Omer Reingold, February 2024

My research is focused on a wide range of topics within the Foundations of Computer Science, and most notably in computational complexity, cryptography and the societal impact of computation.

Current Academic Employment:

- The Rajeev Motwani Professor of Computer Science, Stanford University. In Stanford since September. 2016.

Education:

- **1994-1998**
  Weizmann Institute of Science, Rehovot, Israel.
  Ph.D. in Computer Science.
  Thesis title: Pseudo-random synthesizers, functions and permutations.
  Advisor: Prof. Moni Naor.

- **1991-1994**
  Tel-Aviv University, Tel-Aviv, Israel.
  B.Sc in Mathematics and Computer Science - Summa Cum Laude.

Selected Awards and distinctions (additional awards below):

- Simons Investigator since 2020.
- The 2009 ***Gödel Prize*** for outstanding papers in the area of theoretical computer science (jointly with Salil Vadhan and Avi Wigderson).
- 2005 **ACM Grace Murray Hopper Award**. Awarded by the Association for Computing Machinery (ACM) to "the outstanding young computer professional of the year."
- **ACM Fellow** (2014)

Previous Academic Employment and Short Term Visits:

- **Feb 2015 – September 2016** Principal Research Engineer, Samsung Research America (SRA)
- **Nov 2014 – Feb 2015** (while on leave from Weizmann)
  Visiting Professor, Computer Science, Stanford University
- **July 2009 – Nov 2014** (while on leave from Weizmann)
  Principal Researcher,
  Microsoft Research Silicon Valley,
  Mountain View, CA, USA
- **Jan 2004 – June 2015** Professor (full Professor since October 2011), Faculty of Mathematics and Computer Science,

Department of Computer Science and Applied Mathematics,
The Weizmann Institute of Science
On sabbatical and leave of absence July 2009 – June 2015

- **August 17 – November 15, 2005**
  Visiting scholar,
  Center for Research on Computation and Society,
  Division of Engineering and Applied Sciences,
  Harvard University.
- **1999 – 2004**
  Senior technical staff member,
  Department of Secure Systems Research,
  AT&T Labs – Research,
  Florham Park, NJ, USA.
- **1999 – 2004** (Concurrent to my employment at AT&T)
  Visiting member of the333 School of Mathematics,
  Institute for Advanced Study, Princeton, NJ, USA.
- **1998 – 1999**
  Postdoctoral fellow,
  Dept. of Applied Math and Computer Science,
  Weizmann Institute of Science, Rehovot, Israel.
  Advisor: Prof. Adi Shamir.

Professional Activities (partial list):

- Co-organizer, Multigroup Fairness and the Validity of Statistical Judgment, Simons Institute for the Theory of Computing, April 2023.
- Director, CS PhD program, Stanford, 2021-
- Director of the Simons Collaboration on the Theory of Algorithmic Fairness, since 2020.
- Director, CS MS program, Stanford, 2018-2021.
- Founding steering committee co-chair: Foundation of Responsible Computing (FORC), since 2019. Local arrangements 2023.
- Steering Committee chair: International Conference on Randomization and Computation (RANDOM) 2018-2020.
- Steering Committee member: Innovations in Theoretical Computer Science (ITCS), International Conference on Randomization and Computation (RANDOM)
- Scientific Advisory Board (SAB) of the Simons Institute, 2019–2022.
- Editorial Board: SIAM Journal on Computing (SICOMP) (retired 2016)
- Editorial Board: IACR Journal of Cryptology (retired 2016)
- Editorial Board: ACM Transactions on Computation Theory (ToCT) (retired 2016)
- Guest Editor: Special Issue of Approx-Random 2007, Algorithmica, Springer.
- Scientific Board: Electronic Colloquium on Computational Complexity (ECCC)

- Chair of program committee: FOCS 2013, CCC 2011, TCC 2009, Random 2007
- Served on the program committee of CRYPTO 2001 and RANDOM 2001, FOCS 2002, TCC 2004, EUROCRYPT 2004, ICALP 2005, FOCS 2005, TCC 2007, CRYPTO 2007, STOC 2008, CCC 2010, ITCS 2016.
- Co-founding and organizing the group research blogs `TOC4Fairness' (as part of the Simons Collaboration on the Theory of Algorithmic Fairness, January 2021), `Theory Dish' (Stanford, May 2017) and `Windows On Theory' (Microsoft Research, April 2012) as forums for exchanging ideas and debating topics of interest to the Theory of Computing (TOC) community. Contributing both technical and non-technical posts and in particular, initiating the research life stories project.
- SIGACT Research Highlights Committee, 2019-2020
- Gödel Prize committee 2017-2019 (last year as chair)
- Co-organizing TOCA-SV meetings of the Sillicon-Valley Theory Community (starting in November 2016)
- Co-Organizing the first ACM-SRC University competition (hosted by MSR-SVC and the Simons Institute), 2013
- Co-Director, Research School of Mathematics and Computer Science, Weizmann Institute (2007 - 2009).

Other Awards and Fellowships (by reversed chronologic order):

- **TCC 2021 Test of Time award** for "Keyword Search and Oblivious Pseudorandom Functions" TCC 2005 (joint with Michael J. Freedman, Yuval Ishai and Benny Pinkas).
- ***2015 IBM Pat Goldberg Memorial Best Paper Award*** (for the paper "The reusable holdout: Preserving validity in adaptive data analysis Science Magazine", joint with Cynthia Dwork, Vitaly Feldman, Moritz Hardt, Toniann Pitassi)
- ***2011 Helen and Martin Kimmel Award for Innovative Investigation***
- 2011 **SIAM** (Society for Industrial and Applied Mathematics) **Outstanding Paper Prize,** for the paper "Statistically Hiding Commitments and Statistical Zero-Knowledge Arguments from Any One-Way Function", joint with Iftach Haitner, Minh-Huyen Nguyen, Shien Jin Ong, and Salil Vadhan
- The 2006 ***Prof. Pazy Memorial Research Award***, given annually to the most outstanding and original BSF supported project in mathematics and computer science (awarded for my BSF grant joint with Prof. Luca Trevisan and Prof. Salil Vadhan).
- 2007 ***Morris L. Levinson Prize in Mathematics*** awarded yearly by the Scientific Council of the Weizmann Institute to a single member of the Weizmann Institute.
- **CRYPTO 2006 best paper award** for the paper "On the Power of the Randomized Iterate" (joint with Iftach Haitner and Danny Harnik).
- **ICALP 2006, track C, best paper award** for the paper "Efficient Pseudorandom Generators from Exponentially Hard One-Way Functions" (joint with Iftach Haitner and Danny Harnik).
- **STOC 2005 best paper award** for the paper "Undirected ST-connectivity in log-space".

- **Rothschild award for postdoctoral studies**, 1999. Awarded yearly by Yad-Hanadiv, Jerusalem, Israel to up to eighteen Israeli students of all areas, for postdoctoral studies abroad.
- **J. F. Kennedy prize for achievements in Ph.D. studies**, 1999. Awarded yearly by the Weizmann Institute of Science, Israel to four Ph.D. students of the Weizmann Institute.
- **Levi Eshkol scholarship for postdoctoral studies**, 1998, Israel. Awarded by the ministry of science to students of Israeli universities.
- **The Dimitris N. Chorafas foundation prize for engineering and technology**, 1998, Switzerland. Awarded yearly to 20-30 students of 26 "partner universities."
- **Clore scholars award for Ph.D. studies**, 1996, Israel. Awarded yearly to ten students of Israeli universities, in all fields of the natural sciences, including mathematics, physics, chemistry, the life sciences, earth sciences, agriculture, engineering and technology.
- **Undergraduate studies in the Excelling Program, Tel-Aviv University**, Israel.
- **Yekutiel Federman scholarship**, 1992, Israel.
- **Dean's honors lists**, Tel-Aviv University, 1991-1994, Israel.

Interns, Students, and Postdoctoral fellows:

- Lee Cohen, (Postdoc, Stanford, current) 2023 -
- Sumegha Garg, (Postdoc, Stanford) 2022-2023
- Christopher Jung, (Postdoc, Stanford, current) 2022-
- Inbal Livni Navon (Postdoc, Stanford) 2021-
- Dean Doron, (Motwani Postdoc, Stanford) 2019-2021
- Avishay Tal (Motwani Postdoc, Stanford) 2017-2019
- Eyal Rozenman, Postdoctoral fellow, Weizmann, 2004-2005.

- Jabari Hastings, Current PhD student, Stanford, co-advised with Aviad Rubinstein
- Charlotte Peale, Current PhD student, Stanford
- Judy Hanwen Shen, Current PhD student, Stanford
- Lunjia Hu, Current PhD student, Stanford, co-advised with Moses Charikar
- Brian Axelrod, Current PhD student, Stanford, co-advised with Greg Valiant
- Benjamin Plaut, PhD student, Stanford, co-advised with Ashish Goel, completed 2021.
- Michael P. Kim, PhD student, Stanford, completed 2020.
- Huacheng Yu (PhD Stanford, Stanford, co-advising with Ryan Williams during his final quarters)
- Amir Abboud (PhD Stanford, Stanford, co-advising with Virginia Williams during his final quarters)
- Shachar Lovett, Ph.D., Weizmann, started 2006, completed 2010
- Ronen Gradwohl, direct Ph.D., Weizmann, started 2004, completed 2009.
- Iftach Haitner, Ph.D., Weizmann, started 2004, completed 2008.

- Ron Rothblum, MSR-SV Summer Intern, 2013
- Kat Ellis, MSR-SV Summer Intern, 2013, 2014
- Raghu Meka, MSR-SV Summer Intern, 2011

- Shubhangi Saraf, MSR-SV Summer Intern, 2010

- Sergey Novikov, Masters, Weizmann, started 2008.
- Klim Efremenko, Masters, Weizmann, started 2007, completed 2008.
- Tal Kramer, Masters, Weizmann, started 2006, completed 2007.
- Michal Igell, Masters, Weizmann, started 2004, completed 2005.

Publication List:

Each of my publications appears only once in this list. In case a paper was published both in a conference and in a journal, then usually the journal reference will appear first, directly followed by reference to the preliminary version.

Author's order is alphabetical as customary in my field (with very few exceptions in non-theory venues). Publications appear in chronological order according to date of first publication:

1. M. Naor and O. Reingold, *Synthesizers and their application to the parallel construction of pseudorandom functions*, Journal of Computer and System Sciences (JCSS), 58(2), pp. 336-375, 1999.

   Preliminary Version: Proc. 36th IEEE Symp. of Foundations of Computer Science (FOCS 1995), pp. 170-181, 1995.

2. M. Naor and O. Reingold, *On the construction of pseudorandom permutations: Luby-Rackoff revisited*, J. of Cryptology, vol. 12, pp. 29-66, 1999.

   Preliminary Version: Proc. 29th Ann. ACM Symp. on Theory of Computing, (STOC 1997), pp. 189-199, 1997.

3. M. Naor and O. Reingold, *Number-Theoretic constructions of efficient pseudorandom functions*, J. ACM vol. 51(2), pp. 231-262, 2004.

   Preliminary Version: Proc. 38th IEEE Symp. on Foundations of Computer Science (FOCS 1997), pp.458-467, 1997.

4. R. Canetti, D. Micciancio and O. Reingold, *Perfectly one-way probabilistic hash functions*, Proc. 30th Ann. ACM Symp. on Theory of Computing (STOC 1998), pp. 131-140, 1998.

5. M. Naor and O. Reingold, *From unpredictability to indistinguishability: A simple construction of pseudorandom functions from MACs*, Advances in Cryptology - CRYPTO 1998, pp. 267-282, 1998.

6. E. Biham, D. Boneh and O. Reingold, *Breaking generalized Diffie-Hellmann modulo a composite is no easier than factoring*, Information Processing Letters 70(2), pp. 83-87, 1999.

7. R. Raz and O. Reingold, *On recycling the randomness of states in space bounded computation*, STOC 1999, pp. 159-168, 1999.

8. R. Raz, O. Reingold and S. Vadhan, *Extracting all the randomness and reducing the error in Trevisan's extractors*, J. Comput. Syst. Sci. (JCSS), vol. 65(1), pp. 97-128, 2002.

   Preliminary Version: STOC 1999, pp. 149-158, 1999.

9. M. Naor, B. Pinkas and O. Reingold, *Distributed pseudorandom functions and KDCs*, Advances in Cryptology - EUROCRYPT 1999, pp. 327-346, 1999.

10. C. Dwork, M. Naor, O. Reingold and L. J. Stockmeyer, *Magic functions*, J. ACM vol. 50(6), pp. 852-921, 2003.

    Preliminary Version: FOCS 1999, pp. 523-534, 1999.

11. R. Raz, O. Reingold and S. Vadhan, *Error reduction for extractors*, FOCS 1999, pp. 191-201, 1999.

12. M. Naor, O. Reingold and A. Rosen, *Pseudorandom functions and factoring*, SIAM J. Comput., vol. 31(5), pp. 1383-1404, 2002.

    Preliminary Version: STOC 2000, pp. 11-20, 2000.

13. Y. Gertner, S. Kannan, T. Malkin, O. Reingold and M. Viswanathan, *The relationship between public key encryption and oblivious transfer*, FOCS 2000, pp. 325-335, 2000.

14. O. Reingold, R. Shaltiel and A. Wigderson, *Extracting randomness via repeated condensing*, SIAM J. Comput., 35(5), 1185-1209, 2006.

    Preliminary Version: FOCS 2000, pp. 22-31, 2000.

15. O. Reingold, S. Vadhan and A. Wigderson, *Entropy waves, the Zig-Zag graph product, and new constant-degree expanders and extractors*, FOCS 2000, pp. 3-13, 2000.

    Full Version of part of this work: Annals of Mathematics, vol. 155(1), 2001.

16. W. Aiello, Y. Ishai and O. Reingold, *Priced oblivious transfer: how to sell digital goods*, EUROCRYPT 2001, pp. 119-135, 2001.

17. M. Naor and O. Reingold: *Constructing pseudorandom permutations with a prescribed structure*, J. Cryptology, vol. 15(2), pp. 97-102, 2002.

Preliminary Version: SODA 2001, pp. 458-459, 2001.

18. W. Aiello, S. M. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A. D. Keromytis, and O. Reingold: *Just fast keying: Key agreement in a hostile internet*. ACM Trans. Inf. Syst. Secur. vol. 7(2), pp. 242-273, 2004.

    Preliminary Version: *Efficient, DoS-Resistant, Secure Key Exchange for Internet Protocols*. Security Protocols Workshop 2001: pp. 27-39, 2001.

19. Y. Gertner, T. Malkin and O. Reingold, *On the impossibility of basing trapdoor functions on trapdoor predicates*, FOCS 2001, pp. 126-135, 2001.

20. M. R. Capalbo, O. Reingold, S. Vadhan and A. Wigderson, Randomness conductors and constant-degree lossless expanders, Joint session: STOC 2002, pp. 659-668, and IEEE Conference on Computational Complexity 2002, pp. 15, 2002.

21. Bar-Yossef, O. Reingold and R. Shaltiel and L. Trevisan, *Streaming computation of combinatorial objects*, IEEE Conference on Computational Complexity 2002, pp. 165-174, 2002.

22. N. Alon, M. Merritt, O. Reingold, G. Taubenfeld, R. N. Wright, *Tight bounds for shared memory systems accessed by Byzantine processes*, Distributed Computing 18(2), 99-109, 2005.

    Preliminary Version: DISC 2002, pp. 222-236, 2002.

23. C.-J. Lu, O. Reingold, S. Vadhan, and A. Wigderson: *Extractors: optimal up to constant factors*, STOC 2003, 602-611, 2003.

24. D. Harnik, M. Naor, O. Reingold, and A. Rosen, *Completeness in two-party secure computation: a computational view*, J. Cryptology 19(4), 521-552, 2006.

    Preliminary Version: STOC 2004, pp. 252-261, 2004.

25. O. Reingold, L. Trevisan, S. Vadhan, *Notions of reducibility between cryptographic primitives*, TCC 2004, 1-20, 2004.

26. C. Dwork, M. Naor, O. Reingold, *Immunizing encryption schemes from decryption errors*, EUROCRYPT 2004, 342-360, 2004.

27. I. Dinur and O. Reingold, Assignment-Testers: towards a combinatorial proof of the PCP-Theorem, SIAM J. Comput. 36(4): 975-1024 (2006) - special issue on "Randomness and Computation".

Preliminary Version: FOCS 2004, 155-164, 2004.

28. M. J. Freedman, Y. Ishai, B. Pinkas and O. Reingold *Keyword search and oblivious pseudorandom functions*, TCC 2005, 303-324.

29. D. Harnik, J. Kilian, M. Naor, O. Reingold, and A. Rosen, *On robust combiners for oblivious transfer and other primitives*, EUROCRYPT 2005: 96-113, 2005.

30. Omer Reingold: *Undirected ST-connectivity in log-space*, J. ACM 55(4): (2008).

    Preliminary Version: STOC 2005: 376-385, 2005. Best paper award.

31. Eyal Kaplan, Moni Naor, Omer Reingold Derandomized Constructions of k-Wise (Almost) Independent Permutations. Algorithmica 55(1): 113-133 (2009)

    Preliminary Version: The 9th International Workshop on Randomization and Computation (RANDOM), 354-365, 2005.

32. R. Gradwohl, G. Kindler, O. Reingold and A. Ta-Shma, On the Error Parameter of Dispersers, The 9th International Workshop on Randomization and Computation (RANDOM), 294-305, 2005.

33. O. Reingold, L. Trevisan and S. Vadhan, Pseudorandom walks on regular digraphs and the RL vs. L problem. STOC 2006: 457-466, 2006.

34. I. Haitner, D. Harnik, O. Reingold, Efficient Pseudorandom Generators from Exponentially Hard One-Way Functions, ICALP 2006, 228-239, 2006. Track C best paper award.

35. I. Haitner, D. Harnik, O. Reingold, *On the Power of the Randomized Iterate*, SIAM J. Comput. 40(6): 1486-1528 (2011).

    Preliminary Version: CRYPTO 2006, 22-40, 2006. Best paper award.

36. Iftach Haitner, Minh-Huyen Nguyen, Shien Jin Ong, Omer Reingold, Salil Vadhan: Statistically Hiding Commitments and Statistical Zero-Knowledge Arguments from Any One-Way Function. SIAM J. Comput. 39(3): 1153-1218 (2009)

    Preliminary Version (part of the work): I. Haitner and O. Reingold, *Statistically-Hiding Commitment from Any One-Way Function*, STOC 2007, 1-10, 2007.

37. K.-M. Chung, O. Reingold and S. Vadhan, *S-T Connectivity on Digraphs with Known Stationary Distribution*, ACM Transactions on Algorithms 7(3): 30 (2011)

    Preliminary Version: CCC 2007, 236-249, 2007.

38. I. Haitner and O. Reingold, *A New Interactive Hashing Theorem*, J. Cryptology 27(1): 109-138 (2014)

Preliminary version: CCC 2007, 319-332, 2007.

39. I. Haitner, J. J. Hoch, O. Reingold and G. Segev, *Finding Collisions in Interactive Protocols -- A Tight Lower Bound on the Round Complexity of Statistically-Hiding Commitments*, SIAM J. Comput. 44(1): 193-242 (2015)

Preliminary version: FOCS 2007, 669-679, 2007.

40. R. Gradwohl and O. Reingold, Fault Tolerance in Large Games, Games and Economic Behavior 86: 438-457 (2014)

Preliminary version: ACM Conference on Electronic Commerce (EC) 2008, 274-283.

41. O. Reingold, L. Trevisan, M. Tulsiani and S. Vadhan, Dense Subsets of Pseudorandom Sets, 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS 08).

42. Ronen Gradwohl, Omer Reingold, Ariel Yadin, Amir Yehudayoff: Players' Effects Under Limited Independence. Math. Oper. Res. 34(4): 971-980 (2009)

43. Iftach Haitner, Omer Reingold, Salil P. Vadhan and Hoeteck Wee: Inaccessible entropy. STOC 2009: 611-620

44. Cynthia Dwork, Moni Naor, Omer Reingold, Guy N. Rothblum and Salil Vadhan: On the complexity of differentially private data release: efficient algorithms and hardness results. STOC 2009: 381-390

45. Ilya Mironov, Omkant Pandey, Omer Reingold and Salil Vadhan: Computational Differential Privacy. CRYPTO 2009: 126-142.

46. Shachar Lovett, Omer Reingold, Luca Trevisan and Salil Vadhan: Pseudorandom Bit Generators That Fool Modular Sums. APPROX-RANDOM 2009: 615-630.

47. Klim Efremenko and Omer Reingold, How Well Do Random Walks Parallelize?. APPROX-RANDOM 2009: 476-489

48. Iftach Haitner, Omer Reingold and Salil Vadhan: Efficiency improvements in constructing pseudorandom generators from one-way functions. SIAM J. Comput. 42(3): 1405-1430 (2013)

Preliminary Version: STOC 2010: 437-446

49. Iftach Haitner, Thomas Holenstein, Omer Reingold, Salil P. Vadhan, Hoeteck Wee: *Inaccessible Entropy II: IE Functions and Universal One-Way Hashing*. Theory Comput.

16: 1-55 (2020)

Preliminary Version: EUROCRYPT 2010: 616-637

50. Ronen Gradwohl and Omer Reingold, Partial Exposure in Large Games, Games and Economic Behavior, Volume 68, Issue 2, March 2010, Pages 602-613.

51. Andrew McGregor, Ilya Mironov, Toniann Pitassi, Omer Reingold, Kunal Talwar, and Salil Vadhan, The limits of two-party differential privacy, 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS 2010), 2010.

52. Parikshit Gopalan, Raghu Meka, Omer Reingold and David Zuckerman, Pseudorandom Generators for Combinatorial Shapes, SIAM J. Comput. 42(3): 1051-1076 (2013).

    Preliminary version: STOC 2011

53. Moshe Babaioff, Liad Blumrosen, Nicolas Lambert, and Omer Reingold, Only Valuable Experts Can Be Valued, in ACM Conference on Electronic Commerce (EC'11), 2011

54. Laura Elisa Celis, Omer Reingold, Gil Segev, and Udi Wieder, Balls and Bins: Smaller Hash Families and Faster Evaluation, SIAM J. Comput. 42(3): 1030-1050 (2013)

    Preliminary version: FOCS 2011

55. Cynthia Dwork, Moritz Hardt, Toniann Pitassi, Omer Reingold, Rich Zemel, Fairness Through Awareness, Innovations in Theoretical Computer Science (ITCS) 2012

56. Ilya Mironov, Omkant Pandey, Omer Reingold and Gil Segev, Incremental Deterministic Public-Key Encryption, J. Cryptology 31(1): 134-161 (2018). Preliminary version: EUROCRYPT, 2012.

57. Parikshit Gopalan, Raghu Meka, and Omer Reingold, DNF Sparsification and Faster Deterministic Approximate Counting of Satisfying Assignments, Computational siComplexity 22(2): 275-310 (2013). Preliminary version in CCC 2012

58. Parikshit Gopalan, Raghu Meka, Omer Reingold, Luca Trevisan, Salil P. Vadhan: Better Pseudorandom Generators from Milder Pseudorandom Restrictions. *FOCS 2012: 120-129*

59. Omer Reingold, Thomas Steinke, Salil P. Vadhan: Pseudorandomness for Regular Branching Programs via Fourier Analysis. APPROX-RANDOM 2013: 655-670

60. Omer Reingold, Ron D. Rothblum, Udi Wieder: *Pseudorandom Graphs in Data Structures*. ICALP (1) 2014: 943-954

61. Raghu Meka, Omer Reingold, Guy N. Rothblum, Ron D. Rothblum: *Fast Pseudorandomness for Independence and Load Balancing*, ICALP (1) 2014: 859-870

62. Raghu Meka, Omer Reingold, Yuan Zhou: *Deterministic Coupon Collection and Better Strong Dispersers*. APPROX-RANDOM 2014: 872-884

63. Cynthia Dwork, Vitaly Feldman, Moritz Hardt, Toniann Pitassi, Omer Reingold, Aaron Leon Roth: *Preserving Statistical Validity in Adaptive Data Analysis*. STOC 2015: 117-126

64. Cynthia Dwork, Vitaly Feldman, Moritz Hardt, Toniann Pitassi, Omer Reingold, Aaron Leon Roth: *The reusable holdout: Preserving validity in adaptive data analysis*, Science 7 August 2015: Vol. 349 no. 6248 pp. 636-638

65. Cynthia Dwork, Moni Naor, Omer Reingold, Guy Rothblum: *Pure Differential Privacy for Rectangle Queries via Private Partitions*, ASIACRYPT (2) 2015: 735-751

66. Cynthia Dwork, Vitaly Feldman, Moritz Hardt, Toniann Pitassi, Omer Reingold, Aaron Roth: Generalization in Adaptive Data Analysis and Holdout Reuse, NIPS 2015: 2350-2358

67. Kat Ellis, Moises Goldszmidt, Gert Lanckriet, Nina Mishra and Omer Reingold, Attention Exchange: Equality and Social Mobility in Online Communities, WSDM 2016: 523-532

68. Omer Reingold, Guy N. Rothblum and Ron D. Rothblum: *Constant-Round Interactive Proofs for Delegating Computation*, SIAM J. Comput. 50(3) 2021

    Preliminary version: STOC 2016: 49-62

69. Omer Reingold, Nina Narodytska: Adaptive Condorcet-Based Stopping Rules Can Be Efficient. ECAI 2016: 1704-1705

70. Omer Reingold, Shai Vardi: New techniques and tighter bounds for local computation algorithms. J. Comput. Syst. Sci. 82(7): 1180-1200 (2016)

71. Moshe Babaioff, Yishay Mansour, Noam Nisan, Gali Noti, Carlo Curino, Nar Ganapathy, Ishai Menache, Omer Reingold, Moshe Tennenholtz, Erez Timnat: ERA: A Framework for Economic Resource Allocation for the Cloud. WWW (Companion Volume) 2017: 635-642

72. Cynthia Dwork, Vitaly Feldman, Moritz Hardt, Toniann Pitassi, Omer Reingold, Aaron Roth: Guilt-free data reuse. Commun. ACM 60(4): 86-93 (2017)

73. Jack Murtagh, Omer Reingold, Aaron Sidford, Salil P. Vadhan, Derandomization Beyond Connectivity: Undirected Laplacian Systems in Nearly Logarithmic Space. SIAM J.

Comput. 50(6): 1892-1922 (2021)

Preliminary version: FOCS 2017: 801-812, 2017

74. Eshan Chattopadhyay, Pooya Hatami, Omer Reingold and Avishay Tal, Improved Pseudorandomness for Unordered Branching Programs through Local Monotonicity, STOC 2018: 363-375 2018

75. Úrsula Hébert-Johnson, Michael P. Kim, Omer Reingold and Guy N. Rothblum, *Calibration for the (Computationally-Identifiable) Masses*, ICML 1944-1953, 2018

76. Omer Reingold, Guy N. Rothblum and Ron Rothblum, *Efficient Batch Verification for UP*, CCC 2018: 22:1-22:23

77. Michael P. Kim, Omer Reingold and Guy N. Rothblum, *Fairness Through Computationally-Bounded Awareness*, NuerIPS 2018

78. Iftach Haitner, Noam Mazor, Rotem Oshman, Omer Reingold and Amir Yehudayoff, *On the Communication Complexity of Key-Agreement Protocols*, ITCS 2019 40:1-40:16

79. Raghu Meka, Omer Reingold, Avishay Tal, *Pseudorandom Generators for Width-3 Branching Programs*, STOC 2019

80. Cynthia Dwork, Michael P. Kim, Omer Reingold, Guy N. Rothblum and Gal Yona, *Learning from Outcomes: Evidence-Based Rankings*, FOCS 2019: 106-125

81. Sumegha Garg, Michael P. Kim, Omer Reingold, *Tracking and Improving Information in the Service of Fairness*, EC 2019*: 809-824*

82. Jack Murtagh, Omer Reingold, Aaron Sidford and Salil P. Vadhan: *Deterministic Approximation of Random Walks in Small Space*, Theory Comput. 17: 1-35 (2021)

Preliminary version: APPROX-RANDOM 2019: 42:1-42:22

83. Omer Reingold, *Through the lens of a passionate theoretician*, Commun. ACM 63(3): 25-27, 2020

84. Katrina Ligett , Charlotte Peale and Omer Reingold: *Bounded-Leakage Differential Privacy*, Foundations of Responsible Computing (FORC) 2020: 10:1-10:20.

85. Cynthia Dwork, Michael P. Kim, Omer Reingold, Guy N. Rothblum and Gal Yona: *Outcome indistinguishability*, STOC 2021: 1095-1108

86. Dean Doron, Raghu Meka, Omer Reingold, Avishay Tal, Salil P. Vadhan: *Pseudorandom Generators for Read-Once Monotone Branching Programs*, APPROX-RANDOM 2021:

58:1-58:21.

87. Lunjia Hu, Omer Reingold: *Robust Mean Estimation on Highly Incomplete Data with Arbitrary Outliers*, AISTATS 2021: 1558-1566.

88. Michael P. Kim, Christoph Kern, Shafi Goldwasser, Frauke Kreuter and Omer Reingold, *Universal adaptability: Target-independent inference that competes with propensity scoring*, Proceedings of the National Academy of Sciences (PNAS), 119(4), 2022

89. Parikshit Gopalan, Adam Tauman Kalai, Omer Reingold, Vatsal Sharan, Udi Wieder. *Omnipredictors*. ITCS 2022: 79:1-79:21

90. Monika Henzinger, Charlotte Peale, Omer Reingold, Judy Hanwen Shen, *Leximax Approximations and Representative Cohort Selection*, FORC 2022: 2:1-2:22

91. Lunjia Hu, Charlotte Peale, Omer Reingold, *Metric Entropy Duality and the Sample Complexity of Outcome Indistinguishability*, ALT 2022: 515-552

92. Parikshit Gopalan, Omer Reingold, Vatsal Sharan, Udi Wieder: *Multicalibrated Partitions for Importance Weights*, ALT 2022: 408-435.

93. Cynthia Dwork, Michael P. Kim, Omer Reingold, Guy N. Rothblum, Gal Yona, *Beyond Bernoulli: Generating Random Outcomes that cannot be Distinguished from Nature*, ALT 2022: 342-380.

94. Omer Reingold, *Bringing Research-Life to Centerstage*, Bull. EATCS 138 (2022).

95. Parikshit Gopalan, Lunjia Hu, Michael P. Kim, Omer Reingold, Udi Wieder, *Loss Minimization Through the Lens Of Outcome Indistinguishability*, ITCS 2023: 60:1-60:20.

96. Inbal Livni Navon, Charlotte Peale, Omer Reingold, Judy Hanwen Shen, *Bidding Strategies for Proportional Representation in Advertisement Campaigns*, FORC 2023: 3:1-3:22.

97. Cynthia Dwork, Omer Reingold, Guy N. Rothblum, *From the Real Towards the Ideal: Risk Prediction in a Better World*, FORC 2023: 1:1-1:17.

98. Lunjia Hu, Inbal Livni Navon, Omer Reingold, *Generative Models of Huge Objects*, CCC 2023: 5:1-5:20.

Submissions and Unpublished Manuscripts:

- Moni Naor and Omer Reingold, *A Pseudo-Random Encryption Mode*, manuscript
- Moni Naor, Yael Naor and Omer Reingold, *Applied Kid Cryptography, or How to Convince Your Children You Are Not Cheating*, 1999

- C. Dwork, M. Langberg, M. Naor, K. Nissim and O. Reingold, *Succinct proofs for NP and spooky interactions*, manuscript, 2001.
- O. Reingold, S. Vadhan and A. Wigderson. *A Note on Extracting Randomness from Santha-Vazirani Sources,* manuscript 2004.
- Omer Reingold, Luca Trevisan, Madhur Tulsiani, and Salil P. Vadhan, *New Proofs of the Green–Tao–Ziegler Dense Model Theorem: An Exposition*, manuscript 2008

- Omer Reingold, Judy Hanwen Shen, Aditi Talati, *Dissenting Explanations: Leveraging Disagreement to Reduce Model Overreliance*

- Sumegha Garg, Christopher Jung, Omer Reingold, Aaron Roth, Oracle Efficient Online Multicalibration and Omniprediction

- Parikshit Gopalan, Michael P. Kim, Omer Reingold, Characterizing notions of omniprediction via multicalibration.