Aloni Cohen

www.aloni.net · aloni@uchicago.edu · March 13, 2024

Education

Massachusetts Institute of Technology June 2019
Ph.D., Electrical Engineering and Computer Science, June 2019
Advisor: Shafi Goldwasser
Thesis: New Guarantees for Cryptographic Circuits and Data Anonymization

Massachusetts Institute of Technology June 2015
S.M., Computer Science and Engineering, June 2015
Advisor: Shafi Goldwasser
Thesis: Pseudorandom Functions with Structure: Extensions and Implications

University of California, Berkeley December 2012
B.S., Electrical Engineering and Computer Science
B.S., Engineering Mathematics and Statistics

Employment

Assistant Professor January 2022 – present
Department of Computer Science
Data Science Institute

Postdoctoral Associate August 2019 – December 2021
Hariri Institute for Computing at Boston University
Boston University School of Law

Research Intern Summer 2016
Microsoft Research New England

Publications

Publications are listed in chronological order. Authors are listed in alphabetical order as is customary in theoretical computer science, except where indicated by an asterisk. Scientific journals are underlined. Publications marked "Best Paper" received the highest award conferred for research at the corresponding conference.

Computer Science (Journals and Peer-Reviewed Conferences)

1. Faster Optimal Planning with Partial Order Pruning
   *David Leo Wright Hall, Aloni Cohen, David Burkett, Dan Klein
   International Conference on Automated Planning and Scheduling (ICAPS), 2013

2. Aggregate Pseudorandom Functions and Connections to Learning
   Aloni Cohen, Shafi Goldwasser, Vinod Vaikuntanathan
   Theory of Cryptography Conference (TCC), 2015

3. Multilinear Pseudorandom Functions
   Aloni Cohen, Justin Holmgren
   International Colloquium on Automata, Languages, and Programming (ICALP), 2015

4. The GGM Function Family Is a Weakly One-Way Family of Functions
   Aloni Cohen, Saleet Klein
   Theory of Cryptography Conference (TCC), 2016

5. Cryptography with Updates
   Prabhanjan Ananth, Aloni Cohen, Abhishek Jain
   International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2017

6. Watermarking Cryptographic Capabilities
   Aloni Cohen, Justin Holmgren, Ryo Nishimaki, Vinod Vaikuntanathan, Daniel Wichs
   SIAM Journal on Computing, 47(6), 2018
   Symposium on Theory of Computing (STOC), 2016

7. What About Bob? The Inadequacy of CPA Security for Proxy Re-encryption
   Aloni Cohen
   International Workshop on Public Key Cryptography (PKC), 2019

8. From Soft Classifiers to Hard Decisions: How Fair Can We Be?
   Ran Canetti, Aloni Cohen, Nishanth Dikkala, Govind Ramnarayan, Sarah Scheffler, Adam Smith
   Conference on Fairness, Accountability, and Transparency (FAccT), 2019

9. Linear Program Reconstruction in Practice
   Aloni Cohen, Kobbi Nissim
   Journal of Privacy and Confidentiality, 10(1), 2020

10. Towards Formalizing the GDPR Notion of Singling Out
    Aloni Cohen, Kobbi Nissim
    Proceedings of the National Academy of Sciences (PNAS), 117(15), 2020

11. Census TopDown: Investigating the Impacts of Differential Privacy on Redistricting
    Aloni Cohen, Moon Duchin, JN Matthews, Bhushan Suwal
    Symposium on the Foundations of Responsible Computing (FORC), 2021

12. Private Numbers in Public Policy: Census, Differential Privacy, and Redistricting
    Aloni Cohen, Moon Duchin, JN Matthews, Bhushan Suwal
    Harvard Data Science Review, 2022

13. Attacks on Deidentification's Defenses
    Aloni Cohen
    USENIX Security Symposium, 2022 (**Best Paper**)

14. Multi-Regulation Computing: Examining the Legal and Policy Questions that Arise from Secure Multiparty Computation
    *Mayank Varia, Aloni Cohen, Andrew Sellars, Azer Bestavros
    ACM Symposium on Computer Science and Law, 2022

15. Can the Government Compel Decryption? Don't Trust — Verify
Aloni Cohen, Sarah Scheffler, Mayank Varia
ACM Symposium on Computer Science and Law, 2022

16. Control, Confidentiality, and the Right to be Forgotten
Aloni Cohen, Adam Smith, Marika Swanberg, Prashant Nalini Vasudevan
ACM Conference on Computer and Communications Security (CCS), 2023

17. Private PAC Learning May Be Harder than Online Learning
Mark Bun, Aloni Cohen, Rathin Desai
International Conference on Algorithmic Learning Theory (ALT), 2024 (**Best Paper**)

Law Review Articles

18. Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries
Aloni Cohen, Sunoo Park
Harvard Journal of Law & Technology, 32, 2018

19. What a Hybrid Legal-Technical Analysis Teaches Us About Privacy Regulation: The Case of Singling Out
Micah Altman, Aloni Cohen, Kobbi Nissim, Alexandra Wood
Boston University Journal of Science & Technology Law, 27(1), 2021

Manuscripts

A Principled Approach to Defining Anonymization as Applied to EU Data Protection Law
Micah Altman, Aloni Cohen, Francesca Falzon, Evangelia Anna Markatou, Kobbi Nissim, Michel Jose Reymond, Sidhant Saraogi, Alexandra Wood

Secure Data Distribution in Wireless Networks using Proxy Re-Encryption
Aloni Cohen, David Cousins, Nicholas Genise, Yuriy Polyakov, Saraswathy RV

Invited Articles

Data Protection's Composition Problem
*Aaron Fluitt, Aloni Cohen, Micah Altman, Kobbi Nissim, Salome Viljoen, Alexandra Wood
European Data Protection Law Review, 5(3), 2019

Other

Toward a 21st Century National Data Infrastructure: Managing Privacy and Confidentiality Risks with Blended Data (Consensus Study Report)
Panel on Approaches to Sharing Blended Data in a 21st Century Data Infrastructure (*editors Jerome P. Reiter, Jennifer Park*)
Committee on National Statistics, National Academies of Sciences, Engineering, and Medicine, 2024

Policy Comments and Briefs

Comment on Proposed CCPA Regulations,
Aloni Cohen
First 15-Day Comment Period, 2019

Comment on Proposed CCPA Regulations
Aloni Cohen
45-Day Comment Period, 2019

Amicus Brief of Data Privacy Experts
Ryan Calo, Ran Canetti, Aloni Cohen, Cynthia Dwork, Roxana Geambasu, Somesh Jha, Nitin Kohli, Aleksandra Korolova, Jing Lei, Katrina Ligett, Deirdre K. Mulligan, Omer Reingold, Aaron Roth, Guy N. Rothblum, Benjamin Rubinstein, Aleksandra (Sesa) Slavkovic, Adam Smith, Kunal Talwar, Salil Vadhan, Larry Wasserman, Daniel J. Weitzner
State of Alabama v United States Department of Commerce, 2021

RFI Response: Privacy-Enhancing Technologies
Micah Altman, Aloni Cohen, Salil Vadhan
RFI on Advancing Privacy-Enhancing Technologies
Science and Tehchnology Policy Office, Federal Register Notice 87 FR 35250, 2022

Comments from Researchers at Boston University and the University of Chicago
Ran Canetti, Aloni Cohen, Chris Conley, Stacey L. Dogan, Marco Gaboardi, Woodrow Hartzog, Rory Van Loo, Christopher T. Roberston, Katharine Baird Silbaugh
AI Accountability Policy RFC
National Telecommunications and Information Administration, Federal Register Notice 88 FR 22433, 2023

Popular Press

Can you Even Find This Puzzle
Aloni Cohen, Sunoo Park, Adam Sealfon
The Boston Globe, 2017

Can You Think Like a Bar Code?
Aloni Cohen, Sunoo Park, Adam Sealfon
The Boston Globe, 2017

CCPA, Cross-Device Tracking, and Probabilistic Identifiers
Aloni Cohen
Protego Press, 2019

The Boldest American Consumer Privacy Statute in a Generation is in Flux
Aloni Cohen
Protego Press, 2020

Grants (PI or co-PI)

Optimized Relations Auditing for Compliance with Laws and Ethical Statements (ORACLES)

DARPA, 2020 – 2024

Investigating the Impact of Census' Disclosure Avoidance System on Marginalized Communities
Boston University Center for Antiracist Research, 2021 – 2022

Institute for Data, Econometrics, Algorithms and Learning (IDEAL)
NSF, 2022 – 2027

Posterior Inference from Noisy Census Data
University of Chicago Data Science Institute, 2023 – 2024

Honors and Awards

Tau Beta Pi, 2009 – 2012

UC Berkeley Departmental Citation Award, 2012

National Science Foundation Graduate Research Fellowship, 2014 – 2018

Facebook Fellowship, 2018 – 2019

Berkman Klein Center for Internet & Society Affiliate, 2018 – 2020

Aspen Technology Policy Fellow, Summer 2019

Distinguished Paper Award, USENIX Security Symposium, 2022

Outstanding Paper Award, Algorithmic Learning Theory (ALT), 2024

Recognition

Cited in petition for writ of certiorari in *Pennsylvania v Davis*, 2020

Cited in Department of Justice motion in *State of Alabama v United States Department of Commerce*, 2021

"New system to protect census data may compromise accuracy, some experts say", Washington Post, 2021

"Common Deidentification Methods Don't Fully Protect Data Privacy", ACM TechNews, 2022

Invited Talks

2015 Simons Institute for the Theory of Computing
Greater Tel Aviv Area Cryptography Seminar
Weizmann Institute of Science Theory Lunch
Technion Theory Lunch
MIT Cryptography and Information Security Seminar

2016 New York Crypto Day
MIT Cryptography and Information Security Seminar

2017 Oberwolfach Workshop on Cryptography
MIT Cryptography and Information Security Seminar

2018 AEGIS EU-US Roundtable on the Interplay of Technology and Policy in Data Privacy
Differential Privacy Meets Multi-Party Computation Workshop
Simons Institute for the Theory of Computing
Boston University Cyber Alliance

2019 Simons Institute for the Theory of Computing
Differential Privacy Meets Multi-Party Computation Workshop
Charles River Crypto Day
Privacy Tools Project Retreat
Stanford Security Lunch

2020 DIMACS Workshop on Co-development of Computing and Law
Northwestern CS+X Colloquium Series

2021 Northwestern Law+Computation Symposium
Harvard Privacy Tools Project Bridging Privacy Definitions Working Group

2022 CS+Law Research Workshop
University of Chicago MSCAPP Speaker Series
Simons Institute: Data Privacy Foundations and Applications Reunion Workshop
Simons Institute: Workshop on Societal Considerations and Applications
Boston Differential Privacy Summer School Google Research Privacy Seminar

2023 CS+Law Research Workshop
6th HomomorphicEncryption.org Standards Meeting (canceled for medical reasons)
2nd Workshop on PETs for the Public Interest (canceled for medical reasons)
UCLA Synthetic Data Workshop (**Keynote**)
Workshop on Trust Perspectives in Machine Learning, Law and Public Policy

---

Service

Organizer

Co-organizer "Data Privacy: Academia, Industry, Policy, and Society"
(NeurIPS, December 2020)
Steering Committee, CS+Law Research Workshop (monthly, 2021–2023)
Co-chair, Theory and Practice of Differential Privacy Workshop (2023)
Co-chair, Theory and Practice of Differential Privacy Workshop (2024)
Publicity Chair, ACM Symposium on Computer Science and Law (2024)

Editorial Board

Harvard Data Science Review (HDSR), Associate Editor, 2023–
Journal of Privacy and Confidentiality (JPC), 2023–2024

Program Committee Member

ACM Symposium on Computer Science and Law, 2019
International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2020
Theory of Cryptography Conference (TCC), 2020
Conference on Fairness, Accountability, and Transparency (FAccT), 2021 (**Area Chair: Security and Privacy**)
Symposium on Foundations of Responsible Computing (FORC), 2021
IEEE European Symposium on Security and Privacy (EuroS&P), 2022
Symposium on Foundations of Responsible Computing (FORC), 2022
Symposium on Applications of Contextual Integrity, 2022
ACM Conference on Computer and Communications Security (CCS), 2022
ACM Conference on Computer and Communications Security (CCS), 2023 (**Top Reviewer Award**)
Symposium on Foundations of Responsible Computing (FORC), 2023
ACM Symposium on Computer Science and Law, 2024
IEEE Conference on Secure and Trustworthy Machine Learning (SaTML), 2024
ACM Conference on Computer and Communications Security (CCS), 2024
Symposium on Foundations of Responsible Computing (FORC), 2024

Journal Reviewer

Journal of Cryptology
Journal of Privacy and Confidentiality (JPC)
Journal of the ACM (JACM)
Proceedings of the National Academy of Sciences (PNAS)
Journal of Machine Learning Research (JMLR)

Departmental Service

Faculty Search Student Committee, MIT, 2016
Graduate Student Admissions Committee, University of Chicago, 2022–23
External Relations Committee, University of Chicago, 2022–
Committee on Data Science Proposal Committee, University of Chicago, 2023–24
Graduate Student Affairs Committee, University of Chicago, 2023–

Advising

Doctoral students

Christian Cianfarani, 2022–present
JN Matthews, 2022–present
Gabe Schoenbach, 2022–present

Doctoral thesis committees

Francesca Falzon, University of Chicago, 2023
Akshima, University of Chicago, 2023

Emily Wenger, University of Chicago, 2023
Jesse Stern, University of Chicago, 2024
Alex Hoover, University of Chicago, 2024

Teaching

The Beauty and Joy of Computing *(Teaching Assistant in Training)* — Fall 2010
University of California, Berkeley

Cryptography and Cryptanalysis *(Teaching Assistant)* — Spring 2015
Massachusetts Institute of Technology

Advanced Topics in Cryptography *(Co-instructor)* — Fall 2016
Massachusetts Institute of Technology

Law for Algorithms *(Co-instructor)* — Fall 2019
Cross-listed at Boston University School of Law
Boston University Computer Science
University of California, Berkeley Computer Science

Law for Algorithms *(Co-instructor)* — Spring 2021
Cross-listed at Boston University School of Law
Boston University Computer Science

Topics in Privacy: Privacy, Policy, and the US Census — Winter 2022
University of Chicago, CSMC 33211

Introduction to Cryptography — Spring 2022
University of Chicago, CSMC 28400

Introduction to Cryptography — Autumn 2022
University of Chicago, CSMC 28400

Advanced Topics in Law & Computing *(Co-instructor)* — Spring 2023
University of Chicago, CSMC 33221, LAWS 53472-1, DATA 33221

Introduction to Cryptography — Winter 2024
University of Chicago, CSMC 28400