

# 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* 2020 - 2024
- **Sharif University of Technology** Tehran, Iran  
*B.Sc. - Electrical Engineering (Minor: Computer Science); GPA: 3.53/4.00* 2016 - 2020

## RESEARCH INTERESTS

---

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

## PUBLICATIONS

---

- [1] Benedikt Bünz, Tushar Mopuri, and Sriram Sridhar Alireza Shirzad. *DewTwo: a transparent PCS with quasi-linear prover, logarithmic verifier and 4KB proofs from falsifiable assumptions*. Submitted to Eurocrypt 2025.
- [2] Michel Dellepere, Pratyush Mishra, and Alireza Shirzad. *Garuda and Pari: Faster and Smaller SNARKs via Equiefficient Polynomial Commitments*. Cryptology ePrint Archive, Paper 2024/1245. Submitted to Eurocrypt 2025. URL: <https://eprint.iacr.org/2024/1245>.
- [3] Alireza Shirzad. "Designing a Succinct Argument System Based on GKR Protocol Via Polynomial Commitment Schemes". MA thesis. Sharif University Of Technology, 2023. URL: <https://library.sharif.ir/parvan/resource/>.

## SKILLS

---

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

## EXPERIENCE

---

- **University of Pennsylvania** Philadelphia, USA  
*Teaching Assistant* May 2019 - Sep 2019
  - **Courses:** CIS 5560: Cryptography, CIS 5510: Computer and network security
- **Sharif Information and Computer Technology (Sharif ICT)** Remote  
*Lecturer (Part-time)* May 2019 - Sep 2019
  - **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 until January 2024
- Ranked in the top 25% in B.S and Granted Master Scholarship, Sharif University of Technology: - January 2020
- Ranked 32nd among 200000 participants in Iranian Nationwide Mathematics University Entrance Exam - September, 2016

## SERVICE

---

- **Pre-reviewer** Tehran, Iran  
*The 19<sup>th</sup> ISC International Journal of Information Security* 2021 - 2023
- **SUPenn Security and Privacy Seminar Organizer** Philadelphia, USA  
*Organizing seminars, contacting people for giving talks* September 2024 - Present

## REFERENCES

---

- **Pratyush Mishra** prat@seas.upenn.edu  
*Assistant Professor, Dept of Computer and Information Science, University of Pennsylvania*