# Madhu Sudan

**Principal Researcher, Microsoft Research**

Microsoft Research
One Memorial Drive
Cambridge, MA 02142, USA
Tel: +1.857.453.6048
email: madhu@microsoft.com
http://research.microsoft.com/~madhu


Last updated: November 22, 2014

## Areas of Special Interests

Theory of Computer Science, Algorithms, Computational Complexity, Reliable Communication, Optimization.

## Ph.D. Title

*Efficient Checking of Polynomials and Proofs and the Hardness of Approximations.*
Supervisor: Umesh Vazirani

## Educational Background

| | |
|---|---|
| Ph.D. | Computer Science; University of California at Berkeley, 1992 |
| B.Tech. | Computer Science; Indian Institute of Technology at New Delhi, 1987 |

## Work Experience

| | |
|---|---|
| 1990 Summer | Student Researcher at IBM Almaden Research Center |
| 1992-1997 | Research Staff Member, IBM Thomas J. Watson Research Center<br>Mathematical Sciences Department |
| Sept. 1997 - Dec. 2002 | Associate Professor, Massachussetts Institute of Technology<br>Department of Electrical Engineering and Computer Science |
| Jan. 2003 - Jan. 2005 | Professor, MIT EECS. |
| Feb. 2005 - June 2011 | Fujitsu Chair Professor, MIT EECS (on leave since June 2009) |
| July 2005 - June 2011 | Danny Lewin Outstanding Professor, MIT EECS (on leave since June 2009) |
| July 2007 - June 2009 | Associate Director, MIT CSAIL |
| June 2009 - present | Principal Researcher, Microsoft Research |
| December 2011 - present | Adjunct Professor, MIT EECS |

## Awards

| | |
|---|---|
| Sakrison Memorial Award (Ph.D. Thesis, EECS, Berkeley) | 1993 |
| ACM Doctoral Dissertation Award | 1993 |
| Sloan Foundation Fellowship | 1998 |
| NSF Career Award | 1999 |
| Information Theory Paper Award | 2000 |
| Gödel Prize | 2001 |
| Nevanlinna Prize | 2002 |
| Felicitation, Indian Assoc. Computing Research | 2002 |
| Distinguished Alumnus Award, University of California at Berkeley, | 2003 |

| | |
|---|---|
| CS Division | |
| Radcliffe Fellowship | 2003-2004 |
| Distinguished Alumnus Award, Indian Institute of Technology at New Delhi | 2004 |
| Guggenheim Fellowship | 2005-2006 |
| ACM Fellow | 2009 |
| IEEE Fellow | 2010 |
| American Academy of Arts and Sciences Member | 2010 |
| AMS Fellow | 2013 |

## Patents:

| | |
|---|---|
| A scheme for order invariant fuzzy commitment, Ari Juels & Madhu Sudan | US Patent 7,602,904, October 13, 2009 |

## Current Organization Membership

Association of Computing Machinery

Society of Industrial and Applied Mathematics

IEEE

American Mathematical Society

## Professional Service:

| Activity | Beginning | Ending |
|---|---|---|
| **Journal activities** | | |
| **(Founding) Editor-in-chief**, Foundations and Trends in Theoretical Computer Science | June 2004 | present |
| **Editor-in-chief**, SIAM Journal on Computing | 2010 | December 2012 |
| Associate Editor, SIAM Journal on Discrete Mathematics | 1997 | 2002 |
| Associate Editor, SIAM Journal on Computing | 2000 | 2009 |
| Associate Editor, Information and Computation | 2000 | 2006 |
| Guest Editor, Journal of Computer and System Sciences, Special issue devoted to papers from *Complexity '2001* | May 2001 | May 2002 |
| Editor, Journal of the ACM | 2003 | 2008 |
| Guest Co-Editor, SIAM Journal on Computing, Special Issue on *Randomness and Complexity* | May 2004 | May 2006 |
| Associate Editor, IEEE Transactions on Information Theory | 2005 | 2006 |
| Associate Editor, Theory of Computing | 2009 | present |

## Conference Program Committee Activities

| | | |
|---|---|---|
| **Chair**, Program Committee, *Complexity 2001*, IEEE Conference on Computational Complexity | 2001 | 2001 |
| **Chair**, Program Committee, *FOCS 2003*, IEEE Symposium on Foundations of Computer Science | November 2002 | November 2003 |
| Member, Program Committee, *STOC '95*, ACM Symposium on Theory of Computing | May 1995 | |
| Member, Program Committee, *FOCS '97*, IEEE Symposium on Foundations of Computer Science | October 1997 | |
| Member, Program Committee, *SODA '98*, ACM-SIAM Symposium on Discrete Algorithms | January 1998 | |
| Member, Program Committee, *RANDOM '98*, Workshop on Randomization and Approximation | October 1998 | |
| Member, Program Committee, *COCOON '99*, International Computing and Combinatorics Conference | July 1999 | |
| Member, Program Committee, *FCT '99*, Int'l Symposium on Fundamentals of Computing Theory | September 1999 | |
| Member, Program Committee, *FOCS '2001*, IEEE Symposium on Foundations of Computer Science | October 2001 | |
| Member, Program Committee, *FSTTCS '2001*, Foundations of Software Technology and Theoretical CS | December 2001 | |
| Member, Program Committee, *STOC '2006*, ACM Symposium on Theory of Computing | May 2006 | |
| Member, Program Committee, *ISIT '2006*, International Symposium on Information Theory | July 2006 | |
| Member, Program Committee, *CCC '2006*, IEEE Conference on Computational Complexity | July 2006 | |
| Member, Program Committee, *RANDOM '2006*, 10th Annual Workshop on Randomization and Computation | August 2006 | |
| Member, Program Committee, *EuroComb '2007*, European Conf. Combinatorics, Graph theory, Applications | March 2007 | |
| Member, Program Committee, *FOCS '2008*, IEEE Symposium on Foundations of Computer Science | April 2008 | |
| Member, Program Committee, *ITCS '2012*, ACM Innovations in Theoretical Computer Science | January 2012 | |
| Member, Program Committee, *CCC '2013*, IEEE Conference on Computational Complexity | July 2013 | |
| Member, Program Committee, *FOCS '2013*, IEEE Symposium on Foundations of Computer Science | October 2013 | |

## Steering Committees

| | | |
|---|---|---|
| Member of Scientific Board, Electronic Colloquium on Computational Complexity | 1994 | present |
| Conference Committee Member, IEEE Conference on Computational Complexity | 1999 | 2002 |
| Scientific Advisory Committee, Claude Shannon Institute, UC Dublin, Ireland | 2005 | 2012 |
| Scientific Advisory Board, Mathemicshe Forschungsinstitut, Oberwolfach, Germany | 2007 | present |

| | | |
|---|---|---|
| Steering Committee Member, ACM Innovations in Theoretical Computer Science (ITCS) | 2009 | present |
| Steering Committee Member, IEEE Conference on Computational Complexity | 2012 | present |

## Other activities

| | | |
|---|---|---|
| Chair, Session on Approximation Algorithms 16th Mathematical Programming Symposium | June 1994 | |
| Co-organizer, Dagstuhl Workshop on Combinatorial Optimization Problems | January 2000 | |
| Co-organizer, IAS Workshop on Asymptotic and Computational Aspects of Coding Theory | March 2001 | |
| Member, Committee on Fundamentals of Computer Science, Computer Science and Telecommunications Board, National Academies of Sciences | January 2001 | December 2002 |
| Panelist, NSF Workshop on the interface between Information Theory and Computer Science | 2003 | 2003 |
| Co-organizer, IMA special thematic year (2006-2007) on Algebraic Geometry and its Applications | March 2003 | June 2007 |
| Co-organizer, Oberwolfach meeting on Complexity Theory | May 2003 | May 2003 |
| Co-organizer, Radcliffe Symposium on Privacy and Security: Technology, Policy and Society | September 2003 | March 2004 |
| Co-organizer, Banff International Research Station Workshop on Advances in Complexity Theory | April 2004 | July 2004 |
| Co-moderator, ACM Computing Research Repository (CoRR), Information Theory Section | April 2004 | present |
| Member, Springer LNCS Series Editorial Board. | April 2004 | December 2012 |
| Co-organizer, Oberwolfach meeting on Complexity Theory | June 2005 | June 2005 |
| Member, SIGACT Committee on TCS Funding | June 2005 | June 2007 |
| Co-organizer, Banff International Research Station Workshop on Advances in Complexity Theory | May 2006 | August 2006 |
| Co-organizer, IMA Workshop on Complexity, Coding, and Communications | June 2006 | April 2007 |
| Member, Morningside Medal of Mathematics Award Committee, | May 2007 | June 2007 |
| Co-organizer, Oberwolfach meeting on Complexity Theory | June 2007 | June 2007 |
| Organizer, Session on list-decoding at AAECC'07 | December 2007 | December 2007 |
| Co-organizer, Oberwolfach meeting on Complexity Theory | November 2009 | November 2009 |
| Member, 2010 Nevanlinna Prize Committee | April 2008 | June 2010 |
| Chair, Editor-in-Chief Selection Committee, ACM Transactions on Algorithms | July 2010 | October 2010 |
| Co-organizer, Oberwolfach meeting on Complexity Theory | November 2012 | November 2012 |

## Principal Lectures and Addresses

- Courses, mini-courses, lecture series
  - Six lecture mini-course on *Property Testing*, Warsaw University, Warsaw, October 2007.
  - One week course on *Coding Theory in Modern Computational Complexity*, Barbados, March 2006.
  - Four week course on *Probabilistic Checking of Proofs* at the Scuola Normale Superiore, organized by the Scuola Matematica Interuniversitaria, Cortona, Italy, July 2005.

- Mini-course on *Coding Theory* at the Estonian Winter School in Computer Science, Palmse, Estonia, March 2004.
- Mini-course on *Coding Theory* at the IBM Almaden Research Center, November 2000.
- Mini-course on *Probabilistic Checking of Proofs*, Part of Graduate Summer School on Computational Complexity organized by the Park City Mathematical Institute at the Institute for Advanced Study, Princeton, New Jersey, July-August, 2000.
- Mini-course on *Coding Theory* at the IBM Thomas J. Watson Research Center, January 2000.
- Lecture series on *Probabilistic verification of proofs* at the Fields Institute, Toronto, April 1998.
- Lecture series at the school on *Approximate Solutions to Hard Combinatorial Optimization Problems* at the CISM, Udine, Italy, September 1996.
- Lecture series on *Approximability of Optimization Problems* at the IBM Tokyo Research Laboratory, March 1996.
- Lecture series on *Hardness of Approximation Problems* at the IBM Almaden Research Center, October 1995.
- Mini-course on *Hardness of Approximation Problems* at the University of Toronto, February 1993.

• Invited seminars

- Workshop in honor of Tom Høholdt's 60th Birthday, Lyngby, Denmark, June 2005.
- Plenary speaker, *Information Theory Workshop*, San Antonio, Texas, October, 2004.
- Oberwolfach Meetings on *Coding Theory*, Germany, May 2000, and December 2003.
- Plenary speaker, Winter meeting of the Canadian Mathematical Society, December 6, 2003.
- Plenary speaker, Annual meeting of the German Mathematical Society, September 30, 2003.
- New York Theory Day, May 2003.
- Nevanlinna Prize Lecture, International Congress of Mathematicians, Beijing, 3 August 2002.
- Workshop on Information Theory in honor of Philippe Delsarte's 60th Birthday at Universite Catholique du Louvain, Belgium, 31 May 2002.
- Erdös Memorial Lecture Series, Hebrew University, Jerusalem, 14-20 March 2002.
- Invited speaker at Applied Algebra, Algebraic Algorithms, and Error-correcting codes (AAECC'01), Melbourne, 26-30 November, 2001.
- Invited Tutorial on *Coding theory* at IEEE Symposium on Foundations of Computer Science, Las Vegas, 14-17 October, 2001.
- Oberwolfach Meetings on *Complexity Theory*, Germany, 1994, 1996, and 2000.
- Invited speaker, Symposium on Discrete Mathematics 2000, Technische Universität, München, 5-6 October 2000.
- Keynote plenary invited speaker at the International Conference IFIP TCS 2000, Sendai, Japan, August 2000.
- Invited speaker, DIMACS Workshop on Computing Approximate Solutions to NP-hard Problems, Princeton, New Jersey, February 20-22, 2000.
- Invited speaker, RANDOM '99, Third International Workshop on Randomization and Approximation Techniques in Computer Science, Berkeley, California, August 1999.
- International Congress of Mathematicians, Berlin, August 1998.
- Foundations of Software Technology and Theoretical Computer Science, Kharagpur, December 1997.
- Workshop in honor of Michael Rabin's 65th Birthday, Jerusalem, June 1997.
- Israeli Theory Seminar, Tel Aviv, April 1994 and January 1997.

– Seminar on Complexity in honor of Shmuel Winograd's 60th Birthday at IBM Yorktown Heights, May 1996.

– *20th Theory Day*, Columbia University, 1992.

– *Bay Area Theory Seminar*, Berkeley, 1990.

# Courses taught

**Summary**

| Term | Subject | Title | Role |
|---|---|---|---|
| ST93 | *Columbia U.* | Hardness of Approximations | Lectures |
| FT97 | 6.046 | Analysis of Algorithms | Recitations + Lectures (w. S. Goldwasser) |
| FT97 | | Complexity seminar | Seminar (w. S. Goldwasser) |
| ST98 | 6.001 | Structure and Interpretation of Computer Programs | Recitations |
| ST98 | | Complexity seminar | Seminar |
| FT98 | 6.966 | Algebra and Computation | Lectures + Development |
| ST99 | | Complexity seminar | Seminar |
| FT99 | 6.893 | Approximability of Optimization Problems | Lectures + Development |
| ST00 | 6.045 | Automata, Computability, and Intractability | Lectures |
| FT00 | 6.046 | Introduction to Algorithms | Lectures (w. S. Teller) |
| FT00 | 6.897 | Complexity Seminar | Seminar |
| ST01 | 6.046 | Introduction to Algorithms | Lectures (w. P. Indyk) |
| FT01 | 6.897 | Algorithmic Coding Theory | Lectures + Development |
| ST02 | 6.841 | Advanced Complexity Theory | Lectures |
| FT02 | 6.896 | Essential Coding Theory | Lectures + Development |
| ST03 | 6.841 | Advanced Complexity Theory | Lectures |
| FT04 | 6.895 | Essential Coding Theory | Lectures |
| ST05 | 6.841 | Advanced Complexity Theory | Lectures |
| FT05 | 6.885 | Algebra and Computation | Lectures |
| ST06 | 6.441 | Transmission of Information | Lectures |
| FT06 | 6.885 | Introduction to Algorithms | Lectures (w. E. Demaine) |
| ST07 | 6.841 | Advanced Complexity Theory | Lectures |
| ST07 | 6.899 | Advanced Seminar in Complexity and Cryptography | Seminar |
| FT07 | 6.046 | Introduction to Algorithms | Lectures (with R. Rubinfeld) |
| FT07 | 6.899 | Reading seminar in Algorithms, Complexity and Cryptography | Seminar |
| ST08 | 6.440 | Essential Coding Theory | Lectures |
| ST09 | 6.841 | Advanced Complexity Theory | Lectures |
| ST12 | 6.S897 | Algebra and Computation | Lectures |
| ST13 | 6.440 | Essential Coding Theory | Lectures |

## Theses Supervised by Madhu Sudan

Engineer's Theses

- Hon, Kenneth, S., "Design of Prototype Real-Time Broadcast System over the Internet," January 1998.
- Feng, Yuan, "Analysis and Implementation of Generic MPEG Header and Transport Decoders," May 1999.
- Krevat, Elie, "Scheduling Algorithms to improve utilization in Toroidal Interconnected Systems", May 2003.
- Preda, Daniel, "Quantum Communication Complexity Revisited", May 2003.

Master's Theses

- Dodis, Yevgeniy, "Space-Time Tradeoffs for Graph Properties," May 1998.
- Sherman, Alexander, "Distributed Web Caching System with Consistent Hashing," February 1999.
- Guruswami, Venkatesan, "Query-Efficient Checking of Proofs and Improved PCP Characterizations of NP," May 1999.
- Harsha, Prahladh, "Small PCPs with low query complexity," May 2000.
- Shelat, Abhi, "Evaluating Grammar-Based Data Compression Algorithm", August 2001.
- Smith, Adam, "Multi-party Quantum Computation", August 2001.
- Grigorescu, Elena, "Local decoding and testing of Homomorphisms", August 2006.
- Kopparty, Swastik, "The list-decoding radius for Reed-Solomon codes," August 2006.
- Saraf, Shubhangi, "Kakeya sets and the Method of Multiplicities", June 2009.
- Guo, Alan, "Some closure features of locally testable affine-invariant properties", February 2013.

Doctoral Theses, Reader

- Khanna, Sanjeev, "A Structural View of Approximation," Stanford University, August 1996.
- Alimonti, Paola, "Local Search and approximability of MAX SNP problems," University of Rome, September 1997.
- Micciancio, Daniele, "On the Hardness of the Shortest Vector Problem," MIT, September 1998.
- Sahai, Amit, "Frontiers in Zero Knowledge", MIT, September 2000.
- Ramzan, Zulfikar, "A Study of Luby-Rackoff Ciphers", MIT, January 2001.
- Reyzin, Leonid, "Zero-knowledge without public keys", MIT, May 2001.
- Nielsen, Rasmus Refslund, "List-decoding of Linear Block Codes", Denmark Technical University, Lyngby, Denmark, November 2001.
- Forster, Jürgen, "Some Results Concerning Arrangements of Half Spaces and Relative Loss Bounds", Universitat Bochum, February 2002.
- Lysyanskaya, Anna, "Signature Schemes and Applications to Cryptographic Protocol Design," May 2002.

- Raskhodnikova, Sofya, "Property Testing: Theory and Applications," May 2003.
- Feldman, Jonathan, "Decoding Error-Correcting Codes via Linear Programming," May 2003.
- Bazzi, Louay, "Error Correcting Codes Minimum Distance versus: Encoding Complexity, Symmetry, and Pseudo-randomness", August 2003.
- Chan, Albert, "A Framework for Low-Complexity Iterative Interference Cancellation in Communication Systems," June 2004.
- Newman, Alantha, "Algorithms for String and Graph Layout," August 2004.
- Immorlica, Nicole, "Computing with Strategic Inputs," June 2005.
- Kleinberg, Robert David, "Online Decision Problems with Large Strategy Sets," June 2005.
- shelat, abhi, "Etudes in Zero-Knowledge", December 2005.
- Bădoiu, Mihai, "Algorithmic Embeddings", May 2006.
- Pass, Rafael, "A Precise Computational Approach to Knowledge", May 2006.
- Rademacher, Luis, "Dispersion of Mass and the Complexity of Geometric Problems," MIT, May 2007.
- Woodruff, David P., "Efficient and Private Distance Approximation in the Communication and Streaming Models," MIT, Summer 2007.
- Akavia, Adi, "Learning Noisy Characters, Multiplication Codes, and Cryptographic Hardcore Predicates," MIT, August 2007.
- Harvey, Nicholas James Alexander, "Matchings, Matroids, and Submodular Functions," MIT, May 2008.
- Valiant, Paul, "Testing Symmetric Properties of Distributions," MIT, June 2008.
- Nolte, Tina Ann, "Virtual Stationary Timed Automata for Mobile Networks," MIT, October 2008.
- Vaikuntanathan, Vinod, "Randomized Algorithms for Byzantine Agreement," MIT, October 2008.
- Mukhopadhyay, Partha, "Polynomial Identity Testing and Related Problems", Institute of Mathematical Sciences, Chennai, India, May 2009.
- Nelson, Jelani, "Sketching and Streaming High-Dimensional Vectors", MIT, May 2011.
- Moitra, Ankur, "Vertex Sparsification and Universal Rounding Algorithms", MIT, May 2011.
- Bhattacharyya, Arnab, "Testability of Linear-Invariant Properties," MIT, July 2011.
- Maymounkov, Petar, "Dynamics of Spectral Algorithms for Distributed Routing", MIT, February 2012.
- Xie, Ning, "Testing k-wise Independent Distributions," MIT, July 2012.
- Haeupler, Bernhard , "Probabilistic Methods for Distributed Information Dissemination", MIT June 2013.

Ph.D. Supervision (Completed)

- Dodis, Yevgeniy, "Exposure-Resilient Cryptography," MIT, August 2000. (Currently Professor at NYU.)
- Guruswami, Venkatesan, "List-decoding of Error-Correcting Codes" MIT, August 2001. (Currently Professor at CMU.)

- Lehman, Eric, "Approximation Algorithms for Grammar-based Data Compression", MIT, January 2002. (Currently at Google.)
- O'Donnell, Ryan William, "Computational Applications of Noise Sensitivity", MIT, June 2003. (Currently an Associate Professor at CMU.)
- Alekhnovitch, Mikhail, "Propositional Proof Systems: Efficiency and Automatizability", MIT, June 2003. (Died in a tragic accident, August 5, 2006)
- Smith, Adam Davison, "Maintaining Secrecy when Information Leakage is Unavoidable", MIT, June 2004. (Currently an Associate Professor at Penn. State U.)
- Harsha, Prahladh, "Robust PCPs of Proximity and Shorter PCPs", MIT, August 2004. (Currently an Assistant Professor at Tata Institute of Fundamental Research, Mumbai, India).
- Lehman, April Rasala, "Network Coding", MIT, January 2005. (Currently at Google.)
- Kelner, Jonathan A., "New Geometric Techniques for Linear Programming and Graph Partitioning", (I was co-supervisor on this thesis for formal reasons only; real supervisor was Dan Spielman at Yale University), MIT, September 2006. (Currently at Associate Professor at MIT.)
- Yekhanin, Sergey, "Locally Decodable Codes and Private Information Retrieval Schemes", MIT, July 2007. (Currently at Microsoft.)
- Chen, Victor, "The Gowers Norm in the testing of Boolean Functions", MIT, May 2009. (Currently at Google.)
- Grigorescu, Elena, "Symmetries in Algebraic Property Testing", MIT, August 2010. (Currently an Assistant Professor at Purdue.)
- Juba, Brendan, "Universal Semantic Communication", MIT, August 2010. (Currently an Assistant Professor at Washington University in St. Louis.)
- Kopparty, Swastik, "Algebraic Methods in Randomness and Pseudorandomness", MIT, August 2010. (Currently an Assistant Professor at Rutgers University.)
- Rossman, Benjamin, "Average-Case Complexity of Detecting Cliques", MIT, August 2010. (Currently an Assistant Professor at the National Institute of Informatics, Tokyo.)
- Saraf, Shubhangi, "The Method of Multiplicities", MIT, June 2010. (Currently an Assistant Professor at Rutgers University.)

Ph.D. Supervision (Current)

- Bavarian, Mohammad (expected 2017)
- Guo, Alan (expected 2017)
- Ghazi, Badih (expected 2018)

Post-Doctoral Supervision

- Trevisan, Luca: September 1997 - August 1998.
- Vadhan, Salil: September 1999 - August 2000.
- Engebretsen, Lars: September 2000 - August 2001.
- Ben-Sasson, Eli: September 2001 - August 2003.

- Shpilka, Amir: August 2002 - July 2003.
- Chuzhoy, Julia: August 2004 - July 2006.
- Kaufman, Tali: August 2007 - July 2009.
- Nordström, Jakob: August 2008 - July 2010.
- Juba, Brendan: August 2010 - June 2011.

# Publications

1. Books and Book Chapters.

    1. Madhu Sudan. **Efficient Checking of Polynomials and Proofs and the Hardness of Approximation Problems**. ACM Distinguished Theses. Lecture Notes in Computer Science, no. 1001, Springer, 1996.
    2. Nadia Creignou, Sanjeev Khanna, and Madhu Sudan. **Complexity Classifications of Boolean Constraint Satisfaction Problems**. SIAM Press, Philadeplhia, PA, USA, March 2001.
    3. Madhu Sudan. Chapter on "Cryptography" in **Computer Science: Reflections on the Field, Reflections from the Field**, Mary Shaw (Chair), pages 144–150, The National Academies Press, Washington D.C., 2004.
    4. Madhu Sudan. Chapter on "Probabilistically checkable proofs", in **Computational Complexity Theory**, Steven Rudich and Avi Wigderson (Eds.), pages 349–389, IAS/Park City Mathematics Series, volume 10, American Mathematical Society, 2004.
    5. Madhu Sudan. Chapter on "Reliable Transmission of Information", in **Princeton Companion to Mathematics**, Tim Gowers (Ed.), Chapter VII.6, pages 878–887, Princeton University Press, 2008.
    6. Madhu Sudan, Chapter on "Il problema P = NP" in **La matematica, vol. 4**, Pensare il mondo, edited by Claudio Bartocci and Piergiorgio Odifreddi, pages 161–179, Einaudi, Torino, 2010.

2. Papers in refereed journals.

    1. Peter Gemmell and Madhu Sudan, "Highly resilient correctors for multivariate polynomials," Information Processing Letters, 43(4): 169–174, September 1992.
    2. Marshall Bern, Daniel H. Greene, Arvind Raghunathan, and Madhu Sudan, "Online algorithms for locating checkpoints," Algorithmica, 11(1): 33–52, January 1994.
    3. Rajeev Motwani and Madhu Sudan, "Computing roots of graphs is hard," Discrete Applied Mathematics, 54(1):81–88, September 1994.
    4. Ronitt Rubinfeld and Madhu Sudan, "Robust characterizations of polynomials with applications to program testing," SIAM Journal on Computing, 25(2):252–271, April 1996.
    5. Alok Aggarwal, Amotz Bar-Noy, Don Coppersmith, Rajeev Ramaswami, Baruch Schieber, and Madhu Sudan, "Efficient routing algorithms in optical networks," Journal of the ACM, 43(6):973–1001, November 1996.
    6. Andres Albanese, Johannes Blömer, Jeff Edmonds, Michael Luby, and Madhu Sudan, "Priority encoding transmission," IEEE Transactions on Information Theory, Special Issue on Codes and Complexity, 42(6): 1737–1744, November 1996.
    7. Mihir Bellare, Don Coppersmith, Johan Håstad, Marcos Kiwi, and Madhu Sudan, "Linearity testing over characteristic two," IEEE Transactions on Information Theory, Special Issue on Codes and Complexity, 42(6): 1781–1795, November 1996.
    8. Madhu Sudan, "Decoding of Reed Solomon codes beyond the error-correction bound," Journal of Complexity, special issue dedicated to Shmuel Winograd, 13(1): 180–193, March 1997.
    9. Guy Even, Joseph (Seffi) Naor, Baruch Schieber, and Madhu Sudan, "Approximating minimum feedback sets and multicuts in directed graphs," Algorithmica, 20(2): 151–174, February 1998.
    10. David Karger, Rajeev Motwani, and Madhu Sudan, "Approximate graph coloring by semidefinite programming," Journal of the ACM, 45(2): 246–265, March 1998.
    11. Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy, "Proof verification and the hardness of approximation problems," Journal of the ACM, 45(3): 501–555, May 1998.

12. Mihir Bellare, Oded Goldreich, and Madhu Sudan, "Free bits, PCP and non-approximability — towards tight results," SIAM Journal on Computing, 27(3): 804–915, June 1998.
13. Amotz Bar-Noy, Alain Mayer, Baruch Schieber, and Madhu Sudan, "Guaranteeing fair service to persistent dependent tasks," SIAM Journal on Computing, 27(4): 1168–1189, August 1998.
14. Sanjeev Khanna, Rajeev Motwani, Madhu Sudan, and Umesh Vazirani, "On syntactic versus computational views of approximability," SIAM Journal on Computing, 28(1): 164–191, February 1999.
15. Sigal Ar, Richard J. Lipton, Ronitt Rubinfeld, and Madhu Sudan, "Reconstructing algebraic functions from mixed data," SIAM Journal on Computing, 28(2): 487–510, April 1999.
16. Benny Chor and Madhu Sudan. "A geometric approach to betweenness," SIAM Journal on Discrete Mathematics, 11(4): 511–523, November 1998.
17. Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan, "Private information retrieval," Journal of the ACM 45(6): 965–981, November 1998.
18. Venkatesan Guruswami and Madhu Sudan, "Improved decoding of Reed-Solomon codes and algebraic-geometric codes," IEEE Transactions on Information Theory, 45(6): 1757–1767, September 1999.
19. Oded Goldreich and Madhu Sudan, "Computational indistinguishability: A sample hierarchy," Journal of Computer and System Sciences, 59(2): 253–269, October 1999.
20. Oded Goldreich, Dana Ron, and Madhu Sudan, "Chinese remaindering with errors," IEEE Transactions on Information Theory, 46(4): 1330–1338, July 2000.
21. Oded Goldreich, Ronitt Rubinfeld, and Madhu Sudan, "Learning polynomials with queries: The highly noisy case," SIAM Journal on Discrete Mathematics, 13(4): 535–570, November 2000.
22. Prahladh Harsha and Madhu Sudan, "Small PCPs with low query complexity," Computational Complexity, 9(3-4): 157–201, 2000.
23. Luca Trevisan, Gregory B. Sorkin, Madhu Sudan, and David P. Williamson, "Gadgets, approximation, and linear programming," SIAM Journal on Computing, 29(6): 2074–2097, December 2000.
24. Allan Borodin, Jon Kleinberg, Prabhakar Raghavan, Madhu Sudan, and David P. Williamson, "Adversarial queueing theory," Journal of the ACM, 48(1): 13–38, January 2001.
25. Madhu Sudan, Luca Trevisan, and Salil Vadhan, "Pseudorandom generators without the XOR Lemma," Journal of Computer and System Sciences, 62(2): 236–266, March 2001.
26. Sanjeev Khanna, Madhu Sudan, Luca Trevisan, and David P. Williamson, "The approximability of constraint satisfaction problems," SIAM Journal on Computing, 30(6): 1863-1920, March 2001.
27. Venkatesan Guruswami and Madhu Sudan, "On representations of algebraic-geometric codes," IEEE Transactions on Information Theory, 47(4): 1610–1613, May 2001.
28. Yonatan Aumann, Johan Håstad, Michael O. Rabin, and Madhu Sudan, "Linear consistency testing," Journal of Computer and System Sciences, 62(4): 589–607, July 2001.
29. Ronald Fagin, Anna Karlin, Jon Kleinberg, Prabhakar Raghavan, Sridhar Rajagopalan, Ronitt Rubinfeld, Madhu Sudan, and Andrew Tomkins, "Random walks with "Back Buttons"," Annals of Applied Probability, 11(3): 810–862, 2001.
30. Venkatesan Guruswami, Johan Håstad, Madhu Sudan, and David Zuckerman, "Combinatorial bounds for list decoding," IEEE Transactions on Information Theory, 48(5):1021–1034, May 2002.
31. Venkatesan Guruswami, Johan Håstad, and Madhu Sudan, "Hardness of approximate hypergraph coloring," SIAM Journal on Computing, 31(6):1663–1686, 2002.
32. Ilya Dumer, Daniele Micciancio, and Madhu Sudan, "Hardness of approximating the minimum distance of a linear code," IEEE Transactions on Information Theory, 49(1):22–37, January 2003.
33. Sanjeev Arora and Madhu Sudan, "Improved low degree testing and its applications," Combinatorica, 23(3):365–426, July 2003.

34. Ari Juels and Madhu Sudan, "A Fuzzy Vault Scheme," Designs, Codes and Cryptography, 38(2):237–257, February 2006.
35. Lars Engebretsen and Madhu Sudan, "Harmonic broadcasting is bandwidth-optimal assuming constant bit rate," Networks, 47(3):172–177, February 2006.
36. Oded Goldreich and Madhu Sudan, "Locally testable codes and PCPs of almost-linear length," Journal of the ACM, 53(4):558–655, July 2006.
37. Eli Ben-Sasson and Madhu Sudan, "Robust locally testable codes and products of codes," Random Structure and Algorithms, 28(4): 387–402, July 2006.
38. Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, and Salil P. Vadhan, "Robust PCPs of proximity, shorter PCPs, and applications to coding", SIAM Journal on Computing, 36(4):889–974, December 2006.
39. Noga Alon, Venkatesan Guruswami, Tali Kaufman, and Madhu Sudan, "Guessing secrets efficiently via list decoding", ACM Transactions on Algorithms, 3(4), pages 42:1–42:16, November 2007.
40. Eli Ben-Sasson and Madhu Sudan, "Short PCPs with Polylog Query Complexity", SIAM Journal on Computing *Special Issue Dedicated to Papers from STOC 2005*, 38(2): 551-607, May 2008.
41. Shubhangi Saraf and Madhu Sudan, "An improved lower bound on the size of Kakeya sets over finite fields", Analysis & PDE, 1(3): 375–379, 2008.
42. Eli Ben-Sasson, Venkatesan Guruswami, Tali Kaufman, Madhu Sudan, and Michael Viderman, "Locally Testable Codes Require Redundant Testers", SIAM Journal on Computing, 39(7): 3230–3247, July 2010.
43. Silvio Micali, Chris Peikert, Madhu Sudan, and David A. Wilson "Optimal Error Correction for Computationally Bounded Noise", IEEE Transactions on Information Theory, 56(11): 5673–5680, November 2010.
44. Gagan Aggarwal, Amos Fiat, Andrew Goldberg, Jason Hartline, Nicole Immorlica, and Madhu Sudan. "Derandomization of Auctions", Games and Economic Behavior, 7(1):1-11, May 2011.
45. Arnab Bhattacharyya, Victor Chen, Madhu Sudan, and Ning Xie. "Testing Linear-Invariant Non-Linear Properties", Theory of Computing, 7(1):75–99, 2011.
46. Swastik Kopparty, Vsevolod F. Lev, Shubhangi Saraf, and Madhu Sudan. "Kakeya-type sets in finite vector spaces", Journal of Algebraic Combinatorics, 34(3): 337–355, November 2011.
47. Oded Goldreich, Brendan Juba, and Madhu Sudan. "A theory of goal-oriented communication ", Journal of the ACM, 59(2): Article 8 (65 pages), April 2012.
48. Elena Grigorescu, Tali Kaufman, and Madhu Sudan, "Succinct representation of codes with applications to testing". SIAM Journal on Discrete Mathematics, 26(4): 1618–1634, November 2012.
49. Elena Grigorescu, Tali Kaufman, and Madhu Sudan, "2-transitivity is insufficient for local testability", Computational Complexity, 22(1): 137–158, March 2013.
50. Elad Haramaty, Amir Shpilka, and Madhu Sudan, "Optimal testing of multivariate polynomials over small prime fields", SIAM Journal on Computing, 42(2): 536–562 March 2013.
51. Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan, "Extensions to the method of multiplicities, with applications to Kakeya sets and mergers" SIAM Journal on Computing, Special Section on the Fiftieth Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009), 42(6): 2305–2328, November 2013.
52. Noga Ron-Zewi and Madhu Sudan, "A new upper bound on the query complexity of testing generalized Reed-Muller codes," Theory of Computing, 9:783–807, 2013.
53. Joel Spencer, Madhu Sudan, and Kuang Xu, "Queueing with future information", The Annals of Applied Probability, 24(5): 2091–2142, October 2014.

3. Papers in refereed conferences.

    1. Marshall Bern, Daniel H. Greene, Arvind Raghunathan, and Madhu Sudan, "Online algorithms for locating checkpoints," Proceedings of the Twenty Second Annual ACM Symposium on Theory of Computing, pages 359-368, Baltimore, Maryland, 14-16 May 1990.
    2. Peter Gemmell, Richard Lipton, Ronitt Rubinfeld, Madhu Sudan, and Avi Wigderson, "Self-testing/correcting for polynomials and for approximate functions," Proceedings of the Twenty Third Annual ACM Symposium on Theory of Computing, pages 32-42, New Orleans, Louisiana, 6-8 May 1991.
    3. Ronitt Rubinfeld and Madhu Sudan, "Self-testing polynomial functions efficiently and over rational domains," Proceedings of the Third Annual ACM-SIAM Symposium on Discrete Algorithms, pages 23–32, Orlando, Florida, 27-29 January 1992.
    4. Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy, "Proof verification and hardness of approximation problems," Proceedings of the 33rd Annual Symposium on Foundations of Computer Science, pages 14–23, Pittsburgh, Pennsylvania, 24-27 October 1992.
    5. Sigal Ar, Richard J. Lipton, Ronitt Rubinfeld, and Madhu Sudan, "Reconstructing algebraic functions from mixed data," Proceedings of the 33rd Annual Symposium on Foundations of Computer Science, pages 503–512, Pittsburgh, Pennsylvania, 24-27 October 1992.
    6. Alok Aggarwal, Amotz Bar-Noy, Don Coppersmith, Rajeev Ramaswami, Baruch Schieber, and Madhu Sudan, "Efficient routing and scheduling algorithms for optical networks," Proceedings of the Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, pages 412–423, Philadelphia, Pennsylvania, 23-25 January 1994.
    7. Avrim Blum, Prasad Chalasani, Don Coppersmith, Bill Pulleyblank, Prabhakar Raghavan, and Madhu Sudan, "The minimum latency problem," Proceedings of the Twenty-Sixth Annual ACM Symposium on the Theory of Computing, pages 163–171, Montreal, Quebec, Canada, 23-25 May 1994.
    8. Mihir Bellare and Madhu Sudan, "Improved non-approximability results," Proceedings of the Twenty-Sixth Annual ACM Symposium on the Theory of Computing, pages 184–193, Montreal, Quebec, Canada, 23-25 May 1994.
    9. David Karger, Rajeev Motwani, and Madhu Sudan, "Approximate graph coloring by semidefinite programming," Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pages 2–13, Santa Fe, New Mexico, 20-22 November 1994.
    10. Christos Papadimitriou, Prabhakar Raghavan, Madhu Sudan, and Hisao Tamaki, "Motion planning on a graph," Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pages 511–520, Santa Fe, New Mexico, 20-22 November 1994.
    11. Andres Albanese, Johannes Blömer, Jeff Edmonds, Michael Luby, and Madhu Sudan, "Priority encoding transmission," Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pages 604–612, Santa Fe, New Mexico, 20-22 November 1994.
    12. Sanjeev Khanna, Rajeev Motwani, Madhu Sudan, and Umesh Vazirani, "On syntactic versus computational views of approximability" Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pages 819–830, Santa Fe, New Mexico, 20-22 November 1994.
    13. Katalin Friedl and Madhu Sudan, "Some improvements to total degree tests," Proceedings of the 3rd Annual Israel Symposium on Theory of Computing and Systems, pages 190-198, Tel Aviv, Israel, 4-6 January 1995.
    14. Amotz Bar-Noy, Alain Mayer, Baruch Schieber, and Madhu Sudan, "Guaranteeing fair service to persistent dependent tasks," Proceedings of the Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, pages 243-252, San Francisco, California, 22-24 January 1995.
    15. Benny Chor and Madhu Sudan, "A geometric approach to betweenness," Third European Symposium on Algorithms, Lecture Notes in Computer Science v. 979, pages 227–239, Corfu, Greece, September 1995.

16. Guy Even, Joseph (Seffi) Naor, Baruch Schieber, and Madhu Sudan, "Approximating minimum feedback sets and multicuts in directed graphs," Proceedings of the 4th MPS Conference on Integer Programming and Combinatorial Optimization, Copenhagen, Denmark, Lecture Notes in Computer Science, v. 920, pages 14–28, 29-31 May 1995.
17. Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan, "Private information retrieval," Proceedings of the 36th Annual Symposium on Foundations of Computer Science, pages 41–50, Milwaukee, Wisconsin, 23-25 October 1995.
18. Oded Goldreich, Ronitt Rubinfeld, and Madhu Sudan, "Learning polynomials with queries: The highly noisy case," Proceedings of the 36th Annual Symposium on Foundations of Computer Science, pages 294–303, Milwaukee, Wisconsin, 23-25 October 1995.
19. Mihir Bellare, Oded Goldreich, and Madhu Sudan, "Free bits, PCPs and non-approximability – towards tight results," Proceedings of the 36th Annual Symposium on Foundations of Computer Science, pages 422–431, Milwaukee, Wisconsin, 23-25 October 1995.
20. Mihir Bellare, Don Coppersmith, Johan Håstad, Marcos Kiwi, and Madhu Sudan, "Linearity testing in characteristic two," Proceedings of the 36th Annual Symposium on Foundations of Computer Science, pages 432–441, Milwaukee, Wisconsin, 23-25 October 1995.
21. Allan Borodin, Jon Kleinberg, Prabhakar Raghavan, Madhu Sudan, and David P. Williamson, "Adversarial queueing theory," Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, pages 376–385, Philadelphia, Pennsylvania, 22-24 May 1996.
22. Madhu Sudan, "Maximum likelihood decoding of Reed Solomon codes," Proceedings of the 37th Annual Symposium on Foundations of Computer Science, pages 164-172, Burlington, Vermont, 14-16 October 1996.
23. Luca Trevisan, Gregory B. Sorkin, Madhu Sudan, and David P. Williamson, "Gadgets, approximation, and linear programming," Proceedings of the 37th Annual Symposium on Foundations of Computer Science, pages 617–626, Burlington, Vermont, 14-16 October 1996.
24. Sanjeev Khanna, Madhu Sudan, and David P. Williamson, "A complete classification of the approximability of maximization problems derived from Boolean constraint satisfaction," Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing, pages 11-20, El Paso, Texas, 4-6 May 1997.
25. Sanjeev Arora and Madhu Sudan, "Improved low degree testing and its applications," Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing, pages 485–495, El Paso, Texas, 4-6 May 1997.
26. Sanjeev Khanna, Madhu Sudan, and Luca Trevisan, "Constraint satisfaction: The approximability of minimization problems," Proceedings of the 12th Annual IEEE Conference on Computational Complexity, pages 282–296, Ulm, Germany, 24-27 June, 1997.
27. Oded Goldreich and Madhu Sudan, "Computational indistinguishability: A sample hierarchy," Proceedings of the Thirteenth Annual IEEE Symposium on Computational Complexity, pages 24–33, Buffalo, New York, 15-18 June, 1998.
28. Venkatesan Guruswami, Daniel Lewin, Madhu Sudan, and Luca Trevisan, "A tight characterization of NP with 3-query PCPs," Proceedings of the 39th Annual Symposium on Foundations of Computer Science, pages 8–17, Palo Alto, California, 8-11 November, 1998.
29. Madhu Sudan and Luca Trevisan, "Probabilistically checkable proofs with low amortized query complexity," Proceedings of the 39th Annual Symposium on Foundations of Computer Science, pages 18–27, Palo Alto, California, 8-11 November, 1998.
30. Venkatesan Guruswami and Madhu Sudan, "Improved decoding of Reed-Solomon and algebraic-geometric codes," Proceedings of the 39th Annual Symposium on Foundations of Computer Science, pages 28-37, Palo Alto, California, 8-11 November, 1998.
31. Oded Goldreich, Dana Ron, and Madhu Sudan, "Chinese remaindering with errors," Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing, pages 225-234, Atlanta, Georgia, 1-4 May 1999.

32. Madhu Sudan, Luca Trevisan, and Salil Vadhan, "Pseudorandom generators without the XOR lemma." Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing, pages 537-546, Atlanta, Georgia, 1-4 May 1999.

33. Yonatan Aumann, Johan Håstad, Michael O. Rabin, and Madhu Sudan, "Linear consistency testing," Randomization, Approximation and Combinatorial Optimization, D. Hochbaum et al. (Eds), Proceedings of the 3rd International Workshop on Randomization and Approximation Techniques in Computer Science, Berkeley, California, 8-11 August 1999, Lecture Notes in Computer Science, vol. 1671, Springer, Berlin, pages 109-120, 1999.

34. Ilya Dumer, Daniele Micciancio, and Madhu Sudan, "Hardness of approximating the minimum distance of a linear code," Proceedings of the 40th Annual Symposium on Foundations of Computer Science, pages 475-484, New York City, New York, 17-19 October, 1999.

35. Venkatesan Guruswami and Madhu Sudan, "List decoding algorithms for certain concatenated codes," Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, pages 181-190, Portland, Oregon, 21-23 May 2000.

36. Ronald Fagin, Anna Karlin, Jon Kleinberg, Prabhakar Raghavan, Sridhar Rajagopalan, Ronitt Rubinfeld, Madhu Sudan, and Andrew Tomkins, "Random walks with "Back Buttons"," Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, pages 484-493, Portland, Oregon, 21-23 May 2000.

37. Venkatesan Guruswami and Madhu Sudan, "On representations of algebraic-geometric codes for list decoding," Proceedings of the 8th Annual European Symposium on Algorithms, pages 244-255, Saarbrücken, Germany, September 5-8, 2000.

38. Venkatesan Guruswami, Johan Håstad, and Madhu Sudan, "Hardness of approximate hypergraph coloring," Proceedings of the 41st Annual Symposium on Foundations of Computer Science, pages 149-158, Redondo Beach, California, 12-14 November, 2000.

39. Venkatesan Guruswami, Amit Sahai, and Madhu Sudan, ""Soft-decision" decoding of Chinese remainder codes," Proceedings of the 41st Annual Symposium on Foundations of Computer Science, pages 159-168, Redondo Beach, California, 12-14 November, 2000.

40. Prahladh Harsha and Madhu Sudan, "Small PCPs with low query complexity," *STACS 2001*, Afonso Ferreira and Horst Reichel (Eds.), Proceedings of the 18th Annual Symposium on Theoretical Aspects of Computer Science, Dresden, Germany, 15-17 February 2001. Lecture Notes in Computer Science, vol. 2010, Springer, Berlin, pages 327-338, 2001.

41. Noga Alon, Venkatesan Guruswami, Tali Kaufman, and Madhu Sudan, "Guessing secrets efficiently via list decoding," Proceedings of the Thirteenth Annual ACM-SIAM Symposium on Discrete Algorithms, pages 254–262, San Francisco, California, 6-8 January 2002.

42. Lars Engebretsen and Madhu Sudan, "Harmonic broadcasting is optimal," Proceedings of the Thirteenth Annual ACM-SIAM Symposium on Discrete Algorithms, pages 431–432, San Francisco, California, 6-8 January 2002.

43. Venkatesan Guruswami and Madhu Sudan, "Decoding concatenated codes using soft information", Proceedings of the Seventeenth Annual IEEE Conference on Computational Complexity, pages 148–157, Montreal, Canada, 21-24 May, 2002.

44. Ari Juels and Madhu Sudan, "A fuzzy vault scheme", Proceedings of the IEEE International Symposium on Information Theory, A. Lapidoth and E. Teletar, Eds., page 408, Lausanne, Switzerland, 30 June - 5 July, 2002.

45. Oded Goldreich and Madhu Sudan, "Locally testable codes and PCPs of almost-linear length", Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, pages 13–22, Vancouver, Canada, 16-19 November, 2002.

46. Don Coppersmith and Madhu Sudan. "Reconstructing curves in three (and higher) dimensional spaces from noisy data." Proceedings of the Thirty Fifth Annual ACM Symposium on Theory of Computing, pages 136–142, San Diego, California, 9-11 June 2003.

47. Eli Ben-Sasson, Madhu Sudan, Salil Vadhan, and Avi Wigderson. "Randomness-efficient low degree tests and short PCPs via $\epsilon$-biased sets", Proceedings of the Thirty Fifth Annual ACM Symposium on Theory of Computing, pages 612–621, San Diego, California, 9-11 June 2003.
48. Eli Ben-Sasson, Oded Goldreich, and Madhu Sudan. "Bounds on 2-query codeword testing", In Sanjeev Arora, Klaus Jansen, Jos D. P. Rolim, Amit Sahai (Eds.): Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques, 6th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2003 and 7th International Workshop on Randomization and Approximation Techniques in Computer Science, RANDOM 2003, Princeton, NY, USA, August 24-26, 2003. Lecture Notes in Computer Science 2764 Springer 2003, ISBN 3-540-40770-7, pages 216–227.
49. Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, and Salil Vadhan. " Robust PCPs of proximity, shorter PCPs and applications to coding", Proceedings of the Thirty Sixth Annual ACM Symposium on Theory of Computing, pages 1–10, Chicago, Illinois, June 13-15, 2004.
50. Eli Ben-Sasson and Madhu Sudan. "Robust locally testable codes and products of codes", In Klaus Jansen, Sanjeev Khanna, Jos D. P. Rolim, and Dana Ron (Eds.): Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques, 7th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2004 and 7th International Workshop on Randomization and Approximation Techniques in Computer Science, RANDOM 2004, Radcliffe Institute, Cambridge, MA, USA, August 22-24, 2004, pages 286–297.
51. Silvio Micali, Chris Peikert, Madhu Sudan, and David A. Wilson. Optimal error-correction against computationally bounded noise. Second Annual Theory of Cryptography Conference, pages 1–16, MIT, Cambridge, Massachusetts, February 10-12, 2005.
52. Eli Ben-Sasson and Madhu Sudan. "Simple PCPs with Poly-log Rate and Query Complexity", Proceedings of the Thirty Seventh Annual ACM Symposium on Theory of Computing, pages 266–275, Baltimore, Maryland, May 22-24, 2005.
53. Gagan Aggarwal, Amos Fiat, Andrew Goldberg, Jason Hartline, Nicole Immorlica, and Madhu Sudan. "Derandomization of Auctions", Proceedings of the Thirty Seventh Annual ACM Symposium on Theory of Computing, pages 619–625, Baltimore, Maryland, May 22-24, 2005.
54. Eli Ben-Sasson, Oded Goldriech, Prahladh Harsha, Madhu Sudan, and Salil Vadhan. "Short PCPs verifiable in polylogarithmic time", Proceedings of the Twelfth Annual IEEE Conference on Computational Complexity, pages 120–134, San Jose, California, June 12-15, 2005.
55. Shafi Goldwasser, Madhu Sudan, and Vinod Vaikuntanathan, "Distributed Computing with Imperfect Randomness", Proceedings of DISC 2005, Cracow, Poland, September 26-29, 2005, Springer Lecture Notes in Computer Science, volume 3724, pages 288-302, 2005.
56. Irit Dinur, Madhu Sudan, and Avi Wigderson, "Robust local testability of tensor products of LDPC codes", Proceedings of APPROX-RANDOM, August 28-30 2006, Barcelona, Spain, Springer Lecture Notes in Computer Science, vol. 4110, pages 304–315, 2006.
57. Elena Grigorescu, Swastik Kopparty, and Madhu Sudan, "Local decoding and testing for homomorphisms", Proceedings of APPROX-RANDOM, August 28-30 2006, Barcelona, Spain, Springer Lecture Notes in Computer Science, vol. 4110, pages 375–385, 2006.
58. Ran Canetti, Ronald L. Rivest, Madhu Sudan, Luca Trevisan, Salil P. Vadhan, and Hoeteck Wee, "Amplifying collision resistance: a complexity-theoretic treatment", Proceedings of CRYPTO 2007, 27th Annual International Cryptology Conference, August 19-23 2007, Santa Barbara, CA, USA, Lecture Notes in Computer Science, vol. 4622, pages 264–283, Springer, 2007.
59. Tali Kaufman and Madhu Sudan, "Sparse random linear codes are locally decodable and testable", Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science, pages 590–600, Providence, RI, USA, October 20-23, 2007.
60. Brendan Juba and Madhu Sudan, "Universal semantic communication I", Proceedings of the Thirty Seventh Annual ACM Symposium on Theory of Computing, pages 123–132, Victoria (BC), Canada, May 17-20, 2008.

61. Irit Dinur, Elena Grigorescu, Swastik Kopparty, and Madhu Sudan, "Decoding group homomorphisms beyond the Johnson bound", Proceedings of the Thirty Seventh Annual ACM Symposium on Theory of Computing, pages 275–284, Victoria (BC), Canada, May 17-20, 2008.
62. Tali Kaufman and Madhu Sudan, "Algebraic property testing: The role of invariance", Proceedings of the Thirty Seventh Annual ACM Symposium on Theory of Computing, pages 403–412, Victoria (BC), Canada, May 17-20, 2008.
63. Elena Grigorescu, Tali Kaufman, and Madhu Sudan, "2-transitivity is insufficient for local testability", Proceedings of the 23rd IEEE Conference on Computational Complexity, pages 259–267, University of Maryland, College Park, Maryland, USA, June 23-26th, 2008.
64. Arnab Bhattacharyya, Victor Chen, Madhu Sudan, and Ning Xie, "Testing linear-invariant nonlinear properties", Proceedings of the 26th International Symposium on Theoretical Aspects of Computer Science (STACS 2009), pages 135–146, Freiburg, Germany, February 26-28, 2009.
65. Eli Ben-Sasson, Venkatesan Guruswami, Tali Kaufman, Madhu Sudan, and Michael Viderman, "Locally testable codes require redundant testers", Proceedings of the 24th Annual IEEE Conference on Computational Complexity, pages 52–61, Paris, France, July 15-18, 2009.
66. Elena Grigorescu, Tali Kaufman, and Madhu Sudan, "Succinct representation of codes with applications to testing". Proceedings of APPROX-RANDOM 2009, Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, 12th International Workshop, APPROX 2009, and 13th International Workshop, RANDOM 2009, Lecture Notes in Computer Science, volume 5687, Springer 2009, pages 534–547, Berkeley, CA, USA, August 21-23, 2009.
67. Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan, "Extensions to the method of multiplicities, with applications to Kakeya sets and mergers", Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, pages 181–190, Atlanta, Georgia, USA, October 24-27, 2009.
68. Arnab Bhattacharyya, Swastik Kopparty, Grant Schoenebeck, Madhu Sudan, and David Zuckerman, "Optimal testing of Reed-Muller codes", Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science, pages 488–497, Las Vegas, Nevada, USA, October 23-26, 2010.
69. Adam Kalai, Michael Mitzenmacher, and Madhu Sudan, "Tight asymptotic bounds for the deletion channel with small deletion probabilities", Proceedings of the 2010 IEEE International Symposium on Information Theory, pages 997–1001, Austin, Texas, USA, June 13-18, 2010.
70. Brendan Juba and Madhu Sudan. "Efficient Semantic Communication via Compatible Beliefs", Proceedings of Innovations in Computer Science (ICS 2011), pages 22-31, Tsinghua University, Beijing, China, January 7-9 2011.
71. Brendan Juba, Adam Kalai, Sanjeev Khanna, and Madhu Sudan, "Compression without a common prior: an information-theoretic justification for ambiguity in language", Proceedings of Innovations in Computer Science (ICS 2011), pages 79-86, Tsinghua University, Beijing, China, January 7-9 2011.
72. Victor Chen, Madhu Sudan, and Ning Xie, "Property testing via set-theoretic operations" Proceedings of Innovations in Computer Science (ICS 2011), pages 211-222, Tsinghua University, Beijing, China, January 7-9 2011.
73. Eli Ben-Sasson, Ghid Maatouk, Amir Shpilka, and Madhu Sudan. "Symmetric LDPC codes are not necessarily locally testable", Proceedings of the 26th Annual IEEE Conference on Computational Complexity (CCC 2011), pages 55-65. San Jose, California, USA, June 8-10, 2011.
74. Oded Goldreich, Brendan Juba, and Madhu Sudan. "Brief announcement: A theory of goal-oriented communication", Proceedings of the 30th Annual ACM Symposium on Principles of Distributed Computing, PODC 2011, pages 299-300, San Jose, CA, USA, June 6-8, 2011.
75. Eli Ben-Sasson and Madhu Sudan. "Limits on the rate of locally testable affine-invariant codes", Proceedings of Approximation, Randomization, and Combinatorial Optimization: Algorithms and

Techniques — 14th International Workshop, APPROX 2011, and 15th International Workshop, RANDOM 2011, pages 412-423, Princeton, NJ, USA, August 17-19, 2011.

76. Eli Ben-Sasson, Elena Grigorescu, Ghid Maatouk, Amir Shpilka, and Madhu Sudan. "On Sums of Locally Testable Affine Invariant Properties", Proceedings of Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques — 14th International Workshop, APPROX 2011, and 15th International Workshop, RANDOM 2011, pages 400-411, Princeton, NJ, USA, August 17-19, 2011.
77. Elad Haramaty, Amir Shpilka, and Madhu Sudan. "Optimal testing of multivariate polynomials over small prime fields", Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science, pages 629–637, Palm Springs, California, USA, October 23-25, 2011.
78. Sanjeev Khanna and Madhu Sudan. "Delays and the Capacity of Continuous-time Channels", Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science, pages 758–767, Palm Springs, California, USA, October 23-25, 2011.
79. Noga Ron-Zewi and Madhu Sudan. "A new upper bound on the query complexity for testing generalized Reed-Muller codes," Proceedings of Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques — 15th International Workshop, APPROX 2012, and 16th International Workshop, RANDOM 2012, pages 639–650, Cambridge, MA, USA, August 15-17, 2012.
80. Eli Ben-Sasson, Noga Ron-Zewi, and Madhu Sudan. "Sparse affine-invariant linear codes are locally testable", Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science, pages 561–570, New Brunswick, New Jersey, October 20-23, 2012.
81. Alan Guo, Swastik Kopparty, and Madhu Sudan. "New affine-invariant codes from lifting," Proceedings of Innovations in Theoretical Computer Science (ITCS '13), pages 529–540. Berkeley, CA, USA, January 9-12, 2013.
82. Elad Haramaty, Noga Ron-Zewi, and Madhu Sudan. "Absolutely Sound Testing of Lifted Codes," Proceedings of Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques — 16th International Workshop, APPROX 2013, and 17th International Workshop, RANDOM 2013, pages 671–682, Berkeley, CA, USA, August 21-23, 2013.
83. Joel Spencer, Madhu Sudan, and Kuang Xu. "Queueing with future information," SIGMETRICS Performance Evaluation Review, 41(3): 40–42, 2013.
84. Michael Kapralov, Sanjeev Khanna, and Madhu Sudan. "Approximating matching size from random streams," Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014, pages 734–751, Portland, Oregon, USA, January 5-7, 2014.
85. David Gamarnik and Madhu Sudan. "Limits of local algorithms over sparse random graphs," Proceedings of Innovations in Theoretical Computer Science (ITCS 2014), pages 369–376, Princeton, NJ, USA, January 12-14, 2014.
86. Elad Haramaty and Madhu Sudan. "Deterministic compression with uncertain priors," ITCS 2014: Proceedings of Innovations in Theoretical Computer Science (ITCS 2014), pages 377–386, Princeton, NJ, USA, January 12-14, 2014.
87. Mohsen Ghaffari, Bernhard Haeupler, and Madhu Sudan. "Optimal error rates for interactive coding I: adaptivity and other settings," Proceedings of Symposium on Theory of Computing, STOC 2014, pages 794–803, New York, NY, USA, May 31 - June 03, 2014.
88. Alan Guo and Madhu Sudan. "List decoding group homomorphisms between supersolvable groups," Proceedings of Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques — 17th International Workshop, APPROX 2014, and 18th International Workshop, RANDOM 2014, pages 737–747, Barcelona, Spain, September 4-6, 2014.

4. Invited (unrefereed) papers.

1. Madhu Sudan, "On the role of algebra in the efficient verification of proofs," Workshop of Algebraic Methods in Complexity Theory (AMCOT), Indian Institute of Mathematical Sciences, Chennai, India, December 1994.
2. Jonathan Hosking, Edwin Pednault, and Madhu Sudan, "A statistical perspective on data mining," Future Generation Computer Systems, Special Issue on Data Mining, 13(2-3): 117–134, November 1997.
3. Madhu Sudan, "Decoding Reed-Solomon codes beyond the error-correction diameter," Proceedings of the 35th Annual Allerton Conference on Communication, Control and Computing, Monticello, Illinois, pages 215–224, 29 September – 1 October, 1997.
4. Madhu Sudan, "Algorithmic issues in coding theory," Proceedings of the 17th Annual Conference on Foundations of Software Technology and Theoretical Computer Science, Kharagpur, India, 18-20 December, 1997. S. Ramesh and G. Sivakumar (Eds.) Lecture Notes in Computer Science, 1346:184–199, Springer, Berlin, 1997.
5. Madhu Sudan, "Probabilistic verification of proofs," Proceedings of the International Congress of Mathematicians, Berlin 1998, August 18–27, Documenta Mathematica, Extra Volume ICM 1998, III, 461–470.
6. Madhu Sudan, "List decoding: Algorithms and applications," SIGACT News, Volume 31, Number 1, pp. 16–27, March 2000 (Whole Number 114).
7. Madhu Sudan, "List decoding: Algorithms and applications," Proceedings of the International Conference IFIP TCS 2000, Sendai, Japan, 17-19 August, 2000. In Lecture Notes in Computer Science, Volume 1872, J. van Leeuwen, O. Watanabe, M. Hagiya, P.D. Mosses, T. Ito (Eds.), Springer, pages 25–41, August 2000.
8. Venkatesan Guruswami, Johan Håstad, Madhu Sudan, and David Zuckerman, "Combinatorial bounds for list decoding," Proceedings of the 38th Annual Allerton Conference on Communication, Control and Computing, pages 603–612, Monticello, Illinois, 4-6 October, 2000.
9. Madhu Sudan, "Coding theory: Tutorial & Survey," Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science, pages 36–53, Las Vegas, Nevada, 14-17 October 2001.
10. Madhu Sudan, "Ideal error-correcting codes: Unifying algebraic and number-theoretic algorithms," Proceedings of AAECC-14, the Fourteenth Symposium on Applied Algebra, Alegbraic Algorithms, and Error Correcting Codes, Melbourne, Australia, 26-30 November 2001. In Lecture Notes in Computer Science, Volume 2227, Serdar Boztaş and Igor E. Shparlinksi (Eds.), Springer, pages 36–45, November 2001.
11. Nadia Creignou, Sanjeev Khanna, and Madhu Sudan, "Complexity classifications of Boolean constraint satisfaction problems", SIGACT News, Volume 32, Number 4, Whole Number 121, Complexity Theory Column 34, pages 24-33, December 2001.
12. Venkatesan Guruswami and Madhu Sudan, "Reflections on "Improved Decoding of Reed-Solomon and Algebraic-Geometric Codes"", IEEE Information Theory Society Newsletter, Volume 52, Number 1, ISSN 1059-2362, pages 6-12, March 2002.
13. Madhu Sudan, "Quick and Dirty Refereeing?", Science, Volume 301, pages 1191–1192, 29 August 2003.
14. Madhu Sudan, "Modelling Errors and Recovery for Communication," Proceedings of LATIN 2006, Valdivia, Chile, Springer Lecture Notes in Computer Science, volume 3887, pages 25–25, 2006.
15. Jaikumar Radhakrishnan and Madhu Sudan, "On Dinur's proof of the PCP theorem," Bulletin (New Series) of the American Mathematical Society, 44(1):19–61, January 2007.
16. Madhu Sudan, "Algebraic algorithms and coding theory," Proceedings of ISSAC 2008, International Symposium on Symbolic and Algebraic Computation, ISSAC 2008, Linz/Hagenberg, Austria, July 20-23, 2008, pages 337–337, ACM Press, 2008.

17. Madhu Sudan, "Probabilistically Checkable Proofs," Communications of the ACM, 52(3):76–84, March 2009.
18. Madhu Sudan, "Invariance in Property Testing," In *Property Testing: Current Research and Surveys*, Oded Goldreich (Ed.), Lecture Notes in Computer Science, vol. 6390, pages 211–227, Springer, July 2010.
19. Arnab Bhattacharyya, Victor Chen, Madhu Sudan, and Ning Xie, "Testing linear-invariant non-linear properties," In *Property Testing: Current Research and Surveys*, Oded Goldreich (Ed.), Lecture Notes in Computer Science, vol. 6390, pages 260–268, Springer, July 2010.
20. Arnab Bhattacharyya, Swastik Kopparty, Grant Schoenebeck, Madhu Sudan, and David Zuckerman, "Optimal testing of Reed-Muller codes", In *Property Testing: Current Research and Surveys*, Oded Goldreich (Ed.), Lecture Notes in Computer Science, vol. 6390, pages 269–275, Springer, July 2010.
21. Madhu Sudan. "Guest column: Testing Linear Properties: Some General Themes", SIGACT News 42(1):59–80, March 2011.
22. Madhu Sudan. "Patterns hidden from simple algorithms", Technical Perspective, Communications of the ACM, 54(4):107, April 2011.
23. Oded Goldreich, Madhu Sudan, and Luca Trevisan. "From Logarithmic Advice to Single-Bit Advice", In *Studies in Complexity and Cryptography*, Oded Goldreich (Ed.), Lecture Notes in Computer Science, volume 6650, pages 109–113, Springer, 2011.
24. Madhu Sudan. "Physical Limits of Communication (Invited talk)", Proceedings of the IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2011, December 12-14, 2011, Mumbai, India, Supratik Chakraborty and Amit Kumar (Eds.), pages 4–5, LIPIcs series volume 13, Schloss Dagstuhl Publishing - Leibniz-Zentrum fuer Informatik, 2011.
25. Madhu Sudan. "Communication amid uncertainty", Proceedings of the Information Theory Workshop (ITW), 2012 IEEE September 3-7, 2012, Lausanne, Switzerland, pages 158–161, IEEE Press, 2012.

5. Technical reports

    1. Milena Mihail and Madhu Sudan, "Connectivity properties of matroids," Technical Report, Computer Science Division, University of California at Berkeley, CSD-91-662, 1991.
    2. Sanjeev Khanna and Madhu Sudan, "The optimization complexity of constraint satisfaction problems," Technical Note, Stanford University, Computer Science Department, CS-TN-96-29, January 1996.
    3. Brendan Juba and Madhu Sudan, "Universal Semantic Communication II: A Theory of Goal-Oriented Communication", Electronic Colloquium on Computational Complexity (ECCC), TR08-095, October 2008.
    4. Alan Guo and Madhu Sudan, "Some closure features of locally testable affine-invariant properties," Electronic Colloquium on Computational Complexity (ECCC) TR12-048, 25 April, 2012.
    5. David Gamarnik and Madhu Sudan, "Performance of the Survey Propagation-guided decimation algorithm for the random NAE-K-SAT problem," arXiv:1402.0052 [math.PR], 1 February, 2014.
    6. Venkatesan Guruswami, Madhu Sudan, Ameya Velingker, and Carol Wang, "Limitations on testable affine-invariant codes in the high-rate regime," Electronic Colloquium on Computational Complexity (ECCC) TR14-067, 4 May 2014.

6. Seminars: Approximately 300 invited seminars.