *"Scalable Security Monitoring on Chiplet-Based Systems."*
Pouya Aghanoury, Sneha Swaroopa, Dao Xian Ding, Farshad Firouzi, and **Nader Sehatbakhsh**.
Proceedings of the 27th International Symposium on Quality Electronic Design, 2026.

- **[MWSCAS'26]** *"HERA: A Substrate-Level Covert Channel Detector for Heterogeneous Chiplet Systems."*
Sneha Swaroopa and **Nader Sehatbakhsh**.
Proceedings of the IEEE 68th International Midwest Symposium on Circuits and Systems, 2026.

- **[IEEE CAL]** *"Security helper chiplets: a new paradigm for secure hardware monitoring."*
Pouya Aghanoury, Santosh Ghosh, and **Nader Sehatbakhsh**.
IEEE Computer Architecture Letters, 2025.

- **[IEEE S&PW'24]** *"SideGuard: Non-Invasive On-Chip Malware Detection in Heterogeneous IoT Systems by Leveraging Side-Channels."*
Fatemeh Arkannezhad, Pouya Aghanoury, Justin Feng, Hossein Khalili, and **Nader Sehatbakhsh**.
Proceedings of IEEE Security and Privacy Workshops (SafeThings), 2024.

- **[IEEE CAL]** *"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**.
IEEE Computer Architecture Letters, 2024.

- **[DAC'23]** *"Hybrid obfuscation of chiplet-based systems."*
Yousef Safari, Pouya Aghanoury, Subramanian S Iyer, **Nader Sehatbakhsh**, and Boris Vaisband.
Proceedings of the 60th Annual ACM/IEEE Design Automation Conference, 2023.

- **[IMWUT'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, 2023.

- **[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**.
Proceedings of the 22nd International Conference on Information Processing in Sensor Networks, 2023.

Thrust 2: Secure and Efficient Embedded Systems:

- **[SenSys'26]** *"TIRA: Task-Based Intermittent Remote Attestation."*
Fatemeh Arkannezhad and **Nader Sehatbakhsh**.
Proceedings of the ACM/IEEE International Conference on Embedded Artificial Intelligence and Sensing Systems, 2026.

- **[AdaptFM@ICML '26]** *"Adaptive Safety Probing for Resource-Efficient Vision-Language-Action Models."*
Seongbin Park, Fan Zhang, Hossein Khalili, and **Nader Sehatbakhsh**.
ICML Workshop on Resource-Adaptive Foundation Model Inference (AdaptFM), 2026.

- **[IEEE TC]** *"BISen: A Robust Framework for Efficient CNN Inference on Battery-Free Intelligent Sensory Nodes."*
Sepehr Tabrizchi, Shayan Gerami, Justin Feng, **Nader Sehatbakhsh**, David Pan, and Arman Roohi.
IEEE Transactions on Computers, 2026.

- **[Usenix Security'25]** *"Chimera: Creating Digitally Signed Fake Photos by Fooling Image Recapture and Deepfake Detectors."*
Seongbin Park, Sasha Vilesov, Jinghui Zhang, Hossein Khalili, Yuan Tian, Achuta Kadambi, and **Nader Sehat-**

bakhsh.
Proceedings of the 34th USENIX Conference on Security Symposium, 2025.

- **[SPIE Defense'25]** *"Developing new solutions for data provenance and deepfake detection using physics, hardware, and machine learning."*
Nader Sehatbakhsh, Yuan Tian, and Achuta Kadambi.
SPIE Defense + Commercial Sensing: Synthetic Data for Artificial Intelligence and Machine Learning: Tools, Techniques, and Applications III., 2025.

- **[Philosophical Transactions]** *"Secure artificial intelligence at the edge."*
Nader Sehatbakhsh, Sudhakar Pamarti, Vwani Roychowdhary, and Subramanian Iyer.
Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2025.

- **[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**.
Proceedings of the 30th ACM Annual International Conference on Mobile Computing and Networking, 2024.

- **[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.
Proceedings of the 22nd ACM International Conference on Mobile Systems, Applications, and Services, 2024.

- **[NDSS'24]** *"IDA: Hybrid Attestation with Support for Interrupts and TOCTOU."*
Fatemeh Arkannezhad, Justin Feng, and **Nader Sehatbakhsh**.
Proceedings of the Network and Distributed System Security (NDSS) Symposium, 2024.

- **[MobiCom'23]** *"Enc^2:Privacy-Preserving Inference for Tiny IoTs via Encoding and Encryption."*
Hao-Jen Chien, Hossein Khalili, Amin Hass, and **Nader Sehatbakhsh**.
Proceedings of the 29th Annual International Conference on Mobile Computing and Networking, 2023.

- **[IEEE JIoT]** *"Context-Aware Hybrid Encoding for Privacy-Preserving Computation in IoT Devices."* Hossein Khalili, Hao-Jen Chien, Amin Hass, and **Nader Sehatbakhsh**.
IEEE Internet of Things Journal, 2023.

PATENTS

- Nader Sehatbakhsh, "Systems and Methods for Deterministic Real-time Attestation in Safety-critical Robotic Systems," U.S. Patent 64/077,638, June 2026.

TEACHING

My teaching spans both undergraduate and graduate programs in computer architecture, embedded systems, and cybersecurity. I have developed or co-developed **three courses** at UCLA, including **two graduate-level courses** and **one undergraduate course**; two of these courses have since received permanent course numbers and become part of the regular curriculum. Teaching evaluations have been consistently **well above the departmental average**, with average instructor ratings ranging from **7.64/9 to 8.68/9** across undergraduate and graduate offerings. Additional course materials and teaching information are available on my Teaching Page.

- *ECE-M116/CS-M151* Computer Architecture Systems
Undergraduate (300+ students). Average teaching evaluation: **8.49/9**. Winter'21, Fall'21, Fall'22, Fall'23, Fall'24, Fall'25

- *ECE-202C* IoT Security (COURSE DEVELOPED)
Graduate (50+ students). Average teaching evaluation: **8.68/9**. Spring'21, Winter'22, Spring'23, Winter'24, Winter'25, Spring'26

- *ECE-M117* Secure Computer Systems (COURSE DEVELOPED)
  Undergraduate (40+ students). Average teaching evaluation: **8.46/9**. Spring'22, Winter'23
- *ECE-209AS* Secure and Advanced Computer Architecture (COURSE DEVELOPED)
  Graduate (50+ students). Average teaching evaluation: **8.40/9**. Spring'24, Spring'25
- *ECE-115C* Digital Electronic Circuits
  Undergraduate (100+ students). Average teaching evaluation: **7.64/9**. Winter'25

SERVICE

I maintain an active record of professional service to the computer architecture, cybersecurity, and embedded systems communities, including leadership roles at flagship conferences, recurring service on premier program committees, participation on NSF review panels, and invited talks and panels at major academic, government, and industry venues.

Conference Leadership

- **Track Program Co-Chair**, IEEE/ACM ICCAD 2026.
- **Associate Program Chair**, NDSS 2025.
- **General Co-Chair**, IEEE SafeThings 2025.
- **Poster Co-Chair**, ACM SenSys 2025.
- **Lightning Talks Chair**, ASPLOS 2024.

Program Committee and Editorial Service

- **Program Committee Member**: **IEEE Security & Privacy/Oakland** (2025–2026), **NDSS** (2024–2026), **HPCA** (2025–2027), **ISCA** (2021–2022, 2025–2026), **MICRO** (2022, 2024–2026), **ICCAD** (2023–2026), **CCS** (2024), and **SenSys** (2023, 2025).
- **Journal Reviewer**: **TIFS** (2022–2026), **TDSC** (2022–2024), **TVLSI** (2024–2026), **TCAD** (2024–2026), **IoTJ** (2023–2025), **TC** (2024–2025), **TMC** (2025), and **TCPMT** (2025).

Federal Agency Service

- **NSF Review Panels**: Invited panelist for the NSF Secure and Trustworthy Cyberspace (**SaTC**) program (twice) and the NSF Computer Systems Research (**CSR**) program (twice), 2023–2026.

Invited Talks, Tutorials, and Panels at Conferences or Symposia

Delivered 15+ invited talks, tutorials, and panel presentations at leading academic, government, and industrial venues, including Dagstuhl, IEEE Computer Society, AMD, Nokia Bell Labs, Google, NIST, and BAE Systems.

- **MPSoC Forum**, "Toward Dynamic Attestation and Root of Trust of SoCs," 2026.
- **Special Sessions at IEEE ISQED and MWSCAS**, "Chiplet and IoT Security," 2026.
- **DARPA MTO Spark Tank**, "HARPIE – High Performance, Battery-Free Computing," 2025.
- **Panel at SAE World Congress Experience (WCX)**, "Surveillance Under the Hood: Privacy Risks in Connected Cars," 2025.
- **DARPA Workshop on Low-Resource Computing**, "Weird is the New Efficient: Side-Channels for Good in IoT & CPS," 2025.
- **Nokia Bell Labs Invited Faculty Talks**, "The Long Island Iced Tea: Toward Optimizing the Privacy-Latency Tradeoff for Private Machine Learning at Edge," 2025.

- **IEEE VTS Special Session**, "Leveraging LLMs for Physical Side-Channel Modeling and Analysis," 2025.
- **Dagstuhl Seminar on Security and Privacy of Current and Emerging IoT Devices and Systems**, "Security and Privacy Challenges for IoT Collaborations," 2024.
- **IEEE Computer Society Distinguished Talk Series**, "Securing Heterogeneous Chiplet Systems: Navigating Design Challenges and Opportunities," 2024.
- **Panel at NIST/NAPMP Advanced Packaging Summit**, "Emerging Challenges to Advanced Packaging," 2024.
- **AMD Distinguished Talk Series**, "Expanding Trust: Modernizing TEEs for Complex, Multi-Tenant, Heterogeneous Computing Systems," 2024.
- **Panel at Workshop on Chiplet-based Heterogeneous Integration and CO-design (CHICO) - co-located with DAC**, "Can Chiplet-Based Heterogeneous Integration Enhance Security?" 2024.
- **Tutorial at Summer School on Real-World Crypto and Privacy,** "Lightweight Privacy-Preserving Machine Learning Techniques for IoT Devices," 2023.
- **BAE Systems Invited Talk Series,** "Side-Channel for Good," 2023.
- **Google Visiting Faculty Talk,** "Privacy-Preserving Computing for Tiny IoTs," 2022.
- **Panel at Microelectronics Packaging and Test Engineering Council (MEPTEC)**, "Supply Chain Security," 2021.

University and Student Service

- **Faculty Advisor, UCLA IEEE Student Branch** (2022–Present). Faculty advisor for UCLA's largest engineering student organization, supporting more than **100 undergraduate and graduate student members**. Provide mentorship and strategic guidance for technical, professional development, and outreach activities. Under my advisement, UCLA IEEE received national recognition through the **IEEE Best Advanced Group Project Award** and **IEEE Best Beginner Group Project Award** in 2025.
- **Co-Organizer of the Los Angeles Computing Circle** (2022–2023). LACC is an outreach program focused on advanced computing education and research opportunities for Los Angeles area high school students (more than 40 students enrolled).

STUDENT MENTORSHIP AND TRAINING

Currently advising **eight Ph.D. students** and **one postdoctoral scholar**. Since joining UCLA, I have also mentored more than **20 undergraduate researchers**, many of whom have contributed to publications, research projects, and graduate study opportunities. Additional information about current and former group members is available here. My students have received multiple competitive fellowships, dissertation awards, and national recognitions as listed below.

- **UC LEADS Fellowship**, awarded to Edward Almaraz, 2026.
- **Amazon AI Ph.D. Fellowship**, awarded to Hossein Khalili, 2025.
- **Eugene Cota-Robles Fellowship**, awarded to Seongbin Park, 2025.
- **UCLA Graduate Division Student Award (GDSA)**, awarded to Sneha Swaroopa, 2025.
- **DAC Young Fellow**, awarded to four members of my research group (Fatemeh, Sneha, Dao Xian, and Edward), 2025–2026.
- **ECE Department Dissertation Year Award (DYA)**, awarded to Justin Feng, 2024.