Adam Sealfon

Email: asealfon@berkeley.edu

Employment

UC Berkeley, Statistics department, postdoctoral scholar. September 2019-present. Supervised by Jacob Steinhardt and Michael Jordan.

Education

Massachusetts Institute of Technology, Ph.D in computer science, August 2019. GPA 5.0/5.0. Member of Theory of Computation (ToC) and Cryptography and Information Security (CIS) groups. Advised by Shafi Goldwasser.

Harvard University, S.M. in computer science, May 2013. GPA 4.0/4.0.

Harvard University, A.B. summa cum laude in mathematics, May 2013. GPA 3.97/4.0. Advised by Salil Vadhan.

Stuyvesant High School, Valedictorian, 2009.

Research Overview

My research is on provable guarantees for privacy, robustness and security in machine learning and algorithmic settings.

Selected Awards and Fellowships

Best Student Paper Award, PODS 2016, "Shortest Paths and Distances with Differential Privacy."

Department of Energy Computational Science Graduate Fellow (DOE CSGF), 2014-2018.

NSF Graduate Research Fellowship Program (GRFP) Fellow, 2013-2014

Siebel Scholar, 2012-2013, fellowship awarded for academic excellence and demonstrated leadership.

Seymour E. and Ruth B. Harris Dunster House Prize for combined achievement in academics, character, and extracurricular activities, Harvard University, 2013.

Phi Beta Kappa, early election, 2012.

Intel Science Talent Search Finalist, computer science, 2009, "Complexity Gap between Adaptive and Nonadaptive Algorithms for Property Testing of Hypergraphs."

Publications

1. Inbar Kaslasi, Guy N. Rothblum, Ron D. Rothblum, Adam Sealfon, and Prashant Nalini Vasudevan. Batch verification for statistical zero knowledge proofs. TCC 2020.
2. Adam Sealfon and Jon Ullman. Efficiently estimating Erdős–Rényi graphs with node differential privacy. NeurIPS, 2019. ***Also invited and accepted to Journal of Privacy and Confidentiality (JPC).***
3. Sunoo Park and Adam Sealfon. It wasn't me! Repudiability and (un)claimability of ring signatures. In *Proceedings of the 39th International Cryptology Conference (CRYPTO)*, 2019.
4. Ron D. Rothblum, Adam Sealfon, and Katerina Sotiraki. Towards non-interactive zero-knowledge for NP from LWE. In *22nd IACR International Conference on Practice and*

Theory of Public-Key Cryptography (PKC), 472-503, 2019. ***Also invited and accepted to Journal of Cryptology (JoC).***

5. Shafi Goldwasser, Rafail Ostrovsky, Alessandra Scafuro, and Adam Sealfon. Population stability: regulating size in the presence of an adversary. *Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing (PODC)*, 397-406, 2018.
6. Ranjit Kumaresan, Srinivasan Raghuraman, and Adam Sealfon. Network oblivious transfer. *Proceedings of the 36th International Cryptology Conference (CRYPTO)*, 366-396, 2016.
7. Adam Sealfon. Shortest paths and distances with differential privacy. *Proceedings of the 35th ACM Symposium on Principles of Database Systems (PODS)*, 29-41, 2016. ***Recipient of Best Student Paper award.***
8. Gilad Braunschvig, Alon Brutzkus, David Peleg, and Adam Sealfon. Truth tellers and liars with fewer questions. *Discrete Mathematics* 338(8): 1310-1316, 2015.
9. Gilad Braunschvig, Shiri Chechik, David Peleg, and Adam Sealfon. Fault tolerant additive and (μ,α) spanners. *Theoretical Computer Science* 580: 94-100, 2015.
10. Adam Sealfon and Katerina Sotiraki. Agreement in partitioned dynamic networks (brief announcement). *Proceedings of the 28th International Symposium on Distributed Computing (DISC)*, 555-556, 2014.

Teaching

Fall 2016: With Aloni Cohen, Justin Holmgren and Sunoo Park, developed and taught MIT 6.889: Advanced Topics in the Theory of Cryptography, a topics course targeted at students who have already taken a graduate-level cryptography class.

Spring 2016: Teaching assistant for MIT 6.875: Cryptography and Cryptanalysis, an introductory graduate cryptography class.

Invited Talks

1. Population stability: regulating size in the presence of an adversary. Boston University Security Seminar, Boston, MA 12/6/2017; Harvard/MIT/MSR Theory Reading Group, Cambridge, MA 3/9/2018.
2. Network oblivious transfer. MIT Cryptography and Information Security Seminar, Cambridge, MA 3/11/2016; Simons Institute Cryptography Reunion Workshop, Berkeley, CA 9/12/2016; Northeastern University Theory Seminar, Boston, MA 2/16/2017; Brown University Cryptography and Security Seminar, Providence, RI 4/3/2017.
3. Interactive and zero-knowledge proofs. MathILy (mathematical summer program for gifted high school students), Bryn Mawr, PA 7/30/2015.

Research Visits and Internships

Visiting graduate student at the **Simons Institute** program on **"Data Privacy: Foundations and Applications,"** spring 2019, and **"Foundations of Deep Learning,"** summer 2019.

Visitor at **Interdisciplinary Center Herzliya (IDC)** and **Tel Aviv-Yafo Technical College (MTA)**, summer 2017. Research in cryptography with Alon Rosen and Adi Akavia.

Intern at **Lawrence Berkeley National Laboratory**, summer 2015. Research in parallel graph algorithms with Aydın Buluç.

Visiting student at **Weizmann Institute of Science**, spring 2015. Research in cryptography with Shafi Goldwasser.

Weizmann Institute Kupcinet-Getz Summer Science Program participant, summer 2012. Research in graph theory, algorithms, distributed computing, and combinatorics with David Peleg.

OUTREACH AND SERVICE

Program committee, TPDP 2020

Reviewer for FOCS, NeurIPS, PODC, PODS, EUROCRYPT, CRYPTO, TCC, CCS, PKC, ICALP.

With Aloni Cohen and Sunoo Park, wrote two **popular science columns**, "Can you even find this puzzle?" and "Can you think like a bar code?", published in the Ideas section of the Boston Globe (January 15, 2017 and September 8, 2017). The articles contained puzzles introducing ideas from cryptography and other areas of computer science.

Since 2010, have given **guest lectures** in math research and math team classes at Stuyvesant High School.

Active alumnus, 2009 **teaching assistant** and frequent **general helper** at the Research Science Institute (RSI) research-based summer program at MIT for gifted high school students, where my roles over many years have included assisting in research mentorship, providing feedback on papers and presentations, serving on the 2016 final presentation judging panel, and meeting with students both as a group and one-on-one.