July 12, 2018

David Zuckerman

Computer Science Department, University of Texas at Austin, 2317 Speedway, Stop D9500, Austin, TX 78712
diz@cs.utexas.edu http://www.cs.utexas.edu/~diz (512) 471-9729

Research Interests

The role of randomness in computation, pseudorandomness, complexity theory, coding theory, distributed computing, cryptography, approximability, random walks.

Professional Experience

University of Texas at Austin, Department of Computer Science
Endowed Professorship, September 2010 - present;
Professor, September 2003 - present;
Associate Professor (tenured), September 1998 - August 2003;
Assistant Professor, January 1994 - August 1998.

Simons Institute for the Theory of Computing, U.C. Berkeley
Visiting Scholar and Co-organizer of the *Pseudorandomness* program, Spring 2017.

Institute for Advanced Study, School of Mathematics
Member, September 2011 - August 2012.

Harvard University, Radcliffe Institute for Advanced Study and DEAS
Radcliffe Fellow, Guggenheim Fellow, and Visiting Scholar, July 2004 - June 2005.

University of California at Berkeley, Computer Science Division
Visiting Scholar and Visiting McKay Lecturer, January 1999 - December 2000.

Hebrew University of Jerusalem, Institute for Computer Science
Lady Davis Postdoctoral Fellow, Oct. - Dec. 1993. Sponsor: Avi Wigderson.

Massachusetts Institute of Technology, Laboratory for Computer Science
NSF Mathematical Sciences Postdoctoral Fellow, 1991-93. Sponsor: Silvio Micali.

Education

Ph.D., University of California at Berkeley, Computer Science, 1991.
Advisor: Umesh Vazirani. AT&T Bell Labs Fellowship, NSF Graduate Fellowship.

A.B., Harvard University, Mathematics, 1987. Summa cum laude, Phi Beta Kappa.

Major Honors and Awards

Simons Investigator Award, 2016-21

Best Paper Award, STOC 2016

ACM Fellow, 2013

John S. Guggenheim Memorial Foundation Fellowship, 2004-05

David and Lucile Packard Fellowship for Science and Engineering, 1996-2006

Alfred P. Sloan Research Fellowship, 1996-2000

NSF Young Investigator Award, 1994-2000

Machtey Award (Best Student Paper Award), FOCS 1990

William Lowell Putnam Mathematical Competition
1986: Putnam Fellow – scored among top 6 in nation.
1985: Scored 8th highest in nation.

Other Grants

National Science Foundation, 2017-21
Fine-Grained Derandomization (with co-PI Dana Moshkovitz)

National Science Foundation, 2015-18
Fundamental Connections in Randomness and Complexity

National Science Foundation, 2012-15
Pseudorandomness and Randomness Extraction

U.S.Israel Binational Science Foundation, 2011-15
Algebraic Approaches to Problems in Pseudorandomness (with Shaltiel, Ta-Shma, and Umans)

National Science Foundation, 2009-13
Pseudorandomness, Codes, and Distributed Computing

Texas Higher Education Coordinating Board, Advanced Research Projects, 2008-11
Randomness Extraction and Distributed Computing

National Science Foundation, 2006-10
Randomness Extraction and Applications

National Science Foundation, 2003-07
Pseudorandomness, Codes, and Cryptography

National Science Foundation, 2000-04
Pseudorandomness and Fault Tolerance

University Research Institute Summer Research Award, 1994
Investigating Whether Randomness is Necessary for Computation

Ph.D. Advisees

Xue Chen (Ph.D., 2018, soon to be postdoc at Northwestern University)
Eshan Chattopadhyay (Ph.D., 2016, currently postdoc at the Institute for Advanced Study; soon to be Assistant Professor at Cornell)
Abhishek Bhowmick (Ph.D., 2015, currently Senior Research Engineer at Apple)
Xin Li (Ph.D., 2011, currently Assistant Professor at Johns Hopkins)
Raghu Meka (Ph.D., 2011, currently Assistant Professor at UCLA)
Jesse Kamp (Ph.D., 2007, currently Principal Member of Technical Staff at Oracle)
Anindya Patthak (Ph.D., 2007, currently Principal Member of Tech. Staff at Oracle)
Anup Rao (Ph.D., 2007, currently Associate Professor at University of Washington)
William Hoza (in progress); Fu Li (in progress).

Postdocs Sponsored

Pooya Hatami (2016-18, soon to be Assistant Professor at Ohio State University)
Mahdi Cheraghchi (2010-11, currently Assistant Professor at Imperial College)
Ariel Gabizon (Spring 2010, currently Visiting Researcher at the Technion)
Tugkan Batu (2003-04, currently Assistant Professor at London School of Economics)
Amnon Ta-Shma (1999-2000, currently Associate Professor at Tel Aviv University)
Alex Russell (1997-99, currently Professor at University of Connecticut)

Editorial Work

Guest Editor, *Computational Complexity*, special issue devoted to CCC 2015

Editorial Board, *Theory of Computing*, 2005-15

Editorial Board, *ACM Transactions on Computation Theory*, 2008-13

Editorial Board, *SIAM Journal on Discrete Mathematics*, 2003-08

Program Committees

PC Chair, *60th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2019

PC Chair, *30th Computational Complexity Conference (CCC)*, 2015

45th Annual ACM Symposium on Theory of Computing (STOC), 2013

15th International Workshop on Randomization and Computation (RANDOM), 2011

23rd Annual IEEE Conference on Computational Complexity (CCC), 2008

46th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2005

41st Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2000

29th Annual ACM Symposium on Theory of Computing (STOC), 1997

1st Int'l Symp. on Randomization Techniques in Computer Science (RANDOM), 1997

11th Annual IEEE Conference on Computational Complexity (CCC), 1996

Organizing Committees

Simons *Pseudorandomness Reunion* Workshop, UC Berkeley, June 2018

Simons Program *Pseudorandomness*, UC Berkeley, Spring 2017

Simons Workshop *Expanders and Extractors*, UC Berkeley, January-February, 2017

Simons *Pseudorandomness Boot Camp*, UC Berkeley, January, 2017

Principal Organizer, DIMACS Workshop *Pseudorandomness and Explicit Combinatorial Constructions*, Rutgers University, October, 1999

4th Annual German-American Frontiers of Science Symposium, 1998

Review Panels

Various for NSF and Simons Foundation.

Courses Taught

Graduate courses

Approximation Algorithms, Coding Theory, Combinatorics & Graph Theory, Polynomials & Computation, Pseudorandomness, Pseudorandomness & Cryptography, Randomized Algorithms, Randomness & Computation, Theory of Computation.

Undergraduate courses

Algorithms and Complexity, Analysis of Programs, Cryptography, Randomized Algorithms, Theory of Computation.

Publications

In my field, traditionally authors are listed in alphabetical order. Only in unusual cases is this not done.

Randomness Extractors and Applications

- E. Chattopadhyay and D. Zuckerman, "Explicit Two-Source Extractors and Resilient Functions," *48th Annual ACM Symposium on Theory of Computing*, pp. 670-683, 2016. STOC 2016 Best Paper Award.
- E. Chattopadhyay and D. Zuckerman, "New Extractors for Interleaved Sources," *31st Computational Complexity Conference*, pp. 7:1-7:28, 2016.
- A. Bhowmick, A. Gabizon, T.H. Le, and D. Zuckerman, "Deterministic Extractors for Additive Sources," *6th Innovations in Theoretical Computer Science*, 2015, pp. 277-286.
- Y. Dodis, X. Li, T.D. Wooley, and D. Zuckerman, "Privacy amplification and non-malleable extractors via character sums," *SIAM Journal on Computing*, 43 (2014): 800-830. Special issue on FOCS 2011. Preliminary version in *52nd Annual IEEE Symposium on Foundations of Computer Science*, 2011.
- Y. Kalai, X. Li, A. Rao and D. Zuckerman, "Network extractor protocols," *49th Annual IEEE Symposium on Foundations of Computer Science*, 2008, pp. 654-663.
- A. Rao and D. Zuckerman, "Extractors for three uneven-length sources," *12th International Workshop on Randomization and Computation (RANDOM)*, LNCS 5171, Springer-Verlag, pp. 557-570, 2008.
- J. Kamp, A. Rao, S. Vadhan, and D. Zuckerman, "Deterministic extractors for small space sources," *Journal of Computer and System Sciences*, 77 (2011): 191-220. Preliminary version in *38th Annual ACM Symposium on Theory of Computing*, 2006, pp. 691-700.
- D. Zuckerman, "Linear degree extractors and the inapproximability of Max Clique and Chromatic Number," *Theory of Computing*, 3 (2007): 103-128. Preliminary version in *38th Annual ACM Symposium on Theory of Computing*, 2006, pp. 681-690.
- J. Kamp and D. Zuckerman, "Deterministic extractors for bit-fixing sources and exposure-resilient cryptography," *SIAM Journal on Computing*, 36 (2006): 1231-1247. Preliminary version in *44th Annual IEEE Symposium on Foundations of Computer Science*, 2003, pp. 92-101.
- A. Ta-Shma, D. Zuckerman, and S. Safra, "Extractors from Reed-Muller codes," *Journal of Computer and System Sciences*, 72 (2006): 786-812. Special issue on FOCS 2001. Preliminary version in *42nd Annual IEEE Symposium on Foundations of Computer Science*, 2001, pp. 638-647.
- A. Ta-Shma and D. Zuckerman, "Extractor codes," *IEEE Transactions on Information Theory*, 50 (2004): 3015-3025. Preliminary version in *33rd Annual ACM Symposium on Theory of Computing*, 2001, pp. 193-199.
- A. Ta-Shma, C. Umans, and D. Zuckerman, "Lossless condensers, unbalanced expanders, and extractors," *Combinatorica*, 27 (2007): 213-240. Preliminary version in *33rd Annual ACM Symposium on Theory of Computing*, 2001, pp. 143-152.
- O. Goldreich and D. Zuckerman, "Another proof that BPP $\subseteq$ PH (and more)." In O. Goldreich, *Studies in Complexity and Cryptography*, LNCS 6650, Springer-Verlag, 2011, pp. 40-53.
- D. Zuckerman, "Randomness-optimal oblivious sampling," *Random Structures & Algorithms*, 11 (1997): 345-367. Preliminary version, entitled "Randomness-optimal sampling, extractors, and constructive leader election," in *28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 286-295.

- A. Srinivasan and D. Zuckerman, "Computing with very weak random sources," *SIAM Journal on Computing*, 28 (1999): 1433-1459. Preliminary version in *35th Annual IEEE Symposium on Foundations of Computer Science*, 1994, pp. 264-275.
- A. Wigderson and D. Zuckerman, "Expanders that beat the eigenvalue bound: explicit construction and applications," *Combinatorica*, 19 (1999): 125-138. Preliminary version in *25th Annual ACM Symposium on Theory of Computing*, 1993, pp. 245-251.
- N. Nisan and D. Zuckerman, "Randomness is linear in space," *Journal of Computer and System Sciences*, 52 (1996): 43-52. Special issue on STOC 1993. Preliminary version, entitled "More deterministic simulation in Logspace," in *25th Annual ACM Symposium on Theory of Computing*, 1993, pp. 235-244.
- D. Zuckerman, "Simulating BPP using a general weak random source," *Algorithmica*, 16 (1996): 367-391. Special issue on randomized algorithms. Preliminary version in *32nd Annual IEEE Symposium on Foundations of Computer Science*, 1991, pp. 79-89.
- D. Zuckerman, "Computing Efficiently Using General Weak Random Sources," Ph.D. dissertation, University of California at Berkeley, 1991.
- D. Zuckerman, "General weak random sources," *31st Annual IEEE Symposium on Foundations of Computer Science*, 1990, pp. 534-543. FOCS 1990 Machtey Award (Best Student Paper Award).

Other Pseudorandomness and Explicit Constructions

- W. Hoza and D. Zuckerman, "Simple Optimal Hitting Sets for Small-Success RL," *59th Annual IEEE Symposium on Foundations of Computer Science*, 2018.
- Y. Ishai, E. Kushilevitz, X. Li, R. Ostrovsky, M. Prabhakaran, A. Sahai, and D. Zuckerman, "Robust Pseudorandom Generators," *40th International Colloquium on Automata, Languages and Programming*, 2013, pp. 576-588.
- R. Impagliazzo, R. Meka, and D. Zuckerman "Pseudorandomness from Shrinkage," *JACM*, to appear. Preliminary version in *53rd Annual IEEE Symposium on Foundations of Computer Science*, 2012, pp. 111-119.
- P. Gopalan, R. Meka, O. Reingold, and D. Zuckerman, "Pseudorandom generators for combinatorial shapes," *SIAM Journal on Computing*, 42 (2013): 1051-1076. Preliminary version in *43rd Annual ACM Symposium on Theory of Computing*, 2011, pp. 253-262.
- D. Zuckerman, "Pseudorandom financial derivatives," *12th ACM Conference on Electronic Commerce*, 2011, pp. 315-320.
- P. Gopalan, R. O'Donnell, Y. Wu, and D. Zuckerman, "Fooling functions of halfspaces under product distributions," *25th Annual IEEE Conference on Computational Complexity*, 2010, pp. 223-234.
- R. Meka and D. Zuckerman, "Pseudorandom generators for polynomial threshold functions," *SIAM Journal on Computing*, 42 (2013): 1275-1301. Special issue on STOC 2010. Preliminary version in *42nd Annual ACM Symposium on Theory of Computing*, 2010, pp. 427-436.
- R. Meka and D. Zuckerman, "Small-bias spaces for group products," *13th International Workshop on Randomization and Computation (RANDOM)*, LNCS 5687, Springer-Verlag, pp. 658-672, 2009.
- M. Saks, A. Srinivasan, S. Zhou, and D. Zuckerman, "Low discrepancy sets yield approximate min-wise independent permutation families," *Information Processing Letters*, 73 (2000): 29-32. Preliminary version in *3rd International Workshop on Randomization and Approximation Techniques in Computer Science*, LNCS 1671, Springer-Verlag, 1999, pp. 11-15.

- N. Linial, M. Luby, M. Saks, and D. Zuckerman, "Efficient construction of a small hitting set for combinatorial rectangles in high dimension," *Combinatorica*, 17 (1997): 215-234. Preliminary version in *25th Annual ACM Symposium on Theory of Computing*, 1993, pp. 258-267.
- R. Impagliazzo and D. Zuckerman, "How to recycle random bits," *30th Annual IEEE Symposium on Foundations of Computer Science*, 1989, pp. 248-253.

Coding Theory and Curve Fitting

- V. Guruswami and D. Zuckerman, "Robust Fourier and polynomial curve fitting," *57th Annual IEEE Symposium on Foundations of Computer Science*, 2016, pp. 751-759.
- E. Chattopadhyay and D. Zuckerman, "Non-malleable codes against constant split-state tampering," *55th Annual IEEE Symposium on Foundations of Computer Science*, 2014, pp. 306-315.
- A. Bhattacharyya, S. Kopparty, G. Schoenebeck, M. Sudan, and D. Zuckerman, "Optimal testing of Reed-Muller codes," *51st Annual IEEE Symposium on Foundations of Computer Science*, 2010, pp. 488-497.
- P. Gopalan, A.R. Klivans, and D. Zuckerman, "List-decoding Reed-Muller codes over small fields," *40th Annual ACM Symposium on Theory of Computing*, 2008, pp. 265-274.
- C.S. Jutla, A.C. Patthak, A. Rudra, and D. Zuckerman, "Testing low-degree polynomials over prime fields," *Random Structures & Algorithms*, 35 (2009), pp. 163-193. Preliminary version in *45th Annual IEEE Symposium on Foundations of Computer Science*, 2004, pp. 423-432.
- V. Guruswami, J. Hastad, M. Sudan, and D. Zuckerman, "Combinatorial bounds for list decoding," *IEEE Transactions on Information Theory*, 48 (2002), pp. 1021-1034. Preliminary version in *38th Annual Allerton Conference on Communication, Control, and Computing*, 2000, pp. 603-612.
- L.J. Schulman and D. Zuckerman, "Asymptotically good codes correcting insertions, deletions and transpositions," *IEEE Transactions on Information Theory*, 45 (1999), pp. 2552-2557. Preliminary version in *8th ACM-SIAM Symposium on Discrete Algorithms*, 1997, pp. 669-674.
- J. Blomer, M. Kalfane, M. Karpinski, R. Karp, M. Luby, and D. Zuckerman, "An XOR-based erasure-resilient coding scheme," *ICSI Technical Report No. TR-95-048*, 1995.

Communication Complexity

- M. Goos, S. Lovett, R. Meka, T. Watson, and D. Zuckerman, "Rectangles are nonnegative juntas," *SIAM Journal on Computing*, 45 (2016): 18351869. Preliminary version in *47th Annual ACM Symposium on Theory of Computing*, 2015, pp. 257-266.
- H. Klauck, A. Nayak, A. Ta-Shma, and D. Zuckerman, "Interaction in quantum communication," *IEEE Transactions on Information Theory*, 53 (2007): 1970-1982. Preliminary version, entitled "Interaction in quantum communication and the complexity of set disjointness," in *33rd Annual ACM Symposium on Theory of Computing*, 2001, pp. 124-133.

Compression and Lower Bounds

- R. Chen, V. Kabanets, A. Kolokolova, R. Shaltiel, and D. Zuckerman, "Mining circuit lower bound proofs for meta-algorithms," *Computational Complexity*, 24 (2015), pp. 333-392. Special issue on CCC 2014. Preliminary version in *29th Annual IEEE Conference on Computational Complexity*, 2014, pp. 262-273.

- L. Trevisan, S. Vadhan, and D. Zuckerman, "Compression of samplable sources," *Computational Complexity*, 14 (2005), pp. 186-227 . Special issue on CCC 2004. Preliminary version in *19th Annual IEEE Conference on Computational Complexity*, 2004, pp. 1-14.

Cryptography, Distributed Computing, and Security

- R. Gradwohl, S. Vadhan, and D. Zuckerman, "Random selection with an adversarial majority." In *Proceedings of 26th Annual International Cryptology Conference (CRYPTO)*, Lecture Notes in Computer Science, volume 4117, 2006, pp. 409-426.
- D. Song, D. Zuckerman, and J.D. Tygar, "Expander graphs for digital stream authentication and robust overlay networks," *IEEE Symposium on Security and Privacy*, 2002, pp. 258-270.
- A. Russell, M. Saks, and D. Zuckerman, "Lower bounds for leader election and collective coin-flipping in the perfect information model," *SIAM Journal on Computing*, 31 (2002): 1645-1662. Preliminary version in *31st Annual ACM Symposium on Theory of Computing*, 1999, pp. 339-347.
- A. Russell and D. Zuckerman, "Perfect information leader election in $\log^* n + O(1)$ rounds," *Journal of Computer and System Sciences*, 63 (2001), pp. 612-626. Special issue on FOCS 1998. Preliminary version in *39th Annual IEEE Symposium on Foundations of Computer Science*, 1998, pp. 576-583.
- B. Ghosh, F.T. Leighton, B.M. Maggs, S. Muthukrishnan, C.G. Plaxton, R. Rajaraman, A.W. Richa, R.E. Tarjan, and D. Zuckerman, "Tight analyses of two local load balancing algorithms," *SIAM Journal on Computing*, 29 (1999): 29-64. Preliminary version in *27th Annual ACM Symposium on Theory of Computing*, 1995, pp. 548-558.
- E. Kushilevitz, Y. Mansour, M.O. Rabin, and D. Zuckerman, "Lower bounds for randomized mutual exclusion," *SIAM Journal on Computing*, 27 (1998), pp. 1550-1563. Preliminary version in *25th Annual ACM Symposium on Theory of Computing*, 1993, pp. 154-163.
- O. Goldreich, R. Impagliazzo, L. Levin, R. Venkatesan, and D. Zuckerman, "Security preserving amplification of hardness," *31st Annual IEEE Symposium on Foundations of Computer Science*, 1990, pp. 318-326.

Inapproximability

- D. Zuckerman, "On unapproximable versions of NP-complete problems," *SIAM Journal on Computing*, 25 (1996): 1293-1304. Preliminary version, entitled "NP-complete problems have a version that's hard to approximate," in *8th IEEE Conference on Structure in Complexity Theory*, 1993, pp. 305-312.
- N. Alon, U. Feige, A. Wigderson, and D. Zuckerman, "Derandomized graph products," *Computational Complexity*, 5 (1995), pp. 60-75.

Random Walks on Graphs

- P. Winkler and D. Zuckerman, "Multiple cover time," *Random Structures & Algs*, 9 (1996): 403-411.
- D. Zuckerman, "A technique for lower bounding the cover time," *SIAM Journal on Discrete Mathematics*, 5 (1992): 81-87. Preliminary version in *22nd Annual ACM Symposium on Theory of Computing*, 1990, pp. 254-259.
- D. Zuckerman, "On the time to traverse all edges of a graph," *Information Processing Letters*, 38 (1991): 335-337.
- D. Zuckerman, "Covering times of random walks on bounded degree trees and other graphs," *Journal of Theoretical Probability*, 2 (1989): 147-157.

Randomized Algorithms

- M. Luby, A. Sinclair, and D. Zuckerman, "Optimal speedup of Las Vegas algorithms," *Information Processing Letters*, 47 (1993): 173-180. Preliminary version in *2nd Israel Symposium on Theory of Computing and Systems*, 1993, pp. 128-133.

Expository

- D. Zuckerman and E. Chattopadhyay, "How random is your randomness, and why does it matter?" *The Conversation*, September 18, 2016.
- D. Zuckerman, "Can Random Coin Flips Speed Up a Computer?" arXiv:1007.1678, 2010.

Selected Invited Talks

- *Randomness Extractors: An Introduction* STOC 2018 Theory Fest workshop on Randomness Extractors: Constructions and Applications, Los Angeles, June 2018.
- *Simple Optimal Hitting Sets for Small-Success RL.* Simons Pseudorandomness Reunion Workshop, Berkeley, June 2018.
- *Explicit Two-Source Extractors and Resilient Functions.* CMSA Workshop on Probabilistic and Extremal Combinatorics, Harvard University, February 2018; Georgia Tech, November 2016; BIRS Workshop "Computational Complexity," Banff, Canada, September 2016; ICERM Workshop on Algorithmic Coding Theory, Brown University, June 2016; Simons Information Theory Reunion Workshop, Berkeley, June 2016; MIT, April 2016; Harvard University, April 2016; Plenary session, Complexity Theory Meeting, Oberwolfach, Germany, November 2015; TCS+ Online Seminar, October 2015; Simons Workshop on Connections Between Algorithm Design and Complexity Theory, Berkeley, September 2015.
- *Extractors and Expanders.* Four-lecture tutorial in the Pseudorandomness Boot Camp, Simons Institute for the Theory of Computing, Berkeley, January 2017.
- *Randomness.* The Academic Minute, a radio show by NPR-affiliate WAMC, January 2017.
- *When is Randomness Extraction Possible?* Workshop on the Foundations of Randomness, Stellenbosch Institute for Advanced Study, Stellenbosch, South Africa, October 2015.
- *Non-Malleable Codes Against Constant Split-State Tampering.* Simons Workshop on Coding: From Practice to Theory, Berkeley, February 2015; Dagstuhl Workshop on Algebra in Computational Complexity, Dagstuhl, Germany, September 2014.
- *Pseudorandomness from Shrinkage.* Microsoft Research Silicon Valley, July 2014; MIT, May 2014; BIRS Workshop "Computational Complexity", Banff, Canada, July 2013; Weizmann Institute, Israel, June 2013; ELC Tokyo Complexity Workshop, March 2013; Dagstuhl Workshop on Algebraic and Combinatorial Methods in Computational Complexity, Dagstuhl, Germany, October 2012; University of Washington, October 2012.
- *Codes and Pseudorandomness: A Survey.* Workshop on Complexity and Coding Theory, UC San Diego, January, 2014.

- *Randomness Extraction: A Survey.* Satellite Pre-Workshop of ELC Tokyo Complexity Workshop, March 2013; Rutgers University, April 2012; Institute for Advanced Study, February 2012; IPAM Workshop on Mathematics of Information-Theoretic Cryptography, March 2011.
- *Purifying Randomness: How and Why.* After-Hours Conversation (targeting non-scientists), Institute for Advanced Study, March 2012.
- *Privacy Amplification and Non-Malleable Extractors Via Character Sums.* Princeton University, October 2011; Rutgers University, October 2011; Microsoft Research New England, July 2011.
- *Pseudorandom Generators for Polynomial Threshold Functions and Combinatorial Shapes.* Coding, Complexity, and Sparsity Workshop, Ann Arbor, MI, August 2011.
- *The Power of Randomness in Computation.* Targets a lay audience. Liberal Arts and Science Academy (Austin's magnet high school), May 2011; First Bytes program for Austin area high school teachers, August 2008; Radcliffe Institute for Advanced Study, October 2004.
- *Pseudorandom Financial Derivatives from Expander Graphs.* Joint Mathematics Meetings, January 2011; Microsoft Research Silicon Valley, July 2010.
- *Pseudorandom Generators for Polynomial Threshold Functions.* BIRS Workshop "Computational Complexity", Banff, Canada, August 2010.
- *List-Decoding Reed-Muller Codes over Small Fields.* CMU, May 2009; Institute for Advanced Study, October 2008; UC Berkeley, August 2008; BIRS Workshop "Analytic Tools in Computational Complexity", Banff, Canada, August 2008.
- *Linear Degree Extractors and Inapproximability.* California Institute of Technology, April 2007; UC Berkeley, December 2005; Complexity Theory Meeting, Oberwolfach, Germany, June 2005; MIT, May 2005; Featured invited talk at IBM Research/NYU/Columbia Theory Day, April 2005.
- *Deterministic Extractors for Small Space Sources.* BIRS Workshop "Recent Advances in Computational Complexity", Banff, Canada, August 2006; SIAM Conference on Discrete Mathematics, Victoria, Canada, June, 2006.
- *Extracting Randomness.* Harvard University Computer Science Colloquium, February 2005.
- *Extracting Randomness: Past and Future.* Visions Lecture, University of Texas at Austin, November, 2004
- *Some Successes and Failures of Algebra in Constructing Extractors.* IPAM Workshop on Automorphic Forms, Group Theory and Graph Expansion, Los Angeles, February, 2004
- *Deterministic Extractors for Bit-Fixing Sources and Exposure-Resilient Cryptography.* California Institute of Technology, February 2004.
- *Computational Complexity and Entropy.* Featured invited talk at DIMACS Workshop on Computational Complexity, Entropy, and Statistical Physics, Rutgers University, December 2001.
- *Codes in Theoretical Computer Science.* Featured invited talk at DIMACS Workshop on Codes and Complexity, Rutgers University, December 2001.
- *Extractors, Codes, and Polynomials.* Complexity Theory Meeting, Oberwolfach, Germany, November, 2000
- *The Cover Time and Multiple Cover Time.* UC Berkeley, October 2000.
- *Extractors, Codes, and Unbalanced Expanders.* Microsoft Research, May 2000; University of Washington, May 2000; University of British Columbia, May 2000.

- *McKay Lectures: An Introduction to Pseudorandomness and Explicit Combinatorial Constructions; Explicit Expanders: Ramanujan Graphs; Extractors for Weak Random Sources and their Applications.* UC Berkeley, February-March 2000.
- *Collective Coin-Flipping and Leader Election in Asynchronous Environments.* InterTrust STAR Lab, February 2000.
- *Collective Sampling and Leader Election in the Perfect Information Model.* UC Berkeley, April 1999; IBM Research at Almaden, April 1999; Stanford University, April 1999.
- *Advances in Perfect Information Leader Election.* Complexity Theory Meeting, Oberwolfach, Germany, November, 1998
- *Extractors for Weak Random Sources and their Applications.* Featured invited talk at 6th Scandinavian Workshop on Algorithm Theory (SWAT), Stockholm, Sweden, July 1998.
- *Extractors and their Applications.* DIMACS Workshop "Microsurveys in Discrete Probability", June, 1997
- *Constructing Expanders that Beat the Eigenvalue Bound.* Institute for Mathematics and its Applications IMA Workshop on Emerging Applications of Number Theory, Minneapolis, July, 1996
- *Randomness-Optimal Sampling, Extractors, and Constructive Leader Election.* MIT, June 1996; ICSI Workshop "Randomized Algorithms and Computation", December 1995.
- *Diminishing our Reliance on Randomness in Computation.* AMS Special Session on Probability and Combinatorics, Joint Mathematics Meetings, San Francisco, January, 1995
- *Computing With Very Weak Random Sources.* Workshop on Algorithmic Research in the Midsouthwest, November, 1994; Orsay Workshop on Randomized Algorithms, Orsay, France, October, 1994.