

School of Engineering and Applied Sciences  
Maxwell Dworkin 337  
33 Oxford Street  
Cambridge, Massachusetts 02138

Salil P. Vadhan  
Vicky Joseph Professor  
of Computer Science and  
Applied Mathematics



Tel: (617) 496-0439  
Fax: (617) 496-6404  
salil@seas.harvard.edu  
<http://seas.harvard.edu/~salil>

# Salil P. Vadhan

Curriculum Vitae

November 2009

## Contents

Biographical . . . . .	2
Research Interests . . . . .	2
Current Positions . . . . .	2
Previous Positions . . . . .	2
Education . . . . .	3
Honors . . . . .	3
Professional Activities . . . . .	5
Graduate Research Advising . . . . .	6
Undergraduate Research Advising . . . . .	7
Postdoctoral Fellows . . . . .	8
Visitors Hosted . . . . .	9
University and Departmental Service . . . . .	9
Teaching . . . . .	10
External Funding . . . . .	11
Chronological List of Research Papers . . . . .	11
Theses, Surveys, and Books . . . . .	18
Other Work from Research Group . . . . .	18
Invited Talks at Workshops and Conferences . . . . .	21
Departmental Seminars and Colloquia . . . . .	23

## Biographical

School of Engineering and Applied Sciences  
Harvard University  
33 Oxford Street, Room 337  
Cambridge, MA 02138  
salil@seas.harvard.edu  
<http://www.seas.harvard.edu/~salil>

Office: (617) 496-0439  
Fax: (617) 496-6404  
Citizenship: United States  
Spouse: Jennifer Sun (married 7/99)  
Children: Kaya Tsai-Feng Vadhan (5/03)  
Amari Tsai-Ming Vadhan (6/05)

## Research Interests

- Computational Complexity, Cryptography, and Randomness in Computation

## Current Positions

HARVARD UNIVERSITY Cambridge, MA

- Vicky Joseph Professor of Computer Science and Applied Mathematics (with tenure), July 2009–present.
- Director, Harvard Center for Research on Computation and Society (CRCS), August 2008–present.

## Previous Positions

MICROSOFT RESEARCH Mountain View, CA

- Consultant, June 2008–July 2008.

UNIVERSITY OF CALIFORNIA Berkeley, CA

- Miller Visiting Professor, September 2007–June 2008.

HARVARD UNIVERSITY Cambridge, MA

- 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

- *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).
- *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:
  - “Are PCPs Inherent in Efficient Arguments?” (with Guy Rothblum), invited to *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), invited to *SIAM Journal on Computing* Special Issue on FOCS ‘06.
  - “The Round Complexity of Random Selection” (with Saurabh Sanghvi), to appear 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,” to appear 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), to appear 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

- Local Arrangements Chair, 25th IEEE Conference on Computational Complexity, Cambridge, MA, May 2010.
- 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–present.
- SIGACT Committee for the Advancement of Theoretical Computer Science, 2007–present.
- 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–present.
- 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, STOC ‘07, CRYPTO ‘09.
- Grant reviewing: NSF Theory of Computing Program (panelist), NSF Cybertrust Program (panelist), Israel Science Foundation, US-Israel Binational Science Foundation.
- Extensive journal and conference refereeing.

## Graduate Research Advising

EMANUELE VIOLA

Sept. '01–Aug. '06

- Ph.D. dissertation: *The Complexity of Hardness Amplification and Derandomization*.
- Winner of 2006 SIAM Student Paper Award for paper “Pseudorandom Bits for Constant-Depth Circuits with Few Arbitrary Symmetric Gates” (CCC '05, SICOMP '06).
- Current position: Assistant Professor, College of Computer and Information Science, Northeastern University, Boston, MA.

MINH-HUYEN NGUYEN

June '01–June '06

- Ph.D. dissertation: *Zero Knowledge with Efficient Provers*.
- DEAS Teaching Fellow Award, Fall '01.
- Certificate of Distinction in Teaching, Spring '04, Fall '01.
- Current position: Actuarial Assistant, Liberty Mutual Group

ZHENMING LIU

September '05–January '07

- S.M. Research on Random Selection Protocols.

SHIEN JIN ONG

June '04–June '07

- Ph.D. dissertation: *Unconditional Relationships within Zero Knowledge*.
- Current position: Research Associate, Goldman Sachs.

GUY ROTHBLUM

June '06–May '09

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

STEPHAN HOLZER

Sept. '08–May '09

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

CURRENT STUDENTS

- Kai-Min Chung (5th year Ph.D.)
- Colin Jia Zheng (2nd year Ph.D.)
- Jon Ullman (1st year Ph.D.)

## Undergraduate Research Advising

DAVID XIAO '03

Spring '02–Spring '03

- A.B. thesis *The Evolution of Expander Graphs* awarded Thomas Temple Hoopes Prize for outstanding undergraduate work and received highest honors in computer science.
- Currently a Ph.D. student in computer science at Princeton 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.

SAURABH SANGHVI '04

Summer '03–June '04

- Supported in part by the Harvard College Research Program.
- A.B. thesis *A Study of Two-Party Random Selection Protocols* awarded Thomas Temple Hoopes Prize for outstanding undergraduate work, and received highest honors in computer science.
- Work led to paper “The round complexity of two-party random selection” in *37th ACM Symposium on Theory of Computing (STOC '05)*, also accepted to *SIAM Journal on Computing* Special Issue on STOC '05.

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* received highest honors in mathematics.
- Work led to paper “The computational complexity of Nash equilibria in concisely represented games” in *7th ACM Conference on Electronic Commerce (EC '06)*.
- Currently a Ph.D. student in computer science at U.C. Berkeley.

DRAGOS FLORIN CIOCAN '07

Sept. '06–present

- A.B. thesis *Constructions and Characterizations of Non-interactive Zero-Knowledge* awarded Thomas Temple Hoopes Prize for outstanding undergraduate work, and received highest honors in computer science.
- 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)*.

YAKIR RESHEF '09

Sept. '09–present

- A.B. thesis *Resilient and Exposure-Resilient Functions* received high honors in mathematics.

ELEANOR BIRRELL '09

August '08–present

- A.B. thesis *Composition of Zero-Knowledge Proofs* received high honors in computer science.
- Work led to paper “Composition of Zero-Knowledge Proofs with Efficient Provers,” to appear in the *7th IACR Theory of Cryptography Conference (TCC ‘10)*.

#### OTHER STUDENTS

- Supervising research of Olga Zverovich ‘10 on boolean satisfiability problems, Summer ‘09.
- Supervising research of Zachary Abel ‘10 on lattice-based cryptography, Summer ‘09.
- Co-advised 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

ELI BEN-SASSON Sept. ‘01–Aug. ‘03

- Co-hosted with Madhu Sudan (MIT).
- Member of 2003–04 Radcliffe Cluster on Randomness and Computation.
- Current position: Senior Lecturer in Computer Science, The Technion, Israel.

DAN GUTFREUND Sept. ‘05–Aug. ‘07

- Supported in part by a DEAS Applied Math Lectureship.
- Current position: Lecturer in Mathematics, MIT.

ALON ROSEN Sept. ‘05–July ‘07

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

- Current position: Faculty Member, School of Computer Science, Herzliya Interdisciplinary Center, Israel.

TAL MORAN

Sept. '08–present

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

## Visitors Hosted

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), Ronitt Rubinfeld (NEC and MIT), Madhu Sudan (MIT), plus several additional affiliates and visitors.
- Supported by fellowships from the Radcliffe Institute for Advanced Study.

DAVID ZUCKERMAN (UT AUSTIN)

2004–05, Summer '06

- Supported in '04–'05 by a fellowship from the Radcliffe Institute for Advanced Study.

OMER REINGOLD (WEIZMANN INSTITUTE)

Aug. '05–Nov. '05

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

## University and Departmental Service

- 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–present.
- 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

AM 106/206: APPLIED ALGEBRA Fall '09

- Combined undergraduate/graduate course.
- Enrollments (106/206): 27/12.

CS 120: INTRODUCTION TO CRYPTOGRAPHY Fall '01, Spring '03, Fall '06

- New undergraduate course.
- Enrollments: 12, 21, 7
- CUE overall course ratings (5.0 scale): 4.9, 4.5, 4.7
- CUE overall instructor ratings (5.0 scale): 5.0, 4.8, 5.0
- In Fall '06, also offered as Extension course CSCI E-177 (enrollment 5).

CS 121: INTRODUCTION TO FORMAL SYSTEMS AND COMPUTATION Fall '04, Fall '05, Fall '08

- Required theory course for all undergraduate computer science concentrators.
- Enrollments: 57, 45, 80
- CUE overall course ratings (5.0 scale): 4.3, 4.3, 3.8
- CUE overall instructor ratings (5.0 scale): 4.6, 4.5, 4.1
- Also offered as Extension course CSCI E-207 (enrollments 21,20)

CS 225: PSEUDORANDOMNESS Spring '02, Spring '04, Spring '07, Spring '09

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

CS 221: COMPUTATIONAL COMPLEXITY Fall '02, Spring '06

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

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 at IAS/Park City Mathematics Institute (PCMI) Summer School on Computational Complexity Theory, Summer 2000.
- Invited tutorial “Randomness Extractors and their Many Guises” given at FOCS 2002.
- Invited tutorial “Randomness Extractors and their Cryptographic Applications” given at TCC 2008.

## External Funding

- NSF Early Career Development Award. “A Unified Theory of Pseudorandomness.” \$350,000 plus \$6,000 REU Supplement, 6/02–5/07.
- Alfred P. Sloan Research Fellowship. \$40,000, 9/02–9/04.
- 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.
- 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.
- 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.
- Radcliffe Institute Research Fellowship, \$20,000, 10/03.
- NSF Cybertrust grant, “New Complexity-Theoretic Techniques in Cryptography,” \$399,999, 9/04–8/08.
- ONR Young Investigator Award, “Pseudorandomness and Applications,” \$300,000, 6/04–8/07.
- Guggenheim Fellowship, 8/07–7/08, \$30,000.
- NSF Cybertrust grant, “The Assumptions for Cryptography,” \$400,000, 9/08–8/11.

## Chronological List of Research Papers

All of the conference proceedings (and journals) listed below are refereed.

- [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. In J. Kilian, editor, *Advances in Cryptology—CRYPTO '01*, volume 2139 of *Lecture Notes in Computer Science*, pages 1–18. Springer-Verlag, 19–23 August 2001.
- [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*.
- [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. In *Proceedings of the 7th ACM Conference on Electronic Commerce (EC '06)*, pages 270–279, 11–15 June 2006. Preliminary version as *ECCC* TR05-52, May 2005.
- [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. In *Proceedings of the 8th International Workshop on Randomization and Computation (RANDOM '05)*, number 3624 in Lecture Notes in Computer Science, pages 318–329, Berkeley, CA, August 2005. Springer.
- [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. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing (STOC '06)*, pages 691–700, 21–23 May 2006.
- [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.
- [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. In *Proceedings of the 22nd Annual IEEE Conference on Computational Complexity (CCC '07)*, pages 236–249, 12–16 June 2007. Full version posted as *ECCC TR07-030*, to appear in *ACM Transactions on Algorithms*.
- [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] Michael Mitzenmacher and Salil Vadhan. Why simple hash functions work: Exploiting the entropy in a data stream. In *Proceedings of the 19th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA '08)*, pages 746–755, 20–22 January 2008.
- [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*.
- [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] Kai-Min Chung and Salil Vadhan. Tight bounds for hashing block sources. In *Proceedings of the 12th International Workshop on Randomization and Computation (RANDOM '08)*, *Lecture Notes in Computer Science*, pages 357–370. Springer-Verlag, 25–27 August 2008. Full version posted as [arXiv:0806.1948v1](https://arxiv.org/abs/0806.1948v1).
- [59] 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.
- [60] 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.
- [61] 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.
- [62] 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.
- [63] 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.
- [64] 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*.
- [65] Guy Rothblum and Salil Vadhan. Are PCPs inherent in efficient arguments? In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity (CCC '09)*, pages 81–92, 15–18 July 2009.
- [66] 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.
- [67] 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.
- [68] 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)*, Lecture Notes on Computer Science. Springer-Verlag, 9–11 February 2010. To appear.
- [69] Iftach Haitner, Omer Reingold, Salil Vadhan, and Hoeteck Wee. Universal one-way hash functions via inaccessible entropy. Unpublished manuscript, October 2009.
- [70] Iftach Haitner, Omer Reingold, and Salil Vadhan. A more efficient construction of pseudorandom generators from one-way functions. Unpublished manuscript, November 2009.

- [71] Cynthia Dwork, Guy Rothblum, and Salil Vadhan. Boosting and differential privacy. Unpublished manuscript, November 2009.

## Theses, Surveys, and Books

- [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 Vadhan. The unified theory of pseudorandomness. *SIGACT News*, 38(3), September 2007.
- [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.

## 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 & Security*, 2009. To appear.
- [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. To appear.
- [33] Kai-Min Chung, Feng-Hao Liu, Chi-Jen Lu, and Bo-Yin Yang. Efficient string-commitment from weak bit-commitment and full-spectrum theorem for puzzles. Unpublished manuscript, 2009.
- [34] Kai-Min Chung, Zhenming Liu, and Michael Mitzenmacher. Testing  $k$ -wise independence over streaming data. In submission, 2009.
- [35] Tyler Moore and Tal Moran. The phish market protocol: Securely sharing attack data between competitors, 2009. In submission.

## 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.

## 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*, Rehovot, 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.