SALEH DARZI

Post-Quantum and Applied Cryptography Researcher

salehdarzi@usf.edu | 8135779609 | Tampa, Florida, USA | www.salehdarzi.com | scholar.google.com/salehdarzi
www.linkedin.com/in/salehdarzi | https://github.com/TheSalehDarzi | 0000-0002-3465-1173
Visa Status: F-1, I-485 Pending

EXPERTISE & RESEARCH INTERESTS:

- **Applied Cryptography Researcher**
- **Post-Quantum Cryptography Specialist**
- **Network Security Engineer**
- **Privacy-Preserving Machine Learning**
- **Designing Security Frameworks** for Wireless Networks, Artificial Intelligence (AI), Internet-of-Things (IoT), and Blockchain

EDUCATION

Ph.D. in Computer Science and Engineering
University of South Florida, Tampa, Florida — Dec 2021 – Jan 2027

Thesis title: Post-Quantum Secure Authentication and Privacy-Preserving Frameworks for Next-Generation Wireless Networks

M.Sc. Electrical Engineering (Communication-System)
K. N. Toosi University of Technology, Tehran, Iran — Sept 2017 – Dec. 2020

Thesis title: Improving Privacy-Preserving Techniques for Smart Grid using Lattice-based Cryptography

B.Sc. Electrical Engineering (Electronic)
Islamic Azad University of Central Tehran Branch, Tehran, Iran — Sept. 2013 – Jan. 2017

Thesis title: Cognitive Radio: Analysis of spectrum sensing in Cognitive Radio Networks)

SKILLS

Languages & DevOps: C | C++ | Python | Java | Scripting | Bash | Git | MATLAB | x86 Asembly | Ansible | Rust | Go | Latex | HTML | MySQL | Docker | Prometheus

Libraries & Tools: OpenSSL | Lib-OQS | HElib | NTL (Number Theory Library) | GMP | LibTomCrypt | Libsodium (NaCl) | Crypto++ | libpqcrypto | SageMath | Microsoft SEAL | PALISADE | OpenFHE | ZK-SNARK | PBC | WolfSSL | MIRACL | ecc-cpp | Libschnorr | pqm4

EXPERIENCE

Graduate Research Associate
University of South Florida — May 2024 – Ongoing

- ***Funded By:*** NSF–SNSF, Cisco Systems
- Serving as lead researcher, author, and security framework designer on NSF-funded projects, including the international **SATUQ** collaboration with **ZHAW** and the 5G authentication project with **Purdue University**, **UT Dallas**, and **Muma College of Business**. Designed and evaluated **post-quantum secure, scalable, and resilient cybersecurity frameworks** for hybrid satellite–terrestrial and next-generation wireless networks.
- Conducted extensive research and development across a broad spectrum of **cryptographic primitives**, including **post-quantum digital signatures**, **identity-based and group signatures**, **ring signatures**, **anonymous credentials**, **private information retrieval**, **post-quantum Tor**, **proof-of-work and time-lock puzzles**, **key encapsulation mechanisms**, and **distance-bounding protocols**, utilizing multiple cryptographic libraries for secure design, implementation, and benchmarking.

System Administrator and Technical Support
USF Bellini College of Artificial Intelligence, Cybersecurity and Computing — April 2024 – Jan 2025

- Implemented enterprise security and compliance measures by deploying **Rapid7 agents** across multi-platform systems (Windows, Red Hat, Ubuntu, macOS) and automating **CIS Level 1 & 2 validation** through **Ansible playbooks**.

- Administered the **GAIVI computing cluster**, resolving capacity and node failures, developing diagnostic automation scripts, and performing on-site data-center maintenance and server deployments.
- Created a **centralized audit and configuration repository** to log, document, and remotely monitor all departmental servers and workstations.
- Designed and maintained a **Grafana-based monitoring dashboard** for real-time visualization of network and system performance across the department.
- Automated routine IT operations by developing **Ansible scripts** for remote configuration, updates, and digital signage control, reducing manual workload and downtime.
- Installed and maintained hardware components (**GPUs, memory, printers**) across labs and data centers, ensuring optimal performance and reliability.
- Configured **network protocols, user environments, and software setups** for faculty and research staff, ensuring secure, stable, and consistent access across heterogeneous systems.

Graduate Research Assistant
University of South Florida
December 2021 – May 2024

- Lead researcher and security framework designer on multiple NSF- and industry-funded projects, including the **SaTC** initiative on secure distributed computing for 5G/6G networks, the **CAREER** project on post-quantum lightweight authentication for IoT, and the **Cisco Research Award** project on privacy-preserving and resilient cybersecurity frameworks for next-generation networks.
- Conducted research, design, and implementation of diverse **advanced cryptographic constructions**, including **post-quantum digital signatures**, **fully homomorphic encryption**, **multi-party computation**, **zero-knowledge proofs**, **anonymous credentials**, **private information retrieval**, **Counter-DoS mechanisms**, **privacy-preserving machine learning**, and **key encapsulation schemes**, employing multiple cryptographic libraries for development and performance evaluation.

Graduate Research Assistant
K. N. Toosi University of Technology
Jan 2019 – Dec 2021

- Served as a **research investigator** in the **National Smart Metering Program (Iran)**, focusing on privacy-preserving techniques for smart grids using lattice-based cryptography.
- Authored 2 papers and led the design and implementation of **fully homomorphic encryption (FHE)** and **post-quantum digital signature schemes**, focusing on security, privacy, and performance optimization of smart grid networks.

Instructor & Graduate Teachning Assistant
University of South Florida & K. N. Toosi University of Technology
January 2019 – May 2024

- **Courses:** CIS 4930/6930 Cryptography: Theory and Practice | CIS4200: Penetration Testing for IT | CIS 4212/6214: Privacy-Preserving and Trustworthy Cyber-Infrastructures | Lattice-Based Cryptography | Information Theory | Network Security
- Served as **instructor and lecturer** for advanced cryptography and cybersecurity courses, covering **PQC, lattice-based cryptography, and ECC**.
- Designed and delivered **hands-on cryptographic exercises, coding projects, and practical labs** in C/C++ and Python using libraries such as **OpenSSL, LibTomCrypt, LibOQS, NTL, GMP**, and others.

Internship
Noor Tab Tavan Technical and Engineering Company (Iran)
June 2017 – December 2017

- Served as an **Electronic Engineer and Project Supervisor** for an **electrical grid modernization project**, overseeing system design, implementation, and performance testing.

SELECTED PUBLICATIONS

Patents

- Saleh Darzi, Attila A. Yavuz, "System and Method for Secure Location-Proof and Anonymous Privacy-Preserving Spectrum Access", TTO ref. 24T238PR-CS, Submitted: 06/16/2025: Provisional-Filed.
- Attila Altay Yavuz, Saleh Darzi, "Resilient Authentication for Next-Generation Wireless Networks with Lawful Interception and Quantum-Safe Forgery Detection," TTO ref. 25T059PR-CS, Submitted: 11/22/2024: Provisional-Filed.

- Attila Altay Yavuz, Saleh Darzi, "A System and Method for Privacy-preserving and Post-quantum Secure Counter Denial of Service for Spectrum Management in Next-Generation Wireless Network," TTO ref. 24T238PR-CS, Submitted: 06/21/2024: Provisional-Filed.

Conferences

- Saleh Darzi, Attila A. Yavuz, "Privacy-preserving and post-quantum counter denial of service framework for wireless networks," in MILCOM 2024-2024 IEEE Military Communications Conference (MILCOM), pp. 1076–1081, 2024.
- Saleh Darzi, Attila A. Yavuz, "SLAP: Secure Location-proof and Anonymous Privacy-preserving Spectrum Access," in the IEEE SVCC 2025: Silicon Valley Cybersecurity Conference (SVCC 2025), 2025.
- Saleh Darzi, Attila A. Yavuz, "Counter denial of service for next-generation networks within the artificial intelligence and post-quantum era," in the 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA), pp. 138–147, 2024.
- Attila A. Yavuz, Kiarash Sedghighadikolaei, Saleh Darzi, Saif E. Nouma, "Beyond basic trust: Envisioning the future of nextgen networked systems and digital signatures," in the 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), pp. 267–276, 2023.

Journals

- Attila A. Yavuz, Saleh Darzi, Saif E. Nouma, "LiteQSign: Lightweight and Quantum-Safe Signatures for Heterogeneous IoT Applications," IEEE Access, 2025.
- Saleh Darzi, Bahareh Akhbari, Hassan Khodaiemehr, "LPM2DA: a lattice-based privacy-preserving multi-functional and multi-dimensional data aggregation scheme for smart grid", in Springer Cluster Computing journal, vol. 25, no. 1, pp. 263–278, 2022.

E-Prints

- Saleh Darzi, Mirza Rahman, Karim Imtiaz, Rouzbeh Behnia, Attila A. Yavuz, Elisa Bertino, "Authentication Against Insecure Bootstrapping for 5G Networks: Feasibility, Resiliency, and Transitional Solutions in Post-Quantum Era," in arXiv preprint arXiv:2510.23457, 2025 under review at IEEE Transactions on Dependable and Secure Computing.
- Saleh Darzi, Saif E. Nouma, Kiarash Sedghighadikolaei, Attila A. Yavuz, "QPADL: Post-Quantum Private Spectrum Access with Verified Location and DoS Resilience," in arXiv preprint arXiv:2510.03631, 2025, under review at IEEE Transactions on Information Forensics and Security (TIFS).
- Saleh Darzi, Attila A. Yavuz, Rouzbeh Behnia, "Post-Quantum Security for Trustworthy Artificial Intelligence: An Emerging Frontier," in Authorea Preprints, 2024.
- Saleh Darzi, Kasra Ahmadi, Saeed Aghapour, Attila Altay Yavuz, Mehran Mozaffari Kermani, "Envisioning the future of cyber security in post-quantum era: A survey on pq standardization, applications, challenges and opportunities," in arXiv preprint arXiv:2310.12037, 2023.

SERVICES & ENGAGEMENT

Program Committee (PC) & Chair:

- Publication Chair of ACM CCS Workshop on Quantum-Resistant Cryptography and Security (QRSEC 2025), Taiwan.
- Program Committee of the IEEE Silicon Valley Cybersecurity Conference (SVCC 2025, SVCC 2026)

Reviewer:

- Reviewer of ACM Conference on Computer and Communications Security (ACM CCS-2025)
- Reviewer of USENIX Security conference (2025, 2026)
- Reviewer of IEEE Transactions on Dependable and Secure Computing Journal (TDSC)
- Reviewer of IEEE Transactions on Information Forensics and Security Journal (TIFS)
- Reviewer of ACM Computing Surveys Journal
- Reviewer of IEEE Transactions on Smart Grid Journal
- Reviewer of Annual Computer Security Applications Conference (ACSAC)
- Reviewer of IEEE IoT Journal
- Reviewer of Journal of Information Security and Applications
- Reviewer of Cluster Computing Journal
- Reviewer of Concurrency and Computation: Practice and Experience

Invited Talks & Conference Presentations:

- Presented research papers at major venues, including "IEEE MILCOM 2024", "Silicon Valley Cybersecurity Conference (SVCC 2025)", "IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS 2025)", and other international cryptography and network security conferences.
- Delivered a public research talk on my patents concerning post-quantum security for spectrum access systems at the Innovation Match: Become the Founder of a USF Spinout, organized by the University of South Florida Technology Transfer Office.
- Presentation of "Trustworthy AI Systems Through Lenses of Post-Quantum Security and Privacy-Enhancing Techniques" at the cyberbay 2025, Tampa, Florida.

Awards & Grants:

- Recipient of multiple travel grants and research support awards for international conferences and NSF-funded projects including NSF travel grant for MILCOM, NSF travel grant for IEEE TPS, and USF's travel grant.

Open-Source Contributions:

- Developer and maintainer of several **open-source cryptography projects** hosted on GitHub, including implementations of post-quantum authentication for 5G (**BORG**), post-quantum spectrum access (**QPADL**), and other related repositories.

Professional Memberships:

- Member, **Institute of Electrical and Electronics Engineers (IEEE)**, **IEEE Communications Society Membership**, **IEEE Young Professionals**, **Association for Computing Machinery (ACM)**, **Iranian Society of Cryptology**.

REFERENCES

Prof. Attila A. Yavuz
University of South Florida, Tampa, FL, 33620
@ attilaayavuz@usf.edu
+1 (813) 974 0419

Prof. Xinming (Simon) Ou
University of South Florida, Tampa, FL, 33620
@ xou@usf.edu
+1 (813) 974-4522

Prof. Yao Liu
University of South Florida, Tampa, FL, 33620
@ xou@usf.edu
+1 (813) 974-4522

Prof. Reza Azarderakhsh
Florida Atlantic University, Boca Raton, FL, 33431
@ razarderakhsh@fau.edu
+1 (561) 297-4980

Prof. Kwang-cheng Chen
University of South Florida, Tampa, FL, 33620
@ kwangcheng@usf.edu
+1 (813) 974-1023

Prof. Rouzbeh Behnia
University of South Florida, Tampa, FL, 33620
@ behnia@usf.edu
+1 (941) 359-4605