Kiarash Sedghi

kiarashs@usf.edu | kiarashsedghi.com

LinkedIn | Github | Scholar

Tampa, FL - 33620, USA

Research Background and Interests

My current research lies at the intersection of **post-quantum cryptography (PQC)** and **secure multiparty computation (MPC)**. Specifically, I focus on the design and development of threshold lattice-based digital signatures, including the NIST standards ML-DSA and Falcon. My work aims to tackle state-of-the-art open problems in these constructions, with an emphasis on improving round complexity, communication efficiency, and signature compactness to enable scalable and practical quantum-resistant protocols.
In parallel, I actively participate in regular security working group meetings (*e.g.,* HE standardization group) to explore the theoretical foundations of cryptography, with a particular emphasis on the cryptanalysis of lattice-based schemes, which remains one of my core research interests.
My prior work centered on lightweight authentication mechanisms, such as hash-based post-quantum digital signatures, optimized for next-generation Internet of Things (IoT) environments, including smart grids, medical devices, and other cyber-physical systems. This research has led to peer-reviewed journal and conference publications and filed patents.

Skills

- **Cryptography:** Lattice-based and Hash-based Cryptography, Distributed (inc. threshold) Cryptography

- **Programming Languages:** C/C++/Python/Rust (Proficient); CUDA (basic familiarity)

Patents and Publications

C=Conference, J=Journal, P=Patent, E=E-Prints, T=Thesis

[C] **Sedghighadikolaei**, K., Sun C., Hoang T., Hamdaoui, B., and Yavuz, A. A. 2026. A Full Threshold NIST PQC-Compliant Framework for Distributed Trust in Federal Public Key Infrastructure. IEEE S&P 26 (Accepted).

[E] **Sedghighadikolaei**, K., *et al.*, 2026. Lightweight Authentication for Data Provenance with DKG (TBS).

[E] **Sedghighadikolaei**, K., *et al.*, 2026. PQ-secure Aggregate Signature (TBS).

[J] **Sedghighadikolaei**, K., and Yavuz, A. 2025. A Survey of Threshold Signatures: NIST Standards, Post-Quantum Cryptography, Exotic Techniques, and Real-World Applications. ACM Computing Surv. 58, no. 6 (2025): 1-39.

[E] Darzi, S., Nouma, S., **Sedghighadikolaei** K., and Yavuz, A. "QPADL: Post-Quantum Private Spectrum Access with Verified Location and DoS Resilience." arXiv preprint arXiv:2510.03631 (2025).

[J] Aghapour, S., **Sedghighadikolaei**, K., Yavuz, A. A., Hamdaoui, B., and Mozaffari-Kermani, M. "Efficient Fault-Detection Architectures for Barrett Reduction and Multiplication in Classical and Post-Quantum Cryptographic Systems." *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2025.

[J] **Sedghighadikolaei**, K., Yavuz, A., and Nouma, S. Signer-Optimal Multiple-Time Post-Quantum Hash-Based Signature for Heterogeneous IoT Systems. Internet of Things (2025): 101694.

[P] Yavuz, A., and **Sedghighadikolaei**, K., A Lightweight Multiple-Time Post-quantum Signature for Heterogeneous Internet of Things, TTO Ref. 25T013PR-CS, Submitted: August 20, 2024, Status: Provisional Patent Filed.

[P] Yavuz, A., and **Sedghighadikolaei**, K., Efficient, Scalable and Post-Quantum Authentication for Real-time Next Generation Networks with Probabilistic Data Structures, TTO Ref. 24T240PR-CS, Submitted: June 28, 2024, Status: Provisional Patent Filed.

[C] **Sedghighadikolaei**, K., and Yavuz, A. 2024. Fast and Post-Quantum Authentication for Real-time Next Generation Networks with Bloom Filter. In 2024 6^{th} IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)

[E] **Sedghighadikolaei**, K., and Yavuz, A. 2024. Privacy-Preserving and Trustworthy Deep Learning for Medical Imaging. arXiv preprint arXiv:2407.00538.

[C] Yavuz, A., **Sedghighadikolaei**, K., Darzi, S., and Nouma, S. 2023. Beyond Basic Trust: Envisioning the Future of NextGen Networked Systems and Digital Signatures. In 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) (pp. 267–276).

Experience

- **University of South Florida (USF) [🌐]** *Spring 2025 – Present*
  Research Assistant Tampa, USA
  - Conducting research on the design and implementation of threshold digital signatures with post-quantum security.
- **University of South Florida (USF) [🌐]** *Spring 2023 – Fall 2024*
  Teaching Assistant Tampa, USA
  - Developing instructional materials for the course *IT Data Structures*.
  - Assessment and grading of *IT Security Systems*, *IT Concepts*, *Cloud Computing*, and *Introduction to Databases*.
- **University of Isfahan [🌐]** *Spring 2019 and Fall 2020*
  Teaching Assistant Isfahan, Iran
  - Developing instructional materials and grading for the course *Data Structures*.
  - Preparing instructional content and evaluating student performance for *Compiler Design*.

Education

- **University of South Florida (USF)** *Expected Graduation: 2027*
  Ph.D. of Computer Science & Engineering Tampa, USA
  - GPA: 4.00/4.00
  - ***Research***: Design and implementation of post-quantum-secure threshold digital signatures with a specific focus on lattice-based cryptography. Additionally, I actively follow developments in lattice cryptanalysis.
  - ***Specialized Fields***: Multi-party Computation (MPC) and Post-quantum Cryptography (Lattice-based Cryptography)
- **University of South Florida (USF)** *Fall 2025*
  Master in Computer Science (MSCP) Tampa, USA
  - GPA: 4.00/4.00
- **University of Isfahan** *September 2021*
  B.Sc. Computer Science & Engineering Isfahan, Iran
  - GPA: 18.04/20.00
  - ***Thesis***: Design and implementation of a Smart Grid gateway enabling interoperability between IEC 61850 and DNP3 protocols, designed to operate on cost-effective single-board computers like the Raspberry Pi 4.

Projects

- **Open Threshold Post-Quantum [Self-maintained cryptographic library]** *November 2025 - Present*
  Tools: [C++, Linux] [🐙]
  - A self-maintained cryptographic library to establish a common framework for implementing threshold lattice-based signature schemes, facilitating rigorous benchmarking aligned with NIST's call for threshold cryptography.
- **Sparse LWE Kit** *October 2024 - Present*
  Tools: [Lattice-estimator] [🐙]
  - SparseLWEkit is a research-oriented toolkit that provides transparent security estimation and parameter guidance for LWE/RLWE-based FHE schemes with sparse secret keys. The project aims to improve rigor, comparability, and transparency in sparse-secret parameter selection as cryptanalysis continues to evolve.
- **FHE ML Inference Benchmark** *October 2024 - Present*
  Tools: [OpenFHE, Python3] [🐙]
  - I have been involved in this project since the October 2024 Homomorphic Encryption Standards meeting in Salt Lake City. Following several technical meetings, I am preparing to submit FHE benchmarking results for the BERT language model.
- **mumhors [Journal and Patent implementation]** *October 2024*
  Tools: [C Language, Linux] [🐙]
  - Implementation of the Journal paper "Signer-Optimal Multiple-Time Post-Quantum Hash-Based Signature for Heterogeneous IoT Systems" and the patent "A Lightweight Multiple-Time Post-quantum Signature for Heterogeneous Internet of Things".
- **tvpdhors [Conference and Patent implementation]** *April 2024*
  Tools: [C Language, Linux] [🐙]
  - Implementation of the conference paper "Fast and Post-Quantum Authentication for Real-time Next Generation Networks with Bloom Filter" and the patent "Efficient, Scalable and Post-Quantum Authentication for Real-time Next Generation Networks with Probabilistic Data Structures".
- **xv6 [Project of Ph.D. Operating Systems core course]** *December 2023*
  Tools: [C Language, xv6-riscv] [🐙]
  - Contribution to the xv6 operating system (RISC-V based) by implementing key kernel-level services, including the scheduler and virtual memory management, and extending user-level functionality with shell enhancements.

- **kfw [Project of B.Sc. Internet Engineering course]** *July 2020*
  Tools: [C Language, Linux]
  ◦ A new firewall system for the Linux kernel featuring an interface inspired by Cisco MQC. This system is designed to simplify and streamline the configuration process, replacing the complexity of the widely-used iptables with a more intuitive and user-friendly approach for system administrators.
- **karpg [Project of B.Sc. Internet Engineering course]** *July 2020*
  Tools: [C Language, Linux]
  ◦ A CLI-based ARP packet generator that offers a streamlined set of functionalities that significantly reduce time expenditure compared to GUI-based alternatives.
- **jenkinsc [Project of B.Sc. Software Engineering course]** *May 2020*
  Tools: [Python3, Jenkins, Windows]
  ◦ A CLI-based program to streamline Jenkins server configuration, reducing the time required for setup via the Web interface to optimize the Continuous Integration and Continuous Development (CI/CD) process.
- **luluc [Project of B.Sc. Compiler Design course]** *December 2019*
  Tools: [Python3, ANTLR4, Linux] **[]**
  ◦ A compiler developed for the Lulu programming language.

Professional Volunteer Services

- **Subreviewer for Usenix Security** *Since August 2025*
- **Reviewer for Elsevier Internet of Things (IoT)** *Since July 2025*
- **Reviewer for ACM Transactions on Privacy and Security (TOPS)** *Since April 2025*
- **Reviewer for IEEE Transactions on Networking (TON)** *Since April 2025*
- **Reviewer for IEEE International Symposium on Hardware Oriented Security and Trust (HOST)** *Since January 2025*
- **Reviewer for ACM Transactions on Internet of Things (TIOT)** *Since January 2025*
- **Reviewer for IEEE Transactions on Information Forensics and Security (TIFS)** *Since December 2024*
- **Reviewer for IEEE Transactions on Dependable and Secure Computing (TDSC)** *Since October 2024*
- **Reviewer for IEEE Transactions on Network Science and Engineering (TNSE)** *Since October 2024*
- **Reviewer for IEEE Internet of Things (IoT) Journal** *Since September 2024*

Project Grants and Fundings (supporting my projects)

- **Collaborative Research: SaTC: CORE: Medium: Distributed Computing in Effect: Towards Trustworthy, Resilient and Secure NextG Mobile Networks - *Awarded $1.2M*** *August 2024*
  National Science Foundation (NSF CNS-2350213) (PI: Attila A. Yavuz, Co-PIs: Mehran Mozaffari Kermani, Thang Hoang, and Bechir Hamdaoui)
- **Trustworthy Digital Forensics for Heterogeneous Internet of Things (220159)** *August 2019-2022*
  Cisco (PI: Attila A. Yavuz)
- **CAREER: Light-Weight and Fast Authentication for Internet of Things - *Awarded $405,162*** *August 2018*
  National Science Foundation (NSF CNS-2350213) (PI: Attila A. Yavuz)

Honors and Awards

- **Travel: NSF Student Travel Grant for 6th IEEE International Conference on Trust, Privacy, and Security in Intelligent Systems and Applications (IEEE TPS 2024) – *Awarded $1,000*** *September 2024*
  National Science Foundation (NSF CNS-2431905)
- **IEEE TPS 2024 Conference Travel Grant – *Awarded $2,450*** *September 2024*
  University of South Florida (USF 109085)
- **Ranked 3rd in GPA among B.Sc. degree andidates** *July 2021*
  University of Isfahan
- **Rank top 0.6% of the University Entrance Exam** *September 2017*
  Iran
- **Ranked 2nd in provincial Geometry Olympiad** *August 2016*
  Iran
- **Recognized exceptional talent by NODET** *June 2013*
  Iran

Attended Workshops

- **Cryptography 10 Years Later: Obfuscation, Proof Systems, and Secure Computation** *Summer 2025*
  Host: [Simons Institute] **[]**
- **7^{th} HomomorphicEncryption.org Standards Meeting** *October 2024*
  Host: [Kurt Rohloff (Duality Technologies)] **[]**
- **Summit on Responsible Decentralized Intelligence** *August 2024*
  Host: [Berkeley University] **[]**
- **WPEC 2024: NIST Workshop on Privacy-Enhancing Cryptography** *September 2024*
  Host: [National Institute of Standards and Technology (NIST)] **[]**
- **Lattices: Algorithms, Complexity, and Cryptography [Simons Institute]** *August 2024*
  Instructors: [Daniele Micciancio, Stephens-Davidowitz, Chris Peikert, Vinod Vaikuntanathan, et al.] **[]**

CERTIFICATIONS

- **IEEE Transactions on Dependable and Secure Computing (TDSC) Reviewer Certification** *Fall 2025*
- **Linux Embedded Systems Certification** *September 2021*
- **CCNP R&S Certification** *January 2021*
- **CCNA & CCNP Collaboration Certification** *August 2020*
- **CCNA R&S Certification** *November 2019*
- **Microsoft MCSA Certification** *October 2019*
- **Linux LPIC-2 Certification** *July 2019*
- **Linux Bash Scripting Certification** *August 2018*
- **Linux LPIC-1 Certification** *May 2018*