

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: 3.91/4.00* 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

Applied Cryptography, Building provably secure systems from Cryptography

PUBLICATIONS

-
- [1] Bharath Namboothiry, Alireza Shirzad, Spencer Solit, Ryan Marcus, and Pratyush Mishra. “TruthTable: A Verifiable Query Engine”. In: *ZKProof VIII (2026), SeQureDB 2026. Bharath and Alireza contributed equally to this work.*
 - [2] Alireza Shirzad, Sriram Sridhar, Dimitrios Papadopoulos, and Charalampos (Babis) Papamanthou. *Relaxed Modular PCS from Arbitrary PCS and Applications to SNARKs for Integers.*
 - [3] Benedikt Bünz, Tushar Mopuri, Alireza Shirzad, and Sriram Sridhar. “DewTwo: A Transparent PCS with Quasi-Linear Prover, Logarithmic Verifier and 4.5KB Proofs from Falsifiable Assumptions”. In: *Advances in Cryptology – CRYPTO 2025. Authors listed in alphabetical order.*
 - [4] Hossein Hafezi, Alireza Shirzad, Benedikt Bünz, and Joseph Bonneau. “IronDict: Transparent Dictionaries from Polynomial Commitments”. In: *Usenix 2026, RWC 2026. Hossein and Alireza contributed equally to this work.*
 - [5] Michel Dellepère, Pratyush Mishra, and Alireza Shirzad. “Garuda and Pari: Smaller and Faster SNARKs via Equiefficient Polynomial Commitments”. In: *Usenix 2026, zk-Summit-25, SBC25. Authors listed in alphabetical order.*
 - [6] Alireza Shirzad. “Designing a Succinct Argument System Based on GKR Protocol Via Polynomial Commitment Schemes”. MA thesis. Aryamehr (Sharif) University Of Technology.
 - [7] Soroush Goodarzi, Vahid Kayvanfar, Alireza Haji, and Alireza Shirzad. *Cold Supply Chain Planning including Smart Contracts: An Intelligent Blockchain-based approach.*

TALKS

-
- **TruthTable: A Verifiable Query Engine**
 - NYU Cryptography and Security Seminar, New York, USA May 2026
 - **IronDict: Transparent Dictionaries from Polynomial Commitments**
 - UPenn Security and Privacy Seminar, Philadelphia, USA October 2025
 - Berkeley Crypto Seminars, Remote October 2025
 - **Garuda and Pari: Smaller and Faster SNARKs via Equiefficient Polynomial Commitments**
 - Science of Blockchain Conference, Berkeley, USA August 2025
 - SBC 2025 Online Science Fair, Remote July 2025
 - Berkeley Crypto Seminars, Berkeley, USA December 2024
 - CMU LayerZero Crypto Seminar, Pittsburgh, USA December 2024
 - Stanford Security Seminar, Stanford, USA December 2024
 - Sumcheck Builders Club, Remote November 2024
 - University of Maryland Crypto Reading Group, College Park, USA November 2024
 - NYU Cryptography and Security Seminar, New York, USA October 2024
 - UPenn Security and Privacy Seminar, Philadelphia, USA October 2024

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
 - **CIS 7000: Provably Secure Systems with Cryptography** Fall 2025
 - **Sharif Information and Computer Technology (Sharif ICT)** Remote
 - **Blockchain and Web3** January 2021 - September 2023

TEACHING ASSISTANT EXPERIENCE

- **University of Pennsylvania** Philadelphia, USA
 - CIS 5560: Cryptography *Spring 2026*
 - CIS 5510: Computer and Network Security *Fall 2024*
 - CIS 5560: Cryptography *Spring 2024*
- **Sharif University Of Technology** Tehran, Iran
 - Linux/Python Lab *Fall 2022*
 - IoT Security *Fall 2022*
 - Object Oriented Programming (Head TA) *Spring 2022*
 - Provable Security *Spring 2022*
 - Numerical Computation *Fall 2021*
 - Object Oriented Programming (Head TA) *Spring 2021*
 - Signals and Systems *Spring 2021*
 - Data Communication Network *Spring 2020*

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 coordinator** *September 2024 - September 2025*
- **Schlein cybersecurity center local seminar coordinator** *January 2026 - Present*
- **Penn Iranian Academic Network (PIRAN) President** *March 2026 - Present*