617-365-0958
Cambridge, MA
akarchmer0@gmail.com

Ari Karchmer

Academic webpage:
https://arikarchmer.com

Current Appointment

- **Postdoctoral Fellow**, *Harvard University.* July 2024 – present

Area of study: Data-centric AI/ML
Host: professor Seth Neel.

Education

- **Ph.D. in Computer Science**, *Boston University.* 2018 — 2024

Dissertation: On Learning from Lower Bounds.
Supervisor: professor Ran Canetti.

- **B.S. in Mathematics and Computer Science**, *Brandeis University.* 2015 — 2018

Awards

- **Best Student Paper**—ITCS 2024
- **Selected for Spotlight presentation** (3.5% of submissions)—ICML 2024

Previous Positions

- **Research and Teaching Fellow** 2018 — present
  Dept. Computer Science, Boston University. *Boston, MA*
- **Visiting Researcher** Jan 2023 — June 2023
  Simons Institute for the theory of computing, UC Berkeley. *Berkeley, CA*
- **ML Research Fellow** Sep 2019 — Dec 2019
  WarnerMedia, Applied Analytics. *Boston, MA*

Publications

- Karchmer, Ari. On Stronger Computational Separations Between Multimodal and Unimodal Machine Learning. To appear in *International Conference on Machine Learning* (**ICML** 2024). PMLR. **Spotlight presentation.**

- Karchmer, Ari. Agnostic Membership Query Learning with Nontrivial Savings: New Results, Techniques. In *35th International Conference on Algorithmic Learning Theory* (**ALT** 2024). PMLR.

- Karchmer, Ari. Distributional PAC-Learning from Nisan's Natural Proofs. In *15th Innovations in Theoretical Computer Science Conference* (**ITCS** 2024). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik. **Winner of ITCS Best Student Paper award. Invited for publication at TheoretiCS.**

• Karchmer, Ari. Theoretical Limits of Provable Security Against Model Extraction by Efficient Observational Defenses. In *2023 IEEE Conference on Secure and Trustworthy Machine Learning* (**SaTML**, 2023). IEEE.

• Canetti, Ran & Karchmer, Ari. Covert Learning: How to Learn with an Untrusted Intermediary. In *Theory of Cryptography: 19th International Conference* (**TCC** 2021). Springer. **Invited to Journal of Cryptology special issue.**

Teaching Fellowships

• **Teaching fellow, CDS 682: Responsible AI, Law, Ethics and Society** Spring 2022
Boston University
with Shlomi Hod et al.

• **Teaching fellow, CS 558: Network Security** Spring 2019
Boston University
with professors Ran Canetti and Sharon Goldberg.

• **Teaching fellow, CS 235: Algebraic Algorithms** Spring 2018
Boston University
with professor Leonid Levin.

Invited Talks

• **SAFR AI Lab Seminar, Harvard University, Cambridge, MA** 2024
Undetectable Model Stealing and more with Covert Learning

• **Vector Institute, Toronto, CA** 2024
Cryptography and Complexity Theory in the Design and Analysis of ML

• **CIS Seminar, MIT, Cambridge, MA** 2024
Distributional PAC-learning from Nisan's Natural Proofs

• **Algorithms Seminar, Google Research, Mountain View, CA** 2024
Undetectable Model Stealing and more with Covert Learning

• **Encryption for Secure Search and other Algorithms (ESSA 2023), Bertinoro, Italy** 2023
Covert Learning and its Applications

• **Simons Institute, UC Berkeley, Berkeley, CA** 2023
New Approaches to Heuristic Learning vs PRFs

• **Privacy-preserving ML workshop, CRYPTO, Santa Barbara, CA** 2022
On the Limits of Provable Security Against Model Extraction

• **Charles River Crypto Day, MIT, Cambridge, MA** 2021
Covert Learning: How to Learn with an Untrusted Intermediary

Skills

• **Tools and Languages** Python, especially ML workflows (e.g. PyTorch, Pandas, Scikit-learn).

• **Core Competencies** Quantitative methods (e.g. analysis of algorithms, theory of machine learning, natural language processing, probability, linear algebra, many other advanced methods in theoretical computer science research). Technical research. Technical writing, and public speaking.

MISCELLANEOUS

Played on varsity soccer team for 3 years at Brandeis University. Fluent in Spanish.