Ari Karchmer

24 Washburn Avenue Unit 3
Cambridge, Massachusetts, USA, 02140

arikarchmer.com
arika@bu.edu

Education

Boston University — 2018 – Present
PhD. in Computer Science; Advisor: Ran Canetti

Brandeis University — 2015 - 2018
Bachelors degree in Mathematics and Computer Science

Research Papers

Agnostic Membership Query Learning with Nontrivial Savings: New Results and Techniques — 2023
Ari Karchmer
Manuscript, in submission and available by request

Distributional PAC-Learning from Nisan's Natural Proofs — 2023
Ari Karchmer
ECCC Report, in submission

Theoretical Limits of Provable Security Against Model Extraction by Efficient Observational Defenses — 2023
Ari Karchmer
Conference on Secure and Trustworthy Machine Learning Conference (SaTML)

Covert Learning: How to Learn with an Untrusted Intermediary — 2021
Ran Canetti, Ari Karchmer
Theory of Cryptography Conference (TCC); Invited to Journal of Cryptology

Research Experience

Graduate Research Fellow — Jan. 2019 – present
Boston University

Visiting Graduate Student – Meta Complexity Program — Jan. 2023 – May 2023
Simons Institute – Berkeley, CA, USA

Graduate Research Fellow — Sep. 2019 – Dec. 2019
WarnerMedia – Boston, MA

- Participated on a research team focused on recommender systems
- Developed an independent content metadata inference project based on compressive sensing techniques

Teaching Fellowships

Responsible AI, Law, Ethics and Society
Spring 2022, Boston University

Network Security
Fall 2019, Boston University

Algebraic Algorithms
Fall 2018, Boston University

Select Talks

Talk materials (videos, slides) can be found on my personal webpage.

Covert Learning and its Applications
Encryption for Secure Search and other Algorithms workshop (ESSA23)

New Approaches to Heuristic PAC-Learning vs PRFs
Lower Bounds, Learning, and Average-Case Complexity workshop at Simons Institute '23

On The Limits of Provable Security Against Model Extraction
Privacy Preserving ML Workshop at Crypto '22

Covert Learning: How to Learn with an Untrusted Intermediary
Charles River Crypto Day at MIT Nov '21

Professional Service

TCC Reviewer — 2023

FOCS Reviewer — 2023

Directer of BU Cryptography Research Seminar — 2020-2022