MATAN SHTEPEL

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

Last updated: April 2025. ◇ Most recent version: https://matanshtepel.com/matan_shtepel_cv.pdf

OVERVIEW

I'm a first year Ph.D. student at Carnegie Mellon University, working primarily in cryptography ∪ coding theory and broadly interested in theory and AI safety. Outside of my technical passions, I like Bob Dylan, blockchains, Australian rock music, rationality, small apartments, running, surfing, and beans. I'm also intrested in outreach, particularly to community college students.

EDUCATION

Carnegie Mellon University August 2024 - Ongoing
Computer Science PhD student.

University of Pennsylvania October 2023 - June 2024
Cryptography Research Assistant.
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 Computer Science (concentration in pure math) with honors.
GPA: 3.86
Research in cryptography
Primary advisor: Prof. Rafail Ostrovsky (UCLA)
Secondary advisor: Prof. Brett Falk (Upenn)
Founded and organized Theory@UCLA.

Las Positas Community College June 2020 - May 2021
A.S Computer Science with honors.
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

PAPERS

Authors in alphabetical order unless stated otherwise.

- **FICS and FACS: Fast IOPPs and Accumulation via Code-Switching**
  We give IOPPs and accumalation scheme (key building blocks for zkSNARK) achieving state of the art asymptotic efficiency. We develop RBRBKS, 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.

FUNDING & AWARDS

- **NSF Graduate Research Fellowship Program (GRFP), 2025 cycle.** Received the NSF GRFP in 2025. 1/2 to receive the award for the study of "Comp/IS/Eng - Computer Security and Privacy," encompassing the range between hardware-level applied security to the complexity-theoretic foundations of cryptography. Award: $159,000 spread across 3 years.
- **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.
- **USENIX'23 Student Travel Grant.** All attendance and (partial) travel costs covered by USENIX'23.
- **The 10'th Heidelberg Laureate Forum + Full Travel Grant.** 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.
- **NSF REU Funding for Summer 2022.** Granted for work on secure multiparty computation advised Prof. Rafail Ostrovsky at UCLA.
- **Outliers 23'.** Participate in competitively selected applied cryptography/web3 focused, VC-backed, summer program.
- **Hack Lodge (sponsored by ETH university) 2023.** Participate in competitively selected applied cryptography/Ethereum ecosystem-focused hacker house.
- **Stanford Blockchain Club Hacker House, Summer 2022.** Participate in SBC hacker house ran by Daniel Marin in SF.

TALKS

- *From CC to PhD: Why You Should Do it and How You Can Achieve it* — October {8, 10}th
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

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

- Organize the CMU crypto seminar with Quang Dao.

Undergraduate Research Mentor Oct 2022 - present
Cryptography research at UCLA

- Mentor Felix Adena on cryptography research: implementing privacy-preserving, money laundering detection protocols in `C++`.
- Mentor Nakul Khambhati on cryptography research: proving lower bounds on sublinear message complexity information-theoretic MPC in the many-server model.
- Mentor Stephen Kelman on cryptography research: implementing high-performance, novel MPC protocols in `C++` (3 party malicously secure DORAM).

Founder & Organizer Sep 2022 - May 2023
Theory@UCLA

- Found and organize the Theory@UCLA, UCLA's (first?) theoretical computer science community. Meet on a weekly basis, to discuss various readings in theoretical computer science.
- The Guild continues in Fall'23 under Nakul Khambhati's leadership.

How-to-Research Advising and Programming May 2023 - Sep 2023
UCLA Undergraduate Research Center

- Created how-to-research programming for UCLA students and participated in office hours.

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.
- Invited to speak at the Engineering Transfer Day Research Panel (only current undergraduate) at UCLA Engineering Transfer Day.
- Research-oriented talk Las Positas / Chabot Community College (expected, December 2023)

WORK EXPERIENCE

Teaching Assistant Jan 2024 - June 2024
University of Pennsylvania

- TA Prof. Pratyush Mishra Cryptography (CIS 5560) course.

Research Assistant September 2023 - present
University of Pennsylvania, University of California, Los Angeles

- Work with Prof. Brett Falk and Prof. Pratyush Mishra (UPenn) in the interface of cryptography and coding theory.
- Member of Penn's Security and Privacy Lab
- Jan.–Mar. 2024, also sponsored by Prof. Rafail Ostrovsky (UCLA).

REU Researcher September 2023 - present
University of California, Los Angeles, sponsored by the National Science Foundation

- Cryptography research Summer 2022, Summer 2023 with Prof. Rafail Ostrovsky at UCLA.

STEM Tutor July 2019 - March 2021
Matan's Tutoring Business & Pleasanton Unified School District *Pleasanton, CA*

- Independently tutor middle and high school students primarily in math, but also in biology, programming, and history.
  - Over the entire period, had about 7 students, on average meeting with 3 students a week, each for an hour.
- Tutored for the Pleasanton Unified School District
  - Tutor at Fairlands Elementary School after-school program, twice a week during the 2019 schoolyear until COCIV (march 2019).
  - Tutor at summer school 2019 for English and math.

Founder, Designer, Advertiser, ... June 2019 - June 2020
RAWGNARLY! (fashion brand) *Pleasanton, CA*

- Founded and operated RAWGNARLY! a fashion brand all about having not-too-serious fun with your friends.
- Sold about 120 garments, both locally in Pleasanton (about 100) and all across the US (about 20).
- Designed garments, photographed lookbooks, created advertisements, built website, negotiated with vendors (US & abroad).

Sales Associate, Pizzaboy August 2018 - May 2019
Skechers & Pizza Guys *Livermore, Pleasanton, CA*

- Retail associate at Skechers Footwear at the Livermore outlets and pizza boy at Pizza Guys' Pleasanton branch.

RELEVANT COURSEWORK

- *CMU*: Graduate discrete math, graduate randomized algorithms.
- *UPenn*: Theory and practice of succinct proofs, 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.