Nojan Sheybani

San Diego, CA · nojansheybani@gmail.com · (804) 919-4282 · nojansheybani.github.io
US Citizen

Education

University of California San Diego — San Diego, CA
Thesis: Assuring Privacy, Integrity, and Provenance in Real-World Computing Systems
PhD in Electrical and Computer Engineering — May 2025

University of Virginia — Charlottesville, VA
BS in Computer Engineering With Highest Distinction. Cumulative GPA: 3.93 Major GPA: 3.93 — May 2020

Research Interests

Privacy-Preserving Computation, Robust and Trustworthy Machine Learning, Zero Knowledge Proofs, Hardware Security, Computer Architecture, HW/SW Co-design, and IoT applications

Work Experience

Nexus Labs — San Francisco, CA
Member of Technical Staff — July 2025 — Feb 2026

- Led research and development efforts for enshrining Nexus zkVM into Nexus Mainnet and building new applications for enabling verifiable finance at scale
- Designed, developed, and maintained chain infrastructure for Nexus Mainnet, a high-performance L1 blockchain with enshrined verifiable decentralized exchange

University of California San Diego — San Diego, CA
Graduate Research Assistant Advised by Prof. Farinaz Koushanfar — June 2020 — May 2025

- Leveraging hardware and software co-design to develop intelligent, data-intensive and secure embedded computing applications and systems
- Applied efficient zero-knowledge proof (ZKP) protocols in several learning paradigms and generic applications, showing their use cases in distributed systems
- Characterized prominent open-source ZKP libraries and developed open-source environments and benchmarks for each to simplify ZKP framework selection and development
- Developed open-source universal ZK-friendly hashing toolbox on FPGA, including several prominent hashes

Visa Research — Palo Alto, CA
Identity and Authentication Research Intern — May 2023 — August 2023

- Utilized secure multi-party computation to develop private and secure end-to-end scalable biometric identification workflows for powering payments through Visa

Intel Labs — San Diego, CA & Hillsboro, OR
DARPA DPRIVE Security and Privacy Graduate Research Intern — June 2022 — September 2022

- Studied feasibility & practicality of DARPA DPRIVE accelerator to support Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) for Fully Homomorphic Encryption integrity

Security and Arithmetic Circuits Research Intern — June 2021 — September 2021

- Invented 2 novel techniques for efficient hardware implementation of FHE operations for the DARPA DPRIVE accelerator, resulting in co-inventor status on respective invention disclosures
- Developed complex model to simulate core operation for FHE bootstrapping, which shows latency, memory access patterns, and other crucial attributes pertaining to hardware performance

Cisco — San Diego, CA
Security Engineering Intern — August 2020 — September 2020

- Developed the backend of the Cloud Trust Anchor Service, a cloud neutral, self-managed trust anchor service

University of Virginia — Charlottesville, VA
Undergraduate Research Assistant Advised by Prof. Benton Calhoun — September 2016 — May 2020

- Conducted research on low-power digital circuits and low energy electronics for research/medical applications, with a focus on piezoelectric rectifiers

- Characterized tradeoffs between dynamic-leakage suppression transistor configuration and static-CMOS for self-powered systems

Appian McLean, VA
Software Engineering Intern June 2019 — August 2019

- Worked on the Kubernetes Operator written in Go, which deploys the Appian platform in Kubernetes and manages it automatically, and pushed code to internal production daily

AT&T (DIRECTV) El Segundo, CA
Software Engineering Intern May 2018 — August 2018

- Automated generation and upload of channel stream configuration files for ads using Ansible and Yospace API

Trivium Financial Group Charlottesville, VA
Software Engineering Intern July 2017 — August 2017

- Assisted in development of major risk-mitigating financial modeling platform, which condensed the amount of time taken to generate a complex financial model from a few weeks to a few hours

Technical Skills

ECE: VHDL/Verilog, Cadence, Vivado HLS, NI Multisim, NI Ultiboard, LabVIEW, Virtual Bench, Logisim
Courses: VLSI, Embedded Systems, Embedded Testing and Validation, Electronics, Computer Architecture, Computer Networks, Self-Powered IoT Systems, Signal Processing, Probability and Random Processes

CS: Rust, Kubernetes, Docker, PyTorch, Tensorflow, Python, C/C++, Go, React/React Native
Courses: Learning Algorithms, Neural Networks, Operating Systems, Data Structures, Algorithms, Data Science, Software Development

Conference and Workshop Proceedings

PAC to the Future: Zero-Knowledge Proofs of PAC Private Systems *April 2026*
G. Repetto, **N. Sheybani**, G. De Micheli, F. Koushanfar
ACM WWW 2026 Workshop on Zero-knowledge Proof and Blockchain for Web 4.0 link

ZORRO: Zero-Knowledge Attested Client-Side Backdoor Defense in Split Learning *October 2025*
N. Sheybani*, A. Pegoraro*, J. Knauer*, E. Mollakuqe, P. Rieger, F. Koushanfar, A. Sadeghi
**Equal contribution*
CCS 2025 link

Optimizing Privacy-Preserving Primitives to Support LLM-Scale Applications *October 2025*
Y. Jandali, R. Zhang, **N. Sheybani**, F. Koushanfar
**Equal contribution*
ICCAD 2025 link

Gotta Hash 'Em All! Speeding Up Hash Functions for Zero-Knowledge Proof Applications *October 2025*
N. Sheybani*, T. Gong, A. Ahmed, N. Njungle, M. Kinsy, F. Koushanfar
**Equal contribution*
ICCAD 2025 link

AMAZE: Accelerated MiMC Architecture for Accelerating Zero-Knowledge Applications on the Edge *July 2024*
A. Ahmed*, **N. Sheybani***, D. Moreno, N. Njungle, T. Gong, M. Kinsy, F. Koushanfar
**Equal contribution*
Top Picks in Hardware and Embedded Security 2025
ICCAD 2024 link

You Can Have Your Cake and Eat It Too: Ensuring Practical Robustness and Privacy in Federated Learning *March 2024*
N. Sheybani, F. Koushanfar
AAAI Spring Symposium Series link

zPROBE: Zero Peek Robustness Checks for Federated Learning *July 2023*
Z. Ghodsi*, M. Javaheripi*, **N. Sheybani***, X. Zhang*, K. Huang, F. Koushanfar
**Equal contribution*
ICCV 2023 link

NetFlick: Adversarial Flickering Attacks on Deep Learning Based Video Compression *March 2023*
J. Chang, **N. Sheybani**, S. Hussain, M. Javeheripi, S. Hidano, F. Koushanfar
ICLR ML4IoT Workshop 2023 link

ZKROWNN: Zero Knowledge Right of Ownership for Neural Networks *February 2023*
N. Sheybani, Z. Ghodsi, R. Kapila, F. Koushanfar
DAC 2023 link

zPROBE: Zero Peek Robustness Checks for Federated Learning *December 2022*
Z. Ghodsi*, M. Javaheripi*, **N. Sheybani***, X. Zhang*, K. Huang, F. Koushanfar
**Equal contribution*
Outstanding Paper Award
NeurIPS Trustworthy and Socially Responsible Machine Learning Workshop 2022 link

FastStamp: Accelerating Neural Steganography and Digital Watermarking of Images on FPGAs *October 2022*
S. Hussain*, **N. Sheybani***, P. Neekhara*, X. Zhang, J. Duarte, F. Koushanfar
**Equal contribution*
ICCAD 2022 link

Is Revolutionary Hardware for Fully Homomorphic Encryption important? What else is needed? *October 2021*
C. Bonte, R. Cammarota, W. Dai, J. Fryman, H. Gong, D. Kim, R. Kumar, K. Laine, P. Lalwaney, **N. Sheybani**, A. Rajan, A. Reinders , M. Steiner, V. Suresh, S. Taneja, M. Trifan, A. Viand, W. Wang, W. Wang, C. Wilkerson, J. Yang
COSADE 2021 link

A Self-Powered and LoRa-Based Fleet Tracker: Demonstrating Improved Reliability in the IoT *March 2020*
V. Lin, J. Dugan, **N. Sheybani**, N. Krzysztofowicz, M. Miller, H. Powell
IEEE Southeastcon 2020 [link]

Journal Publications

Robust and Secure Code Watermarking for Large Language Models via ML/Crypto Codesign *January 2026*
R. Zhang*, N. Javidnia*, **N. Sheybani**, F. Koushanfar
**Equal contribution*
In review for TAISAP 2026 ***Preprint***

Zero-Knowledge Proof Frameworks: A Systematic Survey *January 2025*
N. Sheybani, A. Ahmed, M. Kinsy, F. Koushanfar
In submission ***Preprint***

Tailor: Altering Skip Connections for Resource-Efficient Inference *July 2023*
O. Weng, G. Marcano, V. Loncar, A. Khodamoradi, **N. Sheybani**, F. Koushanfar, K. Denolf, J. Duarte, R. Kastner
IEEE Transactions on Reconfigurable Technology and Systems link

SenseHash: Computing on Sensor Values Mystified at the Origin *November 2022*
N. Sheybani, X. Zhang, S. U. Hussain, F. Koushanfar
IEEE Transactions of Emerging Topics in Computing Special Section on Hardware Security Journal link

Posters and Presentations

Ensuring Integrity in Real-World Distributed Systems *April 2026*
N. Sheybani
Invited Keynote at ACM Web Conference 2026 Workshop on Zero-knowledge Proof and Blockchain for Web 4.0

Securing AI with Zero-Knowledge Proofs *June, August 2024*
N. Sheybani
Invited Talk at: Microsoft Research Cryptography and Privacy Colloquium, TU Darmstadt

Integrating Zero Knowledge Proofs into Real World Applications *November 2023*
N. Sheybani
ICCAD Zero Trust Hardware Architectures Workshop 2023 link

Tailor: Altering Skip Connections for Resource-Efficient Inference *November 2022*
O. Weng, G. Marcano, V. Loncar, A. Khodamoradi, **N. Sheybani**, F. Koushanfar, K. Denolf, J. Duarte, R. Kastner
Poster for FPGA 2023

Evaluating Hardware Acceleration of Ring-Based Zero Knowledge Proof Generation *September 2022*
N. Sheybani
Intel XCC Technical Showcase

AccHASHTAG: Accelerated Hashing for Detecting Fault-Injection Attacks on Embedded Neural Networks *June 2022*
N. Sheybani, M. Javaheripi, J. Chang, F. Koushanfar
Hardware Demo for HOST 2022

HAtNet: Hardware Attestation of Neural Networks *June 2022*
N. Sheybani, H. Chen, X. Zhang, S. Hussain, F. Koushanfar
Hardware Demo for HOST 2022

The Role of Affective Skills in the Engineering Classroom *March 2020*
N. Sheybani, M. Miller, H. Powell, J. Dugan
Poster for American Society for Engineering Education Southeastern Section Conference 2020 (Accepted but could not attend due to COVID)

Qualitative Skill Development in Engineering Education *May 2019*
Presentation for 2019 Innovations in Pedagogy Summit
N. Sheybani, M. Miller

Patents and Invention Disclosures

Zero Knowledge Proof of Deep Neural Network Ownership *May 2024*
Patent Application Number 63/499,650
N. Sheybani, Z. Ghodsi, R. Kapila, F. Koushanfar

Zero Peek Robustness Checks for Federated Learning *April 2024*
Patent Application Number 63/496,157
Z. Ghodsi, M. Javaheripi, **N. Sheybani**, X. Zhang, K. Huang, F. Koushanfar

Fully Homomorphic Encryption *July 2023*
Patent Application Number 18/217,553
S. K. Mathew, V. B. Suresh, S. Taneja, R. Kumar, R. Cammarota, C. Wilkerson, **N. Sheybani**

Techniques for Twiddle Factor Generation for Number-Theoretic Transform And Inverse-Number-Theoretic-Transform Computations *July 2023*
Patent Application Number 18/217,565
S. Taneja, S. K. Mathew, R. Kumar, **N. Sheybani**, V. B. Suresh

Professional Services

Secure AI for Health, Defense, and Beyond Workshop *Co-Organizer*
IEEE Transactions on Information Forensics & Security *Reviewer*
AAAI Safe, Robust and Responsible Artificial Intelligence Track *Reviewer*
IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems *Reviewer*
USENIX Security *Poster Reviewer*
IEEE Security & Privacy *Poster Reviewer*
The Journal of Supercomputing *Reviewer*
IEEE Transactions on Dependable and Secure Computing *Reviewer*

Teaching Experience

Optimization and Acceleration of Deep Learning on Various Hardware Platforms (ECE 226), UCSD *TA to Prof. Farinaz Koushanfar* Winter 2025
Advanced Digital Design Project (ECE 111), UCSD *TA to Prof. Farinaz Koushanfar* Fall 2021
Computer Architecture (ECE 4435/6435), UVA *TA to Prof. Ronald Williams* Spring 2020
Digital Logic Design (ECE 2330), UVA *TA to Prof. Joanne Dugan* Spring 2020
Nao Robots (ECE 1501), UVA *Instructor* Spring 2019
Electronics (ECE 2660), UVA *TA to Prof. Ronald Williams* Fall 2018

Electronics (ECE 2660), UVA *TA to Prof. Scott Barker* Spring 2018
Introduction to Engineering (ENGR 1620), UVA *TA to Prof. Keith Williams* Fall 2017

Honors and Awards

Top Picks in Hardware and Embedded Security *UCSD* 2025
Qualcomm Innovation Fellowship Finalist *UCSD* 2024
NeurIPS TSRML Outstanding Paper Award *UCSD* 2022
Intel XCC Technical Showcase Invited Speaker *Intel* 2022
UCSD Nominee for Microsoft Research PhD Fellowship *UCSD* 2022
DAC Young Fellow *UCSD* 2021
Halicioğlu Data Science Institute Graduate Prize Fellowship *UCSD* 2020
Electrical and Computer Engineering Department Fellowship *UCSD* 2020
Graduation with Highest Distinction *UVA* 2020
Best Senior Capstone *Awarded to team with best project as decided by UVA ECE faculty* 2020
Raven Society *UVA* 2020
Dean's List *UVA* 2016-2020