Biographical Data

Michael J. Fischer

August 22, 2017

Personal

Born: Ann Arbor, Michigan, April 20, 1942.

Married: Alice E. Waltz, June 1963.

Children: Edward, b. 1969.
Robert, b. 1972.
David, b. 1978.

Education

Graduate (1960) of Ann Arbor High School, Ann Arbor, Michigan.

Higher degrees:

Bachelor of Science in Mathematics University of Michigan	December 1963
Master of Arts in Applied Mathematics Harvard University	June 1965
Doctor of Philosophy in Applied Mathematics Harvard University *Dissertation:* "Grammars with Macro-like Productions." *Advisor:* Professor Sheila A. Greibach	June 1968

Employment

Yale University	
Professor of Computer Science	1981–
Director of Graduate Studies, Computer Science	1992–1999
Director of Undergraduate Studies, Computer Science	1987–1988
University of Washington	
Professor of Computer Science	1975–1981
Director, Computer Science Laboratory	1976–1979
Massachusetts Institute of Technology	
Associate Professor of Electrical Engineering	1973–1975
Assistant Professor of Mathematics	1969–1973
Carnegie-Mellon University	
Assistant Professor of Computer Science	1968–1969
Harvard University	
Teaching Fellow	1965–1967

Summer and Visiting Positions:

University of the Saarland Guest of the Sonderforschungsbereich 124	Fall 1988
Georgia Institute of Technology Visitor in Computer Science	Spring 1980
Eidgenossische Technische Hochschule, Zurich Guest of the Research Institute in Mathematics	Summer 1975

University of Frankfurt Gastprofessor	Summer 1974
University of Toronto Visiting Associate Professor	Spring 1974
University of Warwick Senior Visiting Fellow	Summer 1972
IBM Research Laboratories, research	Summer 1967
Bell Telephone Laboratories, research	Summer 1966
Harvard University, research assistant	Summer 1965
University of Michigan, research assistant	Summer 1964
Lawrence Radiation Laboratory, laboratory technician	Summer 1963
John Hancock Mutual Life Insurance Co., summer student	Summers 1961 and 1962

Honors

Phi Beta Kappa

Phi Kappa Phi

Listed in *Who's Who in America*, *Who's Who in the World*, and *Who's Who in the East*, Marquis Who's Who, Inc., various editions, 1980—.

Selected as ACM Fellow, 1996.

Received "2001 PODC Most Influential Paper Award" with Nancy Lynch and Michael Paterson for refereed publication [30]. Certificate and prize presented August 28, 2001, at the 20th ACM Symposium on Principles of Distributed Computing, Newport, Rhode Island. Prize subsequently renamed as the "Edsger W. Dijkstra Prize in Distributed Computing".

Professional Society Memberships

Association for Computing Machinery

SIGACT (Special Interest Group on Automata and Computability Theory)

European Association for Theoretical Computer Science

American Mathematical Society

Service to Research Community

Member of Technical Committee on Mathematical Foundations of Computing, IEEE Computer Society, 1970–.

Member of program committees, ACM Symposia on Theory of Computing, 1970, 1971, 1972 and 1976.

Secretary-Treasurer, ACM SIGPLAN (Special Insterest Group on Programming Languages), 1971–73.

Guest editor for special issue, *Journal for Computer and System Sciences*, 1972.

Co-organizer (with Professor Meyer), Project MAC Workshop Conference on Concrete Computational Complexity, 1973.

Local Arrangements Chairman for the ACM SIGACT/SIGPLAN Conference on Principles of Programming Languages, 1973.

Member of editorial board, *Journal of Computer Languages*, 1975–85.

Associate Editor, *ACM Transactions on Mathematical Software*, 1976–77.

Member of editorial board, *Acta Informatica*, 1976–.

Program Chairman, 17th IEEE Symposium on Foundations of Computer Science, 1976.

Program Chairman, 11th ACM Symposium on Theory of Computing, 1979.

Area Editor for Algorithms and Complexity Theory, *Journal of the Association for Computing Machinery*, 1979–1982.

Member of editorial board, *Journal of Algorithms*, 1979–1984.

Program Chairman, ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing, August 1982.

Member of program committee, 23rd IEEE Symposium on Foundations of Computer Science, October 1982.

Member of program committee, 10th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages, January 1983.

Member of organizing committee, Symposium on Mathematical Methods for VLSI, Oberwolfach, Germany, November-December, 1983.

Editor-in-Chief, *Journal of the Association for Computing Machinery*, 1982–1986.

Member of executive advisory board for "The Encyclopedia of Physical Science and Technology", Academic Press, 1984–.

Member of editorial board, Wiley–Teubner Series in Computer Science, 1985–.

Member of program committee, Conference on Theoretical Aspects of Reasoning about Knowledge, Asilomar, California, March 1986.

Member of organizing committee, Workshop on Theory and Practice of Fault Tolerant Computing, Asilomar, California, March 1986.

Member of program committee, 18th ACM Symposium on Theory of Computing, May 1986.

Member of advisory board for the journal, *Information and Computation* (formerly *Information and Control*), 1986–1990.

Member of ACM Editorial Committee, 1986–1989.

Member of program committee, 28th IEEE Symposium on Foundations of Computer Science, October 1987.

Member of organizing committee, Symposium on Mathematical Methods for VLSI and Distributed Computing, Oberwolfach, Germany, November, 1987.

Member of program committee, 7th ACM Symposium on Principles of Distributed Computing, August 1988.

Member of program committee, 8th ACM Symposium on Principles of Distributed Computing, August 1989.

Member of program committee, 3rd Conference on Theoretical Aspects of Reasoning about Knowledge, Asilomar, California, March 1990.

Member of program committee, 15th International Symposium on Mathematical Foundations of Computer Science, Banská Bystrica, Czechoslovakia, August 1990.

Member of organizing committee, Symposium on Mathematical Methods for VLSI and Distributed Computing, Oberwolfach, Germany, June, 1991.

Member of program committee, 13th ACM Symposium on Principles of Distributed Computing, August 1994.

Member of program committee, 21st IEEE International Conference on Distributed Computing Systems (ICDCS-21), April 16–19, 2001 in Phoenix, Arizona.

Member of program committee, 5th IEEE International Symposium on Network Computing and Applications (IEEE NCA'06), July 24–26, 2006, Cambridge, MA, USA.

Member of program committee, 10th International Conference on Principles of Distributed Systems (OPODIS'06), December 12–15, 2006, Bordeaux, France.

Program co-chair, 12th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2010), September 20–22, 2010, New York City, USA.

Member of program committee, 33rd Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC), July 2014, Paris, France.

Public Service

Founding member of *TrueVote Connecticut* (TrueVoteCT.org), a public-service organization concerned with voting technology and election integrity in Connecticut, established January 5, 2005.

Vice-chair of State of Connecticut Voting Technology Standards Board. Appointed to board by Governor Jodi Rell; elected vice-chair by the board members. 2005–06.

Member of Board of Advisors (pdf) for Verified Voting.org and Verified Voting Foundation, January 2013–.

Member of the Board of Directors of the Yale Figure Skating Club, Inc., ≈1985–present. Most recents term as President, 2009-2015. Vice-president, 2015–.

Consulting

Applied Data Research on the AMBIT/G project, 1970.

Research and Consulting, Inc., 1974–75.

Xerox Palo Alto Research Center, 1982.

Kencast, Inc., 1994–.

Service on National and International Committees

Committee on Recommendations for U.S. Army Basic Scientific Research, 1978–81.

Advisory Committee to the National Science Foundation, 1978–81.

Review committee for Coordinated Experimental Research program of the National Science Foundation, February 1982.

Site visit panel for Coordinated Experimental Research program of the National Science Foundation, November 1984, February 1988.

Member of the Kosaraju Study Group of the Advisory Committee for Computer Research, National Science Foundation that produced the report "Meeting the Basic-Research Needs of Computer Science", December 1986.

Member of final panel for Coordinated Experimental Research program of the National Science Foundation, February 1987.

Elected member of board of directors of The Computing Research Association, 1988–91.

Founding member of CRA subcommittee on the Status of Women in Computer Science, 1990–93.

Chair of international scientific advisory board (Fachbeirat) for the Max–Planck–Institute für Informatik in Saarbrücken, Germany, 1993–2006.

Member of subcommittee of the Scientific Academic Advisory Committee (SAAC) of the Weizmann Institute of Science, Rehovot, Israel, to review the computer science program, November 4–6, 1998.

Member of the External Advisory Board, Department of Computer Science and Engineering, University of Connecticut, 2000–2014.

Guest professor of Wuhan University and member of Academic Committee of the State Key Laboratory on Software Engineering, Wuhan, China, 2001–03.

External reviewer in the Chancellor's assessment process of the Department of Computer Science and Engineering at the University of Connecticut, April 29–May 1, 2001.

Co-organizer (with Robert Grober) of symposium, "Voting in an e-Democracy", Yale University, April 2, 2004. (See URL `http://www.eng.yale.edu/evoting/`.)

Member of evaluation team for Internaltional Max-Planck Research School for computer science in Saarbrücken, Germany, October 11–12, 2004.

Invitations to Speak and/or Participate

IBM Symposium on the Complexity of Computer Computations, New York, April 1972.

Symposium on Algorithms and Complexity Theory, Oberwolfach, Germany, November 1972.

American Mathematical Society Symposium on Complexity of Real Computational Processes, April 1973.

Symposium on Automata Theory and Formal Languages, Oberwolfach, November 1973.

Symposium on Algorithms and Complexity Theory, Oberwolfach, October 1974.

Second GI Conference on Automata Theory and Formal Languages, Kaiserslautern, May 1975.

Annual meeting of the Association for Symbolic Logic, St. Louis, January 1977.

Symposium on Algorithms and Complexity Theory, Oberwolfach, Germany, October 1977.

Workshop on Interprocess Communication in Highly Distributed Systems, Georgia Institute of Technology, November 20–22, 1978.

Distinguished Lecturer Series in Computer Science and Statistical Computing, University of Texas at Dallas (2 lectures), January 29 and 31, 1979.
Title: "On the Complexity of Synchronization Problems."

Symposium on Algorithms and Complexity Theory, Oberwolfach, Germany, October 1979.
Title: "Concurrent Graph Searching."

Symposium on Efficient Algorithms, Oberwolfach, Germany, February 1981.
Title: "Using Clocks to Improve the Efficiency of Distributed Algorithms."

Distinguished Lecturer Series, Brown University, December 9, 1981.
Title: "Distributed Appointment Calendars."

Conference on Foundations of Computation Theory, Borgholm, Sweden, August 1983.
Title: "The Consensus Problem in Unreliable Distributed Systems (A Brief Survey)."

Symposium on Mathematical Methods for VLSI, Oberwolfach, Germany, November and December, 1983.
Title: "On Distributed Consensus and its Implications for VLSI."

Invited lecture, Columbia Theory Day, New York, March 22, 1985.
Title: "Robust and Verifiable Cryptographically Secure Elections."

Invited address, Workshop on Fault Tolerant Computing, Asilomar, California, March 17–19, 1986.
Title: "A Theoretician's View of Fault Tolerance."

Centenniel Lecture, Georgia Institute of Techology, May 21, 1986.
Title: "Trends in the Theory of Distributed Computing."

Distinguished Lecture, University of Washington, October 9, 1986.
Title: "Trends in the Theory of Distributed Computing,"

Distinguished Lecture, Purdue University, April 13, 1987.
Title: "Trends in the Theory of Distributed Computing,"

Symposium on Mathematical Methods for VLSI and Distributed Computing, Oberwolfach, Germany, November, 1987.
Title: "Relative Knowledge and Belief."

Invited address, HAL Institute of Computer Technology: Osaka campus, September 13, 1988; Nagoya campus, September 14, 1988.
Title: "A Theoretical Approach to Fault-Tolerant Distributed Computing."

Invited address, Symposium on Formal Techniques in Real-Time and Fault-Tolerant Systems, University of Warwick, September 22–23, 1988.
Title: "Reasoning about Uncertainty in Fault-Tolerant Distributed Systems."

Symposium on Complexity Theory, Oberwolfach, Germany, November, 1988.
Title: "Communicating a Secret Bit without Cryptography."

DIMACS Workshop on Connections between Distributed Computing and Cryptography, Princeton, New Jersey, October 4–6, 1989.
Title: "Secret Bit Transmission using a Random Deal of Cards."

Invited address, "Theoretical Computer Science Day," Johns Hopkins University, Baltimore, Maryland, November 17, 1989.
Title: "Secret Bit Transmission using a Random Deal of Cards."

NSF Collaboration Technology and Coordination Theory Workshop, Washington, D.C., June 2–5, 1991.
Title: "Decision Making Based on Practical Knowledge" (presentation of research progress on joint NSF grant).

Symposium on Mathematical Methods for VLSI and Distributed Computing, Oberwolfach, Germany, June 23–29, 1991.
Title: "Multiparty Secret Key Exchange Using a Random Deal of Cards."

Invited speaker, *10th Annual ACM Symposium on Principles of Distributed Computing*, Montreal, Canada, August 19–21, 1991.
Title: "Theory of Distributed Computing: A Decade Later."

Keynote speaker, *60th Birthday Celebration for Professor Günter Hotz*, Saarbrücken, Germany, November 15, 1991.
Title: "Decision Making in the Presence of Noise."

Invited talk, *Weizmann Workshop on Probabilistic Proof Systems And Cryptography, Program Checking And Approximation Problems*, Rehovot, Israel, January 10–13, 1994.
Title: "On the Indistinguishability of Probabilistic Ensembles."

Invited speaker, *Symposium to honor Juris Hartmanis & Richard Stearns 1993 Turing Award Recipients*, Albany and Schenectady, New York, March 17–18, 1994.
Title: "Indistinguishability Relations as Measures of Approximation in Probabilistic Computation."

Invited speaker, *Iowa State 25th Anniversary Celebration, Ames Iowa, April 18, 1994*
Title: "The Role of Theory in the Practical World of Computing."

Invited speaker, *Festkolloquium in celebration of the 60th birthday of Herrn Professor Dr. Arnold Schönhage*, Rheinische Friedrich-Wilhelms-Universität, Bonn, December 1, 1994.
Title: "Indistinguishability Relations as Measures of Approximation in Probabilistic Computation."

Invited speaker for "Distinguished Seminar Series", Washington University, St. Louis, October 11, 1996.
Title: "Reliable Satellite Broadcast of Large Digital Objects."

Invited panelist to "Olmsted Symposium on Instilling Ethics", Yale University, February 27–28, 1998.

Keynote speaker, "Fourth Annual International Computing and Combinatorics Conference (COCOON)", Taipei, Taiwan, August 12–14, 1998.
Title: "Estimating Parameters of Monotone Boolean Functions".

Keynote speaker, "International Symposium on Distributed Computing", Bratislava, Slovac Republic, September 27, 1999.
Title: "What Have We Learned from Two Decades of Distributed Computing Research?"

Invited panelist, "Internet Policy Institute e-Voting Workshop", Arlington, Virginia, October 11–12, 2000.

Invited "Laudatio" address, honorary doctorate degree award ceremony for Professor Günter Hotz, held at the University of Paderborn, Germany, December 15, 2000.
Title: "Günter Hotz—Eminent Master of Computer Science".

Invited speaker, "International Symposium on Software Engineering (ISES'01)", Wuhan, China, March 24, 2001.
Title: "A Simple Game for the Study of Trust in Distributed Systems".

Invited panel moderator, "Regulating Search?: A Symposium on Search Engines, Law, and Public Policy," Yale Law School, December 3, 2005.

Invited participant, "Workshop on Data-Intensive Scalable Computing in Education (DISC 2008)", University of Washington, Seattle, July 16-18, 2008.

Invited speaker, "Lynch Celebration" at PODC'08, Toronto, Ontario, Canada, August 20, 2008.
Title: "Evolution of Distributed Computing Theory: From concurrency to networks and beyond".

Invited speaker, "Mike66 Workshop", University of Warwick, England, September 18, 2008.
Title: "Analysis of Think-a-Dot". (Joint work with Albert R. Meyer and Michael S. Paterson.)

Invited speaker, "Workshop on Decentralized Mechanism Design, Distributed Computing, and Cryptography", Nassau Inn, Princeton, NJ, June 3-4, 2010. Sponsored by DIMACS and the Princeton Center for Computational Intractability.
Title: "Privacy-Enhanced Vickrey Auctions". (Joint work with René Peralta.)

Invited participant, "Meeting on Privacy-Enhancing Cryptography", National Institute of Standards and Technology, Gaithersburg, Maryland, December 8–9, 2011.

Invited panelist, "Apple vs. the FBI: A discussion with Professors Kyle Jensen (SOM), John Witt (Law), Michael Fischer (Computer Science-Cryptography), and Emily Bazelon (Law / NY Times)", Yale School of Management, March7, 2016. Video link.

Invited speaker, "The Impact of Algorithms (IOT) on our Daily Lives", Branford Rotary Club Distinguished Speaker Program, March 9, 2016.

Invited speaker, Symposium on "Programming: Logics, Models, Algorithms and Concurrency", Austin, Texas, April 29–30, 2016. Symposium organized to recognize Jayadev Misra's accomplishments on the occasion of his retirement.
Title: "Why Computer Science Needs Abstract Models". Video link.

Invited speaker to Challenges of Artificial Intelligence, New Technologies and Robots Workshop, Information Society Project, Yale Law School, May 30, 2016.
Title: "Eternally Flawed AI Systems".

Invited panelist, "Hacking the Election" conference, Information Society Project, Yale Law Wchool, September 20, 2016. Video link to panel 2.

Invited speaker, Celebration in Honor of Albert Meyer, M.I.T., Cambridge, Mass., Nov. 11, 2016.
Title: "The Many Faces of Complexity: Albert Meyer's Early Explorations".

Research Grants and Contracts

Co-principal investigator on NSF Grant DCR74–12997-A01, "Algorithmic Complexity," to M.I.T., 1974–77.

Co-principal investigator on NSF Grant MCS77–02474, "Semantics and Complexity of Computation," 1977–80.

Principal investigator on subcontract to Georgia Institute of Technology, "Design and Analysis of Distributed Algorithms," 1980.

Principal investigator on ONR Contract N00014–80–C–0221, "Design and Analysis of Distributed Algorithms," 1979–81.

Co-principal investigator on NSF Grant MCS80–03337, "Theory of Advanced Computing Structures," 1980–81.

Co-principal investigator on NSF Grant MCS80–04111, "A Functionally Integrated Environment for Distributed Computing," 1980–81.

Principal investigator on subcontract to University of Washington, "Design and Analysis of Distributed Algorithms," 1981.

Principal investigator on NSF Grant MCS81–16678, "Theory of Advanced Computing Structures," 1981–84.

Principal investigator on ONR Contract N00014–82–K–0154, "Design and Analysis of Distributed Algorithms," 1982–88.

Co-principal investigator on NSF Grant MCS–8305382, "Theory of Cryptographic Protocols," 1983–84.

Principal investigator on NSA Grant MDA904–84-H-0004, "Theory of Cryptographic Protocols," 1984–87.

Principal investigator on NSF Grant CCR–8405478, "Theory of Algorithms and Distributed Systems", 1984–89.

Co-principal investigator on NSF Grant CCR–8709818, "Complexity Bounds in Parallel Computation", 1987–89.

Co-principal investigator on NSF Grant IRI–9015570, "Decision-Making Based on Practical Knowledge", 1990–92.

Principal investigator for project on "Modeling Belief in Security and Trust Policies", 1999–2001.

Co-principal investigator on NSF Grant CCR–0081823, "ITR: Discreet Proofs for Electronic Commerce Applications", 2000–02.

Principal investigator for Simons Postdoctoral Fellowship Award Grant for Theoretical Computer Science, 2011–13. (Fellow: Georgios Zervas; faculty mentor: Prof. Joan Feigenbaum.)

Doctoral Theses Supervised

David S. Johnson, "Near-Optimal Bin Packing Algorithms," Dept. of Electrical Engineering, M.I.T., May 1973.

Mitchell Wand, "Mathematical Foundations of Language Theory," Dept. of Mathematics, M.I.T., May 1973.

Michael M. Hammer, "Minimally Predictive Grammars and Transformations into Deterministic Top-Down Form," Dept. of Electrical Engineering, M.I.T., August 1973.

Frances F. Yao, "The Complexity of Computing the i-th Largest Element," Dept. of Mathematics, M.I.T., August 1973.

Richard J. Bonneau, "Fast Polynomial Operations Using the Fast Fourier Transform," Dept. of Mathematics, M.I.T., January 1974.

Gary L. Peterson, "The Complexity of Parallel Processes", Dept. of Computer Science, University of Washington, August 1979.

Karl Abrahamson, "Decidability and Expressiveness of Logics of Processes," Department of Computer Science, University of Washington, August 1980.

Nathaniel Mishkin, "Managing Permanent Data Objects," Department of Computer Science, Yale University, December 1984.

Josh D. Cohen Benaloh, "Verifiable Secret-Ballot Elections," Department of Computer Science, Yale University, December 1987.

Ruben Michel, "Knowledge in Distributed Byzantine Environments," Department of Computer Science, Yale University, May 1990.

Rebecca N. Wright, "Achieving Perfect Secrecy Using Correlated Random Variables," Department of Computer Science, Yale University, November 1994.

Sophia A. Paleologou, "Probabilistic Decision Making in Games and Cryptographic Protocols," Department of Computer Science, Yale University, May 1995.

Zoë Diamadi, "Societies of Randomly Interacting Finite-State Automata," Department of Computer Science, Yale University, December 2004. [Co-advised with James Aspnes.]

Hong Jiang, "Stabilizing Computation in Distributed Systems," Department of Computer Science, Yale University, December 2007.

Xueyuan Su, "Efficient Fault-Tolerant Infrastructure for Cloud Computing," Department of Computer Science, Yale University, December 2013.

Syta, Ewa, "Identity Management through Privacy-Preserving Authentication," Department of Computer Science, Yale University, December 2015. [Co-advised with Bryan Ford.]

Publications and Patents

Patents

1. M. Fischer and S. Paleologou. *Method and System for Error-Free Data Transfer*. U.S. patent number 6,012,159, issued January 4, 2000. Assigned to KenCast, Inc., Stamford, CT.
2. W. E. Steele, M. Fischer, and S. Paleologou. *Method and System for Reliable Broadcasting of Data Files and Streams*. U.S. patent number 6,272,658, issued August 7, 2001. Assigned to KenCast, Inc., Stamford, CT.
3. W. E. Steele, M. Fischer, and S. Paleologou. *Method and System for Reliable Broadcasting of Data Files and Streams*. U.S. patent number 6,567,948, issued May 20, 2003. Assigned to KenCast, Inc., Stamford, CT.
4. M. J. Fischer, H. L. Wolfgang, and W. Fang. *System, Method and Apparatus for FEC Encoding and Decoding*. U.S. patent number 7,533,324, issued May 12, 2009. Assigned to KenCast, Inc., Stamford, CT.
5. W. Fang, M. J. Fischer, and H. L. Wolfgang. *System, Method and Apparatus for Reducing Blockage Losses on Information Distribution Networks*. U.S. patent number 7,739,580, issued June 15, 2010. Assigned to KenCast, Inc., Stamford, CT.

Papers in Refereed Journals

6. B. A. Galler and M. J. Fischer. An improved equivalence algorithm. *Commun. ACM*, 7(5):301–303, 1964.
7. B. A. Galler and M. J. Fischer. The iteration element. *Commun. ACM*, 8(6):349, 1965.
8. M. J. Fischer and A. L. Rosenberg. Real-time solutions of the origin-crossing problem. *Math. Syst. Theory*, 2(3):257–263, 1968.
9. R. A. Wagner and M. J. Fischer. The string-to-string correction problem. *J. ACM*, 21(1):168–173, 1974.
10. M. J. Fischer and L. J. Stockmeyer. Fast on-line integer multiplication. *J. Comput. Syst. Sci.*, 9(3):317–331, 1974.
11. N. A. Lynch, A. R. Meyer, and M. J. Fischer. Relativization of the theory of computational complexity. *Trans. Am. Math. Soc.*, 220:243–287, 1976.
12. J. I. Seiferas, M. J. Fischer, and A. R. Meyer. Separating nondeterministic time complexity classes. *J. ACM*, 25(1):146–167, 1978.
13. M. J. Fischer and R. E. Ladner. Propositional dynamic logic of regular programs. *J. Comput. Syst. Sci.*, 18(2):194–211, 1979.
14. N. Pippenger and M. J. Fischer. Relations among complexity measures. *J. ACM*, 26(2):361–381, 1979.
15. R. E. Ladner and M. J. Fischer. Parallel prefix computation. *J. ACM*, 27(4):831–838, October 1980.
16. M. J. Fischer and M. S. Paterson. The fast skew-closure algorithm. *L'Enseignement Mathematique*, XXVI(3–4):345–360, 1980.
17. N. A. Lynch and M. J. Fischer. On describing the behavior and implementation of distributed systems. *Theoretical Comput. Sci.*, 13:17–43, 1981.
18. A. Borodin, M. J. Fischer, D. G. Kirkpatrick, N. A. Lynch, and M. Tompa. A time-space tradeoff for sorting on non-oblivious machines. *J. Comput. Syst. Sci.*, 22(3):351–364, 1981.
19. G. Galbiati and M. J. Fischer. On the complexity of 2-output boolean networks. *Theoretical Comput. Sci.*, 16(2):177–185, 1981.

20. J. E. Burns, P. Jackson, N. A. Lynch, M. J. Fischer, and G. L. Peterson. Data requirements for implementation of N-process mutual exclusion using a single shared variable. *J. ACM*, 29(1):183–205, January 1982.
21. M. J. Fischer, N. D. Griffeth, and N. A. Lynch. Global states of a distributed system. *IEEE Trans. on Softw. Eng.*, SE–8(3):198–202, 1982.
22. M. J. Fischer and N. A. Lynch. A lower bound for the time to assure interactive consistency. *Inf. Process. Lett.*, 14(4):183–186, 1982.
23. M. J. Fischer, A. R. Meyer, and M. S. Paterson. $\Omega(n \log n)$ lower bounds on length of Boolean formulas. *SIAM J. Comput.*, 11(3):416–427, 1982.
24. R. J. Fowler, A. B. Struble, P. A. Thiemens, S. C. Vestal, M. J. Fischer, T. H. Kehl, and E. D. Lazowska. The CSL switch: A microcomputer-controlled multicomputer front-end. *J. Digital Syst.*, VI(3/4):265–278, 1982.
25. M. J. Fischer and S. L. Salzberg. Finding a majority among N votes. *J. Algorithms*, 3(4):375–379, 1982. Solution to Problem 81–5 in Problems section.
26. D. Dolev, M. J. Fischer, R. J. Fowler, N. A. Lynch, and H. R. Strong. An efficient algorithm for Byzantine agreement without authentication. *Inf. and Contr.*, 52(3):257–274, 1982.
27. E. Arjomandi, M. J. Fischer, and N. A. Lynch. Efficiency of synchronous versus asynchronous distributed systems. *J. ACM*, 30(3):449–456, July 1983.
28. N. A. Lynch and M. J. Fischer. A technique for decomposing algorithms which use a single shared variable. *J. Comput. Syst. Sci.*, 27(3):350–377, December 1983.
29. M. J. Fischer and M. S. Paterson. Storage requirements for fair scheduling. *Inf. Process. Lett.*, 17(15):249–250, 1983.
30. M. J. Fischer, N. A. Lynch, and M. S. Paterson. Impossibility of distributed consensus with one faulty process. *J. ACM*, 32(2):374–382, April 1985.
31. M. J. Fischer, N. A. Lynch, and M. Merritt. Easy impossibility proofs for distributed consensus problems. *J. Distrib. Comput.*, 1:26–39, 1986. Reprinted as other publication [55].
32. N. A. Lynch, N. D. Griffeth, M. J. Fischer, and L. J. Guibas. Probabilistic analysis of a network resource allocation algorithm. *Inf. and Contr.*, 68(1–3):47–85, Jan/Feb/Mar 1986.
33. M. J. Fischer and N. Immerman. Interpreting logics of knowledge in propositional dynamic logic with converse. *Inf. Process. Lett.*, 25(3):175–181, May 1987.
34. A. Broder, D. Dolev, M. J. Fischer, and B. Simons. Efficient fault-tolerant routings in networks. *Inf. and Comp.*, 75(1):52–64, October 1987.
35. M. J. Fischer, N. A. Lynch, J. E. Burns, and A. Borodin. Distributed FIFO allocation of identical resources using small shared space. *ACM Trans. Prog. Lang. Syst.*, 11(1):90–114, January 1989.
36. M. J. Fischer, N. D. Griffeth, L. Guibas, and N. A. Lynch. Optimal placement of identical resources in a tree. *Inf. and Comp.*, 96(1):1–54, January 1992.
37. M. J. Fischer, S. Moran, and G. Taubenfeld. Space-efficient asynchronous consensus without shared memory initialization. *Inf. Process. Lett.*, 45:101–105, 1993.
38. M. J. Fischer and R. N. Wright. An application of game-theoretic techniques to cryptography. In J.-Y. Cai, editor, *Advances in Computational Complexity Theory*, volume 13 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 99–118. American Mathematical Society, 1993.
39. M. J. Fischer. Lambda-calculus schemata. *Lisp and Symbolic Comput.*, 6(3/4):259–288, November 1993.
40. M. J. Fischer and M. S. Paterson. Fishspear: A priority queue algorithm. *J. ACM*, 41(1):3–30, January 1994.

41. Y. Afek, H. Attiya, A. Fekete, M. Fischer, N. Lynch, Y. Mansour, D.-W. Wang, and L. Zuck. Reliable communication over unreliable channels. *J. ACM*, 41(6):1267–1297, November 1994.
42. M. J. Fischer and R. N. Wright. Bounds on secret key exchange using a random deal of cards. *J. Cryptology*, 9(2):71–99, 1996.
43. M. J. Fischer, S. Micali, and C. Rackoff. A secure protocol for the oblivious transfer (extended abstract). *J. Cryptology*, 9(3):191–195, 1996.
44. M. J. Fischer, S. Moran, S. Rudich, and G. Taubenfeld. The wakeup problem. *SIAM J. Comput.*, 25(6):1332–1357, December 1996.
45. M. J. Fischer and M. S. Paterson. Optimal layout of edge-weighted forests. *Discrete Applied Mathematics*, 90(1–3):135–159, January 1999.
46. M. J. Fischer and M. Merritt. Appraising two decades of distributed computing theory research. *Distributed Computing*, pages 239–247, 2003.
47. D. Greenbaum, S. M. Douglas, A. Smith, J. Lim, M. Fischer, M. Schultz, and M. Gerstein. Computer security in academia—a potential roadblock to distributed annotation of the human genome. *Nature Biotechnology*, 22(6):771–772, June 2004.
48. D. Angluin, J. Aspnes, Z. Diamadi, M. J. Fischer, and R. Peralta. Computation in networks of passively mobile finite-state sensors. *Distributed Computing*, 18(4):235–253, 2006. DOI 10.1007/s00446-005-0138-3.
49. D. Angluin, J. Aspnes, M. J. Fischer, and H. Jiang. Self-stabilizing population protocols. *ACM Trans. Auton. Adapt. Syst.*, 3(4):1–28, 2008.
50. J. A. Montenegro, M. J. Fischer, J. Lopez, and R. Peralta. Secure sealed-bid online auctions using discreet cryptographic proofs. *Mathematical and Computer Modelling*, 57(11–12):2583 – 2595, 2013. Special issue on Information System Security and Performance Modeling and Simulation for Future Mobile Networks.

Other Publications

Key: $**$ invited paper appearing in published proceedings volume.
$*$ paper accepted for presentation at conference after review of extended abstract and appearing in conference record.

$*$ 1. M. J. Fischer. Grammars with macro-like productions. In *Proc. Ninth IEEE Sympos. Switching and Automata Theory*, pages 131–142, October 1968.
$*$ 2. M. J. Fischer and A. L. Rosenberg. Limited random access Turing machines. In *Proc. Ninth IEEE Sympos. Switching and Automata Theory*, pages 356–367, October 1968.
$*$ 3. M. J. Fischer. Some properties of precedence languages. In *ACM Sympos. Theory Comput.*, pages 181–190, May 1969.
$*$ 4. M. J. Fischer. Two characterizations of the context-sensitive languages. In *Proc. 10th IEEE Sympos. Switching and Automata Theory*, pages 149–156, October 1969.
5. A. R. Meyer and M. J. Fischer. Relatively complex recursive sets (abstract). *J. Symbolic Logic*, 35(4):607–608, May 1970. Paper contributed to the Meeting of the Association for Symbolic Logic, Manchester, 1969.
6. M. J. Fischer, A. R. Meyer, P. O'Neil, and M. S. Paterson. A note on independence of a regularity-preserving operator. *SICACT News*, No. 4:3–7, January 1970.
7. M. J. Fischer. P.I.B. international symposium on computers and automata: A critique. *SIGACT News*, No. 10:13–15, July 1971.
$*$ 8. M. J. Fischer and A. R. Meyer. Boolean matrix multiplication and transitive closure. In *Proc. 12th IEEE Sympos. Switching and Automata Theory*, pages 129–131, October 1971.

∗ 9. A. R. Meyer and M. J. Fischer. Economy of description by automata, grammars, and formal systems. In *Proc. 12th IEEE Sympos. Switching and Automata Theory*, pages 181–191, October 1971.

∗ 10. M. J. Fischer. Lambda calculus schemata. In *Proc. ACM Conference on Proving Assertions about Programs*, pages 104–109, January 1972. Subsequently appeared as refereed publication [39].

∗∗ 11. M. J. Fischer. Efficiency of equivalence algorithms. In R. E. Miller and J. W. Thatcher, editors, *Complexity of Computer Computations*, pages 153–167. Plenum Press, New York, 1972.

12. N. A. Lynch, A. R. Meyer, and M. J. Fischer. Priority arguments in complexity theory (abstract 24). *Recursive Function Theory Newsletter*, 2:7–10, July 1972. University of California, Berkeley.

13. M. Bauer, D. Brand, M. J. Fischer, A. R. Meyer, and M. S. Paterson. A note on disjunctive form tautologies. *SIGACT News*, 5(2):17–20, April 1973.

∗ 14. M. J. Fischer and L. J. Stockmeyer. Fast on-line integer multiplication. In *Proc. Fifth ACM Sympos. Theory Comput.*, pages 67–72, 1973. Subsequently appeared as refereed publication [10].

∗ 15. N. A. Lynch, A. R. Meyer, and M. J. Fischer. Sets that don't help. In *Proc. Fifth ACM Sympos. Theory Comput.*, pages 130–134, 1973.

∗ 16. A. E. Fischer and M. J. Fischer. Mode modules as representations of domains. In *Proc. ACM Sympos. on Principles of Prog. Lang.*, pages 139–143, October 1973.

∗ 17. J. I. Seiferas, M. J. Fischer, and A. R. Meyer. Refinements of the nondeterministic time and space hierarchies. In *Proc. 14th IEEE Sympos. Switching and Automata Theory*, pages 130–137, October 1973.

∗∗ 18. M. J. Fischer and M. S. Paterson. String-matching and other products. In R. M. Karp, editor, *Complexity of Computation*, volume VII of *SIAM-AMS Proceedings*, pages 113–125. American Mathematical Society, 1974.

∗∗ 19. M. J. Fischer and M. O. Rabin. Super-exponential complexity of Presburger arithmetic. In *Complexity of Computation*, volume VII of *SIAM-AMS Proceedings*, pages 27–41. American Mathematical Society, 1974.

∗∗ 20. M. S. Paterson, M. J. Fischer, and A. R. Meyer. An improved overlap argument for on-line multiplication. In *Complexity of Computation*, volume VII of *SIAM-AMS Proceedings*, pages 97–111. American Mathematical Society, 1974.

∗ 21. M. J. Fischer, A. R. Meyer, and M. S. Paterson. Lower bounds on the size of Boolean formulas: Preliminary report. In *Proc. Seventh ACM Sympos. Theory Comput.*, pages 37–44, May 1975. Subsequently appeared as refereed publication [23].

∗∗ 22. M. J. Fischer. The complexity of negation-limited networks—a brief survey. In H. Brakhage, editor, *Automata Theory and Formal Languages, 2nd GI Conference*, volume 33 of *Lecture Notes in Computer Science*, pages 71–82. Springer-Verlag, 1975.

∗ 23. P. A. Bloniarz, M. J. Fischer, and A. R. Meyer. A note on the average time to compute transitive closures. In S. Michaelson and R. Milner, editors, *Automata, Languages and Programming*, pages 425–434. Edinburgh University Press, 1976.

∗ 24. G. L. Peterson and M. J. Fischer. Economical solutions for the critical section problem in a distributed system. In *Proc. Ninth ACM Sympos. Theory Comput.*, pages 91–97, 1977.

∗ 25. M. J. Fischer and R. E. Ladner. Propositional modal logic of programs. In *Proc. Ninth ACM Sympos. Theory Comput.*, pages 286–294, 1977. Subsequently appeared as refereed publication [13].

∗ 26. G. B. Goodrich, R. E. Ladner, and M. J. Fischer. Straight-line programs to compute finite languages. In *A Conference on Theoretical Computer Science*. University of Waterloo, August 1977.

∗ 27. R. E. Ladner and M. J. Fischer. Parallel prefix computation. In *Proc. 1977 International Conference on Parallel Processing*, pages 218–223. IEEE Catalog No. 77CH1253–4C, August 1977. Subsequently appeared as refereed publication [15].

∗ 28. J. E. Burns, M. J. Fischer, P. Jackson, N. A. Lynch, and G. L. Peterson. Shared data requirements for implementation of mutual exclusion using a test-and-set primitive. In *Proc. 1978 International Conference on Parallel Processing*, pages 79–87. IEEE Catalog No. 78CH1321–9C, August 1978. Subsequently appeared as refereed publication [20].

∗ 29. N. A. Lynch and M. J. Fischer. On describing the behavior and implementation of distributed systems (preliminary report). In G. Kahn, editor, *Semantics of Concurrent Computation*, volume 70 of *Lecture Notes in Computer Science*, pages 147–171. Springer-Verlag, 1979. Subsequently appeared as refereed publication [17].

∗ 30. M. J. Fischer, N. A. Lynch, J. E. Burns, and A. Borodin. Resource allocation with immunity to limited process failure. In *Proc. 20th IEEE Sympos. Foundat. Comput. Sci.*, pages 234–254, October 1979.

∗ 31. A. Borodin, M. J. Fischer, D. G. Kirkpatrick, N. A. Lynch, and M. Tompa. A time-space tradeoff for sorting on non-oblivious machines. In *Proc. 20th IEEE Sympos. Foundat. Comput. Sci.*, pages 319–327, October 1979. Subsequently appeared as refereed publication [18].

∗ 32. M. J. Fischer and M. S. Paterson. Optimal tree layout. In *Proc. 12th ACM Sympos. Theory Comput.*, pages 177–189, 1980.

33. M. J. Fischer and J. van Leeuwen. Reducing 3DM to clique and Hamiltonian circuit. *Bull. European Assoc. Theoret. Comput. Sci.*, 11, June 1980.

34. M. J. Fischer. On developing a theory of distributed computing: Summary of current research. Notes of the Workshop on Fundamental Issues in Distributed Computing, Pala Mesa Resort, Fallbrook, California, December 1980. Also appeared as technical report [2].

∗ 35. M. J. Fischer, N. D. Griffeth, L. J. Guibas, and N. A. Lynch. Optimal placement of identical resources in a distributed network. In *Proc. 2nd International Conference on Distributed Computing Systems*. IEEE, April 1981. Subsequently appeared as refereed publication [36].

∗ 36. E. Arjomandi, M. J. Fischer, and N. A. Lynch. A difference in efficiency between synchronous and asynchronous systems. In *Proc. 13th ACM Sympos. Theory Comput.*, pages 128–132, 1981. Subsequently appeared as refereed publication [27].

∗ 37. M. J. Fischer, N. D. Griffeth, and N. A. Lynch. Global states of a distributed system. In *Proc. 1981 IEEE Symposium on Reliability in Distributed Software and Database Systems*. IEEE, July 1981. Subsequently appeared as refereed publication [21].

∗ 38. E. D. Lazowska, H. M. Levy, G. T. Almes, M. J. Fischer, R. J. Fowler, and S. C. Vestal. The architecture of the Eden system. In *8th Symposium on Operating Systems Principles*, pages 148–159, December 1981.

∗ 39. M. J. Fischer and A. Michael. Sacrificing serializability to achieve high availability of data in an unreliable network. In *Proc. ACM SIGACT-SIGMOD Symposium on Principles of Database Systems*, pages 70–75, March 1982.

40. M. J. Fischer. ⟨Problem 80–1⟩ ("Mountain problem"), in Problems section. *J. Algorithms*, 3:177–178, 1982.

∗ 41. N. A. Lynch, M. J. Fischer, and R. Fowler. A simple and efficient Byzantine generals algorithm. In *Proc. 1982 IEEE Symposium on Reliability in Distributed Software and Database Systems*, pages 46–52. IEEE, July 1982.

∗ 42. A. G. Greenberg and M. J. Fischer. On computing weak transitive closure in $\mathcal{O}(\log n)$ expected random parallel time. In *Proc. 1982 International Conference on Parallel Processing*, pages 199–204. IEEE Catalog No. 82CH1794–7, August 1982.

∗ 43. M. J. Fischer, N. A. Lynch, and M. S. Paterson. Impossibility of distributed consensus with one faulty process. In *Proc. 2nd ACM SIGACT-SIGMOD Symposium on Principles of Database Systems*, pages 1–7, March 1983.

∗∗ 44. M. J. Fischer. The consensus problem in unreliable distributed systems (a brief survey). In M. Karpinsky, editor, *Foundations of Computation Theory*, volume 158 of *Lecture Notes in Computer Science*, pages 127–140. Springer-Verlag, 1983.

∗ 45. A. Broder, D. Dolev, M. J. Fischer, and B. Simons. Efficient fault tolerant routings in networks. In *Proc. 16th ACM Sympos. Theory Comput.*, pages 536–541, 1984.

∗ 46. M. J. Fischer and M. S. Paterson. Fishspear: A priority queue algorithm. In *Proc. 25th IEEE Sympos. Foundat. Comput. Sci.*, pages 375–386, 1984. Subsequently appeared as refereed publication [40].

∗ 47. M. J. Fischer, N. A. Lynch, and M. Merritt. Easy impossibility proofs for distributed consensus problems. In *Proc. 4th ACM SIGACT-SIGOPS Symposium on Distributed Computing*, pages 59–70, August 1985.

∗ 48. M. J. Fischer and M. S. Paterson. Dynamic monotone priorities on planar sets. In *Proc. 26th IEEE Sympos. Foundat. Comput. Sci.*, pages 289–292, October 1985.

∗ 49. J. D. Cohen and M. J. Fischer. A robust and verifiable cryptographically secure election scheme. In *Proc. 26th IEEE Sympos. Foundat. Comput. Sci.*, pages 372–382, October 1985.

∗ 50. M. J. Fischer and N. Immerman. Foundations of knowledge for distributed systems. In *Proc. Conf. on Theoret. Aspects of Reasoning about Knowledge*, pages 171–185. Morgan Kaufman, March 1986.

51. M. J. Fischer and L. D. Zuck. Reasoning about uncertainty in fault-tolerant distributed systems. In M. Joseph, editor, *Formal Techniques in Real-Time and Fault-Tolerant Systems*, volume 331 of *Lecture Notes in Computer Science*, pages 142–158. Springer-Verlag, 1988.

52. M. J. Fischer, R. P. Fischer, and R. Beigel. Primitive recursion without implicit predecessor. *SIGACT News*, 20(4):87–91, Fall 1989.

∗ 53. M. J. Fischer, G. Taubenfeld, S. Moran, and S. Rudich. The wakeup problem. In *Proc. 22rd ACM Sympos. Theory Comput.*, pages 106–116, May 1990.

∗∗ 54. M. J. Fischer. A theoretician's view of fault-tolerant distributed computing. In B. Simons and A. Spector, editors, *Fault-Tolerant Distributed Computing*, volume 448 of *Lecture Notes in Computer Science*, pages 1–9. Springer-Verlag, 1990.

∗∗ 55. M. J. Fischer, N. A. Lynch, and M. Merritt. Easy impossibility proofs for distributed consensus problems. In B. Simons and A. Spector, editors, *Fault-Tolerant Distributed Computing*, volume 448 of *Lecture Notes in Computer Science*, pages 147–170. Springer-Verlag, New York, 1990. Reprinted from refereed publication [31].

∗∗ 56. M. J. Fischer, M. S. Paterson, and C. Rackoff. Secret bit transmission using a random deal of cards. In J. Feigenbaum and M. Merritt, editors, *Distributed Computing and Cryptography*, volume 2 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 173–181. American Mathematical Society and the Association for Computing Machinery, 1991.

∗ 57. M. J. Fischer and R. N. Wright. Multiparty secret key exchange using a random deal of cards. In J. Feigenbaum, editor, *Advances in Cryptology—CRYPTO '91 Proceedings*, volume 576 of *Lecture Notes in Computer Science*, pages 141–155. Springer-Verlag, 1992. This paper was presented under the title, *Secret Key Exchange Using a Random Deal of Cards*, at the CRYPTO '91 conference, Santa Barbara, California, August 11–15, 1991.

∗∗ 58. M. J. Fischer and S. A. Paleologou. Decision making in the presence of noise. In J. Buchmann, H. Ganzinger, and W. J. Paul, editors, *Informatik: Festschrift zum 60. Geburtstag von Günter Hotz*, volume 1 of *Teubner-Texte zur Informatik*, pages 145–168. B. G. Teubner Verlagsgesellschaft, Stuttgart; Leipzig, 1992.

∗ 59. M. J. Fischer and R. N. Wright. An efficient protocol for unconditionally secure secret key exchange. In *Proc. Fourth Ann. ACM-SIAM Sympos. on Discrete Algorithms*, pages 475–483, January 1993.

60. M. J. Fischer. Expanding the pipeline: How can men help expand the CS pipeline? *Computing Research News*, 5(3):3, May 1993.

∗∗ 61. M. J. Fischer. Estimating parameters of monotone boolean functions (abstract). In W.-L. Hsu and M.-Y. Kao, editors, *Proceedings of the 4th Annual International Conference on Computing and Combinatorics*, volume 1449 of *Lecture Notes in Computer Science*, page 3. Springer-Verlag, New York, 1998.

∗∗ 62. M. J. Fischer. The reality of information objects. In N. Thompson, editor, *Instilling Ethics*, chapter 13, pages 207–214. Rowman & Littlefield, Lanham, Maryland, April 2000.

∗ 63. J. Aspnes, D. F. Fischer, M. J. Fischer, M.-Y. Kao, and A. Kumar. Towards understanding the predictability of stock markets from the perspective of computational complexity. In *Proceedings of the Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 745–754, New York / Philadelphia, January 2001. Association for Computing Machinery / Society for Industrial and Applied Mathematics.

∗∗ 64. Z. Diamadi and M. J. Fischer. A simple game for the study of trust in distributed systems. *Wuhan University Journal of Natural Sciences*, 6(1–2):72–82, March 2001. Also appears as Yale Technical Report TR–1207, January 2001, available at URL `ftp://ftp.cs.yale.edu/pub/TR/tr1207.ps`.

∗ 65. D. Angluin, J. Aspnes, Z. Diamadi, M. J. Fischer, and R. Peralta. Computation in networks of passively mobile finite-state sensors. In *Proc. 23rd Annual ACM Symposium on Principles of Distributed Computing*, pages 290–299, New York, July 2004. Association for Computing Machinery. Also available as Yale technical report (see [7] in Technical Reports list).

66. M. Fischer and C. Spiesel. Only a paper trail will verify our votes. *New Haven Register*, March 16, 2005.

67. M. J. Fischer. Avoid the DRE train wreck. *Hartford Courant*, May 17, 2005.

∗ 68. D. Angluin, J. Aspnes, M. Chan, M. J. Fischer, H. Jiang, and R. Peralta. Stably computable properties of network graphs. In V. K. Prasanna, S. Iyengar, P. Spirakis, and M. Welsh, editors, *Distributed Computing in Sensor Systems: First IEEE International Conference, DCOSS 2005, Marina del Rey, CA, USA, June/July, 2005, Proceedings*, volume 3560 of *Lecture Notes in Computer Science*, pages 63–74. Springer-Verlag, June 2005.

∗ 69. D. Angluin, J. Aspnes, M. J. Fischer, and H. Jiang. Self-stabilizing population protocols. In *Principles of Distributed Systems: 9th International Conference, OPODIS 2005; Pisa, Italy*, volume 3974 of *Lecture Notes in Computer Science*, pages 103–117, Berlin Heidelberg, December 2005. Springer-Verlag.

∗ 70. D. Angluin, M. J. Fischer, and H. Jiang. Stabilizing consensus in mobile networks. In P. B. Gibbons, T. Abdelzaher, J. Aspnes, and R. Rao, editors, *Distributed Computing in Sensor Systems: Second IEEE International Conference, DCOSS 2006, San Francisco, CA, USA, June 2006, Proceedings*, volume 4026 of *Lecture Notes in Computer Science*, pages 37–50. Springer-Verlag, June 2006.

∗ 71. M. Fischer and H. Jiang. Self-stabilizing leader election in networks of finite-state anonymous agents. In A. A. Shvartsman, editor, *Principles of Distributed Systems: 10th International Conference, OPODIS 2006; Bordeaux, France*, volume 4305 of *Lecture Notes in Computer Science*, pages 395–409, Berlin Heidelberg, December 2006. Springer-Verlag.

∗ 72. M. J. Fischer, X. Su, and Y. Yin. Assigning tasks for efficiency in Hadoop: extended abstract. In *SPAA '10: Proceedings of the 22nd ACM Symposium on Parallelism in Algorithms and Architectures*, pages 30–39, New York, NY, USA, 2010. ACM.

73. S. Dolev, J. Cobb, M. Fischer, and M. Yung, editors. *Stabilization, Safety, and Security of Distributed Systems*, volume 6366 of *Lecture Notes in Computer Science*. Springer, 2010.

∗ 74. M. J. Fischer, M. Iorga, and R. Peralta. A public randomness service. In *Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on*, pages 434–438, July 2011.

∗ 75. E. Syta, M. J. Fischer, D. Wolinsky, A. Silberschatz, G. Gallegos-Garcia, and B. Ford. Private eyes: Secure remote biometric authentication. In *Proceedings of the 12th International Conference on Security and Cryptography (SECRYPT 2015), Colmar, Alsace, France*, pages 243–250. INSTICC, Science and Technology Publications, Lda, July 2015. Also appears as Yale Technical Report TR–1510, March 2015, available at URL `http://cpsc.yale.edu/sites/default/files/files/tr1510.pdf`.

∗ 76. E. Syta, P. Jovanovic, E. Kokoris-Kogias, N. Gailly, L. Gasser, I. Khoffi, M. J. Fischer, and B. Ford. Scalable bias-resistant distributed randomness. In *2017 IEEE Symposium on Security and Privacy, SP 2017, San Jose, CA, USA, May 22-26, 2017*, pages 444–460, 2017. Also appears as Cryptology ePrint Archive, Report 2016/1067, 2016, available at URL `http://eprint.iacr.org/2016/1067`.

Technical Reports Not Available Elsewhere

1. M. J. Fischer and R. E. Ladner. Data structures for efficient implementation of sticky pointers in text editors (extended abstract). Technical Report 79–06–08, Department of Computer Science, University of Washington, June 1979. 16pp.

2. M. J. Fischer. On developing a theory of distributed computing: Summary of current research. Technical Report 80–09–03, Department of Computer Science, University of Washington, September 1980. 12pp. Also appeared as other publication [34].

3. M. J. Fischer and L. D. Zuck. Relative knowledge and belief (extended abstract). Technical Report YALEU/DCS/TR–589, Department of Computer Science, Yale University, December 1987.

4. M. J. Fischer. Lectures on network complexity. Technical Report YALEU/DCS/TR–1104, Department of Computer Science, Yale University, April 1996. This is an electronic version of the widely-circulated "Frankfurt lecture notes" dated June 1974 and revised April 1977.

5. M. J. Fischer and R. Peralta. Counting predicates of conjunctive complexity one. Technical Report YALEU/DCS/TR–1222, Department of Computer Science, Yale University, December 2001. Available at URL `http://cs.yale.edu/publications/techreports/tr1222.pdf`.

6. D. Angluin, J. Aspnes, Z. Diamadi, M. J. Fischer, and R. Peralta. Urn automata. Technical Report YALEU/DCS/TR–1280, Department of Computer Science, Yale University, November 2003. Available at URL `http://cs.yale.edu/publications/techreports/tr1280.pdf`.

7. D. Angluin, J. Aspnes, Z. Diamadi, M. J. Fischer, and R. Peralta. Computation in networks of passively mobile finite-state sensors. Technical Report YALEU/DCS/TR–1281, Department of Computer Science, Yale University, February 2004. Available at URL `http://cs.yale.edu/publications/techreports/tr1281.pdf`.

8. M. J. Fischer, A. R. Meyer, and M. S. Paterson. Think-a-dot. Technical Report YALEU/DCS/TR–1287, Department of Computer Science, Yale University, April 2004. Available at URL `http://cs.yale.edu/publications/techreports/tr1287.pdf`.

9. R. Fischer, M. Selzer, and M. Fischer. Privacy from untrusted web servers. Technical Report YALEU/DCS/TR–1290, Department of Computer Science, Yale University, May 2004. Available at URL `http://cs.yale.edu/publications/techreports/tr1290.pdf`.
10. R. Fischer, H. Jiang, and M. Fischer. Typed computational email for serverless distributed applications. Technical Report YALEU/DCS/TR–1291, Department of Computer Science, Yale University, May 2004. Available at URL `http://cs.yale.edu/publications/techreports/tr1291.pdf`.
11. M. Fischer, X. Su, and Y. Yin. Assigning tasks for efficiency in hadoop. Technical Report YALEU/DCS/TR–1423, Department of Computer Science, Yale University, March 2010. Available at URL `http://cs.yale.edu/publications/techreports/tr1423.pdf`.
12. E. Syta, M. J. Fischer, A. Silberschatz, G. G. Garcia, and B. Ford. Strong theft-proof privacy-preserving biometric authentication. Technical Report YALEU/DCS/TR–1455, Department of Computer Science, Yale University, May 2012.
13. M. J. Fischer, M. S. Paterson, and E. Syta. On backtracking resistance in pseudorandom bit generation (preliminary version). Technical Report YALEU/DCS/TR–1466, Department of Computer Science, Yale University, October 2012. Available at URL `http://cs.yale.edu/publications/techreports/tr1466.pdf`.
14. E. Syta, D. Wolinsky, M. J. Fischer, A. Silberschatz, B. Ford, and G. G. Garcia. Efficient and privacy-preserving biometric authentication. Technical Report YALEU/DCS/TR–1469, Department of Computer Science, Yale University, November 2012. Available at URL `http://cs.yale.edu/publications/techreports/tr1469.pdf`.
15. E. Syta, B. Peterson, D. I. Wolinsky, M. Fischer, and B. Ford. Deniable anonymous group authentication. Technical Report YALEU/DCS/TR–1486, Department of Computer Science, Yale University, February 2014.
16. E. Syta, P. Jovanovic, E. K. Kogias, N. Gailly, L. Gasser, I. Khoffi, M. J. Fischer, and B. Ford. Scalable bias-resistant distributed randomness. Cryptology ePrint Archive, Report 2016/1067, 2016. `http://eprint.iacr.org/2016/1067`.