

SALEH DARZI

Applied and Post-Quantum Cryptography Researcher

@salehdarzi@usf.edu
saleh-darzi-4212b591

8135779609
TheSalehDarzi

Tampa, Florida, USA
0000-0002-3465-1173

www.salehdarzi.com
Visa Status: F-1, I-485 Pending

scholar.google.com/salehdarzi

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 – May 2027 (expected)

Thesis title: Post-Quantum Secure Authentication and Privacy-Preserving Frameworks for Next-Generation Wireless Networks
Applied Cryptography Research Laboratory (ACRL), Bellini College of Artificial Intelligence, Cybersecurity, and Computing. Advisor: Prof. Attila A. Yavuz.

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
Developed **LPM2DA** (lattice-based privacy-preserving data aggregation) and **SPDBlock** (blockchain-based secure and privacy-preserving smart-grid framework).

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

EXPERIENCE

Graduate Research Associate

University of South Florida – Applied Cryptography Research Laboratory

Dec. 2021 – Present

- Lead researcher and security-framework designer across NSF- and industry-funded projects: **NSF-SNSF SATUQ** (satellite-terrestrial security, with **ZHAW**), **NSF SaTC Medium** (distributed computing for 5G/6G, with Virginia Tech and Oregon State), **NSF CAREER** (post-quantum lightweight IoT authentication), the 5G bootstrapping-authentication effort with **Purdue**, **UT Dallas** and **USF Muma College of Business**, and a **Cisco Research Award**.
- Designed, implemented and benchmarked post-quantum and privacy-preserving constructions: digital signatures, identity-based/group/ring signatures, anonymous credentials, private information retrieval, fully homomorphic encryption, secure multi-party computation, zero-knowledge proofs, key encapsulation, time-lock puzzles, distance-bounding and counter-DoS mechanisms.
- Produced peer-reviewed publications at MILCOM, TPS-ISA, SVCC, MobiArch and Elsevier COMNET, three provisional U.S. patents, and open-source reference implementations.

Instructor & Graduate Teaching Assistant

University of South Florida & K. N. Toosi University of Technology

Jan. 2019 – Present

- Courses:** Cryptography: Theory and Practice Privacy-Preserving & Trustworthy Cyber-Infrastructures
Penetration Testing for IT Computer Logic Design Lab Lattice-Based Cryptography Information Theory
Network Security
- Lectured on post-quantum, lattice-based and elliptic-curve cryptography, and built the hands-on lab track in C/C++ and Python using OpenSSL, LibOQS, LibTomCrypt, NTL and GMP.

System Administrator & Technical Support

USF Bellini College of Artificial Intelligence, Cybersecurity and Computing

Apr. 2024 – Jan. 2025

- Deployed **Rapid7** agents across Windows, Red Hat, Ubuntu and macOS, automated **CIS Level 1 & 2** validation through **Ansible**, and built a centralized audit and configuration repository covering all departmental systems.
- Administered the **GAIVI** GPU computing cluster (node failures, capacity, on-site data-center maintenance) and maintained a **Grafana** dashboard for network and system monitoring.

- Research investigator on the **National Smart Metering Program (Iran)**: designed and implemented lattice-based privacy-preserving data aggregation (**LPM2DA**) and post-quantum signature schemes for smart grids, yielding two journal papers.

SELECTED PUBLICATIONS

👥 Conferences

- **Saleh Darzi**, Gökcan Cantali, Dina Abdelhadi, Attila A. Yavuz, Gürkan Gür, "**QLAP**: A Quantum-Resilient Security and Privacy Framework for Dynamic Spectrum Access," in **MobiArch 2026: The 21st ACM Workshop on Mobility in the Evolving Internet Architecture**, in conjunction with ACM MobiCom 2026, Austin, TX, USA, 2026.
- **Saleh Darzi**, Attila A. Yavuz, "**SLAP**: Secure Location-Proof and Anonymous Privacy-Preserving Spectrum Access," in IEEE SVCC 2025: Silicon Valley Cybersecurity Conference, 2025.
- **Saleh Darzi**, Kiarash Sedghighadikolaei, Saif E. Nouma, Attila A. Yavuz, "Trustworthy AI Systems Through Lenses of Post-Quantum Security and Privacy-Enhancing Techniques," in CyberBay 2025: Tampa Bay Center of Excellence for Cybersecurity & AI, 2025.
- **Saleh Darzi**, Attila A. Yavuz, "Privacy-Preserving and Post-Quantum Counter Denial of Service Framework for Wireless Networks" (**PACDoSQ**), in MILCOM 2024 – IEEE Military Communications Conference, pp. 1076–1081, 2024.
- **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

- **Saleh Darzi**, Gökcan Cantali, Attila A. Yavuz, Gürkan Gür, "Privacy-Preserving and Secure Spectrum Sharing for Database-Driven Cognitive Radio Networks" (**SLAPX**), in Elsevier Computer Networks (COMNET) Journal, vol. 286, pp. 112420, issn. 1389-1286, 2026.
- **Saleh Darzi**, Kiarash Sedghighadikolaei, Saif E. Nouma, Attila A. Yavuz, "**QPADL**: Post-Quantum Private Spectrum Access with Verified Location and DoS Resilience," in Elsevier Computer Networks (COMNET) Journal, 2026.
- Attila A. Yavuz, **Saleh Darzi**, Saif E. Nouma, "**LiteQSign**: Lightweight and Quantum-Safe Signatures for Heterogeneous IoT Applications," in 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.

📄 Patents

- Attila A. Yavuz, **Saleh Darzi**, "System and Method for Secure Location-Proof and Anonymous Privacy-Preserving Spectrum Access" (**SLAP**), U.S. Patent Application US 2025/0392478 A1; USF TTO ref. 24T238PR-CS, Provisional Filed: 06/16/2025.
- Attila A. Yavuz, **Saleh Darzi**, "System and Method for Privacy-Preserving and Post-Quantum Secure Counter Denial of Service for Spectrum Management in Next-Generation Wireless Networks" (**PACDoSQ**), U.S. Patent Application US 2025/0392468 A1; USF TTO ref. 24T238PR-CS, Provisional Filed: 06/21/2024.
- Attila A. Yavuz, **Saleh Darzi**, "Resilient Authentication for Next-Generation Wireless Networks with Lawful Interception and Quantum-Safe Forgery Detection," USF TTO ref. 25T059PR-CS, Provisional Filed: 11/22/2024.

📄 E-Prints & Manuscripts Under Review

- **Saleh Darzi**, Mirza Masfiquir Rahman, Imtiaz Karim, Rouzbeh Behnia, Attila A. Yavuz, Elisa Bertino, "A Lightweight Post-Quantum Authentication Framework for 5G Base Station Bootstrapping" (**EMULSION**), arXiv:2606.30542, 2026. *Under review, NDSS Symposium 2027.*
- **Saleh Darzi**, Mirza Masfiquir Rahman, Imtiaz Karim, Rouzbeh Behnia, Attila A. Yavuz, Elisa Bertino, "Future-Proofing Authentication Against Insecure Bootstrapping for 5G Networks: Feasibility, Resiliency, and Accountability" (**BORG**), arXiv:2510.23457, 2025. *Under review, Elsevier Computer Networks (COMNET).*
- Dina Abdelhadi, Gökcan Cantali, **Saleh Darzi**, Attila A. Yavuz, Gürkan Gür, "Public Key Infrastructure for UAVs over 5G NR Sidelink in the Post-Quantum Era," 2026. *Under review, 17th IFIP Wireless and Mobile Networking Conference (WMNC).*
- Gökcan Cantali, Dina Abdelhadi, Gürkan Gür, **Saleh Darzi**, Attila A. Yavuz, "Quantum-Safe Orbital Data Centers and AI: Use Cases, Challenges, and Research Directions," 2026. *Under review, Special Issue on Orbital Edge: Data Centers in Space.*

- **Saleh Darzi**, Attila A. Yavuz, Rouzbeh Behnia, "Post-Quantum Security for Trustworthy Artificial Intelligence: An Emerging Frontier," Authorea Preprints, 2024.
- **Saleh Darzi**, Kasra Ahmadi, Saeed Aghapour, Attila A. Yavuz, Mehran Mozaffari Kermani, "Envisioning the Future of Cyber Security in the Post-Quantum Era: A Survey on PQ Standardization, Applications, Challenges and Opportunities," arXiv:2310.12037, 2023.

SKILLS

Languages & DevOps: C C++ Python Java Scripting Bash Git MATLAB x86 Assembly 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

SERVICES & ENGAGEMENT

Program Committee & Chair:

Publication Chair — ACM CCS QRSEC 2025 Program Committee — IEEE SVCC 2025, IEEE SVCC 2026

Reviewer:

ACM CCS 2025 USENIX Security 2025, 2026 ACSAC IEEE TDSC IEEE TIFS ACM Computing Surveys IEEE Trans. Smart Grid
 IEEE IoT Journal J. Information Security and Applications Cluster Computing Concurrency and Computation: Practice and Experience

Invited Talks & Presentations:

- Delivered the *Major Area Presentation*, "Post-Quantum Secure Authentication and Privacy-Preserving Frameworks for Next-Generation Wireless Networks," University of South Florida, November 2025.
- Presented at IEEE MILCOM 2024, IEEE SVCC 2025, IEEE TPS-ISA 2024, and CyberBay 2025 (Tampa, FL).
- Invited talk on the spectrum-access patent portfolio at *Innovation Match: Become the Founder of a USF Spinout*, USF Technology Transfer Office.

Awards, Grants & Open Source:

- NSF travel grants for MILCOM and IEEE TPS-ISA; USF research and travel support awards.
- Maintainer of open-source cryptography repositories, including post-quantum 5G authentication (**BORG-Scheme**) and GPU-accelerated PIR with proof-of-work generation (**QPADL**).

Memberships: IEEE IEEE Communications Society IEEE Young Professionals ACM

REFERENCES

Full references available upon request. Representative referees:

- **Prof. Attila A. Yavuz** (Ph.D. advisor), University of South Florida — attilaayavuz@usf.edu — +1 (813) 974 0419
- **Prof. Mehran Mozaffari-Kermani**, University of South Florida — mehran2@usf.edu — +1 (813) 974 2671
- **Prof. Reza Azarderakhsh**, Florida Atlantic University — razarderakhsh@fau.edu — +1 (561) 297-4980
- **Prof. Rouzbeh Behnia**, University of South Florida — behnia@usf.edu — +1 (941) 359-4605