MATAN SHTEPEL

(925) · 922 · 9254 ⋄ matan.shtepel@gmail.com ⋄ matanshtepel.com

Last updated: Jan 2026. ⋄ Most recent version: https://matanshtepel.com/matan_shtepel_cv.pdf

OVERVIEW

Second year Ph.D. student at Carnegie Mellon University working on AI Safety. Previously worked on cryptography.

EDUCATION

Carnegie Mellon University August 2024 - Ongoing
PhD @ Computer Science Department.
Advisor: Prof. Andrew Ilyas.
Research in AI Safety.
Graduate student officer at Carnegie AI Safety Initiative (CASI).

University of Pennsylvania October 2023 - July 2024
Research Assistant @ Department of Computer and Information Science.
Advisors: Prof. Brett Falk and Prof. Pratyush Mishra.
Research in cryptography ∩ coding theory.

University of California, Los Angeles September 2021 - March 2023
B.S.E @ CS + pure math concentration, with honors.
GPA: 3.86
Research in cryptography (secure multiparty computation)
Advisors: Prof. Rafail Ostrovsky and Prof. Brett Falk.
Founded and organized Theory@UCLA.

Las Positas Community College June 2020 - May 2021
A.S Computer Science and A.S Math with honors.
GPA: 3.95
Honors project advised by Dr. William Pezzaglia: Quaternion-based rotation engine
Math Club Mu Alpha Theta officer

AWARDS & FUNDING

- **NSF Graduate Research Fellowship Program (GRFP), 2025 cycle.** 1/1000 nationally to receive the award, 1/2 in "Comp/IS/Eng - Computer Security and Privacy." Award: $159,000.
- **Sui Academic Research Award .** Co-I on proposal "Scalable Post-Quantum Transparent SNARKs" which partially funded me as an RA at UPenn. PIs: Prof. Brett Falk and Prof. Pratyush Mishra. Award: $25,000.
- **GEM Fellowship, 2023-24 cycle: Final Round.** Selected for the final round of the GEM fellowship.
- **NSF REU Funding for Summer 2023.** Granted for work on secure multiparty computation advised Prof. Rafail Ostrovsky at UCLA.
- **NSF REU Funding for Summer 2022.** Granted for work on secure multiparty computation advised Prof. Rafail Ostrovsky at UCLA.
- **USENIX'23 Student Travel Grant.** All attendance and (partial) travel costs covered by USENIX'23.

SELECTED EXEPERIENCE

- **Organize CASI-R (Fall '25).** Start CASI-Research (CASI-R) to connect talented ugrads / masters students to experienced AI Safety researchers at CMU to work on scaffold MATS-style projects. Currently co-leading the pilot project (6 ugrads, red-teaming cyber decomposition attacks) with Alex Robey (TML) and Davis Brown (UPenn).
- **MARS AI Safety Research Fellowship (Sum' '25).** Participated in a 3 month research fellowship. Developed an integration of the `Inspect AI` framework and `Weights & Biases`. Internally adopted by UK AISI (and maybe METR).
- **The 10'th Heidelberg Laureate Forum + Full Travel Grant (Fall '23).** Selected one of 200 young researchers (undergraduates, graduates, and postdoctoral fellows) worldwide invited to the 10'th Heidelberg Laureate Forum. All travel and attendance costs covered.
- **Hack Lodge (sponsored by ETH university) (Winter' '23).** Participate in competitively selected applied cryptography/Ethereum ecosystem-focused hacker house.

PAPERS

Authors in alphabetical order unless stated otherwise.

- **Query Optimal IOPPs for Linear Time Encodable Codes**
  We give IOPPs (key technical building blocks for zkSNARK) for a large class of codes with provably optimal prover *and* query complexity and strictly improving on all prior works. Our results builds on a novel "lossy batching" IOR.
  Anubhav Baweja, Pratyush Mishra, Tushar Mopuri, Matan Shtepel.
  In submission to CRYPTO '26.
- **FICS and FACS: Fast IOPPs and Accumulation via Code-Switching**
  We give IOPPs and accumalation scheme (key technical building blocks for zkSNARK) achieving state of the art asymptotic efficiency and develop a novel framework for proving non-interactive knowledge soundness (in the ROM).
  Anubhav Baweja, Pratyush Mishra, Tushar Mopuri, Matan Shtepel.
  Preprint.
- **Malicously secure PIR (almost) for free**
  We show how transform any PIR scheme to a maliciously-secure PIR scheme with very low overhead. Shows the complexity-theoretic equivelance of the primitives.
  B. Falk, Pratyush Mishra, Matan Shtepel.
  Accepted to CRYPTO'25
- **DORAM revisited: Maliciously secure RAM-MPC with logarithmic overhead**
  We give the first malicious construction of Distributed ORAM while matching the asymptotics of the best-known semi-honest constructions. As a corollary, we give the *first* maliciously-secure MPC with logarithmic random access overhead.
  B. Falk, D. Noble, R. Ostrovsky, M. Shtepel, J. Zhang
  Accepted to TCC'23
- **GigaDORAM: Breaking the Billion Address Barrier**
  We construct and implement the most practically efficient Distributed Oblivious RAM (DORAM) protocol to date, outperforming all existing DORAM constructions by over 400x. We hope our construction will enable RAM-MPC to be deployed in practice.
  B. Falk, R. Ostrovsky, M. Shtepel, J. Zhang
  Accepted to USENIX '23
- **On Totalization of Computable Functions in a Distributive Environment**
  Mark Burgin, Matan Shtepel.
  International Journal of Parallel, Emergent and Distributed Systems, Volume 37, Number 3, October 2021.

In-Progress

- **Challenges in Studying CoT Monitorability**
  Identify several challenges in measuring CoT monitorability, including: mitigating false, false positives, quantifying sources of unmonitorability (e.g. internalized reasoning vs monitor mistakes), gathering monitorability-predictive task-features.
  M. Shtepel, A. Ilyas, *Intended submission: ICML '26*

TALKS

- *From CC to PhD: Why You Should Do it and How You Can Achieve it* October {10,11}th 2024
  Las Positas Community College MESA Scholars Program, Math Club.
- *Maliciously-Secure PIR is (almost) Free*, July 15th, 2024
  Workshop in Private Information Retrieval at Privacy Enhancing Technologies Symposium 2024.
- *Maliciously-Secure PIR is (almost) Free*, May 22nd, 2024
  New York University (NYU) Crypto Seminar.
- *Maliciously-Secure PIR is (almost) Free*, Apr. 30th, 2024
  Carnegie Mellon University (CMU) Cylab Crypto Seminar. Video recording,
- *Theory and Practice of RAM-MPC from Distributed ORAM.*, Feb. 16th, 2024
  University of Maryland (UMD) College Park, Crypto Reading Group.
- *Theory and Practice of RAM-MPC from Distributed ORAM.*, Dec. 6th, 2023
  Stanford Security Seminar.
- *Theory and Practice of RAM-MPC from Distributed ORAM.*, Nov. 30th, 2023
  University of Pennsylvania (UPenn) Security and Privacy Lab
- *Theory and Practice of RAM-MPC from Distributed ORAM.* Nov. 29th, 2023
  Boston University (BU) Security Lunch.
- *GigaDORAM: Breaking the Billion Address Barrier* Aug. 10, 2023
  USENIX Security 2023

ACADEMIC SERVICE

Gradute Student Officer Sep '25 - ongoing
Carnegie AI Safety Initiative (CASI) @ CMU

- Organizing CASI-Research, researcher socials, and AI Safety seminar.

Cryptography Seminar Organizer Sep 2024 - Sep 2025
CyLab Crypto Seminar @ CMU

- Organize the CMU crypto seminar with Quang Dao.

Undergraduate Research Mentor Oct 2022 - present
Cryptography research @ UCLA

- Mentor Felix Adena, Nakul Khambhati, and Stephen Kelman on cryptography research on secure graph algorithms, informtion-theoretic MPC, and MPC implemnetation, respectively.

Founder Sep 2022 - May 2023
Theory@UCLA @ UCLA

- Found and organize Theory@UCLA, UCLA's first theoretical computer science club.

Advocate for Community College Researchers Mar 2022 - Sep 2024
UCLA Engineering Transfer Center

- Invited to speak on the Engineering Research Presentations & Panel (only transfer student) at UCLA Engineering Day and at the research Panel of UCLA Engineering Transfer Day (only current undergraduate).

RELEVANT COURSEWORK

- CMU: trustworthy AI, automated reasoning (SAT solvers), Graduate Machine Learning, discrete math, randomized algorithms, cryptography.
- UPenn: SNARKs, Foundations of Deep Learning, algebraic combinatorics.

- UCLA: Graduate cryptography sequence, graduate communication complexity theory, graduate quantum computing, graduate computational complexity theory (winter 23'), graduate theory hits, honors real analysis sequence, probability theory sequence, linear algebra sequence, group theory, enumerative combinatorics, required CS curriculum.