Michael O. Rabin

Thomas J. Watson Sr. Professor of Computer Science
Harvard University

1953	M.Sc., Mathematics, Hebrew University
1957	Ph.D., Mathematics, Princeton University
1956-58	H. B. Fine Instructor, Princeton University
1958	Member, Institute for Advanced Study, Princeton
1958-	Senior Lecturer, Associate Professor and Professor (1965), Hebrew University of Jerusalem
1964-66	Chairman, Institute of Mathematics, Hebrew University
1970-71	Chairman, Computer Science Department, Hebrew University
1972-75	Rector (Academic Head), Hebrew University
1976-80	Pro-Rector, Hebrew University
1980-99	Albert Einstein Chair, Hebrew University
1981-83	Gordon McKay Professor of Computer Science, Harvard University
1983-	Thomas J. Watson Sr. Professor of Computer Science, Harvard University

ACADEMY MEMBERSHIPS:

American Academy of Arts and Sciences (1975-)
Israel Academy of Sciences and Humantities (1982-)
Foreign Associate US National Academy of Sciences (1984-)
Foreign Member American Philosophical Society (1988-)
Associé Étranger, French Academy of Sciences (1995-)
Foreign Member Royal Society (2007)
Elected Member Europeon Academy of Science (2007)

AWARDS:

The C. Weizmann Prize for Exact Sciences, 1960
Rothschild Prize in Mathematics, 1974.
ACM Turing Award in Computer Science, 1976.
Harvey Prize in Science and Technology, 1980.
The Israel Prize in Exact Sciences/Computer Science, 1995.

IEEE Charles Babbage Award in Computer Science, 2000.
ASL Godel Award Lecture,2004.
ACM Kanellakis Theory and Pratice Award, 2004.
The EMET Prize in Exact Sciences/Computer Science, 2004.
Best Teacher Award, Courant Institute of Mathematics, 1970.

HONORARY DOCTORATES:

University of Bordeaux I (1996); Haifa University (1996)
New York University (1998)
Israel Open University Honorary Fellow (1999)
Ben-Gurion University (2000)
Wroclaw University (2007)

CONSULTANT:

Summers	1957, 1958, 1963, 1968, 1969, 1976,1992 IBM Research; 1960, Bell Telephone Laboratories
1966-67	IBM Research
1970-71	IBM Research
1980-92	IBM Science Advisory Committee

SCIENTIFIC SOCIETIES:

1999-03	President, Div. for Logic, Methodology, and Philosophy of Science, IUHPS.

VISITING POSITIONS:

1961-62	Associate Professor of Mathematics, University of California at Berkeley
1962-63	Associate Professor of Mathematics, M. I. T.
1963	(Summer) Research Fellow, Harvard University
1965	Lecturer in Computer Science, Paris University
1967	Visiting Professor of Mathematics, Yale University
1970-71	Visiting Professor of Mathematics and Computer Science, Courant Institute, New York University
1972-78	Visiting Professor of Applied Mathematics, M. I. T.
1979	(Summer) Visiting Professor of Computer Science, Washington State University, Seattle
1980-81	Visiting Professor of Computer Science, Harvard University

1987	Fairchild Scholar, California Institute of Technology
1992	Henry Saville Fellow, Merton College, Oxford England
2000	(Spring) Nach-Diplom Lectures in Mathematics, ETH Zurich
2001	(Spring) Visiting Professor of Computer Science, Courant Institute
2002	(Spring)Visiting Professor of Computer Science, Columbia University
2004	(Spring) Visiting Professor of Computer Science, King's College, London
2004	(Spring) Steward Fellow, Gonville and Caius Colege, Cambridge
2007	(Spring Term) Visiting Professor of Computer Science, Columbia University

EDITORIAL BOARDS:

Journal of Computer and Systems Sciences
Journal of Combinatorial Theory
Journal of Algorithms

INVITED LECTURES:

Over 300 invited lectures, named lecture series and principal lectures at international symposia and congresses, Univ. Colloquia and Distinguished Lecture Series, including:
The American Mathematical Society Gibbs Lecture
London Mathematical Society Hardy Lecturer
New York University, Richard Courant Memorial Lecture
University of California Berkeley, Tarski Memorial Lectures
Yale University, Hahn Memorial Mathematics Lectures
Carnegie Institute, Washington DC, Capital Science Lecture
Weizmann Institute of Science, C. Weizmann Memorial Lecture
The Strachy Memorial Lecture in Computer Science, Oxford
University of Michigan, M. Keeler Lectures in Mathematics
IACR (Intl. Assoc. for Cryptologic Research), Keynote Speaker
International Colloquium on Automata, Languages and Programming
Plenary Invited Speaker (twice).
IEEE Int. Symposium on Information Theory, Keynote Speaker
Int. Math. Union Congress, invited speaker, Nice, France, plenary speaker
Warsaw (declined).
19th Int. Symposium on Theoretical Aspects of Computer Science(STACS),
Keynote Speaker.
14th Int. Parallel & Distributed Processing Symposium (IPDPS), Keynote Speaker

5th Conference on Algorithms and Complexity (CIAC), Plenary Invited Speaker
ITG Conference on Source and Channel Coding, Plenary Invited Speaker
ACM Federated Computer Research Conference, Plenary Invited Speaker.
International Congress for Logic, Philosophy and Methodology of Science,
Plenary Invited Speaker.
Brown University, Kanellakis Memorial Lecture.
J.C. Steward Lectures in Mathematics, Gonville and Caius College, Cambridge.
Association for Symbolic Logic, Godel Award Lecture.
Katzir Memorial Lecture, Tel-Aviv University
Joint ICALP-LICS 2007 Symposia, Plenary Lecture

PUBLICATIONS

1. A theorem on partially ordered sets (Hebrew); Riveon Lematematika, vol. 7 (1953), pp. 26-29.

2. On regular polygons with lattice-point vertices (Hebrew); Riveon Lematematika, vol. 8 (1954), pp. 13-15.

3. Sur la représéntation des idéaux par des idéaux primaires, C. R. de l'acad. des Scien., vol. 237, (1953), pp. 544-545.

4. A note on Helly's theorem, Pac. Journ. of math., vol. 5 (1955), pp. 363-366.

5. Effective computability of winning strategies, Annal of Math. Studies, vol. 39 (1957), pp. 147-157.

6. Two way finite automata, Proc. Summer Institute of Symbolic Logic, l957 at Cornell, pp. 366-369.

7. Recursive unsolvability of group theoretic problems, Annals of Math., vol. 67(1958), pp. 172-194.

8. On codes for checking logical operations, I.B.M. Journal, vol. 3 (1959), pp. 163-168 (with W. Peterson).

9. Finite automata and their decision problems, I.B.M. Journal, vol. 3 (1959), pp. 114-125 (with D. Scott). Russian translation: Konechnye avtomaty i zadachi ikh razresheniya, Kiberneticheskii sbornik, vol. 4 (1962), pp. 58-91. Reprinted in: Sequential Machines, Selected Papers, E. F. Moore(editor) Addison Wesley Publishing Company, Reading, MA (1964), pp. 63-92.

10. An algorithm for a minimum cover of a graph, Proc. Amer.Math. Soc., vol. 10 (1959), pp. 315-319 (with R.Z. Norman).

11. On recursively enumerable and arithmetic models of set theory, J. of Symbolic Logic, vol. 23 (1958), appeared 1959, pp.408-416.

12. Arithmetical extensions with prescribed cardinality, Indag. Math., vol. 21 (1959), pp. 439-446.

13. Speed of computation and classification of recursive sets, Third Convention of Scientific Societies, Israel (1959), pp. 1-2.

14. Computable algebra, general theory and theory of computable fields, Trans. Amer. Math. Soc., vol. 94 (1960), pp. 341-360.

15. Degree of difficulty of computing a function and a partial ordering of recursive sets, Technical Report O.N.R. Contract (1960), pp. 341-360.

16. Non-standard models and the independence of the induction axiom, Essays on the Foundations of Mathematics, (dedicated to A. A. Fraenkel) (1961), pp. 287-299.

17. Diophantine equations and non-standard models of arithmetic, Proc. of Int. Congress for Logic and Methodology of Science, Stanford (1962), pp. 151-158.

18. Classes of structures and sets of sentences with the intersection property, Actes du Colloqe de mathematiques a l'Occasion du Tricentenaire de la Mort de B. Pascal, Tome 1, pp. 39-53.

19. The theory of definite automata, IEEE Transactions on Computers, vol. EC-12 (1963), pp. 233-243 (with Perles and Shamir).

20. Probabilistic Automata, Information and Control, vol. 6 (1963), pp. 230-245. Reprinted in: Sequential Machines, Selected Papers, E. F. Moore (editor) Addison Wesley Publishing Company, Reading, Mass., pp. 98-114.

21. Words in the history of a Turing machine with a fixed input, Journal of the Association for Computing Machinery, vol. 10 (1963), pp. 226-227 (with H. Wang).

22. Real time computation, Israel J. of Math., vol. 1 (1963), pp. 203-211.

23. Universal groups of automorphisms of models, Berkeley International Symp. on the Theory of Models, North-Holland Publishing Co., (1965), pp. 274-284.

24. A simple method for undecidability proofs. Proc. of the (1964) International Congress for Logic, North-Holland Publishing Co., (1965), pp. 58-68.

25. Decidability and undecidability of extensions of second (first) order theory of (generalized) successor, J. Symbolic Logic, vol. 31 (1966), pp. 169-181 (with C. Elgot).

26. Classical and probabilistic automata, Automata Theory (E. B. Cainiello, editor), Academic Press, 1966, pp. 304-313.

27. Mathematical theory of automata, Proc. Symp. Applied Math., vol. 19, Amer. Math. Soc., Providence, R. I., (1968), pp. 153-175.

28. Decidability of Second Order Theories and Automata on Infinite Trees, Bull. of the Amer. Math. Soc., vol. 74 (1968), pp. 1025-1029.

29. Decidability of second-order theories and automata on infinite trees, Trans. Amer. Math. Soc. 141 (1969), pp. 1-35.

30. Weakly definable relations and special automata, Mathematical Logic and Foundations of Set Theory, (Y. Bar-Hillel, editor) North-Holland Publishing Co., (1970), pp. 1-23.

31. Automata on infinite trees and the synthesis problem, ONR Technical Report 37, Jerusalem (1970), pp. 24.

32. Decidability and definability in second-order theories, Proceedings of the International Mathematical Congress, (1b970).

33. Proving simultaneous positivity of linear forms. J. of Computer and Systems Science, vol. 6 (1972).

34. Solving linear equations by means of scalar products, Complexity of Computer Computations, R. E. Miller, Editor, Plenum Press, (1972), pp. 11-20.

35. Automata on infinite objects and Church's problem, Regional Conference Series in Mathematics, No. 13, Amer. Math. Soc., (1972), pp. 22.

36. Fast evaluation of polynomials by rational preparation. Comm. on Pure and Applied Math., vol. 25 (1972), pp. 453-458 (with S. Winograd).

37. Super exponential complexity of Presburger arithmetic, in Complexity of Computations, SIAM-AMS Proc. of Symp., vol. 7, (1974), pp. 27-41 (with M. Fischer).

38. Theoretical impediments to artificial intelligence, Proc. 1974 IFIP Congress, North Holland pub. Co., pp. 615-619.

39. Decidable theories, Handbook of Mathematical Logic, J. Barwise, editor, North Holland Pub. Co., Amsterdam, (1977), pp. 595-629.

40. Probabilistic algorithms, in Algorithms and Complexity, New Directions and Recent Trends, J. F. Traub, editor, Academic Press, New York (1976), pp. 21-39.

41. Digitalized signatures, Foundations of Secure Computations, R. De Millo and R. Lipton, editors, Academic Press, New York (1978), pp. 155-166.

42. Complexity of computations, Comm. of ACM, vol. 20 (1977), pp. 625-633.

43. Probabilistic tests for primality, J. of Number Theory, vol. 12 (1980), pp. 128-138.

44. Probabilistic algorithms in finite fields, SIAM J. on Computing, vol. 9 (1980), pp. 273-280.

45. Linear Disjointness and algebraic complexity (with W. Baur) , L'Enseignement Mathematique, vol. 26 (1980), pp. 333-344.

46. A symmetric and fully distributed solution to the dining philosophers problem (Extended Abstract) (with D. Lehmann), 8th ACM Symp. on Principles of Programming Languages (1981), pp. 133-138.

47. The choice coordination problem, Acta Informatica, vol. 17 (1982), pp. 121-134.

48. N-process mutual exclusion with bounded waiting by 4 $\log_2$N-valued shared variable, Jour. Comp. Sys. Sc., vol. 25 (1982), pp. 66-75.

49. Randomized Byzantine Generals, IEEE 24th Symp. on Foun. of Comp. Sc. (1983) pp. 403-409.

50. Transaction protection by beacons, Jour. Comp. Sys. Sc., vol. 27 (1983).

51. Discovering repetitions in strings, combinatorial algorithms on words (Galil and Apostalico, editors), Springer Verlag Berlin CS series (1985), pp. 279-289.

52. Randomized algorithms in number theory (with J. Shallit), Comm. on Pure and Applied Mathematics, vol. 39 (1986), pp. 239-256.

53. A logic to reason about likelihood, (with J. Halpern), Artificial Intelligence, An Int. Jour., vol. 32 (1987), pp. 379-405.

54. Efficient randomized pattern-matching algorithms (with R. Karp), IBM Jour. of Res. and Dev., vol. 31 (1987), pp. 249-260.

55. Achieving Independence in Logarithmic Number of Rounds, (with B. Chor) *Proceedings of the 6th ACM Conference on Principles of Distributed Computing*, August 1987, pp. 260–268.

56. Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance, Jour. of Assoc. for Comp. Machinery, vol. 38 (1989), pp. 335-348.

57. Biased Coins and Randomized Algorithms, in Randomness and Computing (S. Micali, editor), Advances in Computing vol 5. (1989) JAI Press (Johnson's Associate Inc.), pp. 499-507 (with N. Alon).

58. Maximum Matchings in General Graphs Through Randomization, Jour. of Algorithms, vol. 10, (December 1989) (with V. Vazirani).

59. An Integrated Toolkit for Operating System Security, in Foundations of Data Organization and Algorithms, (W. Litwin and H. J. Schek editors) *3rd International Conference, FODO* 1989 Paris, France, June 1989 Springer-Verlag pp. 2-15 (with J.D. Tygar).

60. The Information Dispersal Algorithm and Its Applications, in Sequences: Combinatorics, Compression, Security, and Transmission (Capocelli, editor), 1990 Springer-Verlag, NY, pp 406-419.

61. Set Systems with No Union of Cardinality 0 Modulo m (with N. Alon, et al.), Graphs and Combinatorics, Vol. 7 (1991) pp. 97-99.

62. Efficient Program Transformation for Resilient Computation via Randomization (with Z.M. Kedem, K.V. Palem, and A. Raghunathan), Proceedings of the Annual ACM Symposium on the Theory of Computing, (STOC), (1992), pp. 306-318.

63. Randomized Mutual Exclusion Algorithms Revisited (with E. Kushilevitz), Proceedings of Principles of Distributed Computed (PODC), August 1992, pp. 235-283.

64. Fast PRAM Simulation on Fully Asynchronous Parallel Systems (with Y. Aumann), Proceedings of the 33rd Annual Symposium on Foundations of Computer Science (FOCS), October 1992, pp. 147-156.

65. Optimal Parallel Pattern Matching Through Randomization, Sequences II - Methods in Communication, Security, and Computer Science (R. Capocelli, et al. editors), Springer-Verlag, 1993, pp. 292-299.

66. Highly efficient asynchronous execution of large-grained parallel programs (with Y. Aumann, Z. Kedem, and K. Palem), Proceedings of 34th IEEE Annual Symposium on Foundations of Computer Science (FOCS), 1993, pp. 271-280.

67. Lower Bounds for Randomized Mutual Exclusion (Extended Abstract) (with E. Kushilevitz, Y. Mansour, and D. Zuckerman), Proceedings of the 25th Annual Symposium on the Theory of Computing (STOC), May 16-18, 1993, pp. 154-163.

68. The Advantages of Free Choice: A symmetric and Fully Distributed Solution for the Dining Philosophers Problem (with D. Lehmann), in A Classical Mind: Essays in Honour of C.A.R. Hoare, Prentice-Hall Intl. Ser. in Comp. Sci., (A.W. Roscoe, editor) (1994), pp. 337-356.

69. Clock Construction in Fully Asynchronous Parallel Systems and PRAM Simulation, (with Y. Aumann) Theoretical Computer Science, 128 (1994), pp. 3-30.

70. On Lotteries with Unique Winners (with E. Kushilevitz, and Y. Mansour), SIAM J. Disc. Math, Vol 8, No. 1, pp. 93-98, Feb. 1995.

71. Parallel Processing on Networks of Workstations: A Fault-Tolerant, High Performance Approach (with P. Dasgupta, and Z. Kedem), Proc. of the 15th International Conference on Distributed Computing Systems, 1995, (IEEE Outstanding Paper Award).

72. Computationally Hard Algebraic Problems (Invited Lecture), Proceedings of 37th IEEE Annual Symposium on Foundations of Computer Science (FOCS), 1996.

73. Hashing on Strings, Cryptography, and Protection of Privacy, (with S. Micali), in book *Proceedings Compression and Complexity of Sequences* IEEE Computer Society, Los Alamitos, CA, June 11-13, 1997, p. 1.

74. Simplified VSS and Fast-track Multiparty Computations with Applications to Threshold Cryptography, (with R. Gennaro and and T. Rabin). *Proc. 17th ACM Symp. on Principles of Distributed Computation*, ACM, 1998, pp. 101-112.

75. Authentication, Enhanced Security and Error Correcting Codes, (with Y. Aumann). IACR Distinguished Lecture, in Advances in Cryptology-Crypto 98, Lectures in Computer Science 1462, Springer Verlag, 1998, pp. 299-303.

76. Information Theoretically Secure Communication in the Limited Storage Model (with Y. Aumann), in Advances in Cryptology-Crypto 99, Lectures in Computer Science 1666, Springer Verlag, 1999, pp. 65-79.

77. Verifiable Random Functions (with S. Micali, S. Vadhan), Proc. 40th Symp. on Foundations of Computer Science (FOCS), IEEE Computer Society, 1999, pp. 120-130.

78. DNA^2DNA Computations: A Potential Killer Application (with R. Lipton and L. Landweber), Published in DNA Based Computers, III, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Vol 48 (ed. H. Rubin), American Mathematical Society, 1999, pp. 161-172.

79. Linear consistency testing (with Y. Aumann, J. Haastad, and M. Sudan) Jour. of Computer and Syst. Science, vol. 62, pp. 589–607, 2001.

80. Hyper-Encryption and Everlasting Security (with Y. Z. Ding) Proceedings of the 19th International Symposium on Theoretical Aspects of Computer Science (STACS), pages 1-26, Antibes - Juan les Pins, France, March 14-16,

81. Everlasting Security in the Bounded Storage Model (with Y. Aumann and Y. Z. Ding) IEEE Transactions on Information Theory, Volume 48, Issue 6, pages 1668-1680, June 2002.

82. Online Scheduling of Parallel Programs on Heterogeneous Systems with Applications to Cilk. (with M. A. Bender) . Theory of Computing Systems Special Issue on SPAA '00, 35: 289-304, 2002.

83. Zero Knowledge Sets (with S. Micali and J. Kilian), Symposium on Foundations of Computer Science (FOCS), pp. 80-86, October 2003.

84. Identity-Based Zero Knowledge (with J. Katz and R. Ostrovsky), in Security in Communication Networks, 4th Intl. Conf., 2004, Lecture Notes in Computer Science 3352 Springer 2005, pp 180-192.

85. Provably Unbreakable Hyper-Encryption In the Limited Access Model, *Proceedings IEEE Symp. on Information Theory Workshop on Theory and Practice in Information-Theoretic Security*,pp. 34-37 Awaji Island, Japan, 2005.

86. Preventing Piracy While Preserving Privacy, with Dennis E. Shasha in *Dr. Dobb's Journal Computer Security*, CMP Media LLC, 2005

87. Practical Secrecy-Preserving, Verifiably Correct and Trustworthy Auctions (with D. Parkes, S. Shieber, C. Thorpe), in *ICEC '06: Proceedings of the 8th international Conference on Electronic Commerce*, pages 70-81, New York, NY, USA, 2006.ACM Press.

88. Highly Efficient Secrecy-Preserving Proofs of Correctness of Computations and Applications,(with R. A. Servidio and C. Thorpe), LICS 2007,*Proceedings of 22nd Annual IEEE Symposium on Logic in Computer Science*, 14 pages, 2007.

Reports

89. Digitalized signatures and public-key functions as intractable as factor ization, MIT/LCS/TR-212, (1979).

90. Fingerprinting by random polynomials, Center for Research in Computing Technology, Harvard University, TR-15-81, (1981) .

91. An integrated toolkit for operating system security, (with D. Tygar) Center for Research in Computing Technology, Harvard University, Technical Report TR-05-87, (1987).