Alireza Shirzad

Portfolio: alireza-shirzad.github.io
Github: github.com/alireza-shirzad
Email: alrshir@seas.upenn.edu
Mobile: (267) 353-5156

Education

- **University of Pennsylvania** — Philadelphia, USA
  Ph.D. - Computer and Information Science; GPA: 4.00/4.00 — *January 2024 - Present*
- **Sharif University of Technology** — Tehran, Iran
  M.Sc. - Secure Communication and Cryptography; GPA: 4.00/4.00 — *2021 - 2024*
- **Sharif University of Technology** — Tehran, Iran
  B.Sc. - Electrical Engineering (Minor: Computer Science); GPA: 3.53/4.00 — *2016 - 2021*

Research Interests

- **Cryptography**: Proof System design, Zero-Knowledge Proofs, Commitment Schemes
- **System Security**: Secure and Transparent Computation, Network Security, Blockchain

Publications

[1] Benedikt Bünz et al. "DewTwo: A Transparent PCS with Quasi-Linear Prover, Logarithmic Verifier and 4.5KB Proofs from Falsifiable Assumptions". In: *Advances in Cryptology – CRYPTO 2025* (2025). Ed. by Yael Tauman Kalai and Seny F. Kamara, pp. 549–583.

[2] Hossein Hafezi et al. "IronDict: Transparent Dictionaries from Polynomial Commitments". In: (2025). URL: https://eprint.iacr.org/2025/1580.

[3] Michel Dellepere, Pratyush Mishra, and Alireza Shirzad. "Garuda and Pari: Smaller and Faster SNARKs via Equifficient Polynomial Commitments". In: *zk-Summit-25, SBC25* (2024). eprint: https://eprint.iacr.org/2024/1245.pdf.

[4] Alireza Shirzad. "Designing a Succinct Argument System Based on GKR Protocol Via Polynomial Commitment Schemes". MA thesis. Sharif University Of Technology, 2023.

[5] Soroush Goodarzi et al. *Cold Supply Chain Planning including Smart Contracts: An Intelligent Blockchain-based approach*. 2022. arXiv: 2209.10410 [cs.CR].

Work Experience

- **Lagrange Labs** — Remote
  Research Intern - Working with Dr. charalampos papamanthou and Dr. Dimitris Papadopoulos — *Summer 2025*

Teaching Experience

- **University of Pennsylvania** — Philadelphia, USA
  Teaching Assistant — *January 2024 - May 2024*
  - **Courses**: CIS 5560: Cryptography, CIS 5510: Computer and network security
- **Sharif Information and Computer Technology (Sharif ICT)** — Remote
  Lecturer (Part-time) — *January 2021 - September 2023*
  - **Blockchain and Web3 course**: Cryptography fundamentals, Solidity programming
- **Sharif University Of Technology** — Tehran, Iran
  Teaching Assistant — *May 2019 - Sep 2019*
  - **Courses**: Provable Security, Security in IOT, Linux/Python Lab, Advanced Programming Lab, Object Oriented Programming, Data Communication Network

Honors and Awards

- Granted membership of National Elite Foundation for seven consecutive years - October 2016 untill Jan 2024
- Ranked in the top 25% in B.S and Granted Master Scholarship, Sharif University of Technology: - Jan 2020
- Ranked 32nd among 200000 participants in Iranian Nationwide Mathematics University Entrance Exam - Sep, 2016

Service

- **Artifact-Reviewer**
  - 26th Privacy Enhancing Technologies Symposium (PETS 2026)
- **Sub-Reviewer**
  - The 19'th ISC International Journal of Information Security
  - Financial Cryptography and Data Security 2025
  - 46th IEEE Symposium on Security and Privacy
- **Upenn Security and Privacy Seminar Organizer** — Philadelphia, USA
  Organizing seminars, contacting people for giving talks — *September 2024 - Present*

Skills

- **Languages**: Rust, Java, Python, SageMath, Solidity
- **Soft Skills**: Presentation, Teamwork, Writing