Ali Arastehfard

ali.arastehfard@uconn.edu · (860) 634-9491
Homepage · LinkedIn · GitHub · Scholar

Overview. Ph.D. student in *Applied Cryptography* (UConn, exp. May 2027) with 3+ years of research at the intersection of **privacy, AI, and secure computation**. Experienced in **building privacy-preserving ML and retrieval systems** (MPC, PIR, PSI, private RAG) with **hands-on experience in Rust/C++/Python-based cryptographic engineering** and **privacy-preserving model deployment**. Additional experience in **differential privacy**, **LLM security**, and **network security**. Recipient of the **Synchrony** and **Predoctoral Fellowships (Spring 2025); nominated for UConn's Best Teaching Assistant Award (2023)**.

Research Interests

Homomorphic Encryption; Private Information Retrieval (PIR); Private Retrieval-Augmented Generation (RAG); Private Set Intersection (PSI); Privacy-Preserving Machine Learning (PPML); Secure Multi-Party Computation (MPC); Secure Computation; Applied Cryptography.

Research Experience

Research Assistant, University of Connecticut (UConn) Sep 2022 – Present

- Proposed KPIR-C, a novel Keyword PIR scheme enabling arbitrary, non-interactive post-retrieval computation—a capability critical for privacy-preserving AI pipelines and secure data governance. Constructed the scheme based on *Torus Fully Homomorphic Encryption* (TFHE), achieving over a 10× reduction in communication cost while remaining computationally competitive with prior work—despite supporting arbitrary computations that previous schemes could not. Results published in *IACR ePrint 2025/1952*.
  - Led adaptation of the *TFHE-rs* cryptographic library to implement the KPIR-C protocol, manually managing ciphertext noise for optimized retrieval performance. Re-implemented Binary Fuse Filters in Rust and explored key-to-index hashing methods for efficient keyword encoding. Authored the formal security and correctness proofs of the proposed scheme.
- Designed secure two-party protocols for *Adder Neural Networks* (AdderNet) that replace convolution operations in *Convolutional Neural Networks* (CNNs) with additions and inexpensive Boolean comparisons. The resulting secure AdderNet achieved over a 2× reduction in communication compared to its secure CNN counterpart, while maintaining the same runtime. Results published in *arXiv:2509.05552*.
- Implemented the open-source code for *arXiv:2107.04284*, published at IEEE S&P'22 by our group. Worked with video datasets and optimization methods for generating human-imperceptible adversarial perturbations to improve robustness against detection. Code available at *github.com/alarst13/u3d*.

Selected Publications

- A. Arastehfard, W. Liu, Q. Zhou, Z. Shen, L. Peng, L. Qu, S. Feng, Y. Hong. "**KPIR-C: Keyword PIR with Arbitrary Server-Side Computation**." *IACR ePrint 2025/1952*, 2025.
- A. Arastehfard, W. Liu, J. Lee, B. Liu, X. Ban, Y. Hong. "**Secure and Efficient L^p-Norm Computation for Two-Party Learning Applications**." *arXiv:2509.05552*, 2025.

Industry Experience

Co-Founder & Developer, Vegitto Startup · Prototype — Tehran, Iran Sep 2020 – Dec 2021

- Led a 7-member team to design and launch an Android platform for vegetarian/vegan recipe sharing, overseeing AI, Android, and product development through a successful MVP release.

Android Development Intern, RNS Assistant — Hamilton, Ontario (Remote) Oct 2019 – Jul 2020

- Helped develop an AI-powered healthcare system for supervised diagnosis, treatment, and recovery.

Education

University of Connecticut — Ph.D., Computer Science Sep 2022 – Present
Advisor: Dr. Yuan Hong

Amirkabir University of Technology — B.Sc., Computer Engineering 2018 – 2022

Technical Skills

- **Privacy & AI:** Private ML, Privacy-preserving RAG, FHE, PIR, MPC, PSI
- **Security:** LLM vulnerabilities & security, Network Security, Penetration Testing
- **Libraries & Tools:** TFHE-rs, Microsoft SEAL, PyTorch, Hugging Face, Faiss, Docker, Git
- **Programming:** Rust, Python, C++, Java

Teaching Experience

Teaching Assistant, CSE 3140: Cybersecurity Lab — Prof. Amir Herzberg Jan 2023 – Present

- Assisted in teaching an introductory cybersecurity lab on secure system design and penetration testing—covering platform vulnerabilities (weak passwords, XSS), exploitation techniques (Wi-Fi attacks, malware, ransomware, phishing), and defense mechanisms (cryptography, CSP headers); maintained and configured lab infrastructure, coordinated a team of nine TAs, and held office hours.

Teaching Assistant, Principles of Software Design — Dr. Hossein Nourikhah Oct 2021 – Jul 2022

- Guided students in object-oriented software design, UML modeling, and applying design patterns.

Service + Volunteer

- External Reviewer, security conferences — IEEE S&P, USENIX Security, ACM CCS, NDSS (2024–2025); 14 papers.
- External Reviewer, academic journals — IEEE TDSC, AAMAS, IEEE TPS (2022–2024); 8 papers.
- Volunteer program director, UConn Community Outreach (2023–2024).

Awards & Honors

- **Synchrony and Predoctoral Fellowships**, University of Connecticut Spring 2025
- **Nominee**, Best Teaching Assistant Award, University of Connecticut 2023–2024 academic year