

# Ari Karchmer

arika@bu.edu · arikarchmer.com · (617) 365-0958

## Research interests

Cryptography, computational learning theory, meta-complexity, adversarial machine learning, and theoretical computer science broadly.

## Education

- 2018 – Present    **Boston University** – Boston, Massachusetts  
Ph.D. in computer science  
Advisor: Ran Canetti
- 2015 – 2018    **Brandeis University** – Waltham, Massachusetts  
B.S. in mathematics and computer science

## Papers

- 2023    *Theoretical Limits of Provable Security Against Model Extraction by Efficient Observational Defenses*  
Ari Karchmer  
*To appear in the IEEE Conference on Secure and Trustworthy Machine Learning (SATML).*
- 2022    *New Approaches to Heuristic PAC-Learning Via Cryptanalysis*  
Marco Carmosino and Ari Karchmer  
*In submission. Manuscript forthcoming.*
- 2021    *Covert Learning: How to Learn with an Untrusted Intermediary*  
Ran Canetti and Ari Karchmer  
*In Proceedings of the 19<sup>th</sup> Theory of Cryptography Conference (TCC).*  
*Invited to Journal of Cryptology.*

## Research experience

- Jan. 2019 – present    **Boston University, Dept. Computer Science** — Graduate Research Fellow  
BU Security Group
- Sep. 2019 – Dec. 2019    **WarnerMedia Applied Analytics** — Graduate Research Fellow  
Participated on a research team focused on recommender systems. Developed an independent content metadata inference project based on compressive sensing techniques that outperformed previous systems by 35%.

Sep. 2017 – **Brandeis University, Dept. Computer Science** — Undergraduate Research Assistant  
May 2018  
Advisor: Olga Papaemmanouil  
Investigated techniques for predicting the performance and latency of database queries with machine learning. Studied the effect of high variance reward functions on the viability of Thompson sampling for contextual multi-armed bandits.

### Teaching experience

Spring 2022 Teaching fellow, CDS 682: Responsible AI, Law, Ethics and Society (Boston University)  
with Shlomi Hod

Fall 2019 Teaching fellow, CS 558: Network Security (Boston University)  
with professors Ran Canetti and Sharon Goldberg

Fall 2018 Teaching fellow, CS 235: Algebraic Algorithms (Boston University)  
with professor Leonid Levin

### Select Talks

Talk materials are available on my website.

Aug. 2022 *On The Limits of Provable Security Against Model Extraction*  
Privacy Preserving ML Workshop at Crypto '22.

Nov. 2021 *Covert Learning: How to Learn with an Untrusted Intermediary*  
Charles River Crypto Day at MIT.

### Industry experience

May 2017 – **Acadian Asset Management** — Software Engineering Intern — Boston,  
Aug. 2017 Massachusetts

### Professional service

Jan. 2021 – Leading organizer of BU security and cryptography research seminar  
Present