Shafi Goldwasser

RSA Professor of Computer Science, Massachusetts Institute of Technology
Professor of Computer Science and Applied Mathematics, Weizmann Institute of Science

PRINCIPAL FIELDS OF INTEREST

Cryptography, Computational Number Theory, Complexity Theory, Fault Tolerant Distributed Computing, Probabilistic Proof Systems, Approximation Algorithms.

EDUCATION

1979	Carnegie Mellon University, B.S.
1981	University of California at Berkeley, M.S.
1984	University of California at Berkeley, Ph.D. Thesis: Probabilistic Encryption: Theory and Applications Advisor: Professor Manuel Blum.

EMPLOYMENT AND VISITING POSITIONS

Massachusetts Institute of Technology

1997-present	RSA Professor of Electrical Engineering and Computer Science
1992-present	Professor of Electrical Engineering and Computer Science
1995	Co-Leader and Head of the Cryptography and Information Security Group with Ron Rivest
1987-1992	Associate Professor
1983-1987	Assistant Professor
1983	Bantrel Postdoctoral Fellowship

Weizmann Institute of Science

1993-present	Professor of Computer Science and Applied Mathematics

Visiting Positions

1987, 1990, 1993	Hebrew University, Visiting Professor
1988, 1991, 1993	International Computer Science Institute, Visiting Scientist
1992	Visiting Professor, Weizmann Institute
1990	Princeton University,Visiting Professor

AWARDS

1983-85	IBM Young Faculty Development Award
1987-92	NSF Presidential Young Investigator Award
1991-96	NSF Award for Women in Science
1993	SIGACT Gödel Prize for "The Knowledge Complexity of Interactive Proof Systems"
1996	ACM Grace Murray Hopper Award
1998	RSA Award in Mathematics for Outstanding Mathematical Contributions to Cryptograhy
1999	Weizmann Institute Levenson Prize in Mathematics
2001	SIGACT Gödel Prize for "Interactive Proofs and the Hardness of Approximating Cliques"
2006	Distinguished Alumnus Award in Computer Science and Engineering University of California, Berkeley
2008	Athena Lecturer, Association for Computing Machinery's Committee on Women in Computing (ACM-W)
2010	Franklin Institute Benjamin Franklin Medal in Computer and Cognitive Science
2011	IEEE Emanuel R. Piore Award
2012	Simons Foundation Investigator Award
2013	A.M. Turing Award

PROFESSIONAL SOCIETIES

2001	Fellow of American Academy of Arts and Science
2004	Fellow of National Academy of Sciences
2005	Fellow of National Academy of Engineering
2007	IACR Fellow

PROFESSIONAL ACTIVITIES

Theory of Computation Group Head

Cryptography and Information Security Group Co-leader

Weizmann Institute Theory Group Member

SERVICE

- Program chair for CRYPTO 1988, FOCS 1994, and served extensively as Program Committee member for CRYPTO, EUROCRYPT, FOCS, STOC, ICALP, PODC, RANDOM, ANTS, AsiaCrypt, and Structure conferences.
- Panel chair for ICM 2006 on mathematical aspects of computer science.
- Served on Editorial Boards of SIAM, J. of Computing (1987-1996), Mathematical Systems Theory (1990-2001), SIAM J. Discrete Mathematics (1993-2001), Computational Complexity (1990-present), Foundations and Trends in Theoretical CS (2005-present), PNAS Member Editor (2006-present).
- Area 2 chair for graduate studies in computer science at MIT (1995-2001).
- Chair of the Gödel Prize Selection Committee (2007).
- Taught MIT Professional Education summer course on "Cryptography and Information Security," with Mihir Bellare since 1996.
- Organizer of Weizmann Workshop on Randomized Proof Systems 1993, and the Weizmann Workshop on Randomness and Computation 1994, Co-Organizer of Weizmann Workshop on Cryptographic Protocols 1997, Co-organizer of DIMACS workshop on sublinear algorithms 2000, Co-organizer of the first ANTS conference on Computational Number Theory 1994, Co-organizer of Dagshtul Theoretical Foundations of Practical Information Security 2008.
- Member of the University-Wide Promotions Committee (the "committee of 12") at Weizmann Institute of Science for two terms (2001-2003, 2007-2010).
- Organizer of workshop series on "Cryptography in the Clouds," MIT, 2009-2010.
- Founding Member and Steering Committee Member of Theory of Cryptography Conference (TCC, originated 2004).
- Head of Steering Committee for Innovations in Computer Science (ITCS, originated 2009), and Program chair for ITCS 2012.
- General conference chair for the first Theory of Cryptography Conference (TCC 2004), MIT, and Second Theory of Cryptography Conference (TCC 2005), MIT.

STUDENTS SUPERVISED

Massachusetts Institute of Technology

- Johan Hastad Ph.D. thesis, "Computational Limitations on Small Depth Circuits," June 1986. Received 1986 ACM best thesis award.
  Professor in computer science department,University of Stockholm.
- Aiello Bill Ph.D. thesis, "Complexity Aspects of Interactive Proofs," June 1988.
  Chair of computer science department, British Columbia University.
- Kilian Joseph, Ph.D. thesis, "Primality Testing and the Power of Noisy Communication Channel," May 1988.

Received a distinguished mention for 1988 ACM thesis award competition.
Professor of Computer Science, Rutgers University.

- Yishay Mansour, Ph.D. thesis, "On the Complexity of Algebraic Functions," June 1990.
  Computer Science Department in Tel-Aviv University.
- Daniele Micciancio, Ph.D. thesis, "On the Complexity of the Shortest Vector Problem," August 1998.
  Associate Professor in Computer Science, UC San Diego.
- Salil Vadhan, Ph.D. thesis, "Studies In Zero-Knowledge," August 1999.
  Assistant Professor in Applied Mathematics, Harvard University.
- Tal Malkin, Ph.D. thesis, "Secure Data Base Access," December 1999.
  Assistant Professor in Computer Science, Columbia University.
- Amit Sahai, Ph.D. thesis, "Concurrent Cryptography," August 2000.
  Associate Professor in Computer Science Departement, UCLA.
- Stas Jarewcki, Ph.D. thesis,"Threshold Cryptography," February 2001.
  Assistant Professor, Computer Science Department, University of CA, Irvine.
- Yael Tauman Kalai, PhD. thesis,"Attacks on the Fiat-Shamir Paradigm and Program Obfuscation," August 2006.
  Researcher, Microsoft.
- Adi Akavia, Ph.D. thesis, "Learning Noisy Characters, Multiplication Codes and Hardcore Predicates," August 2007.
  Faculty, Tel Aviv College.
- Vinod Vaikuntanathan, Ph.D. thesis,"Randomized Algorithms for Reliable Broadcast," October 2008.
  Faculty, University of Toronto.
- Dah-Yoh Lim, Ph.D. thesis, "The Paradigm of Partial Erasures," September 2008.
  Entrepreneur.
- Guy Rothblum, Ph.D. thesis, "Efficient and Reliable Tools for Delegating Computation," June 2009.
  Researcher, Microsoft.
- Elette Boyle, Ph.D. thesis, "Secure Multi-Party Protocols Under a Modern Lens," May 2013.
  Postdoctoral Research, Cornell University.
- Cheng Chen, Ph.D. thesis in progress.
- Ioana Ivan, Ph.D. thesis in progress.
- David Wilson, Ph.D. thesis in progress.
- Scott Ribe, B.S. thesis, "Paranoid Authentication of Network Principals and Their Communications," September 1985.
- Tony Eng, M.S. thesis, "Generalized Divertible Zero-Knowledge," May 1993.
- Yael Gertner, M.S. thesis, "Distributed Data Base Security," August 1997.

- Yoav Meshulam, M.S. thesis, “An Incremental Editor,” August 1997.
- Amit Sahai, M.S. thesis, “Minimizing Number of Pebbles in Robot Searches,” August 1997.
- Victor Boyko, M.S. thesis, “Preprocessing Discrete Log Computation,” May 1998.
- Nitin Thaper, M.S. thesis, “Using Compression for Source Based Classification of Text,” February 2001.
- Dah-Yoh Lim, M.S. thesis, “3-Round Weak Zero-knowledge Proofs for NP,” April 2004.
- Vinod Vaikuntanathan, M.S. thesis, “Distributed Computing with Imperfect Randomness,” September 2005.
- Rachel Miller, M.S. thesis, “New Cryptographic Protocols With Side-Channel Attack Security,” June 2012.

Weizmann Institute

- Zvika Brakerski, Ph.D. “Cryptographic Methods for the Clouds,” June 2011. Postdoctoral, Stanford University.
- Erez Weisbard, M.Sc thesis: “Transformation of Digital Signature Schemes into Designated Confirmer Signature Schemes,” 2003.
- Assaf Nussbaum , M.Sc thesis, “Huge Pseudorandom Graphs that Preserve Global Properties of Random Graphs,” 2003.
- Dmitriy Kharchenko, M.Sc thesis, “Proof of Plaintext Knowledge for the Ajtai-Dwork Cryptosystem,” 2004.
- Dror Eiger, M.Sc. thesis, “Proactive Secret Sharing with Partial Erasures,” 2007.
- Eran Gat, M.S. thesis, “Probabilistic Polynomial Time Algorithm with Canonical Output,” 2010.

RECENT GOVERNMENT FUNDING

- DARPA Contract Number FA8750-11-2-0225. “Computing on Encrypted Data: Theory and Applications.” 5/25/11 – 1/31/15.
- NSF Grant Number CCF-1018064. “Trustworthy Computing:Securing Programs and Data In Remote and Hostile Environments.” 9/1/10 – 8/31/13.
- NSF Grant Number CFF-0635297. “Program Obfuscation: Foundations and Applications.” 10/1/06 - 9/30/10.
- NSF Grant Number CCF-0729011. "New Handles on Program Correctness." 9/1/07 - 8/31/11.
- NSF Grant Number CCF-0514167. “Learning Fourier Coefficients”. 7/1/05 - 6/30/09.
- NSF Grant Number CNS-0430450. “Cryptographic Foundations of CyberTrust.” 9/1/04 - 8/31/07.

INVITED TALKS (SELECTED)

- Invited speaker, Indiana University, Bloomington, IN March 2014.
- Keynote speaker, Association for Computing Machinery, Delhi, India February 2014.
- Distinguished Lecturer, Weizmann Institute of Science, Rehovot, Israel December 2013.
- Distinguished Lecturer, Carnegie Mellon University, Pittsburg, PA November 2013.
- Distinguished Lecturer, Georgia Tech, Atlanta, GA November 2013.
- Distinguished Lecturer, University of Michigan-Dearborn, Dearborn, MI October 2013.
- Invited speaker, MIT Society of Women Engineers, Cambridge, MA October 2013.
- Invited Lecturer, Weizmann Institute of Science, Rehovot, Israel August 2013.
- Invited Lecturer, Microsoft Research at New England, Cambridge, MA June 2013.
- Invited speaker, Symposium on the Visions of the Theory of Computing, Berkeley, CA May 2013.
- Invited speaker, American Mathematical Society, Boston College, Boston, MA April 2013.
- Invited speaker, United States Naval Academy, Annapolis, MD April 2013.
- Distinguished Lecturer, Stony Brook University Distinguished Lecture Series, Stony Brook, NY April 2013.
- Invited speaker, Microsoft Research at Palo Alto, CA January 2013.
- Invited speaker, Innovations in Theoretical Computer Science, Berkeley, CA January 2013.
- Invited Lecturer, Oberwolfach Workshop, Oberwolfach, Germany, October 2012.
- Rothschild Lecturer, Isaac Newton Institute, Cambridge, England, April 2012.
- Invited speaker, Turing Centennial Celebration, Princeton University, New Jersey, May 2012.
- Rothschild Lecturer, Isaac Newton Institute, Cambridge, England, April 2012.
- Invited speaker, Symposium on Theoretical Aspects of Computer Science (STACS 2012), Paris, France, February 29-March 3, 2012.
- Distinguished Lecturer, University of Washington, Seattle, Washington, February 2012.
- Invited speaker, Adam Mickiewicz University Special Event, Poznan, Poland, November 2011.
- IEEE Emanual R. Piore Award Presentation, FOCS 2011, Palm Springs, CA, October 2011.
- Invited Speaker, AWM Anniversary Conference at Brown University "40 Years and Counting: AWM's Celebration of Women in Mathematics," Providence, RI, September 2011.
- Invited speaker, Courant Institute 75th Anniversary Celebration, New York, May 2011.
- Invited speaker, Stathis Zachos Retirement, New York Colloquium on Algorithms and Complexity, New York, November 2010.
- Invited speaker, Workshop on Elliptic Curves and Computation, Seattle, WA, October 2010.

- Plenary speaker, CIE 2010-Computability in Europe: Programs, Proofs, Processes, University of Azores, Portugal, July, 2010.
- Franklin Institute Award Lecturer, Fantastic Lectures in Computer Science, Drexel University, April 2010.
- Distinguished Lecturer, David Cheriton School of Computer Science, University of Waterloo, September 2009.
- Invited speaker, Department of Computer Science, Purdue University, November 2009.
- ACM Athena Award Lecturer, STOC 2009, Bethesda, Maryland, 2009.
- Plenary speaker, CanadAM09, Montreal, Quebec, Canada, 2009.
- Invited speaker, Eurocrypt, Cologne, Germany, 2009.
- Invited speaker, Women in Theory (WIT) Workshop, Princeton, NJ, 2008.
- Invited speaker, Building Bridges, a Conference on Mathematics and Computer Science in Honour of Laci Lovász, Budapest, Hungary, 2008.
- Invited speaker, Cryptographers' Track at the RSA Conference 2008, San Francisco, California, 2008.
- Invited speaker, Coxeter Lecture series, Toronto, Canada, 2006.
- 2006 Milner Lecturer, University of Edinburg, Scotland, 2006.
- Distinguished Lecturer, Columbia University, Department of Computer Science Distinguished Lecture series, 2005.
- Distinguished Lecturer, "Jon Postel Distinguished Lecture series," UCLA, Department of Computer Science, 2006.
- Distinguished Lecturer, Gerald Salton Distinguished Lecture series, Cornell University, Department of Computer Science, September 2005.
- Invited speaker, Columbia University/NYU/IBM Research Theory Day, Columbia University Computer Science Department, NY, May 2004.
- Plenary speaker, International Congress of Mathematics (ICM02), Beijing, China, August 2002.
- Plenary speaker, International Symposium on Information Theory (ISIT02), Lausanne, Switzerland, July 2002.
- Invited speaker on "Resttablity in Cryptography," Workshop on Distributed Algorithm, Marseille, France, May 2001.
- Plenary speaker in the Federated Computer Research Conference (FCRC99), 1999, on "Property Testing," Atlanta, GE, May 1999.
- Keynote speaker on "Cryptography and Complexity Theory: A Match Made in Heaven," Symposium on the Foundations of Computer Science (FOCS), Miami, FL, October 1997.
- Keynote speaker on "Multi-Party Protocols," the Principles of Distributed Computing Conference (PODC), Santa Barbara, California, August 1997.

- Invited speaker on "Property Testing: Connection to Learning and Approximation," Complexity Workshop, Oberwolfach, Germany, November 1996.
- Invited speaker, Eurocrypt96 International Conference on "Multi-Party Protocols: Past and Present," Sargosa, Spain, May 1996.
- Distinguished Lecturer on "Probabilistically Checkable Proofs and Applications to Cryptography and Approximation," University of Washington Distinguished Lecture series, Washington, Seattle, October 1995.
- Keynote speaker on "Probabilistic Proofs and Their Applications," GISI 95, Zurich, September 1995.
- Invited speaker, Frontiers of Electronic Interaction Lecture series, Frankfurt, Germany, July 1995.
- Invited speaker, Discoveries in Science Lecture series in Technion Institute of Technology, June 1995.
- Keynote speaker, 2nd Annual National Meeting of the Israeli Teachers of Mathematics Society, Jerusalem, June 1995.
- Invited talk on "Security Challenges and Solutions for Information Infrastructure," U.S.-Israel Workshop on HPCC and GII, Ramat Rachael, Jerusalem, October 1994.
- Keynote speaker, ICALP 94, Jerusalem, Israel, July 1994.
- Invited Speaker, *Grace Hopper* Conference on Women in Computing, Washington, D.C., June 1994.
- Keynote speaker on "Efficient Probabilistically Checkable Proofs and Applications to Approximation," in session on discrete mathematics at 2nd International Gauss Symposium, Munich, Germany, July 1993.
- Invited speaker on "Interactive Proofs and Applications to Approximation," 2nd Israel Symposium on Theory of Computing and Systems (ISTCS), Netanya, Israel, June 1993.
- Plenary speaker on "Efficient Probabilistically Checkable Proofs and Applications to Approximation," Jerusalem Combinatorics: an International Combinatorics Conference, Jerusalem, Israel, June 1993.
- Invited speaker on "Low Error and Efficient Multi Prover Proofs and Application to Approximation," the Israeli National Seminar series, January 1993.
- Invited speaker on "Low Error and Efficient Multi-Prover Proofs," Workshop on Complexity Theory, Oberwolfach, Germany, November 1992.
- Distinguished Lecturer on "Probabilistically Checkable Proofs and the Difficulty of Approximation," Carnegie Mellon University Distinguished Lecture series, October 1992.
- Invited survey talk on "Interactive Proofs and Applications to Cryptography and Approximation," National Science Foundation, Washington, D.C., September 1992.
- Plenary talk on "Interactive Proofs and Applications," SIAM Conference on Discrete Mathematics in Vancuver, June 1992.

- Invited speaker, AMS Bi-Annual meeting in San Francisco as of one of ten invited speakers to a day on 'Women in Mathematics', January 1991.
- Distinguished Lecturer, Maryland Computer Science Department Distinguished Lecturer series, December 1990.
- Invited speaker, International Congress of Mathematics (ICM90), Japan, August 1990.
- Keynote speaker, Sixth British Colloquium for Theoretical Computer Science, Manchester University, March 1990.
- Invited speaker, AAAS Annual Conference in New Orleans, February 1990.
- Invited speaker, Oberwolfach Workshop on Cryptography, Oberwolfach, Germany, October 1989.
- Invited Speaker on "Search for Provably Secure Cryptosystems," Boulder, Colorado, August 1989.
- Invited speaker on "The Role of Number Theory in Zero Knowledge Proofs," Workshop on Computational Number Theory, July 1988.
- Invited speaker on "Probabilistic Methods in Complexity Theory," Workshop on Randomness, Ohio State University, April 1988.
- Invited speaker on "Interactive Proof Systems," Short course on Complexity Theory held in the AMS Annual Meeting in Atlanta, January 1988.
- EECS Lecture series on "Primality Testing: 20th Century Mathematics applied to an Ancient Problem," MIT, October 1987.
- Invited speaker on "Primality Testing and Elliptic Curves," Workshop on Randomness and Computational Number Theory, Max Plank Institute, Bonn, Germany, July 1987.
- Invited speaker on " Proofs, Knowledge and Computation," 7th Annual Bar Hillel Philosophy of Science Lecture series, Hebrew University, Israel, May 1987.
- Invited speaker on "The Digital Signature Problem," in Cryptography Day held at the University of Salerno, Italy, August 1986.
- Invited speaker on "Primality Testing Using Elliptic Curves" at the 8th Columbia Theory Day, April 1986.
- Invited speaker on "Public-Key Cryptography: Encryption and Digital Signatures," Course on Cryptography, University of Amsterdam, Holland, November 1985.
- Panel Discussion on "Software Protection," MIT Communication Forum, Cambridge, Massachusetts, February 1985.
- Panel Discussion on "Privacy in Science," American Association for Advancement of Science, MIT, Cambridge, Massachusetts, April 1984.
- Invited keynote speaker on "Security in Today's Office Place," 1984 ACM Northeast Regional Conference, Lowell, Massachusetts, April 1984.

RECENT OUTREACH

- Dutch High School Students Winners of Math Tournament Talk, MIT, Cambridge, MA, October 2011.
- Keynote Address, Advantage Testing Foundation's Math Prize for Girls, MIT, Cambridge, MA, September 2011.

PUBLICATIONS

Books

- "Advances in Cryptology: Proceedings of Crypto88," S. Goldwasser (Ed.), Lecture Notes in Computer Science, Springer, February 1990.
- Goldwasser, S. and Micciancio, D. "Complexity of Lattice Problems: A Cryptographic Perspective." Kluwer international Series in Engineering and Computer Science, Kluwer Academic Publishers, March 2002.

Articles in Refereed Conferences and Journals

- Goldwasser, S., and Micali, S. "Probabilistic Encryption and How to Play Mental Poker Hiding All Partial Information." *Proceedings 14th Annual ACM Symposium on the Theory of Computing (STOC 1982)*, pages 365-377, San Francisco California, May 1982.
- Goldwasser, S., Micali, S., and Tong, P. "Why and How to Establish a Private Code on a Public Network." *Proceedings 23rd Annual Symposium on Foundations of Computer Science (FOCS 1982),* pages 134-144, Chicago, Illinois, October 1982.
- Goldwasser, S., Micali, S., and Yao, A. "Strong Signature Schemes." *Proceedings 15th Annual ACM Symposium on Theory of Computing (STOC 1983),* pages 431-439, Boston Massachusetts, April 1983. Preliminary version by the same authors appeared in Chaum, D. R. L. Rivest and A. T. Sherman eds., *Advances in Cryptology: Proceedings of Crypto 1982*, pages 211-215, 1983. Plenlum Press.
- Goldwasser, S., and Micali, S. "Probabilistic Encryption." Special issue of *J. of Computer and Systems Sciences,* 28(2):270-299, April 1984.
- Goldwasser, S., and C. Rackoff. "On Using the XOR operator as a Security Amplifier: Applications to Factoring Based Encryption." *Advances in Cryptology: Proceedings of EUROCRYPT 84, A Workshop on the Theory and Application of of Cryptographic Techniques*, volume 209 of *Lecture Notes in Computer Science*, 1985. Springer.
- Blum, M., and Goldwasser, S. "An Efficient Probabilistic Public-Key Encryption Schemes which Hides All Partial Information." G.R. Blakely and David Chaum, editors, *Advances in Cryptology: Proceedings of CRYPTO 84*, volume 196 of *Lecture Notes in Computer Science*, pages 289-299, 1985. Springer.
- Goldreich, O., Goldwasser, S., and Micali, S. "How to Construct Random Functions." *Proceedings 25th Annual Symposium on Foundations of Computer Science (FOCS 1984),* pages 464-480, West Palm Beach, FL, October 1984.

- Goldreich O., Goldwasser, S., and Micali, S. "On the Cryptographic Applications of Random Functions." G.R. Blakely and David Chaum, Ed., *Advances in Cryptography: Proceedings of CRYPTO 1984,* volume 196 of *Lecture Notes in Computer Science*, pages 276-288, 1985. Springer.
- Chor, B., Goldwasser S., Micali S., and Awerbuch B. "Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults." *Proceedings of 26th Annual Symposium on the Foundations of Computer Science (FOCS 1985),* pages 383-395, October 1985.
- Chor, B., Goldreich O., and Goldwasser S. "The Bit Security of RSA and Rabin Functions Given Partial Factorization of the Modulos." Williams, H.C., editors, *Advances in Cryptology: Proceedings of Crypto 1985,* volume 218 of *Lecture Notes in Computer Science*, pages 448-457, 1986. Springer.
- Goldwasser, S. and Sipser, M. "Private Coins versus Public Coins in Interactive Proof Systems." *Proceedings of the 18th Annual ACM Symposium on Theory of Computing (STOC 1986),* pages 59-86, Berkeley CA, May, 1986.
- Goldwasser, S., Micali, S., and Rivest, R. "A Paradoxical Solution to the Signature Problem." *Proceedings 25th Annual Symposium on Foundations of Computer Science*, pages 441-449, West Palm Beach, FL, October 1984.
- Goldwasser, S. and Kilian, J. "Almost All Primes Can be Quickly Certified." *Proceedings of the 18th Annual ACM Symposium on the Theory of Computing (STOC 1986),* pages 315-329, Berkeley, CA, May 1986.
- Aiello, B., Goldwasser, S., and Hastad, J. "On the Power of Interaction." *Proceedings of the 27th Annual Symposium on the Foundations of Computer Science (FOCS 1986),* pages 368-379, Toronto, Canada, October 1986.
- Goldreich, O., Goldwasser, S., and Micali, S. "How to Construct Random Functions." *J. of the ACM*, 33(4):792-807, October 1986.
- Goldwasser, S., Micali, S., and Rackoff, C. "The Knowledge Complexity of Interactive Proof Systems." *Proceedings of the 17th Annual ACM Symposium on Theory of Computing (STOC 1985)*, pages 291-304, Providence, RI, May 1985.
- Goldwasser, S., Micali, S., and Rivest, R. "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attack." *SIAM J. of Computing*, 17(2):281-308, April 1988.
- Ben-Or, M., Goldwasser S., Kilian J., and Wigderson A. "Multi-Prover Interactive Proofs: How to Remove Intractability Assumptions." *Proceedings of 20th Annual ACM Symposium on Theory of Computing (STOC 1988),* Chicago, Illinois, pages 113-122, May 1988.
- Ben-Or, M., Goldwasser S., and Wigderson A. "Completeness Theorems for Non-Cryptographic Fault Tolerant Distributed Computation." *Proceedings of 20th Annual ACM Symposium on Theory of Computing (STOC 1988),* Chicago, Illinois, pages 1-10, May 1988. Invited to special issue of *Journal of Computer Science and Systems*.
- Ben-Or, M., Goldreich, O., Goldwasser, S., Hastad, J., Kilian, J., Micali, S., and Rogaway, Ph."Everything Provable is Provable in Zero Knowledge." S. Goldwasser, editor, *Advances in*

Cryptology -Proceedings of the 8th Intl. Cryptology Conference (Crypto88), volume 403 of *Lecture Notes in Computer Science*, pages 37-56, 1988. Springer.

- Goldwasser, S., Micali, S., and Rackoff, C. "The Knowledge Complexity of Interactive Proof Systems." *SIAM J. of Computing*, 18(1):186-208, January 1989.
- Goldwasser, S. "Interactive Proof Systems." *Computational Complexity Theory*, J. Hartmanis (Ed.), *Proceedings of Symposia in Applied Mathematics*, vol. 38, pages 108-128, 1989.
- Bellare, M. and Goldwasser, S. "New Paradigms for Digital Signatures and Message Authentification Based on Non-Interactive Zero Knowledge Proofs." G. Brassard, editor, *Advances in Cryptology - Proceedings of 9th Annual Intl. Cryptology Conference (Crypto89)*, volume 435 of *Lecture Notes in Computer Science*, pages 194-211, 1989.
- Beaver, D. and Goldwasser, S. "Multi Party Fault Tolerant Computation with Faulty Majority." G. Brassard, editor, *Advances in Cryptology - Proceedings of 9th Annual Intl. Cryptology Conference (Crypto89)*, volume 435 of *Lecture Notes in Computer Science*, pages 589-590, 1989. Springer.
- Ben-Or, M., Goldwasser S., Kilian J., and Wigderson A. "Efficient Identification Schemes Using Two Prover Interactive Proofs." G. Brassard, editor, *Advances in Cryptology - Proceedings of 9th Annual Intl. Cryptology Conference (Crypto89)*, volume 435 of *Lecture Notes in Computer Science*, pages 498-506, 1989. Springer.
- Goldwasser, S., and M. Sipser. "Private Coins versus Public Coins in Interactive Proof Systems." Randomness and Computation, vol. 5 of *Advances in Computing Research*, JAI Press, 1989.
- Beaver, D. and Goldwasser, S. "Multi Party Fault Tolerant Computation with Faulty Majority Based on Oblivious Transfer." *Proceedings of 30th Annual Symposium on Foundations of Computer Science (FOCS89)*, Duke, NC, October 1989.
- Bellare, M., Cowen, L., and Goldwasser S. "On the Structure of Secret Key Exchange Protocols." *Proceedings of the DIMACS Workshop on Distributed Computing and Cryptography,* October 1989. Also, in Rump Session of *Crypto 1989*, pages 604-605, 1989.
- Goldwasser, S. "The Search for Provably Secure Cryptosystem." *Cryptography and Computational Number Theory*, C. Pomerance (Ed.), *Proceedings of Symposia in Applied Mathematics*, vol. 42, 1990.
- Bellare, M., Goldreich, O., and Goldwasser S. "Saving Randomness in Interactive Proofs." *Proceedings of the 31st Annual Symposium on Foundations of Computer Science (FOCS 1990)*, pages 563-572, St. Louis, Missouri, May 1990.
- Goldwasser, S. and Levin L. "Fair Computation of General Functions in Presence of Immoral Majority." A. Menezes, S. Vanstone, editors *Advances in Cryptology* (*Proceedings of CRYPTO90*, *Santa Barbara, CA, August 1990*), volume 537 of *Lecture Notes in Computer Science*,1991. Springer.
- Goldwasser, S. "Interactive Proofs and Applications." *Proceedings of the International Congress of Mathematicians,* volume 2, Japan, August 1990.
- Aiello, B., Goldwasser, S., and Hastad, J. "On the Power of Interaction." *Combinatorica* 10(1):3-25, 1990.

- Feige, U., Goldwasser S., Lovasz L., Szegedi M., and Safra S. "Approximating the Clique is Almost NP-Complete." *Proceedings of the 32nd Annual Symposium on Foundations of Computer Science (FOCS 1991)*, Puerto Rico, October 1991.
- Bellare, M., Beigel R., Feigenbaum J., and Goldwasser S. "The Complexity of Decision versus Search." *32nd Annual Symposium on Foundations of Computer Science (FOCS 1991)*, Puerto Rico, October 1991.
- Goldreich, O., Goldwasser S., and Linial N. "Fault Tolerant Distributed Computation in the Full Information Model." *Proceedings of the 32nd Annual Symposium on Foundations of Computer Science (FOCS 1991)*, Puerto Rico, October 1991.
- Goldwasser, S. and Ostrovsky, R. "Non-Interactive Zero Knowledge Proofs are Equivalent to Invariat Digital Signatures." E. Brickell, editor, *Advances in Cryptology* (*Proceedings of CRYPTO92, Santa Barbara, August 1992*), volume 740 of *Lecture Notes in Computer Science,* 1992. Springer.
- Bellare, M., Goldwasser S., Carsten L., and Russel A."Efficient Probabilistically Checkable Proofs with Applications to Approximation." *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing (STOC93)*, San Diego, CA, May 1993.
- Bellare M., Goldreich, O., and Goldwasser S. "Randmoness in Interactive Proofs." *Computational Complexity*, 4(4):319-354, 1993.
- Bellare, M., and Goldwasser, S. "The Complexity of Decision versus Search." *SIAM Journal of Computing*, 23(1):97-119, February 1994.
- Bellare, M., Goldreich O., and Goldwasser S. "Incremental Cryptography: the case of Hashing and Signing." Y. Desmedt, editor, *Advances in Cryptology* (*Proceedings of CRYPTO94*, *Santa Barbara, CA, August 1994*), volume 839 of *Lecture Notes in Computer Science*, 1994. Springer.
- Bellare, M., Goldreich O., and Goldwasser S. "Incremental Cryptography and Applications to Virus Protection." *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing (STOC95)*, pages 45-56, Las Vegas, NV, May 1995.
- Goldreich O., Goldwasser S., and Ron D. "Property Testing and its Connections to Learning and Approximation." *Proceedings of FOCS96*, Burlington, VT, October 1995. Final version Accepted to the *Journal of the ACM*.
- Bellare, M. and Goldwasser, S. "Verifiable partial key escrow". *4th ACM Conference on Computer & Communications Security,* April 1997, Zurich, Switzerland. Currently appears as *Technical Report number CS95-447, Dept of CS and Engineering, UCSD,* October 1995.
- Feige, U., Goldwasser, S., Lovasz, L., Safra, S., and Szegedi. M. "Interactive Proofs and the Hardness of Approximating Cliques. *J. of the ACM*, 43(2):268-292, March 1996.
- Goldreich, O., Goldwasser, S., and Halevi, S. "Eliminating Decryption Errors in the Ajtai-Dwork Cryptosystem." B. Kaliski, Jr., editor, *Advances in Cryptology (Proceedings of CRYPTO 1997*, *Santa Barbara, CA, August 1997*), volume 1294 of *Lecture Notes in Computer Science*, pages 105-111, Springer. 1997.
- Goldreich, O., Goldwasser, S., and Halevi, S. "Public-Key Cryptosystems from Lattice Reduction Problems." B. Kaliski, Jr., editor, *Advances in Cryptology (Proceedings of CRYPTO*

1997, *Santa Barbara, CA, August 1997*), volume 1294 of *Lecture Notes in Computer Science,* pages 112-131, 1997. Springer.

- Bellare, M., Goldwasser, S., and Micciancio, D. "Pseudo-Random Number Generation within Cryptographic Algorithms: The DSS Case." B. Kaliski, Jr., editor, *Advances in Cryptology* (*CRYPTO 1997*, *Santa Barbara, August 1997*), volume 1294 of *Lecture Notes in Computer Science*, pages 277-291, 1997. Springer..
- Goldwasser, S. "Multi-Party Computations: Past and Present." Invited paper to *Proceedings of the Sixteenth Annual ACM Symposium on Principles of Distributed Computing (PODC 1997)*, Santa Barbara, California, USA, August 21-24, 1997.
- Goldwasser, S. "New Directions in Cryptography: Twenty Some Years Later (or Cryptography and Complexity: A Match Made in Heaven)." Invited paper to the *Proceedings of the 38th Annual IEEE Symposium on Foundations of Computer Science, (FOCS 1997)*, Miami Beach, Florida, pages 314-324, October 1997.
- Goldreich, O., Goldwasser S., and Linial, N. "Fault Tolerant Computation in the Full Information Model." *SIAM J. of Computing*, 27(2):506-544, April 1998.
- Goldereich, O. and Goldwasser, S. "On the Limits of Non-Approximability of Lattice Problems." *Proceedings of 30th ACM Sym. on Theory of Computing (STOC 1998)*, Dallas, Texas, pages 1-9, May 1988. Invited to Special Issue of *JCSS*.
- Golderich, O., Goldwasser, S., and Ron, D. "Property Testing and its Connection to Learning and Approximation." *J. of the ACM*, 45(4):653-750, July 1998.
- Goldreich, O., Goldwasser, S., Lehman, E., and Ron, D. "Testing Monotonicity." *39th Annual Symposium on Foundations of Computer Science (FOCS 1998)*, Palo Alto, CA, October 1998.
- Gertner Y., Goldwasser S., and Malkin T. "A Random Server Model for Private Information Retrieval (or How to Achieve Information Theoretic PIR Avoiding Database Replication)." *2nd International Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM 1998)*, Barcelona, Spain, October 1998.
- Canetti R. and Goldwasser S. "An efficient threshold public-key cryptosystem secure against adaptively chosen ciphertext attack." In J. Stern, editor, *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May, 1999*, volume 1592 of *Lecture Notes in Computer Science*, pages 90-106, Springer, 1999.
- Goldwasser, S. and Kilian, J. "Primality Testing based on Elliptic Curves." *J. of the ACM*, 46(4):450-472, July 1999.
- Canneti, R., Goldreich, O., Goldwasser, S., and Micali, S. "Resettable Zero Knowledge." *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC 2000)*, pages 235-244, Portland, Oregon, May 2000.
- Golderich, O. and Goldwasser, S. "On the Limits of Non-Approximability of Lattice Problems." *J. of Computer and System Sciences*, 60(3):540-563, June 2000.
- Golderich, O., Goldwasser, S., Lehman, E., Ron, D., and Samorodnitsky, A. "Testing Monontonicity." *Combinatorica*, 20(3):301–337, 2000.

- Bellare, M., Fischlin, M., Goldwasser, S., and Micali, S. "Identification Protocols Secure Against Reset Attacks." In B. Pfitzmann, editor, *Advances in Cryptology - Eurocrypt 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May, 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 495-511, Springer, 2001.
- Barak, B., Goldreich, O., Goldwasser, S., and Lindell, Y. "Resettably-Sound Zero-Knowledge and its Applications." In *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science (FOCS 2001)*, pages 116-125, Las Vegas, Nevada, October 2001.
- Goldwasser, S. and Lindell, Y. "Secure Computation without Agreement." *Proceedings of the 16th Int'l Symposium on DIStributed Computing (DISC 2002)*, pages 17-32, Toulouse, France, October 2002.
- Goldwasser, S. and Tauman Kalai, Y. "On the (In)security of the Fiat-Shamir Paradigm." *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2003)*, pages 102-113, Cambridge, MA, October 2003.
- Akavia, A., Goldwasser, S., and Safra, S. "Proving Hard-Core Predicates Using List Decoding." *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2003)*, pages 146-157, Cambridge, MA, October 2003.
- Goldreich, O., Goldwasser, S., and Nussboim, A. "On the Implementation of Huge Random Objects." *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2003)*, pages 68-79, Cambridge, MA, October 2003.
- Goldwasser, S. and Waisbard, E. "Transformation of Digital Signature Schemes into Designated Confirmer Signature Schemes." *Theory of Cryptography, First Theory of Cryptography Conference (TCC 2004)*, volume 2951 of *Lecture Notes in Computer Science*, pages 77-100, 2004. Springer.
- Goldwasser, S. and Kharchenko, D. "Proof of Plaintext Knowledge for the Ajtai-Dwork Cryptosystem." *Theory of Cryptopgrahy, Second Theory of Cryptography Conference (TCC 2005)*, volume 3378 of *Lecture Notes in Computer Science*, pages 529-555, 2005. Springer.
- Goldwasser, S., Sudan, M., and Vaikuntanathan, V. "Distributed Computing with Imperfect Randomness." *19th International Symposim on Distributed Computing (DISC 2005)*, Cracow, Poland, pages 288-302, September 2005.
- Goldwasser, S. and Tauman Kalai, Y. "On the Impossibility of Obfuscation with Auxiliary Input." *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2005)*, Pittsburgh, PA, pages 553-562, October 2005.
- Goldwasser, S. and Lindell, Y. "Secure Multi-Party Computation without Agreement." *J. Cryptology* 18(3):247-287, 2005.
- Goldwasser, S., Pavlov, E., and Vaikuntanathan, V. "Fault-Tolerant Distributed Computing in Full-Information Networks." *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2006)*, Berkeley, CA, October 2006.
- Akavia, A., Goldreich, O., Goldwasser, S., and Moshkovitz, D. "On basing one-way functions on NP-hardness." *Proceedings of the 38th ACM Symposium on Theory of Computing (STOC 2006)*, Seattle, Washington, pages 701-710, May 2006.

- Chen, H., Cramer, R., Goldwasser, S., de Haan, R., and Vaikuntanathan, V. "Secure Computation from Random Error Correcting Codes." *EUROCRYPT 2007*, Barcelona, Spain, pages 291-310, May 2007.
- Goldwasser, D., Gutfreund, D., Healy, A., Kaufman, T., and Rothblum, G. "Verifying and decoding in constant depth." *Proceedings of the 39th ACM Symposium on Theory of Computing (STOC 2007)*, San Diego, CA, pages 440-449, June 2007.
- Goldwasser, S. and Rothblum, G. "On Best-Possible Obfuscation." *Theory of Cryptography, 4th Theory of Cryptography Conference (TCC 2007)*, volume 4392 of *Lecture Notes in Computer Science*, pages 194-213, 2007. Springer.
- Canetti, R., Eiger, D., Goldwasser, G., and Lim, D.Y. "How to Protect Yourself without Perfect Shredding." *35th International Colloquium on Automata, Languages and Programming (ICALP 2008)*, pages 511-523, Reykjavik, Iceland, July 2008.
- Goldwasser, S. "Program Obfuscation and One-Time Programs." *Topics in Cryptology - CT-RSA 2008, The Cryptographers' Track at the RSA Conference 2008*, San Francisco, CA, USA, April 2008, volume 4964 of *Lecture Notes in Computer Science*, pages 33-334, Springer, 2008. Invited Talk.
- Goldwasser, G., Tauman Kalai, Y., and Rothblum, G.N. "One-Time Programs." *28th International Cryptology Conference (CRYPTO 2008)*, pages 39-56, Santa Barbara, CA, July 2008.
- Goldwasser, S., Gutfreund, D., Healy, A., Kaufman, T., and Rothblum, G.N. "A (De)constructive Approach to Program Checking." *40th ACM Symposium on Theory of Computing (STOC 2008)*, pages 143-152, Victoria, (BC), Canada, May 2008.
- Goldwasser, S., Tauman Kalai, Y., and Rothblum, G. "Delegating Computation: Interactive Proofs for Muggles." *40th ACM Symposium on Theory of Computing (STOC 2008)*, pages 113-122, Victoria, (BC), Canada, May 2008.
- Goldwasser, S. "Cryptography without (Hardly Any) Secrets?" In Antoine Joux, editor, Advances in Cryptology - EUROCRYPT 2009, 28th International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 2009, volume 5479 of *Lecture Notes in Computer Science*, pages 369-370, 2009. Springer.
- Goldwasser, S. "Athena lecture: Controlling Access to Programs?" *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC 2009)*, Bethesda, MD, pages 167-168, May 31 - June 2, 2009.
- Akavia, A., Goldwasser, S., and Vaikuntanathan, V. "Simultaneous Hardcore Bits and Cryptography against Memory Attacks." In Omer Reingold, editor, *Theory of Cryptography, 6th Theory of Cryptography Conference (TCC 2009), San Francisco, CA*, volume 5444 of *Lecture Notes in Computer Science*, pages 474-495, 2009. Springer.
- Brakerski, Z., Goldwasser, S., Rothblum, G.N., and Vaikuntanathan, V. "Weak Verifiable Random Functions." In Omer Reingold, editor, *Theory of Cryptography, 6th Theory of Cryptography Conference (TCC 2010), San Francisco, CA, March 15-17, 2009*, volume 5444 of *Lecture Notes in Computer Science*, pages 558-576, 2009. Springer

- Akavia, A., Goldreich, G., Goldwasser, S., and Moshkovitz, D. "Erratum for: on basing one-way functions on NP-hardness." *Proceedings of the 42nd ACM Symposium on Theory of Computing (STOC 2010)*, pages 795-796, Cambridge, MA, 2010.
- Brakerski, Z. and Goldwasser, S. "Circular and Leakage Resilient Public-Key Encryption under Subgroup Indistinguishability - (or: Quadratic Residuosity Strikes Back)". In Tal Rabin, editor, *Advances in Cryptology, 30th Annual Cryptology Conference (CRYPTO 2010)*, volume 6223 of *Lecture Notes in Computer Science*, pages 1-20, 2010. Springer.
- Dodis, Y., Goldwasser, S., Kalai, Y.T., Peikert, C., and Vaikuntanathan, V. "Public-Key Encryption Schemes with Auxiliary Inputs." In Daniele Micciancio, editor, *Theory of Cryptography, 7th Theory of Cryptography Conference (TCC 2010)*, volume 5978 of *Lecture Notes in Computer Science*, pages 361-381, February 2010. Springer.
- Goldwasser, S. and Rothblum, G.N. "Securing Computation against Continuous Leakage." In Tal Rabin, editor, *Advances in Cryptology, 30th Annual Cryptology Conference (CRYPTO 2010)*, volume 6223 of *Lecture Notes in Computer Science*, pages 59-79, 2010. Springer.
- Goldwasser, S., Kalai, Y.T., Peikert, C., and Vaikuntanathan, V. "Robustness of the Learning with Errors Assumption." *Innovations in Computer Science (ICS 2010)*, pages 230-240, Beijing, China, January 2010.
- Goldreich, O., Goldwasser, S., and Nussboim, A. "On the Implementation of Huge Random Objects." *SIAM J. on Computing*, 39(7):2761-2822, 2010.
- Brakerski, Z., Goldwasser, S., and Tauman Kalai, Y. "Black-Box Circular-Secure Encryption Beyond Affine Functions." *Theory of Cryptography - Eighth Theory of Cryptography Conference (TCC 2011)*, volume 6597 of *Lecture Notes in Computer Science*, pages 201-218, Providence, RI, 2011. Springer.
- Boyle, E., Goldwasser, S., and Tauman Kalai, Y. "Coin Tossing with Leakage." *Proceedings of the 25th International Symposium on DIStributed Computing,* Rome, Italy, September 20-22, 2011.
- Goldreich, O., Goldwasser, S., and Halevi, S. "Collision-Free Hashing from Lattice Problems." Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation, volume 6650 of Lecture Notes in Computer Science, pages 30-39, 2011. Springer.
- Bitansky, N., Canetti, R., Goldwasser, S., Halevi, S., Tauman Kalai, Y., and Rothblum, G.N. "Program Obfuscation with Leaky Hardware**."** In Dong Hoon Lee, Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 722-739, 2011. Springer
- Goldwasser, S., Lewko, A., and Wilson. D.A. "Bounded-Collusion IBE from Key Homomorphism." In Ronald Cramer, editor, Theory of Cryptography: *Ninth IACR Theory of Cryptography Conference (TCC 2012*)*, Taormina, Italy, March 2012,* volume 7194 of *Lecture Notes in Computer Science*, pages 564-581, 2012. Springer.

- Goldwasser, S. "Pseudo-deterministic Algorithms (Invited Talk)". *29th International Symposium on Theoretical Aspects of Computer Science (STACS 2012)*, pages 29, LIPIcs 14 Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2012.
- Boyle, E., Goldwasser, S., Jain, A., and Tauman Kalai, Y. "Multiparty Computation Secure Against Continual Memory Leakage." *Proceedings of the 44th ACM Symposium on Theory of Computing (STOC),* New York, NY, May 2012.
- Akavia, A., Goldwasser, S., and Hazay, C. "Distributed Public Key Schemes Secure against Continual Leakage." *Proceedings of the 31th Annual ACM Symposium on Principles of Distributed Computing (PODC 2012)*, Funchal, Madeira, Portugal, pages 155-164, July 2012.
- Goldwasser, S. and Rothblum, G. N. "How to Compute in the Presence of Leakage." *Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science*, New Brunswick, NJ, October 2012.
- Goldreich, O., Goldwasser, S., and Ron, D. "On the Possibilities and Limitations of Pseudodeterministic Algorithms**."** *Innovations in Theoretical Computer Science (ITCS 2013),* Berkeley, CA, January 2013.
- Boyle, E., Goldwasser, S., Tessaro, S. "Communication Locality in Secure Multi-party Computation - How to Run Sublinear Algorithms in a Distributed Setting." *Theory of Cryptography Conference (TCC 2013),* pages 356-376, Toyko, Japan, March 2013.
- Goldwasser, S., Tauman Kalai, Y., Popa, R., Vaikuntanathan, V., Zeldovich, N. "How to Run Turing Machines on Encrypted Data." *International Cryptography Conference (CRYPTO 2013)*, pages 536-553, Santa Barbara, CA, August 2013.
- Goldwasser, S., Tauman Kalai, Y., Popa, R., Vaikuntanathan, V., Zeldovich, N. "Reusable garbled circuits and succinct functional encryption." *Proceedings of the 45th ACM Symposium on Theory of Computing (STOC),* pages 555-564, Stanford, CA May 2013.

Technical Reports

- Bellare, M. and Goldwasser, S. "Verifiable partial key escrow**."** Technical Report number CS95-447, Dept of CS and Engineering, University of California, San Diego, October 1995.
- Goldreich, O., Goldwasser, S., and Halevi, S. "Public-Key Cryptosystems from Lattice Reduction Problems." Electronic Colloquium on Computational Complexity (ECCC), 3(56), 1996.
- Goldreich, O., Goldwasser, S., and Ron, D. "Property Testing and its connection to Learning and Approximation." Electronic Colloquium on Computational Complexity (ECCC), 3(57), 1996.
- Goldreich, O., Goldwasser, S., and Halevi, S. "Collision-Free Hashing from Lattice Problems." Electronic Colloquium on Computational Complexity (ECCC), 3(42), 1996.
- Goldreich, O. and Goldwasser, S. "On the Limits of Non-Approximability of Lattice Problems." Electronic Colloquium on Computational Complexity (ECCC), 4(31), 1997.

- Goldreich, O., Goldwasser, S., and Halevi, S. "Eliminating Decryption Errors in the Ajtai-Dwork Cryptosystem." Electronic Colloquium on Computational Complexity (ECCC), 4(18), 1997.
- Canetti, R., Goldreich, O., Goldwasser, S., and Micali, S. "Resettable Zero-Knowledge." Electronic Colloquium on Computational Complexity (ECCC), (42), 1999.
- Goldreich, O., Goldwasser, S., and Micali, S. "Interleaved Zero-Knowledge in the Public-Key Model." Electronic Colloquium on Computational Complexity (ECCC) , 6(24), 1999.
- Bellare, M., Fischlin, M., Goldwasser, S., and Micali, S. "Identification Protocols Secure Against Reset Attacks." IACR Cryptology ePrint Archive 2000: 15, 2000.
- Barak, B., Goldreich, O., Goldwasser, S., and Lindell, Y. "Resettably-Sound Zero-Knowledge and its Applications." IACR Cryptology ePrint Archive 2001: 63, 2001.
- Goldwasser, S. and Lindell, Y. "Secure Computation Without Agreement." IACR Cryptology ePrint Archive 2002: 40, 2002.
- Goldwasser, S. and Tauman, Y. "On the (In)security of the Fiat-Shamir Paradigm." Technical Report MIT-LCS-TR-886, MIT Laboratory for Computer Science, Cambridge, MA, February 2003. Also, Electronic Colloquium on Computational Complexity (ECCC), 10(015), 2003.
- Goldreich, O., Goldwasser, S., and Nussboim, A. "On the Implementation of Huge Random Objects." Electronic Colloquium on Computational Complexity (ECCC)(045), 2003.
- Goldwasser, S. and Tauman, Y. "On the (In)security of the Fiat-Shamir Paradigm." IACR Cryptology ePrint Archive 2003: 34, 2003.
- Goldwasser, S., Gutfreund, D., Healy, A., Kaufman, T., and Rothblum, G. N. "A (De)constructive Approach to Program Checking." Electronic Colloquium on Computational Complexity (ECCC), 14(047) , 2007.
- Canetti, R., Eiger, D., Goldwasser, S., and Lim, D-Y. „How to Protect Yourself without Perfect Shredding." IACR Cryptology ePrint Archive 2008: 291, 2008.
- Brakerski, Z., Goldwasser, S., and Tauman Kalai, Y. "Black-Box Circular-Secure Encryption Beyond Affine Functions." IACR Cryptology ePrint Archive 2009: 485, 2009.
- Brakerski, Z. and Goldwasser, S. "Circular and Leakage Resilient Public-Key Encryption Under Subgroup Indistinguishability (or: Quadratic Residuosity Strikes Back)." IACR Cryptology ePrint Archive 2010: 226, 2010.
- Boyle, E., Goldwasser, S., and Tauman Kalai, Y. "Coin Tossing with Leakage." IACR Cryptology ePrint Archive 2011: 291, 2011.
- Gat, E. and Goldwasser, S. "Probabilistic Search Algorithms with Unique Answers and Their Cryptographic Applications." Electronic Colloquium on Computational Complexity (ECCC), 18: 136, 2011.
- Boyle, E., Goldwasser, S., and Tauman Kalai, Y. "Leakage-Resilient Coin Tossing." IACR Cryptology ePrint Archive 2011: 291, 2011.

- Goldwasser, S., Lin, H., and Rubinstein, A. “Delegation of Computation without Rejection Problem from Designated Verifier CS-Proofs.” IACR Cryptology ePrint Archive 2011: 456, 2011.
- Bitansky, N., Canetti, R., Goldwasser, S., Halevi, S., Tauman Kalai, Y., and Rothblum, G. N. “Program Obfuscation with Leaky Hardware**.”** IACR Cryptology ePrint Archive 2011: 660, 2011.
- Goldwasser, S. and Rothblum, G. N. “How to Compute in the Presence of Leakage.” Electronic Colloquium on Computational Complexity (ECCC), 19: 10, 2012.
- Goldreich, O., Goldwasser, S., and Ron, D. “On the possibilities and limitations of pseudodeterministic algorithms.” Electronic Colloquium on Computational Complexity (ECCC), 19: 101, 2012.
- Boyle, E., Goldwasser, S., Ivan, I. “Functional Signatures and Pseudorandom Functions.” IACR Cryptology ePrint Archive 2013: 401, 2013.
- Cohn, H., Goldwasser, S., Tuaman Kalai, Y. “The Impossibility of Obfuscation with a Universal Simulator.” The Computing Research Repository (CoRR), 1401.0348 January 2014.