617-365-0958
Cambridge, MA
arika@bu.edu

Ari Karchmer

Computer Science Ph.D.

Academic webpage:
https://arikarchmer.com

Final-year Ph.D. candidate in computer science at Boston University, with experience delivering multidisciplinary research from end-to-end. Research contributions advancing foundational understanding of machine learning theory, cryptography, and complexity theory. Further contributions in ML security with the discovery of new attacks and vulnerabilities in ML systems. Academic accomplishments include several published works and manuscripts, invited talks across the United States and in Europe, and a best student paper award at ITCS'24.

Education

Ph.D. Computer Science, *Boston University.* 2018 — June 2024 (expected)
Supervisor: Ran Canetti.

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

Research Publications

On Stronger Computational Separations Between Multimodal and Unimodal Machine Learning. 2024
Ari Karchmer. Submitted for publication.

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

Distributional PAC-Learning from Nisan's Natural Proofs. 2024
Ari Karchmer. 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.

Theoretical Limits of Provable Security Against Model Extraction by Efficient Observational Defenses. 2023
Ari Karchmer. In *2023 IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)*, pages 605–621. IEEE.

Covert Learning: How to Learn with an Untrusted Intermediary. 2021
Ran Canetti and Ari Karchmer. In *Theory of Cryptography: 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8–11, 2021, Proceedings, Part III 19*, pages 1–31. Springer.
Invited to Journal of Cryptology special issue.

Professional Experience

Research and Teaching Fellow 2018 — present
Dept. Computer Science, Boston University *Boston, MA*
Produced multiple solo-authored publications at top-tier CS conferences. Teaching fellow for Algebraic Algorithms, Responsible AI, Cryptography courses. Director of Cryptography research seminar. Peer review for top CS conferences including FOCS, TCC.

Visiting Researcher Jan 2023 — June 2023
Simons Institute for the theory of computing, UC Berkeley. *Berkeley, CA*
Participated in Meta-Complexity research program. Gave talks, proved new theorems connecting complexity theory to ML.

Research Fellow Sep 2019 — Dec 2019
WarnerMedia *Boston, MA*
Participated on a research team focused on recommender systems. Developed a content (e.g. movies) metadata inference system based on compressive sensing techniques, that outperformed previous systems by 25%.

Independent Software Engineer 2018
Co-developed an electronic medical record system for small psychotherapy practices, hosted on Google App Engine. In use at 5 private practices.

Software Engineer Intern May 2017 — Aug 2017
Acadian Asset Management *Boston, MA*

Wrote software for traders to implement business logic and check daily system health.

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.

Awards

ITCS Best Student Paper 2024

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

Distributional PAC-learning from Nisan's Natural Proofs 2024
MIT CIS seminar

Undetectable Model Stealing and more with Covert Learning 2024
Algorithms Seminar, Google Research, MTV

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

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

On the Limits of Provable Security Against Model Extraction 2022
Privacy-preserving ML workshop @ CRYPTO

Covert Learning: How to Learn with an Untrusted Intermediary 2021
Charles River Crypto Day @ MIT

MISCELLANEOUS

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