Mohammad Amin Raeisi

512 Arthur K. Watson Hall, 51 Prospect Street, New Haven, CT 06511
203-435-3764 amin.raeisi@yale.edu linkedin.com/in/mohammadaminraeisi github.com/aminra81

Education

Yale University (GPA: 4.0/4.0) **Sep. 2025 – Present**
Ph.D. in Computer Science *New Haven, CT*

- **Relevant Coursework:** Trustworthy Deep Learning (Ongoing) Computational Biomedical Privacy (Honors), Real-World Cryptography (Honors), Advanced Topics in Cryptography (Honors), Intro to Cryptography (Honors), Zero-Knowledge Proofs (Honors), and Intro to Quantum Computing (Honors).

Sharif University of Technology (GPA: 19.48/20) **Sep. 2020 – Jun. 2025**
B.Sc. in Computer Science *Tehran, Iran*

Research Interests

- **Cryptography:** Proof Systems, Post-Quantum Cryptography, Cryptography for AI
- **System Security:** AI security, LLM Safety, Verifiable ML

Publications

[1] B. Merbaum, **M. A. Raeisi***, W. Wang, C. Papamanthou, K. Sotiraki, F. Zhang. "Maverick: Private and Verifiable LLM Inference Made Practical via Matrix-Vector Multiplication Delegation" (In submission)
arxiv: https://arxiv.org/pdf/2609.10264.

[2] L.-H. Merino, S. Colombo, R. Reyes, A. Azhir, S. Mishra, P. Tennage, **M. A. Raeisi**, H. Zhang, J. R. Allen, B. Tellenbach, V. Estrada-Galiñanes, B. Ford. "TRIP: Coercion-resistant Registration for E-Voting with Verifiability and Usability in Votegral." In: *ACM SIGOPS 31st Symposium on Operating Systems Principles (SOSP)* (2025).
DOI: https://doi.org/10.1145/3731569.3764837.

[3] S. Mitrović, T. Pan, M. Qaempanah, **M. A. Raeisi***. "New Parallel and Streaming Algorithms for Directed Densest Subgraph." In: *NeurIPS* (2025).
arXiv: https://arxiv.org/abs/2509.21729.

[4] R. Bhaumik, **M. A. Raeisi***. "Building a BBB Pseudorandom Permutation using Lai–Massey Networks." In: *IACR Communications in Cryptology, Volume 1* (2024).
ePrint: https://eprint.iacr.org/2023/1834.

*Co-first author, alphabetical order.

Honors and Awards

- Yale University Ph.D. Fellowship, annual support of USD 106,288 (2025–2026)
- Summer@EPFL Fellowship, CHF 5,400 (2024)
- Graduate Studies Opportunity Without Entrance Exam, Sharif University of Technology (2023)
- Summer@EPFL Fellowship, CHF 4,800 (2023)
- Top 0.22% among 155,250 participants, Iranian University Entrance Exam in Mathematics and Physics (2020)
- Silver Medal, Iranian National Olympiad in Informatics (2019)
- Silver Medal, Iranian National Olympiad in Informatics (2018)

Research & Industry Experience

University of Maryland **June. 2026 – Aug 2026**
Faculty Assistant *Remote*

University of California, Davis **Sep. 2024 – May 2025**
Research Collaborator – Directed Densest Subgraph in MPC *Remote*

École Polytechnique Fédérale de Lausanne (EPFL) **Jun. 2024 – Sep. 2024**
Research Intern – Coercion-Resistant Electronic Voting *Lausanne, Switzerland*

École Polytechnique Fédérale de Lausanne (EPFL) **Jun. 2023 – Aug. 2023**
Research Intern – Lai–Massey Security Bounds *Lausanne, Switzerland*

Divar **Jun. 2021 – Sep. 2021**
Software Engineer Intern – Django, Docker, PostgreSQL, Kubernetes *Tehran, Iran*

Teaching Experience

Yale University

Teaching Fellow *New Haven, CT*

- **Course:** Introduction to Cryptography.

Sharif University of Technology **Sep. 2021 – Jun. 2024**

Teaching Assistant *Tehran, Iran*

- **Courses:** Introduction to Cryptography, Analysis of Algorithms, Design Algorithms, Theory of Automata, Data Structures, Game Theory, Linear Algebra, Probability and Applications, Introduction to Linear Algebra, and Basic Programming.

Allame Helli 10, Farzanegan Olympiad Club, Allame Tabatabaei High School **Jun. 2020 – Aug. 2021**

Algorithm Design Lecturer *Tehran, Iran*

- Taught algorithms, data structures, and competitive programming to approximately 40 high-achieving high school students preparing for the International Olympiad in Informatics.
- Students earned one international silver medal and multiple national medals.

Service

- **Sub-Reviewer**
  - ACM Conference on Computer and Communications Security (CCS 2026)
  - IACR ASIACRYPT 2026
  - IACR EUROCRYPT 2027
- **Scientific Committee Member and Final Theoretical Exam Grader**
  - 32nd Iranian National Olympiad in Informatics Summer Camps (2022)
  - 31st Iranian National Olympiad in Informatics Summer Camps (2021)