Harvard University
John A. Paulson School of Engineering and Applied Sciences

Science and Engineering Complex (SEC) 3.327
150 Western Avenue
Boston, MA 02134 USA
salil_vadhan@harvard.edu
http://salil.seas.harvard.edu/

Salil Vadhan
Vicky Joseph Professor
of Computer Science
& Applied Mathematics

Salil P. Vadhan

Curriculum Vitae

February 2026

Contents

Research Interests

- Computational Complexity, Data Privacy, Randomness in Computation, Cryptography.

Current Positions

Harvard University — Cambridge, MA

- Vicky Joseph Professor of Computer Science and Applied Mathematics (with tenure), Harvard John A. Paulson School of Engineering and Applied Sciences, July 2009–present.

Previous Positions

Bocconi University — Milan, Italy

- Visiting Researcher, Department of Computing Sciences, April 2024–June 2024.

University of Sydney — Sydney, Australia

- Visiting Researcher, School of Computer Science and Sydney Mathematical Research Institute, January 2024–March 2024.

National Chiao-Tung University — Hsinchu, Taiwan

- Visiting Chair Professor, Department of Applied Mathematics and Shing-Tung Yau Center, August 2015–July 2016.

Stanford University — Stanford, CA

- Visiting Scholar, August 2011–July 2012.

Microsoft Research Silicon Valley — Mountain View, CA

- Consultant, June 2008–July 2008 and in June 2010.
- Visiting Researcher, August 2011–July 2012.

University of California, Berkeley — Berkeley, CA

- Miller Visiting Professor, September 2007–June 2008.

Harvard University — Cambridge, MA

- Harvard College Professor, 2016–2021
- Area Chair for Computer Science, July 2017–June 2019. (Co-chair with Michael Mitzenmacher from July 2018-June 2019.)
- Director, Harvard Center for Research on Computation and Society (CRCS), August 2008–July 2011, January 2014–April 2015.

- Gordon McKay Professor of Computer Science and Applied Mathematics (with tenure), January 2007–June 2009.
- Thomas D. Cabot Associate Professor of Computer Science, July 2004–December 2006.
- Assistant Professor of Computer Science on the Gordon McKay Endowment, Division of Engineering & Applied Sciences, January 2001–June 2004.
- Fellow, Radcliffe Institute for Advanced Study, Fall 2003. Chair of 2003–04 Radcliffe Cluster on Randomness and Computation.

Institute for Advanced Study — Princeton, NJ

- Visitor, School of Mathematics, September 2000–April 2001.
- Host: Professor Avi Wigderson

Massachusetts Institute of Technology — Cambridge, MA

- NSF Mathematical Sciences Postdoctoral Fellow, September 1999–August 2000.
- Supervisor: Professor Madhu Sudan

Education

Massachusetts Institute of Technology — Cambridge, MA

- Ph.D. in Applied Mathematics, August 1999.
- Advisor: Professor Shafi Goldwasser.
- Thesis: *A Study of Statistical Zero-Knowledge Proofs.*

Churchill College, Cambridge University — Cambridge, England

- Certificate of Advanced Study in Mathematics, *with Distinction*, June 1996. (Part III of the Mathematical Tripos.)

Harvard University — Cambridge, MA

- A.B., *summa cum laude*, in Mathematics and Computer Science, June 1995.
- Advisor: Professor Leslie Valiant.
- Thesis: *The Complexity of Counting.*

Honors

- *Test of Time Award* at CCC 2026 for "Unbalanced Expanders and Randomness Extractors from Parvaresh-Vardy Codes" (with Venkatesan Guruswami and Christopher Umans, CCC 2007).
- *Best Poster/Demo* at NYC Privacy Day 2025 for "Practitioners' Perspectives on a Differential Privacy Deployment Registry" (with Elena Ghazi and Priyanka Nanayakkara).

- *Outstanding Paper Award* at TCC 2025 for "Generalized and Unified Equivalences between Hardness and Pseudoentropy" (with Lunjia Hu).
- Elected to the *American Academy of Arts & Sciences*, 2025.
- *Test of Time Award* at TCC 2024 for "Notions of Reducibility Between Cryptographic Primitives" (with Omer Reingold and Luca Trevisan, TCC 2004).
- *Distinguished Artifact Award* at CCS 2024 for code accompanying the paper "A Framework for Differential Privacy Against Timing Attacks" (with Zachary Ratliff).
- *Distinguished Paper Award* at CCS 2023 for "Concurrent Composition for Interactive Differential Privacy with Adaptive Privacy-Loss Parameters" (with Samuel Haney, Michael Shoemate, Grace Tian, Andrew Vyrros, Vicki Xu, and Wanrong Zhang).
- Co-recipient of 2019 *Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies* for the paper "Bridging the Gap between Computer Science and Legal Approaches to Privacy" (with K. Nissim, A. Bembenek, A. Wood, M. Bun, M. Gaboardi, U. Gasser, D. O'Brien, and T. Steinke).
- *ACM Fellow*, 2018–present.
- *Harvard College Professor*, 2016–2021.
- *Simons Investigator*, August 2013–July 2017, August 2019–present.
- *SIAM Outstanding Paper Prize 2011* for paper "Statistically Hiding Commitments and Statistical Zero-Knowledge Arguments from any One-Way Function" (with Iftach Haitner, Minh Nguyen, Shien Jin Ong, and Omer Reingold).
- *Gödel Prize 2009* for paper "Entropy Waves, the Zig-Zag Graph Product and New Constant-Degree Expanders" (with Omer Reingold and Avi Wigderson).
- *Guggenheim Fellowship*, August 2007–July 2008.
- *Miller Visiting Professorship*, UC Berkeley, January 2008–May 2008.
- *Best Paper Award* at CCC 2007 for "Unbalanced Expanders and Randomness Extractors from Parvaresh–Vardy Codes" (with Venkatesan Guruswami and Christopher Umans).
- *Best Paper Award* at Eurocrypt 2007 for "Zero Knowledge and Soundness are Symmetric" (with Shien Jin Ong).
- 2006 Pazy Memorial Research Award from US–Israel Binational Science Foundation (with Omer Reingold and Luca Trevisan).
- *ONR Young Investigator Award*, June 2004–May 2007.
- *Phi Beta Kappa Award for Excellence in Teaching*, June 2004.
- *Radcliffe Institute Fellowship*, September 2003–January 2004.

- *Alfred P. Sloan Research Fellowship*, September 2002–September 2004.
- *NSF Early Career Development Award*, June 2002–May 2007.
- Nominated for *Everett Mendelsohn Award for Excellence in Mentoring*, Spring 2006.
- *ACM Doctoral Dissertation Award 2000* for the best Ph.D. thesis in computer science.
- *George M. Sprowls Award* (co-winner) for best Ph.D. thesis in Electrical Engineering and Computer Science at MIT.
- *NSF Mathematical Sciences Postdoctoral Fellowship*, September 1999–December 2000.
- Papers invited (and submitted) to special issues:
  - "Concurrent composition for interactive differential privacy with adaptive privacy-loss parameters" (with Samuel Haney, Michael Shoemate, Grace Tian, Salil Vadhan, Andrew Vyrros, Vicki Xu, and Wanrong Zhang), selected among papers at *TPDP '23* for invitation to *J. Privacy & Confidentiality*.
  - "Concurrent Composition of Differential Privacy" (with Tianhao Wang), selected among papers at *TCC '21* for invitation to *J. Cryptology*.
  - "Limitations of the Impagliazzo–Nisan–Wigderson Pseudorandom Generator against Permutation Branching Programs" (with William Hoza and Ted Pyne), invited to *Algorithmica* Special Issue on COCOON '21.
  - "Pseudodistributions that Beat All Pseudorandom Generators" (with Ted Pyne), invited to *Theory of Computing* Special Issue on CCC '21.
  - "Deterministic Approximation of Random Walks in Small Space" (with Jack Murtagh, Omer Reingold, and Aaron Sidford), invited to *Theory of Computing* Special Issue on RANDOM '19.
  - "Derandomization Beyond Connectivity: Undirected Laplacian Systems in Nearly Logarithmic Space (with Jack Murtagh, Omer Reingold, and Aaron Sidford), invited to *SIAM Journal on Computing* Special Issue on FOCS '17.
  - "Differential Privacy on Finite Computers" (with Victor Balcer), invited to *Journal of Privacy and Confidentiality* Special Issue on TPDP '17.
  - "Fingerprinting Codes and the Price of Approximate Differential Privacy" (with Mark Bun and Jonathan Ullman), invited to *SIAM Journal on Computing* Special Issue on STOC '14.
  - "Pseudorandomness and Fourier Growth Bounds for Width 3 Branching Programs" (with Thomas Steinke and Andrew Wan), invited to *Theory of Computing* Special Issue on APPROX/RANDOM '14.
  - "PCPs and the Hardness of Generating Private Synthetic Data" (with Jon Ullman), invited to *Journal of Cryptology* selected papers from TCC '11.
  - "Efficiency Improvements in Constructing Pseudorandom Generators from One-Way Functions" (with Iftach Haitner and Omer Reingold), accepted to *SIAM Journal of Computing* Special Issue on STOC '10.

- "Deterministic Extractors for Small-Space Sources" (with Jesse Kamp, Anup Rao, and David Zuckerman), in *Journal of Computer and System Sciences* Special Issue to celebrate Richard Karp's Kyoto Prize.
- "Are PCPs Inherent in Efficient Arguments?" (with Guy Rothblum), in *Computational Complexity* Special Issue on CCC '09.
- "Statistical Zero-Knowledge Arguments for NP from Any One-Way Function" (with Minh Nguyen and Shien Jin Ong), in *SIAM Journal on Computing* Special Issue on FOCS '06.
- "The Round Complexity of Random Selection" (with Saurabh Sanghvi), in *SIAM Journal on Computing* Special Issue on STOC '05.
- "Compression of Samplable Sources" (with Luca Trevisan and David Zuckerman), in *Computational Complexity* Special Issue on CCC '04.
- "An Unconditional Study of Computational Zero Knowledge," in *SIAM Journal on Computing* Special Issue on Randomness & Complexity.
- "Robust PCPs of Proximity, Short PCPs, and Applications to Coding" (with Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, and Madhu Sudan), in *SIAM Journal on Computing* Special Issue on Randomness & Complexity.
- "Using Nondeterminism to Amplify Hardness" (with Alex Healy and Emanuele Viola), in *SIAM Journal on Computing* Special Issue on STOC '04.
- "Lower Bounds for Non-Black-Box Zero Knowledge" (with Boaz Barak and Yehuda Lindell), in *Journal of Computer and System Sciences* Special Issue on FOCS '03.
- "On Constructing Locally Computable Extractors and Cryptosystems in the Bounded Storage Model" in *Journal of Cryptology* Special Issue on the Bounded Storage Model.
- "Pseudorandom Generators without the XOR Lemma" (with Madhu Sudan and Luca Trevisan) in *Journal of Computer and System Sciences* Special Issue on CCC '99.
- "Extracting All the Randomness and Reducing the Error in Trevisan's Extractors" (with Ran Raz and Omer Reingold), in *Journal of Computer and System Sciences* Special Issue on STOC '99.

- *Charles W. and Jennifer C. Johnson Prize* (co-winner) for best paper among MIT Department of Mathematics Graduate Students ("A Complete Promise Problem for Statistical Zero-Knowledge," joint work with A. Sahai, FOCS 1997).
- *DOD/NDSEG Graduate Fellowship*, 1996–1999.
- *Churchill Scholarship* to study at Churchill College, Cambridge University, 1995–1996. Named sole *Loeb Scholar* among the ten '95–'96 Churchill Scholars.
- *Thomas Temple Hoopes Prize* for outstanding undergraduate work at Harvard University, based on undergraduate thesis "The Complexity of Counting."

Professional Activities

- Chair, Luca Trevisan Award for Expository Work in Theoretical Computer Science, January 2026–present.

- Institute of Information Science Academic Advisory Committee (AAC) at Academia Sinica, Taiwan, January 2026–December 2028.
- Co-organizer, Semester Program on Pseudorandomness and High-Dimensional Expanders, Simons Institute for the Theory of Computing at UC Berkeley, Fall 2026.
- Co-organizer, LucaFest@Simons, in loving memory of Luca Trevisan, 8–9 October 2024.
- Co-organizer, Sydney Privacy Workshop, 13–15 February 2024.
- National Academies Committee on National Statistics (CNSTAT), 2024–present.
- Knuth Prize Selection Committee, 2024–2026.
- Committee for Appointments and Promotions, Bocconi University Department of Computing Sciences, 2023–2027.
- Scientific Advisory Board, Simons Institute for the Theory of Computing, 2023–2025 (as co-chair, 2024–2025).
- National Academies ad hoc consensus panel, A Roadmap for Disclosure Avoidance in the Survey of Income and Program Participation (SIPP), May 2022–October 2023.
- Co-organizer, CynthiaFest symposium in honor of Cynthia Dwork, Cambridge, MA, June 2022.
- J-PAL IDEA Advisory Committee, 2022–2024.
- Search Committee, *Journal of the ACM* Editor-in-Chief, 2021.
- Test-of-time Award Committees, STOC 2021 and STOC 2022 (chair).
- Learning Incubator (LInc) Faculty Fellow, Harvard School of Engineering & Applied Sciences, 2020–21.
- Urban Institute Validation Server Advisory Board, July 2020–July 2025.
- Professional memberships: Association for Computing Machinery (ACM) and ACM Special Interest Group on Algorithms and Computation Theorey (SIGACT), 2013–present; IEEE and IEEE Computer Society, 2013–present; Sigma Xi, 2020–present; Friends of Oberwolfach, 2018–present.
- Editor-in-Chief, *Foundations and Trends in Theoretical Computer Science*, August 2020–present.
- Faculty Associate, *Berkman Klein Center for Internet and Society*, Harvard University, September 2020–present.
- Committee on National Statistics Expert Group on "Postprocessing" in 2020 Census Data Products/Implementing Differential Privacy, May 2020–January 2022.
- Faculty Co-Director, *OpenDP*, a community effort to build a trustworthy, open-source suite of tools for deploying differential privacy, July 2019–present.

- Executive Committee, *Harvard Center for Research on Computation and Society (CRCS)*, Fall 2019–Spring 2023
- Steering Committee, *Theory of Cryptography Conference (TCC)*, November 2019–present.
- Inaugural Steering Committee, *Symposium on the Foundations of Responsible Computing (FoRC)*, September 2019–present.
- Editor, *Foundations and Trends in Theoretical Computer Science*, August 2019–July 2020.
- Co-organizer, *Meeting on Differential Privacy, Census, and Redistricting*, Harvard University, July 2019.
- Co-organizer, *Workshop in Celebration of Shafi Goldwasser*, Simons Institute for the Theory of Computing, January 2019.
- Member, Privacy & Security Committee, Social Science One.
- Local Arrangements Committee, Women in Theory workshop (WIT 2018), June 2018.
- Co-organizer, 2017–18 Program on Combinatorics & Complexity, Harvard Center for Mathematical Sciences & Applications.
- Co-organizer, "Managing Privacy in Research Data Repositories," workshop at Dataverse Community Meeting, Harvard Medical School, July 13, 2016.
- Co-organizer, "Secrecy and Privacy" two-week theme, part of thematic program "Nexus of Information and Computation Theories," Institut Henri Poincaré, Paris, France, Spring 2016.
- Co-organizer, Workshop on "Spectral Graph Theory and Applications," Shing-Tung Yau Center, National Chiao-Tung University, Taiwan, December 9–10, 2015.
- Co-organizer, session "Differential Privacy: Analyzing Sensitive Data and Implications," at AAAS Annual Meeting, San Jose, CA, February 2015.
- Program Committee, IACS-CRCS Symposium on "Privacy in a Networked World," January 2015.
- Vice-chair, Committee of Visitors for NSF Directorate for Computer and Information Science and Engineering (CISE), 2014.
- Co-organizer, workshop on "Integrating Approaches to Privacy across the Research Lifecycle," Harvard University, Sept. 24–25, 2013.
- Advisory Board, Harvard Institute for Applied Computational Science (IACS), May 2014–present.
- Co-Chair, Search Committee for NSF Director of the Division for Computing and Communication Foundations, Spring 2013.
- Chair, SIGACT Committee for the Advancement of Theoretical Computer Science, July 2012–July 2015.

- Program Chair, 43rd Annual ACM Symposium on Theory of Computing, San Jose, CA, June 2011.
- Member-at-large, ACM Council, July 2010–June 2014.
- Local Arrangements Chair, 25th IEEE Conference on Computational Complexity, Cambridge, MA, May 2010.
- Organizer, Oberwolfach Meetings on Computational Complexity, 2012, 2015, 2018, 2021.
- Co-organizer, DIMACS Workshop on Complexity and Cryptography: Status of Impagliazzo's Worlds, Princeton, NJ, June 2009.
- Co-organizer, 60th Birthday Celebration for Leslie Valiant, Bethesda, MD, May 2009.
- Organizer, Workshop on Visions for Theoretical Computer Science, Seattle, WA, May 2008.
- Director, Harvard Center for Research on Computation and Society (CRCS), August 2008–July 2011, January 2014–May 2015.
- SIGACT Committee for the Advancement of Theoretical Computer Science, 2007–2016.
- Program Chair, 4th Theory of Cryptography Conference (TCC '07).
- Program Chair, 6th International Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM '02).
- Editor, *SIAM Journal on Computing*, 2005–2017.
- Editor, *Computational Complexity*, 2003–present.
- Conference Committee, *IEEE Conference on Computational Complexity*, 2005–2008.
- Scientific Board, *Electronic Colloquium on Computational Complexity*, 2005–present.
- Chair, Research Cluster on Randomness & Computation, Radcliffe Institute for Advanced Study, September 2003–August 2004.
- Co-organizer, Special Focus on Privacy and Security, Harvard Center for Research on Computation and Society, 2005–present.
- Chair, Group on Cryptographic Foundations of Networked Computing, NSF Workshop on the Theory of Networked Computing (ToNC), March 2006.
- Program Committees: CRYPTO '00, CCC '01, RANDOM '01, FOCS '01, RANDOM '02, TCC '04, EUROCRYPT '05, CRYPTO '06, TCC '07, STOC '07, CRYPTO '09, STOC '11, STACS '13, TCC '14, TPDP '15, STOC '16, TCC '17, CCC '20, FoRC '21, ICM '22 (panel for Section 14), ICALP '23

- Grant reviewing/panels: NSF Theory of Computing Program; NSF Cybertrust Program; NSF Secure & Trustworthy Cyberspace Program; NSF Algorithmic Foundations Program; NSF Program on Pathways to Open-Source Ecosystems; Israel Science Foundation; US-Israel Binational Science Foundation; Simons Foundation; Guggenheim Fellowships; Sloan Foundation; Hungarian National Research, Development, and Innovation Office; European Research Commission.
- Extensive journal and conference refereeing.

Doctoral Advisees

Current Students

- Prashanth Amireddy (4th year Ph.D.), coadvised with Madhu Sudan
- Elena Ghazi (2nd year Ph.D.), coadvised with Flavio du Pin Calmon
- Walter McKelvie (2nd year Ph.D.), coadvised with Sitan Chen
- Aaron (Louie) Putterman (4th year Ph.D.), coadvised with Madhu Sudan
- Roy Rinberg (3nd year Ph.D.), coadvised with Boaz Barak
- Zachary Ratliff (5th year Ph.D.), coadvised with James Mickens
- Jake Ruotolo (4th year Ph.D.)
- Michael Shoemate (1st year Ph.D.)
- Jiyu Zhang (Bocconi University), coadvised with Alon Rosen

Jayshree Sarathy Sept. '18–June '23

- Co-advised by Jonathan Zittrain.
- Ph.D. dissertation: *Bridging Sociotechnical Gaps for Privacy-Preserving Data Science.*
- Graduate Fellow, Safra Center for Ethics, 2022–2023.
- Position as of Jan. 2024: Postdoctoral Researchers, Columbia University Data Science Institute. (In Fall 2024, will join Northeastern University as a Senior Research Fellow and later as an Assistant Professor of Computer Science.)

Victor Balcer Sept. '15–June '22

- Ph.D. dissertation: *Exploring Models for Implementing Differential Privacy*

Daniel Alabi Sept. '16–June '22

- Ph.D. dissertation: *The Algorithmic Foundations of Private Computational Social Science*
- Facebook Emerging Scholar, 2018–2020
- Position as of Sept. 2022: Junior Fellow, Simons Society of Fellows and Columbia University.

Rohit Agrawal Sept. '16–June '20

- Ph.D. dissertation: *Deriving Indistinguishability from Unpredictability: Tools and Applications in Pseudorandomness*
- Position as of Feb. 2021: Quantitative Trader, Jane Street Capital.

Jack Murtagh Sept.'15–May '20

- Ph.D. dissertation: *Spectral Graph-Theoretic Methods for Derandomizing Space-Bounded Computation*
- Began with pre-doctoral research in the theory and practice of differential privacy, June '14–Aug '15.
- Position as of May 2023: science writer (math and puzzles) for Gizmodo and other publications.

Yi-Hsiu Chen Sept. '14–Aug. '20

- Ph.D. dissertation: *Computational Notions of Entropy: Classical, Quantum, and Applications*
- Certification of Distinction in Teaching, Fall '16.
- First post-Ph.D. position: Research Scientst, Facebook.
- Position as of Jan '24: Applied Cryptographer, Coinbase.

Mark Bun Sept. '12–Aug. '16

- Ph.D. dissertation: *New Separations in the Complexity of Differential Privacy*
- Best Paper Award, ICALP '13 Track A for paper "Dual Lower Bounds for Approximate Degree and Markov–Bernstein Inequalities"
- Certificate of Distinction in Teaching, Fall '13.
- National Defense Science and Engineering Graduate Fellowship.
- First post-Ph.D. position: Postdoctoral Fellow, Princeton University
- Position as of Jan '24: Assistant Professor, Boston University.

Thomas Steinke Sept. '10–Jul. '16

- Ph.D. dissertation: *Upper and Lower Bounds for Privacy and Adaptive Data Analysis*"
- Certificate of Distinction in Teaching, Fall '12, Spring '15.
- Lord Rutherford Memorial Fellowship.
- First post-Ph.D. position: Postdoctoral Fellow, IBM Almaden Research Center
- Position as of Jan '24: Research Scientist, Google DeepMind.

Colin Jia Zheng Sept. '08–Jan '14

- Ph.D. dissertation: *A Uniform Min-Max Theorem and Characterizations of Computational Entropies*.
- First post-Ph.D. position: Software engineer, Google, Mountain View, CA.

Jonathan Ullman — Sept. '09–May '13

- Ph.D. dissertation: *Privacy and the Complexity of Simple Queries.*
- Siebel Scholar
- Certificate of Distinction in Teaching, Fall '13
- First post-Ph.D. positions: Postdoctoral Fellow, Harvard Center for Research on Computation and Society 2013–14; Junior Fellow, Simons Society of Fellows, 2014–15
- Position as of Jan '24: Associate Professor, Khoury College of Computer Sciences, Northeastern University.

Kai-Min Chung — Sept. '05–Aug. '10

- Ph.D. dissertation: *Efficient Parallel Repetition Theorems with Applications to Security Amplification.*
- Student Paper at TCC '10 for paper "Tight Parallel Repetition Theorems for Public-coin Arguments."
- Certificate of Distinction in Teaching, Spring '09.
- First post-Ph.D. position: Simons Postdoctoral Fellow, Cornell University.
- Position as of Jan '24: Research Fellow, Institute of Information Science (IIS), Academia Sinica, Taiwan.

Shien Jin Ong — June '04–June '07

- Ph.D. dissertation: *Unconditional Relationships within Zero Knowledge.*
- Best Paper Award at EUROCRYPT '07 for "Zero Knowledge and Soundness are Symmetric."
- SIAM Outstanding Paper Prize 2011 for "Statistically Hiding Commitments and Statistical Zero-Knowledge Arguments from Any One-Way Function" (in SIAM Journal on Computing Special Issue on STOC '07).
- First post-Ph.D. position: Quantitative Strategist, Goldman Sachs.
- Position as of Jan '24: Professor of Practice, Asia School of Business (ASB), Kuala Lumpur, Malaysia.

Emanuele Viola — Sept. '01–Aug. '06

- Ph.D. dissertation: *The Complexity of Hardness Amplification and Derandomization.*
- SIAM Student Paper Award for paper "Pseudorandom Bits for Constant-Depth Circuits with Few Arbitrary Symmetric Gates" (CCC '05, SICOMP '06).
- First post-Ph.D. position: Postdoctoral Fellow, Institute for Advanced Study, Princeton NJ.
- Position as of Jan '24: Professor, Khoury College of Computer Sciences, Northeastern University, Boston, MA.

Minh-Huyen Nguyen — June '01–June '06

- Ph.D. dissertation: *Zero Knowledge with Efficient Provers.*

- SIAM Outstanding Paper Prize 2011 for "Statistically Hiding Commitments and Statistical Zero-Knowledge Arguments from Any One-Way Function" (in SIAM Journal on Computing Special Issue on STOC '07).
- DEAS Teaching Fellow Award, Fall '01.
- Certificate of Distinction in Teaching, Spring '04, Fall '01.
- First post-Ph.D. position: Actuarial Assistant, Liberty Mutual Group

Other Graduate Research Advising

OpenDP Interns — Summers '24+

- Overall supervisor for graduate-student interns on the OpenDP project (with primary mentoring often provided by others)
- 2025: Onyinye Dibia (U. Vermont), Ephraim Linder (Boston U.)
- 2024: Tudor Cebere (INRIA)

Yanis Vandecasteele — Summer '23–Spring '24

- Harvard M.S. student in Data Science.
- Co-mentored with postdoc Wanrong Zhang.
- Supported in part by an HDSI Public Service Data Science Graduate Fellowship.
- Research on designing a global challenge about applying differential privacy on financial transaction data for public health.

Peihan Liu — Summer '23–Spring '24

- Harvard M.Eng. student in Computation Science and Engineering.
- Co-mentored with postdoc Wanrong Zhang.
- Research on optimal numerical compositors for differential privacy.

Nico Manzonelli — Spring '22–Spring '23

- Harvard M.S. student in Data Science.
- Co-mentored with postdoc Wanrong Zhang.
- M.S. thesis and poster in TPDP '23: *Membership Inference Attacks and Privacy in Topic Modelling*

Jiachen (Tianhao) Wang — Spring '20-Spring '21

- Harvard M.Eng. student in Computational Science and Engineering.
- M.Eng. thesis and paper in TCC '21 (also invited to *J. Cryptology*): *Concurrent Composition of Differential Privacy*

Yanping Zhang — Summer '19

- Duke University M.S. student. in Electrical and Computer Engineering.
- Implementation and research on differentially private synthetic data generation via graphical models.

Jordan Awan — Summer '18

- Pennsylvania State University Ph.D. student in Statistics, advised by Aleksandra Slavkovic.
- Research on differentially private hypothesis testing and causal inference.

Brendan Avent — Summer '16

- University of Southern California Ph.D. student, advised by Aleksandra Korolova.
- Research on differentially private confidence intervals, co-supervised by postdoc Vishesh Karwa.

Ryan Rogers — Summer '15

- University of Pennsylvania Ph.D. student, advised by Aaron Roth.
- Research on differentially private contingency tables and independence testing.

Adam Sealfon — September '14–July '15

- MIT Ph.D. student, primary advisor Shafi Goldwasser.
- Research on differential privacy.

Jack Murtagh — June '14–August '15

- Pre-doctoral research on the composition of differential privacy, both theory and practice.
- Continued on as a Ph.D. student in computer science at Harvard.

Jiapeng Zhang — August '12–July '13

- Visiting student.
- Research on differential privacy and traitor tracing.

Stephan Holzer — Sept. '08-May '09

- Visiting Ph.D. student from from TU Munich, advised by Ernst Mayr.
- Research on derandomization.

Guy Rothblum — June '06–May '09

- MIT Ph.D. student, primary advisor Shafi Goldwasser.
- Research on cryptography, privacy, and computational complexity.

Zhenming Liu — September '05–January '07

- S.M. Research on Random Selection Protocols.

Undergraduate Research Advising

Privacy Tools/OpenDP Interns — Summers '14+

- Overall supervisor for many REU students and other interns on the Privacy Tools Project and OpenDP (with primary mentoring often provided by others)
- 2025: Rita Ionides (U. Michigan '26)
- 2024: Gurman Dhaliwal (UCSD '24), Maxine Park (Harvard '26),
- 2023: Nicolas Berrios (Catholic University of Chile '24), Patrick Song (Harvard '23), Vicki Xu (Harvard '23)
- 2022: Patrick Song (Harvard '23), Vicki Xu (Harvard '23)
- 2021: Sílvia Casacuberta Puig (Harvard '23), Grace Tian (Harvard '22), Connor Wagaman (Harvard '22)
- 2019: Elbert Du (Harvard '22), Wassim Marrakchi (Harvard '21), Sophia Song (Berkeley '22),
- 2018: Holly Cunningham (Princeton '21), Justin Kaashoek (Harvard '21), Ross Mawhorter (Harvey Mudd '19), Julia Vasile (Stony Brook '19), Anton Xue (Yale '19)
- 2017: Christian Baehr (Washington U., St. Louis '17), Katherine Clayton (Dartmouth '18), Alyssa Hu (U. Maryland, College Park '18), Michael LoPiccolo (UT Dallas '18), Kathryn Taylor (Emory '17), Lancelot Wathieu (Georgetown '18).
- 2016: Nabib Ahmed (Harvard '19), David Chang (Harvard '17), Benjamin Glass (Harvard '18), Chan Kang (Harvard '17), Jack Landry (Rutgers '18), Paul Lisker (Harvard '17), Marcelo Novaes (Federal University of Bahia, Brazil '16), Ana Oaxaca (U. New Mexico '16), Grace Rehaut (Princeton '18), Clara Wang (Dartmouth '17), Yisu "Remy" Wang (Tufts '17)
- 2015: Andreea Antuca (U. Essex '15), Jessica Bu (Wellesley '17), Caper Gooden (William & Mary '16), Jimmy Jiang (Harvard '18), Hyun-Woo Lim (UCLA '15), Cameron Merrill (Michigan State '16), Daniel Muise (UMass Lowell '16), Haoqing Wang (Harvard '18)
- 2014: Connor Bain (U. South Carolina '15), Victor Balcer (UC San Diego '15), Naomi Day (Wellesley '17).
- Student majors included computer science, mathematics, economics, international relations, and politics.
- Graduate students, postdocs, and visitors served as direct mentors. Students for whom I was a direct mentor or co-mentor are listed individually below.

Amy Feng '26 — November '25–May '26

- A.B. thesis research on formal verification of differential privacy.
- Co-mentored with Ph.D. student Michael Shoemate.

Vadim Zaripov '26 September '25–May '26

- A.B. thesis research on derandomized graph sparsification.
- Co-mentored with Ph.D. student Louie Putterman.

Easton Singer '26 June '25–May '26

- A.B. thesis research on eigenvalue multiplicities in Abelian Cayley graphs.
- Co-mentored with Ph.D. student Jake Ruotolo.

Jason Tang '25 September '24–May '25

- A.B. thesis research on differentially private mechanisms for facility location.
- Co-mentored with Yannai Gonzcarowski and Ph.D. student Sara Fish.
- Received Thomas Temple Hoopes Prize for Outstanding Undergraduate Work.
- Led to a paper in FORC '26.

Ashley Zhuang '23 March '23–December '23

- A.B. thesis "Sparsity Bounds for Spectral Approximations of Graphs."
- Co-mentored with Ph.D. student Jake Ruotolo.
- Research led to paper in SOSA '23.
- Honorable Mention for CRA Outstanding Undergraduate Researcher Award.

Vicki Xu '23 June '22–December '23

- A.B. thesis "Concurrent Composition of Interactive Mechanisms with Adaptive Privacy-loss Parameters."
- Co-mentored with postdoc Wanrong Zhang.
- Research led to Distinguished Paper Award at CCS '23.
- Honorable Mention for CRA Outstanding Undergraduate Researcher Award.

Patrick Song '23 June '22–December '23

- A.B. thesis "From Theory to Implementation: How Open-Source DP Libraries Shape Mental Models of Privacy Concepts."
- Co-mentored with Ph.D. student Jayshree Sarathy.

Sílvia Casacuberta Puig '23 June '21–May '23

- Research on differential privacy and algorithmic fairness.
- A.B. thesis "From Regularity Lemmas to Algorithmic Fairness," co-advised with Cynthia Dwork, received a Thomas Temple Hoopes Prize for Outstanding Undergraduate Work.
- Supported by Harvard Program for Research in Science and Engineering (PRISE) in Summer '21, research led to paper in CCS '22.
- Winner of CRA Outstanding Undergraduate Researcher Award.
- Position as of September '23: Global Rhodes Scholar at the University of Oxford for a Masters by Research in Computer Science.

Grace Tian '22 June '21–May '22

- A.B. thesis "OpenDP Programming Framework for Renyi Privacy Filters and Odometers."
- Supported by Harvard Program for Research in Science and Engineering (PRISE) in Summer '21 and Herchel Smith-Harvard Undergraduate Science Research Program in Summer '22.

Connor Wagaman '22 June '21–May '22

- A.B. thesis "Finite-Precision Arithmetic Isn't Real: the Impact of Finite Data Types on Efforts to Fulfill Differential Privacy on Computers".
- Research led to paper in CCS '22.
- Supported by the Harvard College Research Program (HCRP) in Summer '21.
- Position as of Sept. '22: Ph.D. student in Computer Science, Boston University.

Louis Golowich '22 January '21–May '22

- A.B. thesis "Random Walks on Expander Graphs" awarded Thomas Temple Hoopes Prize for outstanding undergraduate work.
- Finalist for CRA Outstanding Undergraduate Researcher Award.
- Research led to papers in RANDOM '21, CCC '22, and STOC '23.
- Supported by a Herchel Smith Fellowship in Summer '21.
- Position as of Sept. '22: Ph.D. student in Computer Science, U.C. Berkeley.

Tyler Piazza '21 September '20–May '21

- A.B. thesis "Differentially Private Ridge Regression: the Cost of a Hyperparameter."

Edward (Ted) Pyne '22 November '19–May '22

- A.B. thesis "Towards the Derandomization of Space-Bounded Computation."
- Supported in Summers '20 and '22 by an NSF REU grant.
- Winner of CRA Outstanding Undergraduate Researcher Award.
- Research led to papers in ITCS '21, COCOON '21, CCC '21, SOSA '22, CCC '22, RANDOM '22.
- Position as of Sept. '22: Ph.D. student in EECS, MIT.

Michael Fine '20 May '19–May '20

- A.B. thesis *Provable Differentially Private Data Release with Generative Adversarial Networks.*
- Current position (as of Feb. 2021): privacy researcher and software engineer, Apple.

Alexander Goldberg '18 September '17-May '18

- A.B. thesis *Towards Differentially Private Inference on Network Data."* awarded Thomas Temple Hoopes Prize for outstanding undergraduate work.

Jessica Zhu '18 Spring '17

- Term-time research on differentially private statistical inference.

Allyson Kaminsky (Wake Forest '16) Summer '15

- Research on implementing interactive queries and composition of differential privacy, as part of "Privacy Tools for Sharing Research Data" project.
- Co-supervised by graduate students Jack Murtagh and Thomas Steinke.
- Participant in SEAS REU Site.

Alex Lombardi '16 Summer '15

- Research on pseudorandomness for constant-width branching programs.
- Supported by the Harvard College Research Program.
- Subsequently went on to a Ph.D. program at MIT.

Joy Zheng '15 September '13–May '15

- A.B. thesis *The Differential Privacy of Bayesian Inference* awarded Thomas Temple Hoopes Prize for outstanding undergraduate work.

- Research on expander graphs, Markov chain Monte Carlo, and differential privacy.

Aleksander Makelov '15 June '13–May '15

- A.B. thesis *Expansion in Lifts of Graphs* awarded Thomas Temple Hoopes Prize for outstanding undergraduate work.
- Also did research on Markov Chain Monte Carlo and differential privacy.
- Supported by Harvard College Research Program (HCRP) and Herchel Smith Harvard Undergraduate Research Program.
- Subsequently went on to be a Ph.D. student at MIT.

Sitan Chen '16 June '14–May '15

- Research on pseudorandomness for constant-depth circuits.
- Co-advised by Ph.D. student Thomas Steinke.
- Supported by a Herchel–Smith Research Fellowship in Summer '14.
- Subsequently went on to complete a Ph.D. at MIT.

Paul Handorff '14 Summer '13–June '14

- Research on sample-and-aggregate algorithm for differentially private regression, as part of "Privacy Tools for Sharing Research Data" project.
- Supported by Harvard College Research Program (HCRP).
- Co-supervised by postdoc Jonathan Ullman.

Anna Gavrilman (UMass Boston '14) Summer '13–Spring '14

- Research on implementation and optimization of differentially private algorithms for marginal queries, as part of "Privacy Tools for Sharing Research Data" project.
- Co-supervised by postdoc Jonathan Ullman.
- Participant in SEAS REU Site.

Adam Sealfon '13 Summer '10–June '13

- A.B. thesis *Fault-Tolerant Spanners*.
- Research also on approximating the entropy of low-degree polynomial mappings over finite fields.
- Supported in part by Harvard College Program for Research in Science and Engineering (PRISE).
- Subsequently completed a Ph.D. in computer science at MIT, and went on to a postdoc position at UC Berkeley.

Olga Zverovich '10 Summer '09–June '10

- A.B. thesis *The Minimum Assignment Problem.*
- Supported in part by the Harvard College Research Program (HCRP).
- Subsequently went on to complete a J.D. at Harvard Law School.

Zachary Abel '10 Summer '09–June '10

- A.B. thesis *Lattice Tensor Constructions in the Complexity of the Shortest Vector Problem.*
- Supported in part by Harvard College Program for Research in Science and Engineering (PRISE).
- Subsequently completed a Ph.D. in mathematics at MIT and went on to be a lecturer in the MIT Computer Science and Artificial Intelligence Lab.

Yakir Reshef '09 Sept. '08–Nov. '10

- A.B. thesis *Resilient and Exposure-Resilient Functions.*
- Work led to paper "On Extractors and Exposure-Resilient Functions for Sublogarithmic Entropy," accepted to *Random Structures & Algorithms.*
- Subsequently completed an MD at Harvard Medical School and a PhD in computer science at Harvard, and went on to residency at Brigham and Women's Hospital.

Eleanor Birrell '09 August '08–present

- A.B. thesis *Composition of Zero-Knowledge Proofs.*
- Work led to paper "Composition of Zero-Knowledge Proofs with Efficient Provers," in the *7th IACR Theory of Cryptography Conference (TCC '10).*
- Subsequently completed a Ph.D. in computer science at Cornell University, and went on to become computer science faculty at Pomona College.

Dragos Florin Ciocan '07 Sept. '06–Mar. '08

- A.B. thesis *Constructions and Characterizations of Non-interactive Zero-Knowledge* awarded Thomas Temple Hoopes Prize for outstanding undergraduate work.
- Work led to paper "Interactive and Noninteractive Zero Knowledge are Equivalent in the Help Model" in the *5th IACR Theory of Cryptography Conference (TCC '08).*
- Subsequently completed a Ph.D. in operations research at MIT, and went on to a faculty position in technology and operations management at INSEAD.

Grant Schoenebeck '04 Summer '03–Summer '04

- Supported in part by the Harvard College Research Program.
- A.B. thesis *The Computational Complexity of Finding Nash Equilibria in Succinctly Represented Games.*
- Work led to paper "The computational complexity of Nash equilibria in concisely represented games" in *7th ACM Conference on Electronic Commerce (EC '06).*

- Subsequently completed a Ph.D. in computer science at U.C. Berkeley, and went on to a faculty position at the University of Michigan.

Saurabh Sanghvi '04 — Summer '03–June '04

- A.B. thesis *A Study of Two-Party Random Selection Protocols* awarded Thomas Temple Hoopes Prize for outstanding undergraduate work.
- Work led to paper "The round complexity of two-party random selection" in *37th ACM Symposium on Theory of Computing (STOC '05)*, and invited to *SIAM Journal on Computing* Special Issue on STOC '05.
- Supported in part by the Harvard College Research Program (HCRP).
- Subsequently completed a J.D. at Yale University.

Shien Jin Ong (MIT) '03 — Summer '02

- Supported by an MIT Eloranta Summer Fellowship.
- Work led to paper "Derandomization in cryptography" in *23rd Annual International Cryptology Conference (CRYPTO '03)* and *SIAM Journal on Computing* (2007).
- Subsequently completed a Ph.D. in computer science at Harvard University.

David Xiao '03 — Spring '02–Spring '03

- A.B. thesis *The Evolution of Expander Graphs* awarded Thomas Temple Hoopes Prize for outstanding undergraduate work.
- Subsequently completed a Ph.D. in computer science at Princeton University, and went on to a research scientist position at CNRS, LIAFA, Université Paris 7.

Other Students

- Co-advised Math/CS thesis of Conlan Olson '21 "Algorithmic Fairness, Metric Embedding, and Metric Learning." Primary advisor Pragya Sur (Statistics).
- Co-advised Math/CS thesis of Karl Otness '18 on *Graph Convolutions and Machine Learning*.
- Supervised independent study by Charles Cabot '13 on cryptography, Spring '13.
- Co-supervised (with Ph.D. student Jon Ullman) research of Rebecca Goldstein '13, Stephen Kent '14, and Abiola Laniyonu '13 on privacy for social science research, Summer '11–present.
- Co-advised (with postdoc Dan Gutfreund) research of Shira Mitchell '09 on locally list-decodable error-correcting codes, Summer '07.
- Supervised research of Shrenik Shah '09 on various topics in computational complexity, Summer '06.
- Co-advised Math/CS thesis of John Gregg '03, *On Factoring Integers and Evaluating Discrete Logarithms*.
- Co-advised Math/CS thesis of Neil Agarwal '02, *Automorphisms of the Lattice of Computably Enumerable Sets*.

- Supervised independent study of Inna Zakharevich on *Introduction to the Theory of Computation*, Summer '04.
- Supervised independent study of Robert Scott on an *Elliptic Curve Identification Scheme*, Spring '02.
- Supervised independent study of Marius Niculescu on *Introduction to Cryptography*, Summer '01.

Postdoctoral Fellows and Research Associates

Priyanka Nanayakkara — Sep. '24–Aug. '26

- Postdoctoral Fellow in the Center for Research on Computation and Society (during first year).
- Co-mentored with Martin Wattenberg and Fernanda Viégas.

Chiké Abuah — Mar. '24–Feb. '25

- Research Associate in the OpenDP project.

Vikrant Singhal — Oct. '23–Dec. '25

- Research Associate in the OpenDP project.
- Subsequently joined U. Copenhagen as a fixed-term Assistant Professor.

Chin Ho Lee — Sept. '21–Aug. '23

- Research on computational complexity.
- Subsequently joined the computer science faculty at North Carolina State University.

Wanrong Zhang — July '21–Dec. '23

- Research on differential privacy.
- Postdoc and then Research Associate in the OpenDP project.
- Supported by a CRA-CCC Computing Innovation Fellowship.
- Subsequently a research scientist at Tiktok.

Jiapeng Zhang — Sept. '19–Sept. '20

- Research on computational complexity.
- Subsequently joined the computer science faculty at the University of Southern California.

Vishesh Karwa — Sept. '14–July '17

- Fellow in Center for Research on Computation and Society, working on "Privacy Tools for Sharing Research Data" project.
- Subsequently joined the statistics faculty at Ohio State University, then Temple University.

Or Sheffet — Jan. '14–Aug. '15

- Fellow in Center for Research on Computation and Society, working on "Privacy Tools for Sharing Research Data" project.
- Subsequently joined the faculty of the Department of Computing Science, University of Alberta.

Jonathan Ullman — June '13–June '14

- Fellow in Center for Research on Computation and Society, working on "Privacy Tools for Sharing Research Data" project.
- Subsequently joined the faculty of the College of Computer and Information Sciences, Northeastern University.

Andrew Wan — Sept. '12–Aug. '13

- Co-hosted with Leslie Valiant.
- Subsequently became a Research Staff Member at the Institute for Defense Analyses.

Karthekeyan Chandrasekaran — Sept. '12–Aug. '14

- Supported by the Simons Postdoctoral Fellowship at Harvard University.
- Subsequently joined the faculty of the Department of Industrial and Enterprise Systems Engineering, University of Illinois at Urbana–Champaign.

Tal Moran — Sept. '08–Sept. '11

- Supported by the SEAS Center for Research on Computation and Society.
- Subsequently joined the faculty of the School of Computer Science, Herzliya Interdisciplinary Center, Israel.

Alon Rosen — Sept. '05–July '07

- Supported by the DEAS Center for Research on Computation and Society.
- Subsequently joined the faculty of the School of Computer Science, Herzliya Interdisciplinary Center, Israel.

Dan Gutfreund — Sept. '05–Aug. '07

- Supported in part by a DEAS Applied Math Lectureship.
- Subsequently joined the Machine Learning and Data Mining Group, IBM Haifa Research Lab.

Eli Ben-Sasson — Sept. '01–Aug. '03

- Co-hosted with Madhu Sudan (MIT).
- Member of 2003–04 Radcliffe Cluster on Randomness and Computation.
- Subsequently joined the faculty in the Department of Computer Science, The Technion, Israel.

Visitors Hosted

David Zuckerman (UT Austin) 2004–05, Summer '06, Fall '22

- Supported in '04–'05 by a fellowship from the Radcliffe Institute for Advanced Study.
- Supported in part in Fall '22 by the Center of Mathematical Sciences and Applications (CMSA).

Aleksandar (Sasho) Nikolov (U. Toronto) Oct '21–Dec '21

- Mostly remote visit, supported by sabbatical pay from U. Toronto.

Emanuele Viola (Northeastern U.) Sept. '14–June '15

- Supported by my grants.

Sofya Raskhodnikova (Penn State) Jan. '14–July '14

- Visiting Scholar in the SEAS Center for Research on Computation and Society, supported by my grants.

Adam D. Smith (Penn State) Jan. '14–July '14

- Visiting Scholar in the SEAS Center for Research on Computation and Society, supported by my grants.

David Xiao (U. Paris 7) Dec. '13–Aug. '14

- Visiting Scholar in the SEAS Center for Research on Computation and Society, supported by my grants.

Kobbi Nissim (Ben-Gurion U. and Georgetown U.) Sept. '12–July '17

- Supported in part by the SEAS Center for Research on Computation and Society, and by my grants.

Omer Reingold (Weizmann Institute) Aug. '05–Nov. '05

- Supported by the DEAS Center for Research on Computation and Society.

Radcliffe Cluster on Randomness and Computation 2003–04

- Cluster members: Eli Ben-Sasson (now at the Technion), Oded Goldreich (Weizmann Institute), Dana Ron (Tel-Aviv University), Ronnitt Rubinfeld (NEC and MIT), Madhu Sudan (MIT), plus several additional affiliates and visitors.
- Supported by fellowships from the Radcliffe Institute for Advanced Study.

University and Departmental Service

- Computer Science Director of Graduate Studies, 2025–present.
- SEAS Educational Policy Commitee and Graduate Educational Policy Committee, 2025–present.
- FAS Standing Committee on Women, 2025–present.
- Embedded EthiCS Program Faculty Committee, 2021–23, 2024–present.
- SEAS Values Committee, 2024–25.
- Computer Science Committee on Higher Degrees, 2022–23, 2024–2025. 2025–present (chair)
- FAS Faculty Conduct Committee, 2024–present
- FAS Screening Committee, 2024–present.
- FAS Quantitative Reasoning with Data Review Committee, 2022–23.
- Co-organizer, Symposium for the Mathematical Sciences at Harvard (SMaSH), Spring 2022.
- Electrical Engineering Junior Search Committee, 2021–22.
- Co-Chair, Computer Science Junior Search Committee, 2020–21.
- SEAS Committee on Diversity, Inclusion, and Belonging, 2020–21.
- Computer Science Faculty Awards Committee, 2017–24.
- Area Chair for Computer Science, July 2017–June 2019.
- Presidential Search Faculty Advisory Committee, August 2017–February 2018.
- President's Committee on Electronic Communications Oversight, September 2016–May 2019.
- University Childcare Faculty Advisory Committee, May 2017–September 2017.
- FAS General Education Implementation Committee, September 2016–17.
- SEAS Graduate Admissions Committee and chair of Applied Math subcommittee, 2016–17.
- SEAS Mission, Vision, and Values Committee, 2016–17.
- Speaker at Harvard SEAS Fundraising Events, *Engineering the Future* in Seattle, WA and Mountain View, CA, March 2014.
- Director, Harvard Center for Research on Computation and Society (CRCS), August 2008–July 2011, January 2014–May 2015.
- Co-Director of Undergraduate Studies, Applied Mathematics, July '13–June '15.
- SEAS Task Force on Undergraduates, Spring 2013–Fall 2013.

- Harvard Library Faculty Advisory Council and FAS Standing Committee on the Library, 2012–13.
- Applied Math Search Committee, Fall ‘12–Spring ‘13.
- Applied Math & Theoretical Computer Science Search Committee, Spring ‘12.
- FAS Dean’s Faculty Resources Committee, Fall ‘10–Spring ‘15.
- SEAS Task Force on Applied Mathematics, Fall ‘09.
- Electrical Engineering Faculty Search Committee, Spring ‘09.
- Radcliffe Institute Faculty Advisory Committee, Spring ‘07.
- FAS Educational Policy Committee, Fall ‘06–Spring ‘07.
- FAS Faculty Council, Fall ‘04–Spring ‘07.
- FAS Committee on Undergraduate Education, Fall ‘04–Spring ‘07.
- Committee to revise CUE course evaluation form, Summer ‘05–Spring ‘06.
- FAS summa cum laude committee, Fall ‘05–Spring ‘06.
- Chair, Junior Faculty Committee on the Future of DEAS, Spring ‘06.
- DEAS Graduate Admissions Committee, Fall ‘01–Spring ‘03.
- Organizer, Harvard Theory of Computation Seminar, Fall ‘02–Spring ‘07, Fall ‘08–Spring ‘11.
- Coordinated graduate admissions for Theory of Computation group, Spring ‘02–Spring ‘06.
- Computer Science Faculty Search Committee, Spring ‘02.
- Fay Prize Committee, Spring ‘04, Spring ‘07.
- Applied Math Committee on Undergraduate Studies, Fall ‘05–present.
- Computer Science Committee on Undergraduate Studies, Fall ‘02–present.

Teaching

CS 120(0): Introduction to Algorithms and their Limitations Fall ‘21, ‘22, ‘24, ‘25

- New introductory course in theoretical computer science.
- Co-taught with A. Hesterberg (Fall ‘22) and with A. Anshu (Fall ‘24).
- Also offered through the Harvard Extension School as CSCI E-120 in Fall ‘24, Fall ‘25 (data in parentheses below)
- Enrollment: 89, 238, 181 (12), 137 (29)
- CUE/Q overall course ratings (5.0 scale): 4.1, 4.15, 4.03 (4.0), 4.07 (4.2)
- CUE/Q overall instructor ratings (5.0 scale): 4.5, 4.60, 4.52 (4.5), 4.47 (4.4)

CS 229r: Spectral Graph Theory in Computer Science — Fall '20, Spring '23

- New graduate course.
- Enrollment: 35, 20
- CUE/Q overall course ratings (5.0 scale): 4.6, 4.63
- CUE/Q overall instructor ratings (5.0 scale): 4.8, 4.89

CS 208: Applied Privacy for Data Science — Spring '19, '22, '25

- New Masters-level course.
- Co-taught with James Honaker in all offerings, with Wanrong Zhang in Spring '22, and with Priyanka Nanayakkara in Spring '25.
- Enrollments: 16, 31, 90
- CUE/Q overall course ratings (5.0 scale): 4.8, 4.6, 3.75
- CUE/Q overall instructor ratings (5.0 scale): 5.0, 5.0, 4.53

AM 106/206: Applied Algebra — Fall '09, '10, '18

- Combined undergraduate/graduate course.
- Enrollments (106/206): 27/12, 17/4, 25.
- Q overall course ratings (5.0 scale): 3.8/4.6, 4.3/4.5, 3.7
- Q overall instructor ratings (5.0 scale): 4.2/4.7, 4.5/5.0, 4.1

CS 124: Data Structures and Algorithms — Spring '18

- Co-taught with main instructor Jelani Nelson.
- Enrollment: 257
- CUE/Q overall course ratings (5.0 scale): 4.0
- CUE/Q overall instructor ratings (5.0 scale): 4.4
- Also offered as Extension course CSCI E-124: Enrollment 43

CS 121: Introduction to the Theory of Computation — Fall '04, '05, '08, '12, '17

- Required theory course for all undergraduate computer science concentrators.
- Co-taught with Boaz Barak in Fall '17 to assist with his revamp of the course (mostly behind the scenes so did not have an instructor evaluation).
- Enrollments: 57, 45, 80, 121, 160
- CUE/Q overall course ratings (5.0 scale): 4.3, 4.3, 3.8, 4.2, 3.6
- CUE/Q overall instructor ratings (5.0 scale): 4.6, 4.5, 4.1, 4.4, xx
- Also offered as Extension course CSCI E-121 (previously numbered CSCI E-207). Enrollments 21, 20, 4, 9

AM 107: Graph Theory & Combinatorics — Spring '17

- Enrollment: 23
- Q overall course ratings (5.0 scale): 4.3
- Q overall instructor ratings (5.0 scale): 4.5

CS 225: Pseudorandomness — Spring '02, '04, '07, '09, '11, '15; Fall '16

- New graduate course.
- Enrollments: 32, 19, 18, 11, 13, 13, 13
- CUE/Q overall course ratings (5.0 scale): 4.5, 4.9, 4.7, 5.0, 4.8, 4.4, 4.5
- CUE/Q overall instructor ratings (5.0 scale): 4.7, 4.9, 4.7, 4.9, 4.9, 4.7, 4.7

CS 125: Algorithms & Complexity — Fall '14

- New course developed with Michael Mitzenmacher to be an accelerated introduction to theoretical computer science (as a subsitute for our usual 2-course sequence CS 121 & 124).
- Enrollments: 30
- Q overall course ratings (5.0 scale): 4.4
- Q overall instructor ratings (5.0 scale): 4.7

CS 221: Computational Complexity — Fall '02, Spring '06, '10, '14

- Graduate course.
- Enrollments: 15, 21, 14, 18
- CUE/Q overall course ratings (5.0 scale): 4.7, 4.6, 4.6, 4.4
- CUE/Q overall instructor ratings (5.0 scale): 4.8, 4.7, 4.7, 5.0

CS 127: Introduction to Cryptography (formerly CS 120) — Fall '01, Spring '03, Fall '06, '13

- New undergraduate course.
- Enrollments: 12, 21, 7, 16
- CUE/Q overall course ratings (5.0 scale): 4.9, 4.5, 4.7, 4.8
- CUE/Q overall instructor ratings (5.0 scale): 5.0, 4.8, 5.0, 4.8
- In Fall '06 and '13, also offered as Extension course CSCI E-177/E-127 (enrollments 5,2).

CS 229r: Mathematical Approaches to Data Privacy — Spring '13

- New graduate course.
- Enrollment: 20
- CUE/Q overall course ratings (5.0 scale): 4.4
- CUE/Q overall instructor ratings (5.0 scale): 4.9

CS 229r: Topics in the Theory of Computation — Spring '05

- New graduate course.
- Enrollment: 7
- GSAS evaluation – Would take course again (5.0 scale): 4.7
- GSAS evaluation – Quality of instruction (5.0 scale): 5.0

Additional teaching

- Lecturer, COST-IACR School on Randomness in Cryptography, Pompeu Fabra University, Barcelona, Spain, November 2016.
- Main lecturer for weeklong mini-course on Differential Privacy at McGill Invitational Workshop on Computational Complexity, Bellairs Research Institute, Holetown, Barbados, February 2014.
- Invited tutorial "Randomness Extractors and their Cryptographic Applications" given at TCC 2008.
- Invited tutorial "Randomness Extractors and their Many Guises" given at FOCS 2002.
- Lecturer at IAS/Park City Mathematics Institute (PCMI) Summer School on Computational Complexity Theory, Summer 2000.

External Funding

- Harvard Business School Digital Data Design (D^3) Institute Faculty Associates Program, with G. King, $50,000 (1/26–12/26).
- Gift from Stagwell, Inc. to OpenDP "Stagwell Differential Privacy Fund," with G. King, $250,000 (1/26).
- NSF Privacy-preserving Data Sharing in Practice (PDaSP grant) "Rigorous and Performant Differentially Private Machine Learning via OpenDP," with F. Calmon, $800,000, (10/25–9/28).
- NSF Pathways to Open-Source Ecosystems (POSE) Phase II grant "Building the Differential Privacy Ecosystem through OpenDP," with G. King and S. Iacus, $1,500,000 (8/23–7/25).
- Sloan Foundation grants, "OpenDP: an Open-Source Suite of Differential Privacy Tools," with M. Crosas, J. Honaker, and G. King, $884,838 (7/19-9/20), $750,000 (10/20–9/21), $750,000 (1/22–12/22), $1,500,00 (1/23–12/25).
- NSF Human Networks and Data Science–Infrastructure Track (HNDS-I) grant, "Bringing Differential Privacy to Social Science Data Repositories," with G. King, $860,000, 9/22–8/25.
- US Census Bureau Cooperative Agreement, "Towards an End-to-End Approach to Formal Privacy for Sample Surveys," with M. Gaboardi (Boston U., lead PI), M. Bun (Boston U.), J. Dreschsler (U. Maryland), C. Dwork (Harvard U.), F. Kreuter (U. Maryland), K. Nissim (Georgetown U.), A. Smith (Boston U.), $1.1m (Harvard portion), 9/20–8/25.
- Gift from Mozilla A.I to OpenDP, $200,000, 11/22.
- Gifts from Apple, "Growing the OpenDP Commons," $100,000 (4/21), $100,000 (8/22), $25,000 (7/24), $50,000 (7/25).
- Grant from data.org/New Venture Fund, "Privacy-preserving Challenge Collaboration," $84,000, 5/22–4/23.
- Gift from Facebook, "Implementing a Flexible Framework for Privacy Accounting," $100,000, 7/21–6/22.

- Harvard Data Science Initiative Trust in Science Fund, "Ensuring Privacy in COVID-19 Epidemiological Mobility Data Sets," with co-PIs C. Buckee and G. King, $100,000 (7/20-1/22).

- NSF Algorithmic Foundations Medium grant, "Exploiting Opportunities in Pseudorandomness" with O. Reingold (Stanford University), $550,000 (Harvard portion), 3/18–2/22.

- NSF Algorithmic Foundations EAGER grant, "Identifying Opportunities in Pseudorandomness" with O. Reingold (Stanford University), $125,000 (Harvard portion), 9/17–9/18.

- US Census Bureau Cooperative Agreement, "Formal Privacy Models and Title 13," with K. Nissim (Georgetown, lead PI), A. Smith (Boston U.), U. Gasser (Harvard Law School), $1.2m (Harvard portion), 1/17–12/19.

- NSF Secure & Trustworthy Cyberpace grant, "Computing over Distributed Sensitive Data," (PI K. Nissim, with co-PIs S. Chong, M. Gaboardi, J. Honaker), $1.75m (Harvard portion), 5/16–4/20.

- Sloan Foundation grant, "Applying Theoretical Advances in Privacy to Computational Social Science Practice," (PI M. Altman, with co-PIs M. Crosas, U. Gasser, G. King), $616,000 (Harvard portion), 4/15–9/17.

- NSF Algorithmic Foundations grant, "Pseudorandomness for Space-Bounded Computation and Cryptography," $492,395, 9/14–8/17.

- Simons Investigator Award, $1,440,000, 8/13–7/17, 8/19–7/25.

- NSF Secure & Trustworthy Cyberspace grant, "Privacy Tools for Sharing Research Data," $6,048,707, 10/12–3/18. (Lead PI on multidisciplinary "Frontier" project, with co-PIs E. Airoldi, S. Chong, M. Crosas, U. Gasser, G. King, P. Malone, L. Sweeney.)

- Gift from Google, Inc., "Privacy for Social Science Research," $200,000, 6/11–6/14.

- US–Israel Binational Science Foundation grant, "Computational Notions of Entropy and Cryptographic Applications," with I. Haitner (Tel-Aviv University), $94,000, 10/11–9/15.

- NSF Algorithmic Foundations grant, "Computational Entropy," $450,000, 7/11–6/15.

- NSF Cybertrust grant, "The Assumptions for Cryptography," $450,000, 9/08–8/11.

- Guggenheim Fellowship, 8/07–7/08, $30,000.

- ONR Young Investigator Award, "Pseudorandomness and Applications," $300,000, 6/04–8/07.

- NSF Cybertrust grant, "New Complexity-Theoretic Techniques in Cryptography," $399,999, 9/04–8/08.

- U.S.–Israel Binational Science Foundation grant. "Pseudorandomness and Combinatorial Constructions," with O. Reingold (Weizmann Institute) and L. Trevisan (UC Berkeley). $136,000, 10/07–9/11, plus $10,000 Pazy Memorial Research Award.

- Radcliffe Institute Research Fellowship, $20,000, 10/03.
- U.S.–Israel Binational Science Foundation grant. "Pseudorandomness and Combinatorial Constructions," with O. Reingold (Weizmann Institute) and L. Trevisan (UC Berkeley). $140,000, 9/03–8/07.
- NSF Information Technology Research program, "ITR: Information Theoretic Secure Hyper-Encryption and Protocols," with M. Rabin (Harvard), Y. Ding (Georgia Tech), and R. Lipton (Georgia Tech). $950,000, 8/02–7/06.
- Alfred P. Sloan Research Fellowship. $40,000, 9/02–9/04.
- NSF Early Career Development Award. "A Unified Theory of Pseudorandomness." $350,000 plus $6,000 REU Supplement, 6/02–5/07.

Chronological List of Research Papers

[1] Salil P. Vadhan. The complexity of counting in sparse, regular, and planar graphs. *SIAM Journal on Computing*, 31(2):398–427, 2001. Publicly distributed in May 1997.

[2] D. Wallner, E. Harder, and R. Agee. Key management for multicast: Issues and architectures. Internet RFC 2627, June 1999. Work done by interns Kiran Kedlaya, Noam Shazeer, and Salil Vadhan at NSA Director's Summer Program 1995.

[3] Amit Sahai and Salil Vadhan. A complete problem for statistical zero knowledge. *Journal of the ACM*, 50(2):196–249, March 2003. Extended abstract in *FOCS '97*.

[4] Amit Sahai and Salil Vadhan. Manipulating statistical difference. In Panos Pardalos, Sanguthevar Rajasekaran, and José Rolim, editors, *Randomization Methods in Algorithm Design (DIMACS Workshop, December 1997)*, volume 43 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 251–270. American Mathematical Society, 1999.

[5] Michael A. Bender, Antonio Fernández, Dana Ron, Amit Sahai, and Salil Vadhan. The power of a pebble: exploring and mapping directed graphs. *Information and Computation*, 176(1):1–21, 2002. Extended abstract in *STOC '98*.

[6] Oded Goldreich, Amit Sahai, and Salil Vadhan. Honest-verifier statistical zero-knowledge equals general statistical zero-knowledge. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC '98)*, pages 399–408, Dallas, TX, May 1998. ACM.

[7] Daniel Lewin and Salil Vadhan. Checking polynomial identities over any field: Towards a derandomization? In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC '98)*, pages 438–437, Dallas, TX, May 1998. ACM.

[8] Mihir Bellare, Shai Halevi, Amit Sahai, and Salil Vadhan. Many-to-one trapdoor functions and their relation to public-key cryptosystems. In H. Krawczyk, editor, *Advances in Cryptology — CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 283–299. Springer, 1998.

[9] Ran Raz, Omer Reingold, and Salil Vadhan. Extracting all the randomness and reducing the error in Trevisan's extractors. *Journal of Computer and System Sciences*, 65(1):97–128, August 2002. Special Issue on STOC '99.

[10] Madhu Sudan, Luca Trevisan, and Salil Vadhan. Pseudorandom generators without the XOR lemma. *Journal of Computer and System Sciences*, 62:236–266, 2001. Special issue on CCC '99. Extended abstract in *STOC–CCC '99* joint session.

[11] Oded Goldreich and Salil Vadhan. Comparing entropies in statistical zero-knowledge with applications to the structure of SZK. In *Proceedings of the Fourteenth Annual IEEE Conference on Computational Complexity (CCC '99)*, pages 54–73, Atlanta, GA, May 1999. IEEE Computer Society Press.

[12] Oded Goldreich, Amit Sahai, and Salil Vadhan. Can statistical zero-knowledge be made non-interactive?, or On the relationship of SZK and NISZK. In M. Wiener, editor, *Advances in Cryptology—CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 467–484. Springer-Verlag, 15–19 August 1999.

[13] Ran Raz, Omer Reingold, and Salil Vadhan. Error reduction for extractors. In *Proceedings of the 40th Annual Symposium on the Foundations of Computer Science (FOCS '99)*, pages 191–201, New York, NY, October 1999. IEEE.

[14] Silvio Micali, Michael Rabin, and Salil Vadhan. Verifiable random functions. In *Proceedings of the 40th Annual Symposium on the Foundations of Computer Science (FOCS '99)*, pages 120–130, New York, NY, October 1999. IEEE.

[15] Oded Goldreich, Salil Vadhan, and Avi Wigderson. Simplified derandomization of BPP using a hitting set generator. Technical Report TR00-04, Electronic Colloquium on Computational Complexity, January 2000.

[16] Salil P. Vadhan. On transformations of interactive proofs that preserve the prover's complexity. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC '00)*, pages 200–207, Portland, OR, May 2000. ACM.

[17] Omer Reingold, Salil Vadhan, and Avi Wigderson. Entropy waves, the zig-zag graph product, and new constant-degree expanders. *Annals of Mathematics*, 155(1), January 2001. Extended abstract in *FOCS '00*.

[18] Luca Trevisan and Salil Vadhan. Extracting randomness from samplable distributions. In *Proceedings of the 41st Annual Symposium on Foundations of Computer Science (FOCS '00)*, pages 32–42, Redondo Beach, CA, 17–19 October 2000. IEEE.

[19] Oded Goldreich, Salil Vadhan, and Avi Wigderson. On interactive proofs with a laconic prover. *Computational Complexity*, 11:1–53, 2002. Extended abstract in *ICALP '01*.

[20] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yang. On the (im)possibility of obfuscating programs. *Journal of the ACM*, 59(2):6:1–6:48, May 2012. Preliminary versions in *CRYPTO '01*, *Cryptology ePrint archive* (Report 2001/069), and *ECCC* (TR01-057).

[21] Michael Capalbo, Omer Reingold, Salil Vadhan, and Avi Wigderson. Randomness conductors and constant-degree lossless expanders. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing (STOC '02)*, pages 659–668, Montréal, CA, May 2002. ACM. In joint session with *CCC '02*.

[22] Luca Trevisan and Salil Vadhan. Pseudorandomness and average-case complexity via uniform reductions. *Computational Complexity*, 16(4):331–364, December 2007. Preliminary version in *CCC '02*.

[23] Nenad Dedic, Leonid Reyzin, and Salil Vadhan. An improved pseudorandom generator based on hardness of factoring. In *Security in Communication Networks: Third International Conference (SCN 2002)*, volume 2576 of *Lecture Notes in Computer Science*, pages 88–101. Springer-Verlag, 11–13 September 2002.

[24] Eli Ben-Sasson, Madhu Sudan, Salil Vadhan, and Avi Wigderson. Randomness-efficient low degree tests and short PCPs via epsilon-biased sets. In *Proceedings of the 35th ACM Symposium on Theory of Computing (STOC '03)*, pages 612–621. ACM, 2003.

[25] Chi-Jen Lu, Omer Reingold, Salil Vadhan, and Avi Wigderson. Extractors: optimal up to constant factors. In *Proceedings of the 35th ACM Symposium on Theory of Computing (STOC '03)*, pages 602–611. ACM, 2003.

[26] Boaz Barak, Shien Jin Ong, and Salil Vadhan. Derandomization in cryptography. *SIAM Journal on Computing*, 37(2):380–400, May 2007. Preliminary version in *CRYPTO '03*.

[27] Daniele Micciancio and Salil Vadhan. Statistical zero-knowledge proofs with efficient provers: lattice problems and more. In D. Boneh, editor, *Advances in Cryptology—CRYPTO '03*, volume 2729 of *Lecture Notes in Computer Science*, pages 282–298. Springer-Verlag, 17–21 August 2003.

[28] Salil P. Vadhan. Constructing locally computable extractors and cryptosystems in the bounded-storage model. *Journal of Cryptology*, 17(1):43–77, January 2004. Extended abstract in *CRYPTO '03*.

[29] Boaz Barak, Yehuda Lindell, and Salil Vadhan. Lower bounds for non-black-box zero knowledge. *Journal of Computer and System Sciences*, 72(2):321–391, March 2006. Special Issue on FOCS '03.

[30] Minh Nguyen and Salil Vadhan. Simpler session-key generation from short random passwords. *Journal of Cryptology*, 21(1):52–96, January 2008. Extended abstract in *TCC '04*.

[31] Omer Reingold, Luca Trevisan, and Salil Vadhan. Notions of reducibility between cryptographic primitives. In M. Naor, editor, *Proceedings of the First Theory of Cryptography Conference (TCC '04)*, volume 2951 of *Lecture Notes in Computer Science*, pages 1–20. Springer-Verlag, 19–21 February 2004.

[32] Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, and Salil Vadhan. Robust PCPs of proximity, shorter PCPs, and applications to coding. *SIAM Journal on Computing*, 36(4):889–974, 2006. Special Issue on Randomness & Complexity. Extended abstract in *STOC '04*, and preliminary full version posted on ECCC as TR04-021.

[33] Alex Healy, Salil Vadhan, and Emanuele Viola. Using nondeterminism to amplify hardness. *SIAM Journal on Computing*, 35(4):903–931, 2006. Special Issue on STOC '04.

[34] Luca Trevisan, Salil Vadhan, and David Zuckerman. Compression of samplable sources. *Computational Complexity*, 14(3):186–227, December 2005. Special Issue on CCC '04.

[35] Salil P. Vadhan. An unconditional study of computational zero knowledge. *SIAM Journal on Computing*, 36(4):1160–1214, 2006. Special Issue on Randomness and Complexity. Extended abstract in *FOCS '04*.

[36] Saurabh Sanghvi and Salil Vadhan. The round complexity of two-party random selection. *SIAM Journal on Computing*, 38(2):523–550, 2008. Special Issue on *STOC '05*.

[37] Omer Reingold, Luca Trevisan, and Salil Vadhan. Pseudorandom walks in regular digraphs and the RL vs. L problem. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing (STOC '06)*, pages 457–466, 21–23 May 2006. Preliminary version as *ECCC* TR05-22, February 2005.

[38] Grant Schoenebeck and Salil Vadhan. The computational complexity of Nash equilibria in concisely represented games. *ACM Transactions on Computation Theory*, 4(2), 11–15 June 2012. Preliminary versions as *ECCC* TR05-52 and in *EC '06*.

[39] Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, and Salil Vadhan. Short PCPs verifiable in polylogarithmic time. In *Proceedings of the 20th Annual IEEE Conference on Computational Complexity (CCC '05)*, pages 120–134, 11–15 June 2005.

[40] Venkatesan Guruswami and Salil Vadhan. A lower bound on list size for list decoding. *IEEE Transactions on Information Theory*, 56(11):5681–5688, November 2010. Preliminary version in *RANDOM '05*.

[41] Eyal Rozenman and Salil Vadhan. Derandomized squaring of graphs. In *Proceedings of the 8th International Workshop on Randomization and Computation (RANDOM '05)*, number 3624 in Lecture Notes in Computer Science, pages 436–447, Berkeley, CA, August 2005. Springer.

[42] Daniele Micciancio, Shien Jin Ong, Amit Sahai, and Salil Vadhan. Concurrent zero knowledge without complexity assumptions. In S. Halevi and T. Rabin, editors, *Proceedings of the Third Theory of Cryptography Conference (TCC '06)*, volume 3876 of *Lecture Notes in Computer Science*, pages 1–20. Springer-Verlag, 4–7 March 2006.

[43] Jesse Kamp, Anup Rao, Salil Vadhan, and David Zuckerman. Deterministic extractors for small-space sources. *Journal of Computer and System Sciences*, 77(1):191–220, January 2011. Special issue to celebrate Richard Karp's Kyoto Prize. Extended abstract in *STOC '06*.

[44] Minh Nguyen and Salil Vadhan. Zero knowledge with efficient provers. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing (STOC '06)*, pages 287–295, 21–23 May 2006.

[45] Ronen Gradwohl, Salil Vadhan, and David Zuckerman. Random selection with an adversarial majority. In C. Dwork, editor, *Advances in Cryptology—CRYPTO '06*, number 4117 in Lecture Notes in Computer Science, pages 409–426. Springer-Verlag, 20–24 August 2006. Full version posted as ECCC TR06-26.

[46] Minh-Huyen Nguyen, Shien Jin Ong, and Salil Vadhan. Statistical zero-knowledge arguments for NP from any one-way function. In *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS '06)*, pages 3–13, Berkeley, CA, 22–24 October 2006. Full version invited to *SIAM J. Computing* Special Issue on FOCS '06.

[47] Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *Journal of the ACM*, 56(4):1–34, 2009. Preliminary version recipient of Best Paper Award at *CCC '07*.

[48] Shien Jin Ong and Salil Vadhan. Zero knowledge and soundness are symmetric. In M. Naor, editor, *Advances in Cryptology—EUROCRYPT '07*, volume 4515 of *Lecture Notes in Computer Science*, pages 187–209. Springer-Verlag, 20–24 May 2007. Recipient of Best Paper Award. Preliminary version posted on *ECCC* as TR06-139, November 2006.

[49] Kai-Min Chung, Omer Reingold, and Salil Vadhan. S-T connectivity on digraphs with a known stationary distribution. *ACM Transactions on Algorithms*, 7(3):Art. 30, 21, 2011. Preliminary versions in *CCC '07* and on *ECCC* (TR07-030).

[50] Dana Ron, Amir Rosenfeld, and Salil Vadhan. The hardness of the expected decision depth problem. *Information Processing Letters*, 101(3):112–118, 2007.

[51] Ran Canetti, Ron Rivest, Madhu Sudan, Luca Trevisan, Salil Vadhan, and Hoeteck Wee. Amplifying collision-resistance: A complexity-theoretic treatment. In A. Menezes, editor, *Advances in Cryptology—CRYPTO '07*, number 4622 in Lecture Notes in Computer Science, pages 264–283. Springer-Verlag, 19–23 August 2007.

[52] Kai-Min Chung, Michael Mitzenmacher, and Salil P. Vadhan. Why simple hash functions work: Exploiting the entropy in a data stream. *Theory of Computing*, 9:897–945, 2013. Merge of conference papers from SODA '08 (with the same title) and RANDOM '08 (entitled "Tight Bounds for Hashing Block Sources").

[53] André Chailloux, Dragos Florin Ciocan, Iordanis Kerenidis, and Salil Vadhan. Interactive and noninteractive zero knowledge are equivalent in the help model. In R. Canetti, editor, *Proceedings of the Third Theory of Cryptography Conference (TCC '08)*, volume 4948 of *Lecture Notes in Computer Science*, pages 501–534. Springer-Verlag, 19–21 March 2008.

[54] Shien Jin Ong and Salil Vadhan. An equivalence between zero knowledge and commitments. In R. Canetti, editor, *Proceedings of the Third Theory of Cryptography Conference (TCC '08)*, volume 4948 of *Lecture Notes in Computer Science*, pages 482–500. Springer-Verlag, 19–21 March 2008.

[55] Iftach Haitner, Minh Nguyen, Shien Jin Ong, Omer Reingold, and Salil Vadhan. Statistically hiding commitments and statistical zero-knowledge arguments from any one-way function. *SIAM Journal on Computing*, 39(3):1153–1218, 2009. Special Issue on *STOC '07*. Merge of papers from FOCS '06 and STOC '07. Received *SIAM Outstanding Paper Prize 2011*.

[56] Dan Gutfreund and Salil Vadhan. Limitations on hardness vs. randomness under uniform reductions. In *Proceedings of the 12th International Workshop on Randomization and Computation (RANDOM '08)*, volume 5171 of *Lecture Notes in Computer Science*, pages 469–482. Springer-Verlag, 25–27 August 2008.

[57] Andrej Bogdanov, Elchanan Mossel, and Salil Vadhan. The complexity of distinguishing markov random fields. In *Proceedings of the 12th International Workshop on Randomization and Computation (RANDOM '08)*, volume 5171 of *Lecture Notes in Computer Science*, pages 331–342. Springer-Verlag, 25–27 August 2008.

[58] Shien Jin Ong, David Parkes, Alon Rosen, and Salil Vadhan. Fairness with an honest minority and a rational majority. In O. Reingold, editor, *Proceedings of the Fourth Theory of Cryptography Conference (TCC '09)*, volume 5444 of *Lecture Notes in Computer Science*, pages 36–53. Springer-Verlag, 15–17 March 2009. Preliminary version posted as *Cryptology ePrint Archive* Report 2008/097, March 2008.

[59] Omer Reingold, Luca Trevisan, Madhur Tulsiani, and Salil Vadhan. Dense subsets of pseudorandom sets. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS '08)*, pages 76–85. IEEE, 26–28 October 2008.

[60] Yevgeniy Dodis, Salil Vadhan, and Daniel Wichs. Proofs of retrievability via hardness amplification. In O. Reingold, editor, *Proceedings of the Fourth Theory of Cryptography Conference (TCC '09)*, volume 5444 of *Lecture Notes in Computer Science*, pages 109–127. Springer-Verlag, 15–17 March 2009.

[61] Cynthia Dwork, Moni Naor, Omer Reingold, Guy Rothblum, and Salil Vadhan. On the complexity of differentially private data release: Efficient algorithms and hardness results. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC '09)*, pages 381–390, 31 May–2 June 2009.

[62] Iftach Haitner, Omer Reingold, Salil Vadhan, and Hoeteck Wee. Inaccessible entropy. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC '09)*, pages 611–620, 31 May–2 June 2009.

[63] Luca Trevisan, Madhur Tulsiani, and Salil Vadhan. Regularity, boosting, and efficiently simulating every high-entropy distribution. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity (CCC '09)*, pages 126–136, 15–18 July 2009. Preliminary version posted as *ECCC* TR08-103.

[64] Guy Rothblum and Salil Vadhan. Are PCPs inherent in efficient arguments? *Computational Complexity*, 19(2):265–304, May 2010. Special Issue on *CCC '09*.

[65] Ilya Mironov, Omkant Pandey, Omer Reingold, and Salil Vadhan. Computational differential privacy. In S. Halevi, editor, *Advances in Cryptology—CRYPTO '09*, volume 5677 of *Lecture Notes in Computer Science*, pages 126–142. Springer-Verlag, 16–20 August 2009.

[66] Shachar Lovett, Omer Reingold, Luca Trevisan, and Salil Vadhan. Pseudorandom bit generators that fool modular sums. In *Proceedings of the 13th International Workshop on Randomization and Computation (RANDOM '09)*, volume 5687 of *Lecture Notes in Computer Science*, pages 615–630. Springer-Verlag, 21–23 August 2009.

[67] Eleanor Birrell and Salil Vadhan. Composition of zero-knowledge proofs with efficient provers. In Daniele Micciancio, editor, *Proceedings of the 7th IACR Theory of Cryptography Conference (TCC '10)*, volume 5978 of *Lecture Notes on Computer Science*, pages 572–587. Springer-Verlag, 9–11 February 2010.

[68] Iftach Haitner, Thomas Holenstein, Omer Reingold, Salil Vadhan, and Hoeteck Wee. Inaccessible entropy II: IE functions and universal one-way hashing. *Theory of Computing*, 16(8):1–55, 2020. Preliminary version in EUROCRYPT '10.

[69] Iftach Haitner, Omer Reingold, and Salil Vadhan. Efficiency improvements in constructing pseudorandom generators from one-way functions. *SIAM Journal on Computing*, 42(3):1405–1430, 2013. Special Issue on *STOC '10*.

[70] Cynthia Dwork, Guy Rothblum, and Salil Vadhan. Boosting and differential privacy. In *Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS '10)*, pages 51–60. IEEE, 23–26 October 2010.

[71] Jonathan Ullman and Salil Vadhan. PCPs and the hardness of generating synthetic data. *Journal of Cryptology*, 33:2078–2112, July 2020. Special Issue on *TCC '11*. Preliminary version posted as *ECCC* TR10-017.

[72] Kai-Min Chung, Yael Kalai, and Salil Vadhan. Improved delegation of computation using fully homomorphic encryption. In T. Rabin, editor, *Advances in Cryptology—CRYPTO '10*, volume 6223 of *Lecture Notes in Computer Science*, pages 483–501. Springer-Verlag, 15–19 August 2010. Full version posted as Cryptology ePrint Archive Report 210/241.

[73] Andrew McGregor, Ilya Mironov, Toniann Pitassi, Omer Reingold, Kunal Talwar, and Salil Vadhan. The limits of two-party differential privacy. In *Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS '10)*, pages 81–90. IEEE, 23–26 October 2010.

[74] Zeev Dvir, Dan Gutfreund, Guy Rothblum, and Salil Vadhan. On approximating the entropy of polynomial mappings. In *Proceedings of the Second Symposium on Innovations in Computer Science (ICS 2011)*. Tsinghua University Press, 7–9 January 2011. Full version posted as ECCC TR10-60.

[75] Yakir Reshef and Salil Vadhan. On extractors and exposure-resilient functions for sublogarithmic entropy. *Random Structures & Algorithms*, 42(3):386–401, May 2013. Preliminary version posted as `arXiv:1003.4029` (Dec. 2010).

[76] Mohammad Mahmoody, Tal Moran, and Salil Vadhan. Time-lock puzzles in the random oracle model. In P. Rogaway, editor, *Advances in Cryptology—CRYPTO '11*, volume 6841 of *Lecture Notes in Computer Science*, pages 39–50. Springer-Verlag, 14–18 August 2011.

[77] Yevgeniy Dodis, Thomas Ristenpart, and Salil Vadhan. Randomness condensers for efficiently samplable, seed-dependent sources. In Ronald Cramer, editor, *Proceedings of the 9th IACR Theory of Cryptography Conference (TCC '12)*, volume 7194 of *Lecture Notes on Computer Science*, pages 618–635. Springer-Verlag, 19–21 March 2012.

[78] Mohammad Mahmoody, Tal Moran, and Salil Vadhan. Publicly verifiable proofs of sequential work. In *Innovations in Theoretical Computer Science (ITCS '13)*, pages 373–388. ACM, 9–12 January 2013. Preliminary version posted as Cryptology ePrint Archive Report 2011/553, under title "Non-Interactive Time-Stamping and Proofs of Work in the Random Oracle Model".

[79] Salil Vadhan and Colin Jia Zheng. Characterizing pseudoentropy and simplifying pseudorandom generator constructions. In *Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC '12)*, pages 817–836, 19–22 May 2012. Full version posted as *ECCC* TR11-141.

[80] Yiling Chen, Stephen Chong, Ian A. Kash, Tal Moran, and Salil P. Vadhan. Truthful mechanisms for agents that value privacy. *ACM Transactions on Economics and Computation*, 4(3), 2016. Special issue on EC '13. Preliminary version at `arXiv:1111.5472 [cs.GT]` (Nov. 2011).

[81] Justin Thaler, Jonathan Ullman, and Salil Vadhan. Faster algorithms for privately releasing marginals. In Artur Czumaj, Kurt Mehlhorn, Andrew M. Pitts, and Roger Wattenhofer, editors, *Proceedings of the 39th International Colloquium on Automata, Languages, and Programming (ICALP '12)*, volume 7391 of *Lecture Notes on Computer Science*, pages 810–821. Springer-Verlag, 9–13 July 2012. Full version posted as `arXiv:1205.1758v2`.

[82] Yevgeniy Dodis, Adriana López-Alt, Ilya Mironov, and Salil Vadhan. Differential privacy with imperfect randomness. In Ran Canetti and Rei Safavi-Naini, editors, *Proceedings of the 32nd International Cryptology Conference (CRYPTO '12)*, volume 7417 of *Lecture Notes on Computer Science*, pages 497–516. Springer-Verlag, 19–23 August 2012.

[83] Cynthia Dwork, Moni Naor, and Salil Vadhan. The privacy of the analyst and the power of the state. In *Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS '12)*, pages 400–409. IEEE, 20–23 October 2012.

[84] Parikshit Gopalan, Raghu Meka, Omer Reingold, Luca Trevisan, and Salil Vadhan. Better pseudorandom generators via milder pseudorandom restrictions. In *Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS '12)*, pages 120–129. IEEE, 20–23 October 2012. Full version posted as ECCC TR12-123 and as arXiv:1210.0049 [cs.CC].

[85] Guy N. Rothblum, Salil Vadhan, and Avi Wigderson. Interactive proofs of proximity: delegating computation in sublinear time. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC '13)*, pages 793–802, New York, NY, USA, 2013. ACM.

[86] Ananth Raghunathan, Gil Segev, and Salil P. Vadhan. Deterministic public-key encryption for adaptively-chosen plaintext distributions. *Journal of Cryptology*, 31(4):1012–1063, October 2018. Preliminary versions in EUROCRYPT '13 and Cryptology ePrint report 2013/125.

[87] Salil Vadhan and Colin Jia Zheng. A uniform min-max theorem with applications in cryptography. In Ran Canetti and Juan Garay, editors, *Advances in Cryptology—CRYPTO '13*, volume 8042 of *Lecture Notes on Computer Science*, pages 93–110. Springer, 18–22 August 2013. Full version posted as *ECCC* TR13-101 and *Cryptology ePrint Archive* Report 2013/437.

[88] Omer Reingold, Thomas Steinke, and Salil Vadhan. Pseudorandomness for regular branching programs via Fourier analysis. In Sofya Raskhodnikova and Joseé Rolim, editors, *Proceedings of the 17th International Workshop on Randomization and Computation (RANDOM '13)*, volume 8096 of *Lecture Notes in Computer Science*, pages 655–670. Springer-Verlag, 21–23 August 2013. Full version posted as ECCC TR13-086 and arXiv:1306.3004 [cs.CC].

[89] Parikshit Gopalan, Salil Vadhan, and Yuan Zhou. Locally testable codes and Cayley graphs. In Moni Naor, editor, *Innovations in Theoretical Computer Science (ITCS '14)*, pages 81–92. ACM, 12–14 January 2014. Full version posted as arXiv:1308.5158 [cs.CC].

[90] Kobbi Nissim, Salil Vadhan, and David Xiao. Redrawing the boundaries on purchasing data from privacy-sensitive individuals. In Moni Naor, editor, *Innovations in Theoretical Computer Science (ITCS '14)*, pages 411–422. ACM, 12–14 January 2014. Full version posted as arXiv:1401.4092 [cs.GT].

[91] Mark Bun, Jonathan Ullman, and Salil Vadhan. Fingerprinting codes and the price of approximate differential privacy. *SIAM Journal on Computing*, 47(5):1888–1938, 2018. Special Issue on STOC '14. Preliminary versions in STOC '14 and arXiv:1311.3158 [cs.CR].

[92] Alexandra Wood, David O'Brien, Micah Altman, Alan Karr, Urs Gasser, Michael Bar-Sinai, Kobbi Nissim, Jonathan Ullman, Salil Vadhan, and Michael Wojcik. Integrating approaches to privacy across the research lifecycle: Long-term longitudinal studies. *Berkman Center Research Publication No. 2014-12*, July 2014. Available at SSRN: http://ssrn.com/abstract=2469848.

[93] Thomas Steinke, Salil Vadhan, and Andrew Wan. Pseudorandomness and fourier-growth bounds for width-3 branching programs. *Theory of Computing*, 13(12):1–50, 2017. Special Issue on *RANDOM '14*. Earlier versions posted as ECCC TR14-076 and arXiv:1405.7028 [cs.CC].

[94] Yiling Chen, Or Sheffet, and Salil Vadhan. Privacy games. *ACM Transactions on Economics and Computation*, 8(2), May 2020. Preliminary version in WINE '14.

[95] David O'Brien, Jonathan Ullman, Micah Altman, Urs Gasser, Michael Bar-Sinai, Kobbi Nissim, Salil Vadhan, Michael Wojcik, and Alexandra Wood. Integrating approaches to privacy across the research lifecycle: When is information purely public? *Berkman Center Research Publication No. 2015-7*, March 2015. Available at SSRN: http://ssrn.com/abstract=2586158.

[96] Mark Bun, Kobbi Nissim, Uri Stemmer, and Salil Vadhan. Differentially private release and learning of threshold functions. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science (FOCS '15)*, pages 634–649. IEEE, 18–20 October 2015. Full version posted as arXiv:1504.07553.

[97] Sitan Chen, Thomas Steinke, and Salil P. Vadhan. Pseudorandomness for read-once, constant-depth circuits. *CoRR*, abs/1504.04675, April 2015.

[98] Jack Murtagh and Salil Vadhan. The complexity of computing the optimal composition of differential privacy. *Theory of Computing*, 14(8):1–35, 2018. Preliminary versions on *CoRR* (abs/1507.03113) and in TCC '16-A.

[99] Micah Altman, Alexandra Wood, David R. O'Brien, Salil Vadhan, and Urs Gasser. Towards a modern approach to a privacy-aware government data releases. *Berkeley Technology Law Journal*, 30(3):1967–2072, May 2016.

[100] Cynthia Dwork, Adam Smith, Thomas Steinke, Jonathan Ullman, and Salil Vadhan. Robust traceability from trace amounts. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science (FOCS '15)*, pages 650–669. IEEE, 18–20 October 2015.

[101] Kobbi Nissim, Uri Stemmer, and Salil Vadhan. Locating a small cluster privately. In *Proceedings of the 35th ACM SIGMOD-SIGACT-SIGAI Symposium on Principles of Database Systems (PODS '16)*, pages 413–427. ACM, 26 June–1 July 2016. Full version posted as arXiv:1604.05590 [cs.DS].

[102] Marco Gaboardi, Hyun Woo Lim, Ryan Rogers, and Salil Vadhan. Differentially private chi-squared hypothesis testing: Goodness of fit and independence testing. In M. Balcan and K. Weinberger, editors, *Proceedings of the 33rd International Conference on Machine Learning (ICML '16)*, pages 2111–2120, June 2016. Preliminary version posted as arXiv:1602.03090.

[103] Marco Gaboardi, James Honaker, Gary King, Jack Murtagh, Kobbi Nissim, Jonathan Ullman, and Salil Vadhan. PSI (Ψ): a private data-sharing interface. Poster presentation at the 2nd Workshop on the Theory and Practice of Differential Privacy (TPDP '16), June 2016. Paper posted as arXiv:1609.04340 [cs.CR]. http://privacytools.seas.harvard.edu/publications/psipaper.

[104] Ryan Rogers, Aaron Roth, Jonathan Ullman, and Salil Vadhan. Privacy odometers and filters: Pay-as-you-go composition. In *Advances in Neural Information Processing Systems 29 (NIPS '16)*, pages 1921–1929, December 2016. Full version posted as arXiv:1605.08294 [cs.CR].

[105] Mark Bun, Yi-Hsiu Chen, and Salil Vadhan. Separating computational and statistical differential privacy in the client-server model. In Martin Hirt and Adam D. Smith, editors, *Proceedings of the 14th IACR Theory of Cryptography Conference (TCC '16-B)*, Lecture Notes in Computer Science. Springer-Verlag, 31 October–3 November 2016. Full version posted on *Cryptology ePrint Archive*, Report 2016/820.

[106] Kobbi Nissim, Aaron Bembenek, Alexandra Wood, Mark Bun, Marco Gaboardi, Urs Gasser, David O'Brien, Thomas Steinke, and Salil Vadhan. Bridging the gap between computer science and legal approaches to privacy. *Harvard Journal of Law & Technology*, 31(2), Spring 2018. Workshopped at *PLSC '16*.

[107] Salil P. Vadhan. On learning vs. refutation. In Satyen Kale and Ohad Shamir, editors, *Proceedings of the 30th Conference on Learning Theory (COLT '17)*, volume 65 of *PMLR*, pages 1835–1848, 7–10 July 2017.

[108] Jack Murtagh, Omer Reingold, Aaron Sidford, and Salil Vadhan. Derandomization beyond connectivity: Undirected Laplacian systems in nearly logarithmic space. *SIAM Journal on Computing*, 50(6):1892–1922, 2021. Special Issue on FOCS '17. Preliminary version posted as CoRR abs/1708.04634.

[109] Yi-Hsiu Chen, Kai-Min Chung, Ching-Yi Lai, Salil P. Vadhan, and Xiaodi Wu. Computational notions of quantum min-entropy. *CoRR*, abs/1704.07309, 2017. Poster presention at QIP 2017 and oral presentation at QCrypt 2017.

[110] Vishesh Karwa and Salil Vadhan. Finite Sample Differentially Private Confidence Intervals. In Anna R. Karlin, editor, *9th Innovations in Theoretical Computer Science Conference (ITCS 2018)*, volume 94 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 44:1–44:9,

Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. Also presented at TPDP 2017. Preliminary version posted as arXiv:1711.03908 [cs.CR].

[111] Victor Balcer and Salil Vadhan. Differential Privacy on Finite Computers. *Journal of Privacy and Confidentiality*, 9(2), September 2019. Special Issue on TPDP 2017. Preliminary versions in ITCS 2018 and posted as arXiv:1709.05396 [cs.DS].

[112] Jack Murtagh, Kathryn Taylor, George Kellaris, and Salil P. Vadhan. Usable differential privacy: A case study with PSI. *CoRR*, abs/1809.04103, 2018.

[113] Yi-Hsiu Chen, Mika Göös, Salil P. Vadhan, and Jiapeng Zhang. A tight lower bound for entropy flattening. In Rocco A. Servedio, editor, *33rd Computational Complexity Conference (CCC 2018)*, volume 102 of *LIPIcs*, pages 23:1–23:28. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 22–24 June 2018. Preliminary version posted as ECCC TR18-119.

[114] Rohit Agrawal, Yi-Hsiu Chen, Thibaut Horel, and Salil Vadhan. Unifying computational entropies via Kullback-Leibler divergence. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology — CRYPTO 2019*, volume 11693 of *Lecture Notes in Computer Science*, pages 831–858. Springer, 2019. Full version posted as arXiv:1902.11202 [cs.CR].

[115] Jack Murtagh, Omer Reingold, Aaron Sidford, and Salil Vadhan. Deterministic approximation of random walks in small space. *Theory of Computing*, 17(4):1–35, September 2021. Special Issue on *APPROX-RANDOM '19*. Preliminary version posted as arXiv:1903.06361 [cs.CC].cs.CC].

[116] AmirMahdi Ahmadinejad, Jonathan Kelner, Jack Murtagh, John Peebles, Aaron Sidford, and Salil Vadhan. High-precision estimation of random walks in small space. In *Proceedings of the 61st Annual IEEE Symposium on Foundations of Computer Science (FOCS '20)*, pages 1295–1306, 2020.

[117] Dean Doron, Jack Murtagh, Salil Vadhan, and David Zuckerman. Small-space spectral sparsification via bounded-independence sampling. *ACM Transactions on Computation Theory*, 16(2), 2024. Preliminary versions in *Proc. ICALP '20* and posted as *ECCC* TR20-026.

[118] Daniel Alabi, Audra McMillan, Jayshree Sarathy, Adam Smith, and Salil Vadhan. Differentially private simple linear regression. In *Proceedings on 23rd Privacy Enhancing Technologies Symposium (PoPETS '22)*, pages 2022(2):184–204, 2022. Preliminary version posted as arXiv:2007.05157 [cs.LG] and presented as a poster at TPDP '20.

[119] Marco Gaboardi, Michael Hay, and Salil Vadhan. A programming framework for OpenDP. Poster at *6th Workshop on the Theory and Practice of Differential Privacy (TPDP '20)*. Preliminary version posted at `http://opendp.io/`, May 2020.

[120] William M. Hoza, Edward Pyne, and Salil Vadhan. Pseudorandom Generators for Unbounded-Width Permutation Branching Programs. In James R. Lee, editor, *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, volume 185 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 7:1–7:20, Dagstuhl, Germany, 2021. Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

[121] Edward Pyne and Salil Vadhan. Pseudodistributions that beat all pseudorandom generators (extended abstract). In Valentine Kabanets, editor, *Proceedings of the 36th Computational Complexity Conference (CCC '21)*, volume 200 of *LIPIcs*, pages 33:1–33:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. Invited to *Theory of Computing* Special Issue on CCC '21. Full version posted as ECCC TR21-019.

[122] Dean Doron, Raghu Meka, Omer Reingold, Avishay Tal, and Salil P. Vadhan. Pseudorandom generators for read-once monotone branching programs. In Mary Wootters, editor, *Proceedings of the International Conference on Randomization and Computation (RANDOM '21)*, volume 207 of *LIPIcs*, pages 58:1–58:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. Preliminary version posted as ECCC TR21-018.

[123] Salil Vadhan and Tianhao Wang. Concurrent composition of differential privacy. In Kobbi Nissim and Brent Waters, editors, *Proceedings of the 19th Theory of Cryptography Conference (TCC '21)*, volume 13043 of *Lecture Notes in Computer Science*, pages 582–604. IACR, Springer, November 2021. Also appeared as a poster in TPDP '21 and PPML '21. Preliminary version posted as CoRR abs/2105.14427 and Cryptology ePrint Archive Report 2021/1196.

[124] Daniel G. Alabi and Salil P. Vadhan. Differentially private hypothesis testing for linear regression. *Journal of Machine Learning Research*, 24(361):1–50, 2023. Preliminary versions in NeurIPS '22, posted as arXiv:2206.14449 and presented at TPDP '21 (poster), IMS '22 (oral), and SEA '22 (oral).

[125] Jayshree Sarathy and Salil P. Vadhan. Analyzing the differentially private Theil–Sen estimator for simple linear regression. In *Proceedings of the 25th Privacy Enhancing Technologies Symposium (PoPETS '25)*, volume 1, pages 216–235, Washington, DC, 14–19 July 2025. Preliminary version presented as a poster at TPDP '21 and posted as arXiv:2207.13289 [cs.CR].

[126] William M. Hoza, Edward Pyne, and Salil Vadhan. Limitations of the Impagliazzo–Nisan–Wigderson pseudorandom generator against permutation branching programs. *Algorithmica*, 86:3153–3185, 2024. Special Issue on COCOON '21. Preliminary version posted as ECCC TR21-108.

[127] Jordan Awan and Salil Vadhan. Canonical noise and private hypothesis tests. *The Annals of Statistics*, 51(2):547–572, 2023. Preliminary version posted as CoRR abs/2108.04303 and presented orally at CCS '21 workshop on *Privacy-Preserving Machine Learning* (PPML '21) and NeurIPS '21 workshop on *Privacy in Machine Learning* (PriML '21).

[128] Edward Pyne and Salil Vadhan. Deterministic approximation of random walks via queries in graphs of unbounded size. In Karl Bringmann and Timothy Chan, editors, *Proceedings of the SIAM Symposium on Simplicity in Algorithms (SOSA '22)*, pages 57–67, January 2022. Preliminary version posted as arXiv:2111.01997 [cs.CC].

[129] Louis Golowich and Salil Vadhan. Pseudorandomness of expander random walks for symmetric functions and permutation branching programs. In Anindya De, editor, *Proceedings of the 37th Computational Complexity Conference (CCC '22)*, volume 234 of *LIPIcs*, pages 27:1–27:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. Full version posted as ECCC TR22-024.

[130] Chin Ho Lee, Edward Pyne, and Salil Vadhan. Fourier Growth of Regular Branching Programs. In Amit Chakrabarti and Chaitanya Swamy, editors, *Proceedings of the International Conference on Randomization and Computation (RANDOM '22)*, volume 245 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 2:1–2:21, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. Preliminary version posted as ECCC TR22-034.

[131] Sílvia Casacuberta, Michael Shoemate, Salil Vadhan, and Connor Wagaman. Widespread underestimation of sensitivity in differentially private libraries and how to fix it. In *Proceedings of the 29th ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*, page 471–484, 7–11 November 2022. Preprint posted as arXiv:2207.10635 [cs.CR].

[132] Salil Vadhan and Wanrong Zhang. Concurrent composition theorems for differential privacy. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC '23)*, pages 507–519, 20–23 June 2023. Preliminary versions posted as arXiv:2207.08335 [cs.DS] and presented as a poster at TPDP '22.

[133] Jayshree Sarathy, Sophia Song, Audrey Haque, Tania Schlatter, and Salil Vadhan. Don't look at the data! How differential privacy reconfigures practices of data science. In Albrecht Schmidt, Kaisa Väänänen, Tesh Goyal, Per Ola Kristensson, Anicia Peters, Stefanie Mueller, Julie R. Williamson, and Max L. Wilson, editors, *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*, pages 164:1–164:19. ACM, 23–28 April 2023. Preliminary version presented as a poster at TPDP '22 and posted as arXiv:2302.11775 [cs.HC].

[134] AmirMahdi Ahmadinejad, John Peebles, Edward Pyne, Aaron Sidford, and Salil P. Vadhan. Singular value approximation and sparsifying random walks on directed graphs. In *64th IEEE Annual Symposium on Foundations of Computer Science (FOCS '23)*, pages 846–854. IEEE, 6–9 November 2023. Preliminary version posted as arXiv:2301.13541 [cs.DS].

[135] Merveille Koissi Savi, Akash Yadav, Wanrong Zhang, Navin Vembar, Andrew Schroeder, Satchit Balsari, Caroline O. Buckee, Salil Vadhan, and Nishant Kishore. A standardised differential privacy framework for epidemiological modeling with mobile phone data. *PLOS Digital Health*, 2(10):1–15, 10 2023. Preliminary version posted as medRxiv 2023.03.16.23287382.

[136] Chin Ho Lee, Edward Pyne, and Salil P. Vadhan. On the power of regular and permutation branching programs. In Nicole Megow and Adam D. Smith, editors, *Proceedings of the International Conference on Randomization and Computation (RANDOM '23)*, volume 275 of *LIPIcs*, pages 44:1–44:22. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023.

[137] Samuel Haney, Michael Shoemate, Grace Tian, Salil P. Vadhan, Andrew Vyrros, Vicki Xu, and Wanrong Zhang. Concurrent composition for interactive differential privacy with adaptive privacy-loss parameters. In Weizhi Meng, Christian Damsgaard Jensen, Cas Cremers, and Engin Kirda, editors, *Proceedings of the 30th ACM SIGSAC Conference on Computer and Communications Security (CCS '23)*, pages 1949–1963. ACM, 2023. Received a CCS '23 Distinguished Paper Award and invited to Special Issue of *J. Privacy & Confidentiality* on TPDP '23. Preliminary version presented as a poster at TPDP '23 and posted as arXiv:2309.05901 [cs.CR].

[138] Nico Manzonelli, Wanrong Zhang, and Salil Vadhan. Membership inference attacks and privacy in topic modeling. *Transactions on Machine Learning Research*, 2024. Preliminary version presented as a poster at TPDP '23 and posted as arXiv:2403.04451 [cs.CR].

[139] Lukman Olagoke, Salil Vadhan, and Seth Neel. Black-box training data identification in GANs via detector networks. arXiv:2310.12063v1 [cs.LG], October 2023.

[140] Zachary Ratliff and Salil Vadhan. A framework for differential privacy against timing attacks. In *Proceedings of the 31st ACM SIGSAC Conference on Computer and Communications Security (CCS '24)*, pages 3615–3629. ACM, 2024. Received a CCS '24 Distinguished Artifact Award. Preliminary version presented as a poster at TPDP '24 and posted as arXiv:2409.05623 [cs.CR].

[141] Sílvia Casacuberta, Cynthia Dwork, and Salil Vadhan. Complexity-theoretic implications of multicalibration. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing (STOC '24)*, STOC 2024, pages 1071—1082, New York, NY, USA, 2024. Association for Computing Machinery. Preliminary version posted as CoRR:abs/2312.17223.

[142] Patrick Song, Jayshree Sarathy, Michael Shoemate, and Salil Vadhan. "I inherently just trust that it works": Investigating mental models of open-source libraries for differential privacy. In *Proceedings of the 27th ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW '24)*, volume 8, pages 1–39. ACM, 2024. Also posted as arXiv:2410.09721 [cs.HC].

[143] Clément L. Canonne, Francis E. Su, and Salil P. Vadhan. The Randomness Complexity of Differential Privacy. In Raghu Meka, editor, *Proceedings of the 16th Innovations in Theoretical Computer Science Conference (ITCS 2025)*, volume 325 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 27:1–27:21, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. Preliminary version posted as *ECCC* TR24-169.

[144] Monika Henzinger, Roodabeh Safavi, and Salil Vadhan. Concurrent composition for continual mechanisms. arXiv:2411.03299 [cs.DS], November 2024. To appear in *PODS '26*.

[145] Cassandra Marcussen, Aaron Putterman, and Salil Vadhan. Characterizing the distinguishability of product distributions through multicalibration. In Srikanth Srinivasan, editor, *Proceedings of the 40th Computational Complexity Conference (CCC '25)*, volume 339 of *LIPIcs*, pages 19:1–19:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025. Full version posted as arXiv:2412.03562 [cs.CR].

[146] Tommaso d'Orsi, Chris Jones, Jake Ruotolo, Salil Vadhan, and Jiyu Zhang. Sparsest Cut and Eigenvalue Multiplicities on Low Degree Abelian Cayley Graphs. In Alina Ene and Eshan Chattopadhyay, editors, *Proceedings of the 28th International Conference on Approximation Algorithms for Combinatorial Optimization Problems(APPROX '25)*, volume 353 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 16:1–16:20, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. Preliminary version posted as arXiv:2412.17115 [cs.DS].

[147] Zachary Ratliff and Salil Vadhan. Securing unbounded differential privacy against timing attacks. In Benny Applebaum and Huijia (Rachel) Lin, editors, *Proceedings of the 23rd Theory*

of Cryptography Conference (TCC '25), volume 16271 of *Lecture Notes in Computer Science*, pages 378–414. IACR, Springer, December 2025. Full version posted as arXiv:2506.07868 [cs.CR].

[148] Lunjia Hu and Salil Vadhan. Generalized and unified equivalences between hardness and pseudoentropy. In Benny Applebaum and Huijia (Rachel) Lin, editors, *Proceedings of the 23rd Theory of Cryptography Conference (TCC '25)*, volume 16271 of *Lecture Notes in Computer Science*, pages 258–288, Cham, December 2025. IACR, Springer. Outstanding Paper Award. Preliminary version posted as arXiv:2507.05972 [cs.CC].

[149] Jake Ruotolo and Salil Vadhan. Singular values versus expansion in directed and undirected graphs. arXiv:2508.17539 [math.CO], August 2025.

[150] Priyanka Nanayakkara, Elena Ghazi, and Salil Vadhan. Practitioners' perspectives on a differential privacy deployment registry. arXiv:2509.13509 [cs.CR], September 2025.

Theses, Surveys, Books, and Policy Commentary

[1] Salil P. Vadhan. *The Complexity of Counting*. Undergraduate thesis, Harvard University, Cambridge, MA, 1995.

[2] Salil P. Vadhan. Rapidly mixing Markov chains and their applications. Essay, Churchill College, Cambridge University, May 1996.

[3] Salil P. Vadhan. *A Study of Statistical Zero-Knowledge Proofs*. PhD thesis, Massachusetts Institute of Technology, August 1999. To be published by Springer-Verlag for winning the *ACM Doctoral Dissertation Award 2000*.

[4] Salil Vadhan. Probabilistic proof systems, part I — interactive & zero-knowledge proofs. In S. Rudich and A. Wigderson, editors, *Computational Complexity Theory*, volume 10 of *IAS/Park City Mathematics Series*, pages 315–348. American Mathematical Society, 2004.

[5] Jose Rolim and Salil Vadhan, editors. *Proceedings of 6th International Workshop on Randomization and Approximation in Computer Science (RANDOM '02)*, volume 2483 of *Lecture Notes in Computer Science*. Springer-Verlag, 13–15 September 2002.

[6] Salil Vadhan. Computational complexity. In Henk van Tilborg, editor, *Encyclopedia of Cryptography and Security*. Springer, 2005.

[7] Oded Goldreich and Salil Vadhan, editors. *Special Issue on Worst-Case vs. Average-Case Complexity*, volume 16 (4) of *Computational Complexity*. Birkhäuser Verlag, December 2007.

[8] Salil P. Vadhan, editor. *Proceedings of 4th Theory of Cryptography Conference (TCC '07)*, volume 4392 of *Lecture Notes in Computer Science*. Springer-Verlag, 21–24 February 2007.

[9] Salil P. Vadhan. The unified theory of pseudorandomness. In *Proceedings of the International Congress of Mathematicians*, volume IV, pages 2723–2748. Hindustan Book Agency, 19–27 August 2010. Preliminary version in *SIGACT NEWS* '07.

[10] Salil Vadhan. The complexity of zero knowledge. In V. Arvind and S. Prasad, editors, *FSTTCS 2007: Foundations of Software Technology and Theoretical Computer Science, 27th International Conference*, number 4855 in Lecture Notes in Computer Science, pages 52–70. Springer-Verlag, 12–14 December 2007.

[11] Salil Vadhan, editor. *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing (STOC '11)*. ACM, 6–8 June 2011.

[12] Salil Vadhan, David Abrams, Micah Altman, Cynthia Dwork, Paul Kominers, Scott Duke Kominers, Harry R. Lewis, Tal Moran, and Guy Rothblum. Comments on advance notice of proposed rulemaking: Human subjects research protections: Enhancing protections for research subjects and reducing burden, delay, and ambiguity for investigators, docket id number hhs-ophs–2011–0005. http://www.regulations.gov/#!documentDetail;D=HHS-OPHS-2011-0005-1101, October 2011.

[13] Salil P. Vadhan. *Pseudorandomness*, volume 7 (1–3) of *Foundations and Trends in Theoretical Computer Science*. now publishers, December 2012. 336 pages.

[14] Oded Goldreich and Salil Vadhan, editors. *Special Issue from RANDOM '09*, volume 21 (1) of *Computational Complexity*. Birkhäuser Verlag, December 2012.

[15] Kousha Etessami, Dieter van Melkebeek, Seth Pettie, John Watrous, and Salil Vadhan, editors. *Special section on the 43rd Annual ACM Symposium on Theory of Computing (STOC 2011)*, volume 41 (5) of *SIAM Journal on Computing*, 2012.

[16] Micah Altman, David O'Brien, Salil Vadhan, and Alexandra Wood. Re: Big data study; request for information. Submitted to the White House Office of Science and Technology Policy (OSTP), March 2014. on behalf of the *Privacy Tools for Sharing Research Data Project*.

[17] Daniel J. Weitzner, Hal Abelson, Cynthia Dwork, Cameron Kerry, Daniela Rus, Sandy Pentland, and Salil Vadhan. Consumer privacy bill of rights and big data: Response to white house office of science and technology policy request for information. Submitted to bigdata@ostp.gov, April 2014.

[18] Lorrie Cranor, Tal Rabin, Vitaly Shmatikov, Salil Vadhan, and Danny Weitzner. Towards a privacy research roadmap for the computing community. Computing Community Consortium (CCC) whitepaper, May 2015. Available at http://cra.org/ccc/resources/ccc-led-whitepapers/ and as arXiv:1604.03160 [cs.CY].

[19] Alexandra Wood, Edo Airoldi, Micah Altman, Yves-Alexandre de Montjoye, Urs Gasser, David O'Brien, and Salil Vadhan. Comments on notice of proposed rulemaking: Revising the federal policy for the protection of human subjects, Docket ID number HHS-OPHS-2015-0008-2015. http://www.regulations.gov/#!documentDetail;D=HHS-OPHS-2015-0008-2015, January 2016.

[20] Salil P. Vadhan. The complexity of differential privacy. In Yehuda Lindell, editor, *Tutorials on the Foundations of Cryptography — Dedicated to Oded Goldreich*, pages 347–450. Springer, 2017.

[21] Iftach Haitner and Salil P. Vadhan. The many entropies in one-way functions. In Yehuda Lindell, editor, *Tutorials on the Foundations of Cryptography — Dedicated to Oded Goldreich*, pages 159–217. Springer, 2017. Also posted as *ECCC* TR17-084.

[22] Alexandra Wood, Micah Altman, Suso Baleato, and Salil Vadhan. Comments to the Future of Privacy Forum on the City of Seattle Open Data Risk Assessment. https://privacytools.seas.harvard.edu/publications/city-seattle-open-data-risk-assessment, October 2017.

[23] Alexandra Wood, Micah Altman, Aaron Bembenek, Mark Bun, Marco Gaboardi, James Honaker, Kobbi Nissim, David R. O'Brien, Thomas Steinke, and Salil Vadhan. Differential privacy: A primer for a non-technical audience. *Vanderbilt Journal of Entertainment & Technology Law*, 21(1):209–275, 2018. Preliminary version workshopped at PLSC 2017.

[24] Salil Vadhan. A primer on differential privacy. Creating a Platform for the Sharing of Sensitive Online Data: Whitepapers, November 2018. `https://securelysharingdata.com/whitepapers.html`.

[25] Salil Vadhan. Computational entropy. In Oded Goldreich, editor, *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 693–726. ACM, 2019.

[26] The OpenDP Team. The OpenDP whitepaper. Presented at 1st OpenDP Community Meeting and posted at `http://opendp.io/`, May 2020.

[27] Kai-Min Chung, Michael Mitzenmacher, and Salil Vadhan. When simple hash functions suffice. In Tim Roughgarden, editor, *Beyond the Worst-Case Analysis of Algorithms*, pages 567–585. Cambridge University Press, 2021.

[28] Alexandra Wood, Micah Altman, Kobbi Nissim, and Salil Vadhan. Designing access with differential privacy. In Shawn Cole, Iqbal Dhaliwal, Anja Sautmann, and Lars Vilhuber, editors, *Using Administrative Data for Research and Evidence-based Policy — A Handbook*, chapter 6, pages 173–242. Abdul Latif Jameel Poverty Action Lab (J-PAL), Cambridge, MA, 2020.

[29] Ruobin Gong, Erica L. Groshen, and Salil Vadhan, editors. *Special Issue on Differential Privacy for the 2020 U.S. Census: Can We Make Data Both Private and Useful?* Harvard Data Science Review. June 2022.

[30] National Academies of Sciences, Engineering, and Medicine. *A Roadmap for Disclosure Avoidance in the Survey of Income and Program Participation.* The National Academies Press, Washington, DC, 2023. Member of ad hoc consensus study panel that produced report.

[31] Boaz Barak, Yael Kalai, Ran Raz, Salil Vadhan, and Nisheeth K. Vishnoi. On the works of Avi Wigderson. In Helge Holden and Ragni Piene, editors, *The Abel Prize 2018–2022*. Springer, Cham, 2024. Posted as arXiv:2307.09524 [cs.CC].

[32] Marco Gaboardi, Michael Hay, and Salil Vadhan. Programming frameworks for differential privacy. In *Differential Privacy in Artificial Intelligence: From, Theory to Practice*. Emerald Publishing Limited, July 2025. Preliminary version posted as arXiv:2403.11088 [cs.CR].

[33] William Gasarch (ed.), Lance Fortnow, Oded Goldreich, Johan Håstad, Salil Vadhan, and David Williamson. Open problems in honor of Luca Trevisan. *SIGACT News*, 55(4):32–48, December 2024.

[34] Andrea Clementi, Venkatesan Guruswami, Kristin Kane, Alon Rosen, Nikhil Srivastava, Salil Vadhan, and Riccardo Zecchina. Obituary for Luca Trevisan. *Bulletin of the European Association for Theoretical Computer Science (EATCS)*, 145, February 2025.

[35] Micah Altman, Sharon (Ayalde) Gibbons, Rachel Cummings, Damien Desfontaines, Jack Fitzsimons, Elena Ghazi, Andrew Gruen, James Honaker, Gary Howarth, Nitin Kohli, Chuck McCallum, Deirdre Mulligan, Priyanka Nanayakkara, Joseph P. Near, Robert Pisarczyk, and Salil Vadhan. A community-driven differential privacy deployment registry. Technical Report NIST IR 8588, National Institute of Standards & Technology, September 2025. Initial Public Draft.

Other Work from Research Group

[1] Eli Ben-Sasson. Hard examples for bounded depth frege. *Computational Complexity*, 11:109.136, 2002.

[2] Eli Ben-Sasson. Size space tradeoffs for resolution. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing (STOC '02)*, pages 457–464 (electronic), New York, 2002. ACM.

[3] Mikhail Alekhnovich, Eli Ben-Sasson, Alexander Razborov, and Avi Wigderson. Space complexity in propositional calculus. *SIAM Journal on Computing*, 31(4):1184–1211, 2003.

[4] Michael Alekhnovich, Eli Ben-Sasson, Alexander A. Razborov, and Avi Wigderson. Pseudorandom generators in propositional proof complexity. *SIAM Journal on Computing*, 34(1):67–88 (electronic), 2004.

[5] Eli Ben-Sasson, Russell Impagliazzo, and Avi Wigderson. Near optimal separation of tree-like and general resolution. *Combinatorica*, 24(4):585–603, 2004.

[6] Eli Ben-Sasson, Prahladh Harsha, and Sofya Raskhodnikova. Some 3CNF properties are hard to test. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing (STOC '03)*, pages 345–354 (electronic), New York, 2003. ACM.

[7] Eli Ben-Sasson and Nicola Galesi. Space complexity of random formulae in resolution. *Random Structures and Algorithms*, 23(1):92.109, August 2003.

[8] Eli Ben-Sasson, Oded Goldreich, and Madhu Sudan. Bounds on 2-query codeword testing. In *Approximation, randomization, and combinatorial optimization (APPROX–RANDOM '03)*, volume 2764 of *Lecture Notes in Computer Science*, pages 216–227. Springer, Berlin, 2003.

[9] Mikhail Alekhnovich and Eli Ben-Sasson. Linear upper bounds for random walk on small density random 3-CNFs. In *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS '03)*, pages 352–361, 2003.

[10] Emanuele Viola. The complexity of constructing pseudorandom generators from hard functions. *Computational Complexity*, 13(3-4):147–188, 2004. Preliminary version entitled "Hardness versus Randomness within Alternating Time" in *CCC '04*.

[11] Dan Gutfreund and Emanuele Viola. Fooling parity tests with parity gates. In *Proceedings of the 8th International Workshop on Randomization and Computation (RANDOM '04)*, volume 3122 of *Lecture Notes in Computer Science*, pages 381–392. Springer, August 22–24 2004.

[12] Yevgeniy Dodis, Shien Jin Ong, Manoj Prabhakaran, and Amit Sahai. On the (im)possibility of cryptography with weak sources. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS '04)*, pages 196–205, Rome, Italy, 17–19 October 2004.

[13] Minh-Huyen Nguyen. The relationship between password-authenticated key exchange and other cryptographic primitives. In Joe Kilian, editor, *Proceedings of the 2nd Theory of Cryptography Conference (TCC '05)*, volume 3378 of *Lecture Notes in Computer Science*, pages 457–475. Springer-Verlag, 2005.

[14] Emanuele Viola. On constructing parallel pseudorandom generators from one-way functions. In *Proceedings of the 20th Annual Conference on Computational Complexity (CCC '05)*, pages 183–197. IEEE, June 12–15 2005.

[15] Emanuele Viola. Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates. *SIAM Journal on Computing*, 36(5):1387–1403, 2007. Preliminary version in *CCC '05*. Winner of 2006 SIAM Student Paper Competition.

[16] Rafael Pass and Alon Rosen. Concurrent non-malleable commitments. In *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS '05)*, pages 563–572, Pittsburgh, PA, 22–25 October 2005.

[17] Emanuele Viola. On approximate majority and probabilistic time. In *Proceedings of the 22nd Annual IEEE Conference on Computational Complexity (CCC '07)*, pages 155–168, June 2007. Preliminary version posted as ECCC TR05-137, November 2005.

[18] Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In S. Halevi and T. Rabin, editors, *Proceedings of the Third Theory of Cryptography Conference (TCC '06)*, volume 3876 of *Lecture Notes in Computer Science*, pages 145–166. Springer-Verlag, 4–7 March 2006.

[19] Alexander Healy and Emanuele Viola. Constant-depth circuits for arithmetic in finite fields of characteristic two. In *Proceedings of the 23rd International Symposium on Theoretical Aspects of Computer Science (STACS)*, volume 3884 of *Lecture Notes in Computer Science*, pages 672–683, 2006.

[20] Dan Gutfreund. Worst-case vs. algorithmic average-case complexity in the polynomial-time hierarchy. In *Proceedings of the 10th International Workshop on Randomization and Computation (RANDOM '06)*, volume 4110 of *Lecture Notes in Computer Science*, pages 381–392. Springer, 28–30 August 2006.

[21] Silvio Micali, Rafael Pass, and Alon Rosen. Input-indistinguishable computation. In *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS '06)*, pages 367–378, Berkeley, CA, 22–24 October 2006.

[22] Shafi Goldwasser and Guy N. Rothblum. On best-possible obfuscation. In Salil P. Vadhan, editor, *Proceedings of 4th Theory of Cryptography Conference (TCC '07)*, volume 4392 of *Lecture Notes in Computer Science*, pages 194–213. Springer-Verlag, 21–24 February 2007.

[23] Susan Hohenberger, Guy N. Rothblum, Abhi Shelat, and Vinod Vaikuntanathan. Securely obfuscating re-encryption. In Salil P. Vadhan, editor, *Proceedings of 4th Theory of Cryptography Conference (TCC '07)*, volume 4392 of *Lecture Notes in Computer Science*, pages 233–252. Springer-Verlag, 21–24 February 2007.

[24] Emanuele Viola and Avi Wigderson. Norms, XOR lemmas, and lower bounds for GF(2) polynomials and multiparty protocols. In *Proceedings of the 22nd Annual IEEE Conference on Computational Complexity (CCC '07)*, pages 141–154, June 2007.

[25] Shafi Goldwasser, Dan Gutfreund, Alexander Healy, Tali Kaufman, and Guy N. Rothblum. A (de)constructive approach to program checking. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC '08)*, 2008.

[26] Shafi Goldwasser, Yael Tauman Kalai, and Guy N. Rothblum. Delegating computation: Interactive proofs for muggles. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC '08)*, 2008.

[27] Shafi Goldwasser, Yael Tauman Kalai, and Guy N. Rothblum. One-time programs. In A. Menezes, editor, *Advances in Cryptology—CRYPTO '08*, number 5157 in Lecture Notes in Computer Science, pages 39–56. Springer-Verlag, 17–21 August 2008.

[28] Dan Gutfreund and Guy N. Rothblum. The complexity of local list decoding. In *Proceedings of the 12th International Workshop on Randomization and Computation (RANDOM '08)*, volume 5171 of *Lecture Notes in Computer Science*, pages 455–468. Springer-Verlag, 25–27 August 2008.

[29] Cynthia Dwork, Moni Naor, Guy N. Rothblum, and Vinod Vaikuntanathan. How efficient can memory checking be? In O. Reingold, editor, *Proceedings of the Fourth Theory of Cryptography Conference (TCC '09)*, volume 5444 of *Lecture Notes in Computer Science*, pages 503–520. Springer-Verlag, 15–17 March 2009.

[30] Tal Moran, Moni Naor, and Gil Segev. Deterministic history-independent strategies for storing information on write-once memories. *Theory of Computing*, 5(1):43–67, 2009.

[31] Josh Benaloh, Tal Moran, Lee Naish, Kim Ramchen, and Vanessa Teague. Shuffle-sum: Coercion-resistant verifiable tallying for stv voting. *IEEE Transactions on Information Forensics and Security*, 4(4):685–698, 2009.

[32] Kai-Min Chung and Feng-Hao Liu. Tight parallel repetition theorems for public-coin arguments. In Daniele Micciancio, editor, *Proceedings of the 7th IACR Theory of Cryptography Conference (TCC '10)*, Lecture Notes on Computer Science. Springer-Verlag, 9–11 February 2010. Best Student Paper Award.

[33] Kai-Min Chung, Feng-Hao Liu, Chi-Jen Lu, and Bo-Yin Yang. Efficient string-commitment from weak bit-commitment. In Masayuki Abe, editor, *Proceedings of the 16th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '10)*. Springer-Verlag, 5-9 December 2010.

[34] Vladimir Braverman, Kai-Min Chung, Zhenming Liu, Michael Mitzenmacher, and Rafail Ostrovsky. AMS without 4-wise independence on product domains. In Jean-Yves Marion and Thomas Schwentick, editors, *Proceedings of the 27th Symposium on Theoretical Aspects of Computer Science (STACS '10)*, pages 119–130, 2010.

[35] Tal Moran and Tyler Moore. The phish-market protocol: Secure sharing between competitors. *IEEE Security & Privacy*, 8(4):40–45, 2010. More technical version in FC 2010.

[36] Scott Duke Kominers, Mike Ruberry, and Jonathan Ullman. Course allocation by proxy auction. In *Internet and Network Economics, 6th International Workshop, WINE 2010. Proceedings*, 2010.

[37] John Kelsey, Andrew Regenscheid, Tal Moran, and David Chaum. Attacking paper-based e2e voting systems. In *Towards Trustworthy Elections*, volume 6000 of *Lecture Notes in Computer Science*, pages 370–387. Springer, 2010.

[38] Ching-Hua Yu, Sherman S.M. Chow, Kai-Min Chung, and Feng-Hao Liu. Efficient secure two-party exponentiation. In Aggelos Kiayias, editor, *Proceedings of Cryptographers' Track at the RSA Conference 2010 (CT-RSA '11)*. Springer-Verlag, 14-18 February 2011.

[39] Ian A. Kash, Michael Mitzenmacher, Justin Thaler, and Jonathan Ullman. On the zero-error capacity threshold for deletion channels. *CoRR*, abs/1102.0040, 2011. Appeared in Information Theory and Applications 2011 Workshop.

[40] Anupam Gupta, Moritz Hardt, Aaron Roth, and Jonathan Ullman. Privately releasing conjunctions and the statistical query barrier. In *Proceedings of the 43rd ACM Symposium on Theory of Computing (STOC '11)*, pages 803–812. ACM, 6–8 June 2011. Full version posted as CoRR abs/1011.1296.

[41] Anupam Gupta, Aaron Roth, and Jonathan Ullman. Iterative constructions and private data release. In *Proceedings of the 9th IACR Theory of Cryptography Conference (TCC '12)*, Lecture Notes on Computer Science. Springer-Verlag, 2012. Full version posted as CoRR abs/1107.3731.

[42] Varun Kanade and Thomas Steinke. Learning hurdles for sleeping experts. *ACM Transactions on Computation Theory (TOCT)*, 6(3):11, 2014. Special issue on ITCS '12.

[43] Michael Mitzenmacher, Thomas Steinke, and Justin Thaler. Hierarchical heavy hitters with the space saving algorithm. In *Proceedings of the Meeting on Algorithm Engineering and Experiments*, ALENEX '12, pages 160–174. SIAM, 2012.

[44] Yevgeniy Dodis, Abhishek Jain, Tal Moran, and Daniel Wichs. Counterexamples to hardness amplification beyond negligible. In Ronald Cramer, editor, *Proceedings of the 9th Theory of Cryptography Conference, (TCC '12)*, Lecture Notes on Computer Science. Springer-Verlag, 19–21 March 2012.

[45] Thomas Steinke. Pseudorandomness for permutation branching programs without the group theory. Technical Report TR12-083, Electronic Colloquium on Computational Complexity (ECCC), July 2012.

[46] Shahram Khazaei, Tal Moran, and Douglas Wikström. A mix-net from any cca2 secure cryptosystem. In Xiaoyun Wang and Kazue Sako, editors, *Asiacrypt 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 607–625. Springer, December 2012.

[47] Michael Kearns, Mallesh Pai, Aaron Roth, and Jonathan Ullman. Mechanism design in large games: incentives and privacy. In *Innovations in Theoretical Computer Science (ITCS '14)*, pages 403–410. ACM, 12–14 January 2014. Full version posted as arXiv:1207.4084 [cs.GT].

[48] Jonathan Ullman. Answering $n^{2+o(1)}$ counting queries with differential privacy is hard. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC '13)*, pages 361–370. ACM, 1–4 June 2013. Full version posted on arXiv as arXiv:1207.6945v2 [cs.CR]. Invited to *SIAM J. Computing* Special Issue on STOC '13.

[49] Justin Hsu, Aaron Roth, and Jonathan Ullman. Differential privacy for the analyst via private equilibrium computation. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing (STOC '13)*, pages 341–350. ACM, 1–4 June 2013. Full version posted as arXiv:1211.0877v2 [cs.DS].

[50] Mark Bun and Justin Thaler. Dual lower bounds for approximate degree and Markov–Bernstein inequalities. *Information and Computation*, 243:2—25, August 2015. Special issue for ICALP 2013. Conference version won Best Paper Award for Track A.

[51] Amos Beimel, Kobbi Nissim, and Uri Stemmer. Private learning and sanitization: Pure vs. approximate differential privacy. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques - 16th International Workshop, APPROX 2013, and 17th International Workshop, RANDOM 2013*, pages 363–378. ACM, August 21-23 2013.

[52] Karthekeyan Chandrasekaran, Justin Thaler, Jonathan Ullman, and Andrew Wan. Faster private release of marginals on small databases. In *Innovations in Theoretical Computer Science (ITCS '14)*, pages 387–402. ACM, 12–14 January 2014. Full version posted as arXiv:1304.3754 [cs.DS].

[53] Karthekeyan Chandrasekaran and Santosh Vempala. Integer feasibility of random polytopes. In *Proceedings of the 5th Conference on Innovations in Theoretical Computer Science (ITCS '14)*, pages 449–458. ACM, January 2014.

[54] Andrew Wan, John Wright, and Chenggang Wu. Decision trees, protocols, and the Fourier entropy influence conjecture. In *Proceedings of the 5th Conference on Innovations in Theoretical Computer Science (ITCS '14)*, pages 67–80. ACM, 12-14 January 2014. Preliminary version posted as arXiv:1312.3003.

[55] Adrian Bock, Karthekeyan Chandrasekaran, Jochen Koenemann, Britta Peis, and Laura Sanita. Finding small stabilizers for unstable graphs. In *Integer Programming and Combinatorial Optimization (IPCO '14)*, June 2014.

[56] Justin Hsu, Aaron Roth, Tim Roughgarden, and Jonathan Ullman. Privately solving linear programs. In *International Colloquium on Automata, Languages, and Programming (ICALP '14), Track A*, pages 612–624. Springer, July 8–11 2014. Full version posted as arXiv:1402.3631v1 [cs.DS].

[57] Mark Bun and Justin Thaler. Hardness amplification and the approximate degree of constant-depth circuits. In *International Colloquium on Automata, Languages, and Programming (ICALP '15)*, pages 268–280. Springer, 5–9 July 2015. Full version available at http://arxiv.org/abs/1503.07261.

[58] Mallesh Pai, Aaron Roth, and Jonathan Ullman. An anti-folk theorem for large repeated games with imperfect monitoring. arXiv:1402.2801v1 [cs.GT], February 2014.

[59] Moritz Hardt and Jonathan Ullman. Preventing false discovery in interactive data analysis is hard. In *Symposium on Foundations of Computer Science (FOCS '14)*, pages 454–463. IEEE, Oct 18–21 2014.

[60] Raef Bassily, Adam Smith, and Abhradeep Thakurta. Private empirical risk minimization: Efficient algorithms and tight error bounds. In Boaz Barak, editor, *IEEE Symposium on the Foundations of Computer Science (FOCS)*. IEEE, 2014.

[61] Mark Bun and Thomas Steinke. Weighted polynomial approximations: Limits for learning and pseudorandomness. In *Proceedings of the 19th International Workshop on Randomization and Computation (RANDOM '15)*, pages 625–644. LIPIcs, 24–27 August 2015. Preliminary version posted as ECCC TR14-166 and arXiv:1412.2457.

[62] Karthekeyan Chandrasekaran and Ameya Velingker. Towards constructing Ramanujan graphs using shift lifts. arXiv:1502.07410 [math.CO], February 2015.

[63] Thomas Steinke and Jonathan Ullman. Interactive fingerprinting codes and the hardness of preventing false discovery. In *Proceedings of The 28th Conference on Learning Theory (COLT 2015), Paris, France, July 3-6*, pages 1588–1628, 2015. Preliminary version posted as arXiv:1410.1228 [cs.CR].

[64] Amos Beimel, Kobbi Nissim, and Uri Stemmer. Learning privately with labeled and unlabeled examples. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2015, San Diego, CA, USA, January 4-6, 2015*, pages 461–477, 2015.

[65] Yiling Chen, Kobbi Nissim, and Bo Waggoner. Fair information sharing for treasure hunting. In *Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence, January 25-30, 2015, Austin, Texas, USA.*, pages 851–857, 2015.

[66] Kobbi Nissim and David Xiao. Mechanism design and differential privacy. In Ming-Yang Kao, editor, *Encyclopedia of Algorithms*, pages 1–12. Springer, April 2015.

[67] W. T. Gowers and Emanuele Viola. The communication complexity of interleaved group products. In *47th Annual ACM Symposium on the Theory of Computing (STOC '15)*, June 2015.

[68] Oded Goldreich, Emanuele Viola, and Avi Wigderson. On randomness extraction in AC0. In *30th Computational Complexity Conference (CCC '15)*, June 2015.

[69] Jonathan Ullman. Private multiplicative weights beyond linear queries. In *Symposium on Principles of Database Systems (PODS '15)*. ACM, May 31–June 4 2015.

[70] Xianrui Meng, Seny Kamara, Kobbi Nissim, and George Kollios. Grecs: Graph encryption for approximate shortest distance queries. In *22nd ACM Conference on Computer and Communications Security (CCS '15)*, 12–16 October 2015.

[71] Chin Ho Lee and Emanuele Viola. Some limitations of the sum of small-bias distributions. *Theory of Computing*, 13(16):1–23, 2017. Preliminary version posted as *ECCC* TR15-005.

[72] Thomas Steinke and Jonathan Ullman. Between pure and approximate differential privacy. *Journal of Privacy and Confidentiality*, 7(2):3–22, 2016. Special Issue on TPDP '15. Preliminary version posted as arXiv:1501.06095.

[73] Mark Bun and Justin Thaler. Dual polynomials for collision and element distinctness. arXIv:1503.07261, March 2015. Full version available at http://arxiv.org/abs/1503.07261.

[74] Mark Bun, Kobbi Nissim, and Uri Stemmer. Simultaneous private learning of multiple concepts. In *Innovations in Theoretical Computer Science (ITCS '16)*, pages 369–380. ACM, 14–16 January 2016. Full version available at http://arxiv.org/abs/1511.08552.

[75] Mark Bun and Mark Zhandry. Order-revealing encryption and the hardness of private learning. In *Theory of Cryptography Conference (TCC '16A)*, pages 176–206. Springer, 10–13 January 2016. Full version available at https://eprint.iacr.org/2015/417.

[76] Raef Bassily, Kobbi Nissim, Adam Smith, Thomas Steinke, Uri Stemmer, and Jonathan Ullman. Algorithmic stability for adaptive data analysis. In *48th Annual Symposium on the Theory of Computing (STOC'16)*, June 2016. Preliminary version available at http://arxiv.org/abs/1511.02513.

[77] Andrej Bogdanov, Yuval Ishai, Emanuele Viola, and Christopher Williamson. Bounded indistinguishability and the complexity of recovering secrets. In *Advances in Cryptology (CRYPTO)*, 2016.

[78] Sofya Raskhodnikova and Adam Smith. Lipschitz extensions for node-private graph statistics and the generalized exponential mechanism. In *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016*, 2016.

[79] Sofya Raskhodnikova and Adam D. Smith. Differentially private analysis of graphs. In *Encyclopedia of Algorithms*, pages 543–547. 2016.

[80] Mark Bun and Justin Thaler. Improved bounds on the sign-rank of AC^0. In *Proceedings of the 42nd International Colloquium on Automata, Languages, and Programming (ICALP 2016), Part I*, page 37:1—37:14. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 12–15 July 2016. Full version available as ECCC TR16-075.

[81] Ravi Boppana, Johan Håstad, Chin Ho Lee, and Emanuele Viola. Bounded independence vs. moduli. In *Proceedings of the 20th International Workshop on Randomization and Computation (RANDOM '16)*, 2016.

[82] W. T. Gowers and Emanuele Viola. The multiparty communication complexity of interleaved group products. In *Proceedings of the 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS '16)*, 2016.

[83] Mark Bun and Thomas Steinke. Concentrated differential privacy: Simplifications, extensions, and lower bounds. In *Fourteenth IACR Theory of Cryptography Conference - TCC 2016-B*, October 2016. Preliminary version available as arXiv:1605.02065 [cs.CR].

[84] Mark Bun, Thomas Steinke, and Jonathan Ullman. Make up your mind: The price of online queries in differential privacy. arXiv:1604.04618 [cs.CR], 2016.

[85] Mark Bun and Justin Thaler. Approximate degree and the complexity of depth three boolean circuits. Electronic Colloquium on Computational Complexity TR16-121, September 2016.

[86] Cynthia Dwork, Adam Smith, Thomas Steinke, and Jonathan Ullman. Exposed! a survey of attacks on private data. *Annual Review of Statistics and Its Application*, 4(1), 2017.

[87] Marko Mitrovic, Mark Bun, Andreas Krause, and Amin Karbasi. Differentially private submodular maximization: Data summarization in disguise. In *Proceedings of the 34th International Conference on Machine Learning, ICML 2017*, August 6–11 2017.

[88] Mark Bun and Justin Thaler. A nearly optimal lower bound on the approximate degree of AC^0. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2017)*, October 15–17 2017.

[89] Raef Bassily, Kobbi Nissim, Uri Stemmer, and Abhradeep Guha Thakurta. Practical locally private heavy hitters. In *Advances in Neural Information Processing Systems (NIPS '17)*, pages 2285–2293. Curran Associates, Inc., 4–9 December 2017. Preliminary version posted as arXiv:1707.04982.

[90] Kobbi Nissim and Uri Stemmer. Clustering algorithms for the centralized and local models of differential privacy. In *Algorithmic Learning Theory (ALT '18)*. Springer, 7–9 April 2018. Preliminary version posted as arXiv:1707.04766, under title "Clustering Algorithms for the Centralized and Local Models".

[91] Yi-Hsiu Chen, Kai-Min Chung, and Jyun-Jie Liao. On the complexity of simulating auxiliary input. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part III*, pages 371–390, 2018.

[92] Mark Bun, Jelani Nelson, and Uri Stemmer. Heavy hitters and the structure of local privacy. In *Symposium on Principles of Database Systems (PODS '18)*, pages 435–447. ACM, 10–15 June 2018. Preliminary version posted as arXiv:1711.04740.

[93] Mitali Bafna, Jack Murtagh, and Nikhil Vyas. Thwarting adversarial examples: An l_0-robust sparse fourier transform. In *Advances in Neural Information Processing Systems 31 (NeurIPS '18)*, pages 10096–10106. Curran Associates, Inc., 3–8 December 2018.

[94] Rohit Agrawal. Samplers and Extractors for Unbounded Functions. In Dimitris Achlioptas and László A. Végh, editors, *Proceedings of the 23rd International Conference on Randomization and Computation (RANDOM '19)*, volume 145 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 59:1–59:21, Dagstuhl, Germany, 2019. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[95] Rohit Agrawal. Finite-Sample Concentration of the Multinomial in Relative Entropy. *IEEE Transactions on Information Theory*, 66(10):6297–6302, October 2020. Preliminary version posted as arXiv:1904.02291 [cs, math, stat], April 2019.

[96] Rohit Agrawal. Coin Theorems and the Fourier Expansion. *Chicago Journal of Theoretical Computer Science*, 26:4:1–15, 2020. Preliminary version posted as arXiv:1906.03743 [cs], June 2019.

[97] Alexander Golovnev, Siyao Guo, Thibaut Horel, Sunoo Park, and Vinod Vaikuntanathan. Data structures meet cryptography: 3sum with preprocessing. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2020, page 294–307, New York, NY, USA, 2020. Association for Computing Machinery.

[98] Daniel Alabi. The cost of a reductions approach to private fair optimization. *CoRR*, abs/1906.09613, 2019.

[99] Ryan Alweiss, Shachar Lovett, Kewen Wu, and Jiapeng Zhang. Improved bounds for the sunflower lemma. *Annals of Mathematics*, 194(3):795 – 815, 2021. Preliminary version received Best Paper Award at STOC '20.

[100] Shachar Lovett, Kewen Wu, and Jiapeng Zhang. Decision list compression by mild random restrictions. *Journal of the ACM*, 68(6):45:1–45:17, 2021. Preliminary version in STOC '20.

[101] Victor Balcer and Albert Cheu. Separating local & shuffled differential privacy via histograms. In *First Information-Theoretic Cryptography Conference (ITC)*, 2020.

[102] Shachar Lovett, Raghu Meka, Ian Mertz, Toniann Pitassi, and Jiapeng Zhang. Lifting with sunflowers. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference, ITCS 2022, January 31 - February 3, 2022, Berkeley, CA, USA*, volume 215 of *LIPIcs*, pages 104:1–104:24. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.

[103] Victor Balcer, Albert Cheu, Matthew Joseph, and Jieming Mao. Connecting robust shuffle privacy and pan-privacy. In *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 2384–2403. SIAM, 2021.

[104] Noam Mazor and Jiapeng Zhang. Simple constructions from (almost) regular one-way functions. In *Proceedings of the 19th Theory of Cryptography Conference (TCC '21)*, pages 457–485. Springer, 2021. Best Young Researcher Award.

[105] Rohit Agrawal and Thibaut Horel. Optimal bounds between f-divergences and integral probability metrics. *Journal of Machine Learning Research*, 22(128):1–59, 2021. Preliminary version in Proc. ICML '20.

[106] Louis Golowich. Improved product-based high-dimensional expanders. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2021)*, pages 38:1–38:17. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 16–18 August 2021.

[107] Xi Chen, Anindya De, Chin Ho Lee, Rocco A. Servedio, and Sandip Sinha. Near-optimal average-case approximate trace reconstruction from few traces. In *Proceedings of the 2022 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2022.

[108] Andrej Bogdanov, William M. Hoza, Gautam Prakriya, and Edward Pyne. Hitting Sets for Regular Branching Programs. In Shachar Lovett, editor, *Proceedings of the 37th Computational Complexity Conference (CCC '22)*, volume 234 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 3:1–3:22, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. Full version posted as ECCC TR21-143.

[109] Wanrong Zhang, Yajun Mei, and Rachel Cummings. Private sequential hypothesis testing for statisticians: Privacy, error rates, and sample size. In *The 25th International Conference on Artificial Intelligence and Statistics (AISTATS)*. PMLR, 28–30 March 2022.

[110] Daniel Alabi, Badih Ghazi, Ravi Kumar, and Pasin Manurangsi. Private rank aggregation in central and local models. In *Proceedings of the 2022 AAAI Conference on Artificial Intelligence*, 2022.

[111] John Bowers, Jack Cushman, Jayshree Sarathy, and Jonathan Zittrain. 'Time capsule' archiving through strong dark archives (SDA): Designing trustable distributed archives for sensitive materials. *Journal of Archival Organization*, pages 1–30, 2022.

[112] Joerg Drechsler, Ira Globus-Harris, Audra McMillan, Jayshree Sarathy, and Adam Smith. Nonparametric differentially private confidence intervals for the median. *Journal of Survey Statistics and Methodology*, 10(3):804–829, 2022.

[113] Jayshree Sarathy. From algorithmic to institutional logics: the politics of differential privacy. Presented at the 2021 Privacy Law Scholars Conference (PLSC) and the 2022 Workshop on the Theory and Practice of Differential Privacy (TPDP). Preprint available as SSRN #4079222, 2022.

[114] Mark Bun, Joerg Drechsler, Marco Gaboardi, Audra McMillan, and Jayshree Sarathy. Controlling privacy loss in sampling schemes: An analysis of stratified and cluster sampling. In *3rd Symposium on Foundations of Responsible Computing (FORC 2022)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2022.

[115] danah boyd and Jayshree Sarathy. Differential perspectives: Epistemic disconnects surrounding the us census bureau's use of differential privacy. *Harvard Data Science Review*, 2022.

[116] Xi Chen, Anindya De, Chin Ho Lee, Rocco A. Servedio, and Sandip Sinha. Approximate trace reconstruction from a single trace. In Nikhil Bansal and Viswanath Nagarajan, editors, *Proceedings of the 2023 ACM-SIAM Symposium on Discrete Algorithms, SODA 2023, Florence, Italy, January 22-25, 2023*, pages 605–637. SIAM, 2023.

[117] Aaron (Louie) Putterman and Edward Pyne. Near-optimal derandomization of medium-width branching programs. In Barna Saha and Rocco A. Servedio, editors, *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*, pages 23–34. ACM, 2023.

[118] Wanrong Zhang and Ruqi Zhang. DP-Fast MH: Private, fast, and accurate Metropolis–Hastings for large-scale Bayesian inference. In *International Conference on Machine Learning (ICML'23)*, July 2023.

[119] Aaron (Louie) Putterman and Edward Pyne. Pseudorandom linear codes are list-decodable to capacity. In Venkatesan Guruswami, editor, *15th Innovations in Theoretical Computer Science Conference, ITCS 2024, January 30 to February 2, 2024, Berkeley, CA, USA*, volume 287 of *LIPIcs*, pages 90:1–90:21. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.

[120] Mark Bun, Marco Gaboardi, Marcel Neunhoeffer, and Wanrong Zhang. Continual release of differentially private synthetic data from longitudinal data collections. *Proceedings of the ACM on Management of Data*, 2(2):94, 2024. Preliminary version posted as arXiv:2306.07884

[121] Alyssa Huang, Peihan Liu, Ryumei Nakada, Linjun Zhang, and Wanrong Zhang. Safeguarding data in multimodal AI: A differentially private approach to CLIP training. arXiv preprint arXiv:2306.08173, 2023.

[122] Rachel Cummings, Damien Desfontaines, David Evans, Roxana Geambasu, Yangsibo Huang, Matthew Jagielski, Peter Kairouz, Gautam Kamath, Sewoong Oh, Olga Ohrimenko, Nicolas Papernot, Ryan Rogers, Milan Shen, Shuang Song, Weijie Su, Andreas Terzis, Abhradeep Thakurta, Sergei Vassilvitskii, Yu-Xiang Wang, Li Xiong, Sergey Yekhanin, Da Yu, Huanyu Zhang, and Wanrong Zhang. Advancing Differential Privacy: Where We Are Now and Future Directions for Real-World Deployment. *Harvard Data Science Review*, 6(1), 16 January 2024. https://hdsr.mitpress.mit.edu/pub/sl9we8gh.

[123] Zachary Ratliff, Wittmann Goh, Abe Wieland, James Mickens, and Ryan Williams. Holepunch: Fast, secure file deletion with crash consistency. In *IEEE Symposium on Security and Privacy, SP 2024, San Francisco, CA, USA, May 19-23, 2024*, pages 2705–2721. IEEE, 2024.

[124] Prashanth Amireddy, Amik Raj Behera, Manaswi Paraashar, Srikanth Srinivasan, and Madhu Sudan. Local correction of linear functions over the boolean cube. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 764–775. ACM, 24–28 June 2024. Full version of the paper is available on arxiv at "https://arxiv.org/pdf/2403.20305".

[125] Sanjeev Khanna, Aaron (Louie) Putterman, and Madhu Sudan. Almost-tight bounds on preserving cuts in classes of submodular hypergraphs. In Karl Bringmann, Martin Grohe, Gabriele Puppis, and Ola Svensson, editors, *51st International Colloquium on Automata, Languages, and Programming, ICALP 2024, July 8-12, 2024, Tallinn, Estonia*, volume 297 of *LIPIcs*, pages 98:1–98:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.

[126] Sanjeev Khanna, Aaron Putterman, and Madhu Sudan. Near-optimal size linear sketches for hypergraph cut sparsifiers. In *65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024, Chicago, IL, USA, October 27-30, 2024*, pages 1669–1706. IEEE, 2024.

[127] Prashanth Amireddy, Amik Raj Behera, Manaswi Paraashar, Srikanth Srinivasan, and Madhu Sudan. Low degree local correction over the boolean cube. In *Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 5504–5511. ACM, 12–15 January 2025. Full version of the paper is available on arxiv at "https://arxiv.org/abs/2411.07374.

[128] Kristian Georgiev, Roy Rinberg, Sung Min Park, Shivam Garg, Andrew Ilyas, Aleksander Madry, and Seth Neel. Machine unlearning via simulated oracle matching. In *The Thirteenth International Conference on Learning Representations (ICLR '25)*, 2025. Full version posted as arXiv:2410.23232 [cs.LG] under the title "Attribute-to-Delete: Machine Unlearning via Datamodel Matching".

[129] Sanjeev Khanna, Aaron L Putterman, and Madhu Sudan. Efficient algorithms and new characterizations for csp sparsification. *arXiv preprint arXiv:2404.06327*, 2024. To appear in STOC 2025.

[130] William Kuszmaul, Aaron Putterman, Tingqiang Xu, Hangrui Zhou, and Renfei Zhou. Tight bounds and phase transitions for incremental and dynamic retrieval. In Yossi Azar and Debmalya Panigrahi, editors, *Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2025, New Orleans, LA, USA, January 12-15, 2025*, pages 3974–3997. SIAM, 2025.

[131] Aaron L Putterman and Vadim Zaripov. Bivariate linear operator codes. *arXiv preprint arXiv:2411.16596*, 2024. To appear in ISIT 2025.

[132] Sepehr Assadi, Sanjeev Khanna, and Aaron Putterman. Correlation clustering and (de)sparsification: Graph sketches can match classical algorithms. *CoRR*, abs/2504.04258, 2025. To appear in STOC 2025.

[133] Sanjeev Khanna, Huan Li, and Aaron Putterman. Near-optimal linear sketches and fully-dynamic algorithms for hypergraph spectral sparsification. *CoRR*, abs/2502.03313, 2025. To appear in STOC 2025.

[134] Prashanth Amireddy, Amik Raj Behera, Srikanth Srinivasan, and Madhu Sudan. A near-optimal polynomial distance lemma over boolean slices, 2025. To appear in ICALP '2025.

[135] Sanjeev Khanna, Aaron Putterman, and Madhu Sudan. Near-optimal hypergraph sparsification in insertion-only and bounded-deletion streams. *CoRR*, abs/2504.16321, 2025. To appear in ICALP 2025.

[136] Sanjeev Khanna, Aaron Putterman, and Madhu Sudan. A theory of spectral CSP sparsification. *CoRR*, abs/2504.16206, 2025. To appear in ICALP 2025.

Invited Talks at Workshops and Conferences

[T1] Manipulating statistical difference. *DIMACS Workshop on Randomization Methods in Algorithm Design*, Princeton, NJ, December 1997.

[T2] A complete problem for statistical zero-knowledge. *Fields Institute Workshop on Interactive Proofs, PCP's, and Fundamentals of Cryptography*, May 1998.

[T3] Statistical zero-knowledge: A survey of recent developments. *Oberwolfach Meeting on Complexity Theory*, Oberwolfach, Germany, November 1998.

[T4] Pseudorandom generators without the XOR lemma. *DIMACS Workshop on Pseudorandomness and Explicit Combinatorial Constructions*, New Brunswick, NJ, October 1999.

[T5] Interactive proofs and zero-knowledge proofs (mini-course). *IAS/PCMI Graduate Summer School on Computational Complexity*, Princeton, NJ, August 2000.

[T6] Extracting randomness from samplable distributions. *Oberwolfach Meeting on Complexity Theory*, Oberwolfach, Germany, November 2000.

[T7] Order in pseudorandomness. *5th International Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM '01)*, Berkeley, CA, August 2001.

[T8] Applications of locally list-decodable codes. *DIMACS Workshop on Codes and Complexity*, New Brunswick, NJ, December 2001.

[T9] Randomness extractors and their many guises (tutorial). *43rd Annual Symposium on Foundations of Computer Science (FOCS '02)*, Vancouver, Canada, October 2002.

[T10] The connection between randomness extractors and expander graphs. *American Mathematical Society Sectional Meeting,* Special Session on Probability, Bloomington, IN, April 2003.

[T11] The zig-zag product and expansion close to the degree. *IPAM Workshop on Automorphic Forms, Group Theory, and Graph Expansion*, Los Angeles, CA, February 2004.

[T12] An unconditional study of computational zero knowledge. *CIRM Meeting on Cryptographie*, Luminy, France, November 2004.

[T13] Randomness extractors and their cryptographic applications. *Special Day on Mathematics of Cryptology,* Leiden, The Netherlands, January 2005.

[T14] The complexity of zero knowledge. *IBM/NYU/Columbia Theory Day*, New York, NY, November 2005.

[T15] Zero-knowledge proofs (tutorial). *Workshop on Classical and Quantum Information Security*, Caltech, Pasadena, CA, December 2005.

[T16] Pseudorandom walks in regular digraphs and the RL vs. L problem. *Heilbronn Institute Conference on Randomness and Complexity*, Bristol, England, July 2006.

[T17] The complexity of zero knowledge. *Recent Advances in Computational Complexity*, Banff International Research Station, Alberta, Canada, August 2006.

[T18] The complexity of zero knowledge. *IPAM Workshop on the Foundations of Secure Multiparty Computation and Zero Knowledge and its Applications*, Los Angeles, CA, November 2006.

[T19] Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *Georgia Tech ACO/ARC Theory Day*, Atlanta, GA, February 2007.

[T20] Statistically hiding commitments from any one-way function. *Oberwolfach Meeting on Complexity Theory*, June 2007.

[T21] Statistical zero-knowledge arguments and statistically hiding commitments from any one-way function. *Dagstuhl Seminar on Cryptography*, November 2007.

[T22] The complexity of zero knowledge. *Bay Area Theory Seminar*, November 2007.

[T23] The complexity of zero knowledge. *27th International Conference on Foundations of Software Technology and Theoretical Computer Science Conference (FSTTCS '07)*, December 2007.

[T24] Randomness extractors and their cryptographic applications (tutorial). *5th Theory of Cryptography Conference (TCC '08)*, New York, NY, March 2008.

[T25] Why simple hash functions work: Exploiting the entropy in a data stream. *Analytic Tools in Computational Complexity*, Banff International Research Station, Alberta, Canada, August 2008.

[T26] Inaccessible entropy. *Israel Theory Day*, Open University, Raanana, Israel, March 2009.

[T27] Cryptographic applications of randomness extractors. *Workshop on Cryptography in the Clouds*, Massachusetts Institute of Technology, Cambridge, MA, August 2009.

[T28] Inaccessible entropy. *Oberwolfach Meeting on Complexity Theory*, Oberwolfach, Germany, November 2009.

[T29] Computational complexity in differential privacy. *Workshop on Statistical and Learning-Theoretic Challenges in Data Privacy*, Institute of Pure and Applied Mathematics, Los Angeles, CA, February 2010.

[T30] Are PCPs inherent in efficient arguments? *Verifiable Computation Workshop*, Massachusetts Institute of Technology, Cambridge, MA, August 2010.

[T31] The unified theory of pseudorandomness. *International Congress of Mathematicians*, Hyderabad, India, August 2010.

[T32] Computational entropy. *Michael Rabin 80th Birthday Celebration*, Cambridge, MA, August 2011.

[T33] The many entropies of one-way functions. *6th International Conference on Information-Theoretic Security*, Montreal, Canada, August 2012.

[T34] The privacy of the analyst and the power of the state. *DIMACS Workshop on Differential Privacy across Computer Science*, New Brunswick, NJ, October 2012.

[T35] The computational complexity of differential privacy. *Second Charles River Crypto Day*, Boston University, Boston, MA, November 2012.

[T36] Differential privacy and mechanism design. *New Directions in the Science of Differential Privacy*, Simons Foundation, New York, NY, March 2013.

[T37] Privacy problems in big data and computer science solutions. *Round Table on Computer Science Issues in Big Data*, Simons Foundation, New York, NY, April 2013.

[T38] Differential privacy and mechanism design. *Workshop on Privacy*, Kellogg School of Management, Northwestern University, Evanston, IL, May 2013.

[T39] Pseudorandom generators via mild pseudorandom restrictions. *Computational Complexity*, Banff International Research Station, Alberta, Canada, July 2013.

[T40] Intractability in data privacy. *Workshop on New Insights into Computational Intractability Workshop*, Clay Research Conference, Clay Mathematics Institute, Oxford, UK, October 2013.

[T41] The complexity of differential privacy. *Weizmann Distinguished Lectures Day — Celebration of the Work of Shafi Goldwasser and Silvio Micali*, Weizmann Institute of Science, Rehovot, Israel, December 2013.

[T42] Differential privacy (weeklong course). *McGill Invitational Workshop on Computational Complexity*, Bellairs Research Institute, Holetown, Barbados, February 2014.

[T43] Current developments in differential privacy. *White House–MIT Big Data Privacy Workshop*, Massachusetts Institute of Technology, March 2014.

[T44] Data privacy: Applying fundamental computer science to societal problems. *Engineering the Future*, Harvard SEAS Fundraising Events, Seattle, WA and Mountain View, CA, March 2014.

[T45] Privacy tools for sharing research data. *MIT Big Data Initiative Annual Meeting*, Massachusetts Institute of Technology, November 2014. Part of panel discussion on Big Data and Privacy.

[T46] Privacy tools for sharing research data. *The 6th ASE International Conference on Privacy, Security, Risk, and Trust, and the 4th ASE International Conference on Big Data (PASSAT/BIGDATA 2014)*, Harvard University, Cambridge, MA, December 2014. Keynote lecture.

[T47] The border between possible and impossible in data privacy. *Simons Foundation Mathematics and Physical Sciences Annual Meeting*, New York, NY, October 2015.

[T48] Differential privacy: Theoretical and practical challenges. *The 5th ASE International Conference on Big Data, and the 4th ASE International Conference on Social Informatics (BIGDATA/SocialInformatics 2015)*, Kaohsiung, Taiwan, October 2015. Keynote lecture.

[T49] Expander graphs. *Spectral Graph Theory and Applications*, Shing-Tung Yau Center, National Chiao-Tung University, Taiwan, December 2015.

[T50] Computational entropy in cryptographic constructions from one-way functions. *COST–IACR School on Randomness in Cryptography*, Pompeu Fabra University, Barcelona, Spain, November 2016.

[T51] Pseudorandom generators from one-way functions: the quest for simplicity and efficiency. *Randomness, Complexity and Cryptography: The First Sixty Years of Oded Goldreich*, Weizmann Institute of Science, Rehovot, Israel, April 2017.

[T52] Differential privacy & statistical inference —- a theoretical cs perspective. *Data Privacy: Planning Workshop*, Simons Institute for the Theory of Computing, Berkeley, CA, May 2017.

[T53] Pseudorandom generators from one-way functions via computational entropy. *DIMACS Workshop on Complexity of Cryptographic Primitives and Assumptions*, City College of New York, NY, June 2017.

[T54] PSI: A (differentially) private data-sharing interface. *Mathematical Foundations of Data Privacy*, Banff International Resarch Station, Banff, Canada, May 2018.

[T55] PSI: A private data-sharing interface. *Workshop on the Theory and Practice of Differential Privacy* (TPDP 2018), Toronto, Canada, October 2018.

[T56] The knowledge complexity of Shafi's advising systems (and a tight lower bound for entropy flattening). *Workshop in Celebration of Shafi Goldwasser*, Simons Institute for the Theory of Computing, Berkeley CA, January 2019.

[T57] OpenDP: A pitch for a community effort. *Workshop on Data Privacy: from Foundations to Applications*, Simons Institute for the Theory of Computing, Berkeley CA, March 2019.

[T58] Differential privacy for social science research. *CNSTAT Workshop on Challenges and New Approaches for Protecting Privacy in Federal Statistical Programs*, National Academies, Washington, DC, June 2019.

[T59] Differential privacy: Wider context and remaining questions. *JASON Briefing*, Mitre Corporation, La Jolla, CA, June 2019.

[T60] Remarks on differential privacy for the 2020 census. *Harvard Data Science Review Inaugural Symposium*, Harvard University, Cambridge, MA, October 2019.

[T61] PSI and OpenDP: Toward wider adoption of differential privacy. *International Corporate Standards Meeting*, Microsoft New England, Cambridge, MA, March 2020.

[T62] Differential privacy, WhiteNoise, and OpenDP. *Microsoft AI Show*, special edition for the virtual Build conference, May 2020.

[T63] Derandomizing space-bounded computation via Laplacian solvers. *STOC 2020 Workshop: Derandomizing Space-Bounded Computation*, virtual conference, June 2020.

[T64] OpenDP: an overview. *Responsible Data Summit*, virtual conference organized by Oasis Labs, July 2020.

[T65] The theory and practice of differential privacy. *Thirty-third Annual Conference on Learning Theory (COLT 2020)*, virtual conference, July 2020. Keynote lecture.

[T66] OpenDP: A community effort to build trustworthy differential privacy software. *Workshop on the Theory and Practice of Differential Privacy (TPDP '20)*, virtual conference, November 2020. Invited talk.

[T67] Panel discussion. *Google Differential Privacy Workshop*, virtual conference, February 2021.

[T68] Differential privacy and pandemic research. *NSF PREPARE workshop on DATA: Access, Creation, and Maintenance of Data and Computing Resources*, May 2021. Virtual talk.

[T69] Widespread underestimation of sensitivity in differential privacy libraries and how to fix it. *Apple Privacy-Preserving Machine Learning Workshop*, April 2022. Virtual talk.

[T70] Hiking to the differential privacy goldmine. *CynthiaFest: a symposium in honor of Cynthia Dwork*, American Academy of Arts & Sciences, Cambridge, MA, June 2022.

[T71] Differentially private simple linear regression. *Workshop on Differential Privacy & Statistical Data Analysis*, Fields Institute for Research in Mathematical Sciences, Toronto, Canada, July 2022.

[T72] Differential privacy & pandemic research. *Harvard Data Science Initiative Trust in Science Workshop*, Allston MA, September 2022. Panel discussion.

[T73] OpenDP: Trustworthy tools for deploying differential privacy. *Swiss Data Science & AI for Public Good Seminar*, December 2022. Virtual talk.

[T74] Differential privacy's transition from theory to practice. *Simons Collaboration on Algorithmic Fairness Annual Meeting*, New York, NY, USA, February 2023.

[T75] Tutorial: Using and contributing to the OpenDP library. *Fourth AAAI Workshop on Privacy-Preserving Artificial Intelligence (PPAI-23)*, Washington DC, USA, February 2023.

[T76] UN PET guide: Output privacy (differential privacy). *UN PET Lab Open House* (virtual), March 2023.

[T77] The complexity of differential privacy. *MIT CSAIL 20/60 Celebration*, Cambridge, MA, USA, June 2023.

[T78] Differential privacy: Opportunities & challenges. *Eyes off Data Summit*, Dublin, Ireland, July 2023.

[T79] Spectral graph theory for derandomizing logspace. *Conference on Computational Complexity (CCC '23)*, Warwick, UK, July 2023. Invited Talk.

[T80] Concurrent composition of differential privacy. *Joint Statistical Meetings*, Toronto, Canada, August 2023. Session on "Differential Privacy for Data Science: Opportunities and Challenges".

[T81] Interactive differential privacy in the OpenDP library. *Apple Privacy-Preserving Machine Learning Conference*, virtual talk, February 2024.

[T82] Differential privacy. *data.org PETS for Global Health Showcase*, Harvard University, Boston, MA, November 2024.

[T83] Differential privacy against timing attacks. *Differential Privacy and Its Applications*, NII Shonan Meeting, Japan, November 2024.

[T84] Multicalibration: A new tool for cryptographers. *Theory of Cryptography Conference (TCC) Test-of-Time Award Talk*, Milan, Italy, December 2024. In loving memory of Luca Trevisan.

[T85] Multicalibration: A new tool for security proofs. *Charles River Crypto Day*, MIT, Cambridge, MA, January 2025. In loving memory of Luca Trevisan.

[T86] OpenDP: A community effort to advance the practice of differential privacy. *Eyes Off Data Summit*, Dublin, Ireland, September 2025.

[T87] Applications of multicalibration in complexity and cryptography. *DavidFest: A Pseudorandomness Workshop in Austin, in honor of David Zuckerman's 60th birthday*, Austin, TX, October 2025.

Departmental Seminars and Colloquia

[D1] Honest verifier statistical zero-knowledge equals general statistical zero-knowledge. *IBM T.J. Watson Research Center*, Hawthorne, NY, January 1998.

[D2] Statistical zero-knowledge: A survey of recent developments. *Weizmann Institute of Science*, Rehovat, Israel, January 1999.

[D3] Statistical zero-knowledge: A survey of recent developments. *Institute for Advanced Study*, Princeton, NJ, March 1999.

[D4] Statistical zero-knowledge: A survey of recent developments. *Carnegie Mellon University*, Pittsburgh, PA, November 1999.

[D5] Verifiable random functions. *University of Washington*, Seattle, WA, December 1999.

[D6] Statistical zero-knowledge: A survey of recent developments. *University of Maryland*, College Park, MD, February 2000.

[D7] Pseudorandomness: Connections and constructions. *Cornell University*, Ithaca, NY, February 2000.

[D8] Pseudorandomness: Connections and constructions. *University of California, Berkeley*, Berkeley, CA, March 2000.

[D9] Pseudorandomness: Connections and constructions. *Princeton University,* Princeton, NJ, March 2000.

[D10] Pseudorandomness: Connections and constructions. *Stanford University*, Palo Alto, CA, March 2000.

[D11] A study of statistical zero-knowledge proofs. *Harvard University,* Cambridge, MA, March 2000.

[D12] A study of statistical zero-knowledge proofs. *University of California, Berkeley*, Berkeley, CA, March 2000.

[D13] A study of statistical zero-knowledge proofs. *University of Toronto*, Toronto, Canada, March 2000.

[D14] Extracting randomness from samplable distributions. *Rutgers University*, New Brunswick, NJ, November 2000.

[D15] Randomness conductors and constant-degree lossless expanders. *Georgia Institute of Technology*, Atlanta, GA, February 2002.

[D16] Randomness conductors and constant-degree lossless expanders. *Boston University*, Boston, MA, March 2002.

[D17] Randomness conductors and constant-degree lossless expanders. *University of Texas*, Austin, TX, March 2002.

[D18] The benefits of randomness and interaction in proofs. *Radcliffe Institute for Advanced Study*, Cambridge, MA, November 2003.

[D19] Locally computable extractors and cryptosystems in the bounded storage model. *Worcester Polytechnic Institute*, Worcester, MA, November 2003.

[D20] Locally computable extractors and cryptosystems in the bounded storage model. *Boston University*, Boston, MA, January 2004.

[D21] Using nondeterminism to amplify hardness. *University of Toronto*, Toronto, Canada, March 2004.

[D22] Using nondeterminism to amplify hardness. *Carnegie Mellon University*, Pittsburgh, PA, August 2004.

[D23] An unconditional study of computational zero knowledge. *Massachusetts Institute of Technology*, Cambridge, MA, September 2004.

[D24] An unconditional study of computational zero knowledge. *Institute for Advanced Study*, Princeton, NJ, November 2004.

[D25] Pseudorandom walks in regular digraphs and the RL vs. L problem. *Microsoft Research,* Redmond, WA, March 2005.

[D26] Pseudorandom walks in regular digraphs and the RL vs. L problem. *University of Washington*, Seattle, WA, March 2005.

[D27] Pseudorandom walks in regular digraphs and the RL vs. L problem. *University of California*, Berkeley, CA, March 2005.

[D28] An unconditional study of computational zero knowledge. *Stanford University*, Palo Alto, CA, March 2005.

[D29] An unconditional study of computational zero knowledge. *University of California*, San Diego, CA, March 2005.

[D30] An unconditional study of computational zero knowledge. *Columbia University*, New York, NY, April 2005.

[D31] Pseudorandom walks in regular digraphs and the RL vs. L problem. *California Insititute of Technology*, Pasadena, CA, September 2005.

[D32] The complexity of zero knowledge. *Tufts University*, Medford, MA, March 2006.

[D33] The complexity of zero knowledge. *Yale University*, New Haven, CT, March 2006.

[D34] The complexity of zero knowledge. *University of Chicago*, Chicago, IL, May 2006.

[D35] The complexity of zero-knowledge proofs. *Harvard University*, November 2006.

[D36] Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *Institute for Advanced Study*, Princeton, NJ, February 2007.

[D37] Expander graphs, randomness extractors, and list-decodable codes. *Massachusetts Institute for Technology*, Cambridge, MA, March 2007.

[D38] Expander graphs, randomness extractors, and list-decodable codes. *Stanford University*, Palo Alto, CA, November 2007.

[D39] Why simple hash functions work: Exploiting the entropy in a data stream. *University of California*, Berkeley, CA, November 2007.

[D40] Zero-knowledge proofs: Flipping a coin to protect your privacy. *Radcliffe Institute for Advanced Study Alumni Events*, San Francisco and Palo Alto, CA, January 2008.

[D41] Randomness, interaction, and zero-knowledge proofs. Department of Statistics, *University of California*, Berkeley, CA, February 2008.

[D42] Zero-knowledge proofs: the power of tossing coins. Miller Institute for Basic Research in Science, *University of California*, Berkeley, CA, February 2008.

[D43] The complexity of zero knowledge. Computer Science Distinguished Lecture Series, *University of California*, Davis, CA, April 2008.

[D44] An equivalence between zero knowledge and commitments. *University of Washington*, Seattle, WA, May 2008.

[D45] Inaccessible entropy. *Massachusetts Institute of Technology*, Cambridge, MA, February 2009.

[D46] Inaccessible entropy. *Microsoft Research*, Mountain View, CA, June 2010.

[D47] Computational complexity in differential privacy. Applied Mathematics Colloquium, *Massachusetts Institute of Technology*, Cambridge, MA, April 2011.

[D48] Computational complexity in differential privacy. *Microsoft Research*, Cambridge, MA, May 2011.

[D49] Computational entropy. Electrical Engineering Seminar, *University of California*, Los Angeles, CA, November 2011.

[D50] Computational entropy. *Microsoft Research*, Mountain View, CA, December 2011.

[D51] Computational entropy. Rajeev Motwani Distinguished Lecture Series, *Stanford University*, Stanford, CA, March 2012.

[D52] Computational entropy. *Institute for Advanced Study*, Princeton, NJ, April 2012.

[D53] The privacy of the analyst and the power of the state. *Microsoft Research*, Mountain View, CA, July 2012.

[D54] Differential privacy: Some theoretical and practical challenges. *Microsoft Research New England*, Cambridge, MA, August 2013.

[D55] Differential privacy: Some theoretical and practical challenges. *Google*, Cambridge, MA, August 2013.

[D56] Locally testable codes and Cayley graphs. *Microsoft Research New England*, Cambridge, MA, November 2013.

[D57] The computational complexity of data privacy. *Center of Mathematical Sciences and Applications*, Harvard University, October 2014.

[D58] Differential privacy: Theoretical and practical challenges. *Washington Area Trustworthy Computing Hour (WATCH)*, National Science Foundation, Arlington, VA, January 2015. Webcast live.

[D59] The border between possible and impossible in data privacy. *Department of Applied Mathematics*, National Chiao-Tung University, Taiwan, September 2015.

[D60] Differential privacy: Theoretical and practical challenges. Distinguished Lecture Series, *Institute of Information Science*, Academia Sinica, Taiwan, November 2015.

[D61] The border between possible and impossible in data privacy. Distinguished Professor Lecture, *National Center for Theoretical Sciences*, National Taiwan University, December 2015.

[D62] Robust traceability from trace amounts. *Institute of Statistics*, National Chiao-Tung University, Taiwan, January 2016.

[D63] The border between possible and impossible in data privacy. *Institute of Theoretical Computer Science and Communications*, Chinese University of Hong Kong, April 2016.

[D64] Robust traceability from trace amounts. *Institute of Statistical Science*, Academia Sinica, Taiwan, May 2016.

[D65] Privacy tools for sharing research data. *Distinguished Speaker Series*, University of Buffalo Department of Computer Science and Engineering, Buffalo, NY, April 2018.

[D66] Differential privacy. *Opportunity Insights Lunch*, Harvard University, Cambridge, MA, March 2019.

[D67] Differential privacy. *Statistics Colloquium*, Harvard University, Cambridge, MA, March 2019.

[D68] PSI and OpenDP: Toward wider adoption of differential privacy. Google, Sunnyvale, CA, May 2019.

[D69] PSI and OpenDP: Toward wider adoption of differential privacy. *Computer Science Colloquium*, University of Massachusetts, Lowell, MA, November 2019.

[D70] Derandomization beyond connectivity: High-precision estimation of random walks and Laplacian solvers in nearly logarithmic space. *CS Theory Seminar*, University of Pennsylvania, Philadelphia, PA, December 2019.

[D71] Derandomization beyond connectivity: High-precision estimation of random walks and Laplacian solvers in nearly logarithmic space. *CS Theory Lunch*, University of Southern California, Los Angeles, CA, February 2020.

[D72] Derandomizing algorithms via spectral graph theory. *CMSA Colloquium*, Harvard Center of Mathematical Sciences and Applications, Cambridge, MA, March 2020.

[D73] Differential privacy: Uses and misuses. *Knight First Amendment Institute*, virtual seminar, January 2021.

[D74] The privacy tools project. *Georgetown University-Hebrew University Data Co-Ops Working Group*, April 2022. Virtual talk.

[D75] OpenDP: A community effort. *NITRD Fast-Track Action Committee for Advancing Privacy-Preserving Data Sharing and Analytics (FTAC-PPDSA)*, June 2022. Virtual talk.

[D76] Foundations of computer security & privacy. *Bocconi University*, Milan, Italy, September 2023. To accompany the Lectio Inauguralis of Luca Trevisan as the Invernizzi Chair in Computer Science.

[D77] OpenDP: A community effort to advance the practice of differential privacy. *Cornell Tech Digital Life Seminar*, October 2023.

[D78] OpenDP: A community effort to advance the practice of differential privacy. *University of Melbourne CIS Seminar*, Melbourne, Australia, January 2024.

[D79] OpenDP: A community effort to advance the practice of differential privacy. *Australian Bureau of Statistics MDSD Seminar*, Sydney, Australia, February 2024.

[D80] OpenDP: A community effort to advance the practice of differential privacy. *PETS Sub-Interagency Policy Committee Meeting*, virtual, February 2024.

[D81] Derandomizing algorithms via spectral graph theory. *Sydney Mathematical Research Institute Seminar*, Sydney, Australia, March 2024.

[D82] Differential privacy: From theory to practice and back. *University of Sydney Basser Seminar*, Sydney, Australia, March 2024.

[D83] Differential privacy: From theory to practice and back. *IST Austria Mathematics and Computer Science Seminar*, Vienna, Austria, March 2024.

[D84] Differential privacy: How and why to use it. *Commonwealth Bank of Australia*, Sydney, Australia, March 2024.

[D85] Differential privacy: From theory to practice and back. *OpenMined public talk*, virtual, October 2024.

[D86] Applications of multicalibration in complexity and cryptography. *Algorithms & Theory Seminar*, Boston University, Boston, MA, May 2025. In loving memory of Luca Trevisan.

[D87] Multicalibration: A powerful new tool in complexity theory and cryptography. *Distinguished Lecture Series*, Dipartimento di Informatica Sapiena Università di Roma, Rome, Italy, February 2026. In loving memory of Luca Trevisan.