

CURRICULUM VITAE

ANDREW M. ODLYZKO

PERSONAL DATA

Address: University of Minnesota
Digital Technology Center
499 Walter Library
117 Pleasant St. SE
Minneapolis, Minnesota 55455

Telephone: 612-624-9510
Fax: 612-625-2002

Email: odlyzko@umn.edu

Home page: <http://www.dtc.umn.edu/~odlyzko>

UNIVERSITY EDUCATION

California Institute of Technology: B.S. and M.S. in Mathematics, 1971.

Massachusetts Institute of Technology: Hertz Foundation Fellow (1971–1975), Ph.D. in Mathematics, 1975.

RESEARCH INTERESTS

Computational complexity, cryptography, number theory, combinatorics, coding theory, analysis, probability theory, electronic publishing, electronic commerce, economics of data networks.

PROFESSIONAL EXPERIENCE

Jet Propulsion Laboratory, Pasadena, California: Summers of 1971, 1973, and 1974.

AT&T Bell Laboratories, Murray Hill, New Jersey: Summer of 1972. Member of Technical Staff, 1975–1983. Head, Mathematical Studies Department, 1983–1989. Head, Mathematics of Communication and Computer Systems Department, 1989–1995.

AT&T Labs–Research: Head, Mathematics and Cryptography Research Department, 1996–2001.

Adjunct Professor, Dept. of Combinatorics and Optimization, University of Waterloo, 1994–9.

Assistant Vice President for Research, University of Minnesota, 2001–2006.

Director, Digital Technology Center, University of Minnesota, 2001–.

ADC Telecommunications Chair Professor, University of Minnesota, 2001–.

Professor, School of Mathematics, University of Minnesota, 2001–.

RESEARCH MANAGEMENT EXPERIENCE

Managed projects in security, formal verification, parallel and distributed processing, simulation, parallel architectures, auction software, as well as computing and networking support.

SPECIAL HONORS, LECTURES, AND TEACHING

Doctor of Science, honoris causa, Univ. Marne la Vallée, 2000.

GLOCOM Fellow, 2001–2005.

Invited hour addresses at the annual meetings of the American Mathematical Society (Pittsburgh, 1981), the Australian Mathematical Society (Brisbane, 1983), and the Mathematical Association of America (Toronto, 1998).

Invited 45-minute lecture at International Congress of Mathematicians, Berkeley, 1986.

Invited series of lectures at 9th Latin American School of Mathematics, Santiago, 1988.

Series of lectures at the University of Amsterdam, 1983.

L. Alaoglu lecture at Caltech, 1990.

One of principal lecturers at 43rd British Mathematical Colloquium, Bath, 1991.

Kemeny Lecturer, Dartmouth, 2000.

2001 IACR Distinguished Lecturer, Eurocrypt'01, Innsbruck, Austria.

Distinguished Professor Lecture, Lehman College, 2002.

University Lecture, Univ. Wisconsin in Madison, 2002.

Barnett Lecture, Univ. Cincinnati, 2003.

Dean's Lecture, B. Thomas Golisano College of Computing and Information Sciences at Rochester Institute of Technology, 2004.

Keynote lectures:

ICCC/IFIP conference Electronic Publishing '97: New Models and Opportunities,

STM annual seminar, Washington, DC, 1999.

QofIS minitrack on Internet Charging, Quality of Future Internet Services conference, Berlin, 2000.

Digital Rights Management workshop, Berlin, 2000.

International Learned Journals Seminar, London, 2002.

11th IST Mobile & Wireless Summit, Thessaloniki, 2002.

6th International Precision Agriculture Conference, Minneapolis, 2002.

Raymond James Tri-Tech Conference, Montreal, 2002.

Lyra Imaging Symposium, Palm Springs, 2003.

MITACS Annual Conference, Ottawa, 2003.

Australasian Conference on Information Security and Privacy, Wollongong, Australia, 2003.

Internet Accessible Mathematical Computation workshop, Philadelphia, 2003.

Ethernet Services: A Carrier Class, a Light Reading Live event, Orlando, 2003.

CommsDaySummit, Sydney, Australia, 2004.

Third Stevens Symposium on Cybersecurity and Trustworthy Software, Stevens Inst. Tech., Hoboken, New Jersey, 2004.

WiscNet 2004 Conference, Madison, Wisconsin, 2004.

Innovation Law and Policy Colloquium, Bell University Labs, Univ. Toronto, Toronto, 2004.

Network of Networks Symposium, Amsterdam, The Netherlands, 2004.

Light Reading's Next-Generation Services Roadshow, 2004.

Eighteenth Midwest Conference on Combinatorics, Cryptography, and Computing, Rochester Institute of Technology, 2004.

Over 550 external lectures, including those at industry conferences such as:

RHK STARTRAX, 2000 and 2002.

NGN 2001 and 2002.

Carriers World Asia 2001.

IGI Group's conference on Fiber Bandwidth Glut: Fact or Fiction, 2001.

Gilder Storewidth 2002

Gilder Telecosm, 2002, 2003, and 2004.

Reuters Venture Capital CTO Conference, 2002.

Pulver Fall 2002 VON.

OFC 2004.

Internet Commons Congress, 2004.

FastNet Futures, 2004.

Visitor at Institute for Advanced Study (part-time), 1983–1984.

Member of Ph.D thesis committee of B. Andrianalimanana, Lehigh University, 1979.

Informal supervisor (with R.L. Graham) of Ph.D. thesis of B. Temkin, City University of New York, 1983.

Supervisor of summer research projects at Bell Labs and AT&T Labs:

Margaret Chang Tuttle, 1984

Dana Randall, 1986

Brian LaMacchia, 1989

Linda Green, 1990

Chris Skinner, 1991

Bjorn Poonen, 1992

Eric Rains, 1993

David Moews, 1993

Michael Rubinstein, 1994

Igor Pak, 1995

Stanislaw Jarecki, 1996

Ryan Siders, 1996

Manjul Bhargava, 1997

Kiran Kedlaya, 1997

Yuliy Sannikov, 1998

Qian Chen, 2000

Supervisor of Brian LaMacchia's 1990–1991 research, leading to the 1991 MIT S.M. thesis in Computer Science, "Basis Reduction Algorithms and Subset Sum Problems."

Supervisor of Susanne Wetzel's research on cryptography and parallel computing on a Rotary scholarship during 1993–1994.

EDITORIAL

Editorial Board, *Journal of Algorithms*, 1980–.

Associate Editor for Complexity and Cryptography, *IEEE Trans. Information Theory*, 1983–1986.

Editor, *Aequationes Math.*, 1984–2005.

Editor, *Proc. Amer. Math. Soc.*, 1984–1989.

Associate Editor, *Math. Comp.*, 1985–1988. Member of Editorial Committee, 1989–1998.

Editorial Board, *J. Combinatorial Theory A*, 1987–.

Editorial Board, *Complex Systems*, 1987–.

Editor, *J. Cryptology*, 1988–2000.

Editorial Board, *SIAM J. Discrete Mathematics*, 1988–1991.

Associate Editor, *J. Comp. Sys. Sci.*, 1988–.

Editor of special issue (vol. 36, no. 2, 1988) of *J. Comp. Sys. Sci.* on 17th ACM Symp. Theory Comp.

Editorial Board, *Random Structures and Algorithms*, 1990–.

Editor, *Rev. Mat. Aplicadas*, 1990–1998.

Editorial Board, *Computational Complexity*, 1991–.

Editorial Committee, *J. Amer. Math. Soc.*, 1991–1998.

Editorial Board, *Neural, Parallel, and Scientific Computations*, 1993–1998.

Associate Editor, *J. Fourier Anal. Appl.*, 1993–.

Editorial Board, *Finite Fields Appl.*, 1993–.

Editorial Board, *Mathematical Research Letters*, 1994–.

Editorial Board, *Electr. Trans. Num. Anal.*, 1994–2003.

Editorial Board, *Electr. J. Combinatorics*, 1994–.

Editorial Board, *J. Universal Comp. Sci.*, 1994–.

Editorial Board, *Séminaire Lotharingien de Combinatoire*, 1994–.

Area editor for cryptology, *J. ACM*, 1995–2003.

Editorial Board, *Designs, Codes, and Cryptography*, 1996–.

Editorial Board, *Comm. Appl. Anal.*, 1997–.

Editorial Board, *IEEE Computational Science and Engineering*, 1998. Editorial Board, *Computing in Science and Engineering*, (successor to *IEEE Comp. Sci. Eng.*), 1999–2004.

Editorial Board, *Michigan Math. J.*, 1998–.

Editorial Board, *First Monday*, 2000–.

Advisory Board, *J. Found. Computational Math.*, 2001–2008.

Editorial Board, *Central European Journal of Mathematics*, 2003–.

Advisory Board, *Logical Methods in Computer Science*, 2003–.

Editorial Board, *Internet Mathematics*, 2003–.

Editorial Review Board, *Production and Operations Management*, 2004–.

Associate Editor, *J. American Mathematical Society*, 2004–2007.

One of guest editors of the issue of the *IEEE J. Selected Areas in Communications* on “Price-based access control and economics of networking,” vol. 24, no. 5, May 2006.

PROGRAM COMMITTEES

Chairman of Program Committee, CRYPTO 86.

Chairman of Program Committee, Number Theory Conference in Honor of Harold Stark, Minneapolis, 2004.

Co-chair, 3rd Workshop on Economics and Information Security, Minneapolis, 2004.

Program Committee, CRYPTO 87, CRYPTO 88, CRYPTO 93, CRYPTO 94, CRYPTO 95, CRYPTO 98, and CRYPTO 99.

Program Committee, EUROCRYPT 84, EUROCRYPT 85, EUROCRYPT 93, and EUROCRYPT 96.

Program Committee, ASIACRYPT 94, ASIACRYPT 98, and ASIACRYPT 99.

Program Committee, 17th ACM Symposium on Theory of Computing, 1985 and 20th ACM Symposium on Theory of Computing 1988.

Chairman of Organizing Committee, Joint AMS-IMS-SIAM Summer Research Conference on Computational Number Theory, 1985.

Organizer of a Minisymposium on Number Theory and its Applications at the 4th SIAM Conference on Discrete Mathematics, 1988.

Organizer of a Minisymposium on Parallel Processing in Mathematics at 7th SIAM Conference on Parallel Processing for Scientific Computing, San Francisco, 1995.

Co-organizer of 1989 Workshop on Mathematical Cryptography Theory, Oberwolfach.
Program Committee, 2nd ACM-SIAM Symposium on Discrete Algorithms, 1991.
Program Committee, LATIN '95.
Program Committee, WebNet 96, WebNet 97, WebNet 98, WebNet 99, WebNet 2000, and WebNet 2001.
Program Committee, Algorithmic Number Theory Symposium II, Bordeaux, 1996.
Co-organizer of the Computational Number Theory Workshop at DIMACS, 1991.
Co-organizer of the Workshop on Software for Mathematical Research at DIMACS, 1991.
Organizing Committee for the 1990–91 Special Year on Complexity Theory of Interactive Computation at DIMACS.
Co-organizer of conferences on Algorithms and Number Theory, Schloss Dagstuhl, 1992 and 1994.
Co-organizer of workshops on Cryptography, Schloss Dagstuhl, 1993 and 1997.
Organizing Committee of the Conference on Number Theoretic and Algebraic Methods in Computer Science, Moscow, 1993.
Co-organizer of workshop on the Future of Mathematical Communication, Berkeley, 1994.
Program Committee, Electronic Publishing and the Information Superhighway Conference, Boston, 1995.
Program Committee, Electronic Communications in Mathematics Workshop, Minneapolis, 1996.
Program Committee of the Cryptography and Computer Security Semester at the Isaac Newton Institute, 1996.
Organizing Committee of short course in Emerging Applications of Number Theory, IMA, 1996.
Program Committee, 1997 Information Security Workshop, JAIST.
Organizing Committee of short course in Coding Theory and Cryptography, IMA, 1998.
Organizing Committee, workshop on Algorithmic Number Theory, Schloss Dagstuhl, 1998.
Organizing Committee, Conference on the Mathematics of Public-Key Cryptography, Fields Institute, 1999.
Organizing Committee, workshop on Random Matrices and Their Applications, MSRI. 1999.
Co-organizer of workshop on Cryptography, Luminy, 1999.

Program Committee, ACM Conference on Electronic Commerce, Denver, 1999.

Scientific Committee, The Future of Mathematical Communications conference, Berkeley, 1999.

Organizing Committee, Workshop on Unusual Applications of Number Theory, DIMACS, 2000.

Program Committee, 12th Intern. Conference on Formal Power Series and Algebraic Combinatorics, Moscow, 2000.

Organizing Committee, Fall 2000 Program in Algorithmic Number Theory, MSRI.

Organizing Committee, Clay Mathematics Institute Introductory Workshop in Algorithmic Number Theory, MSRI, 2000.

Public-Key Cryptography and Computational Number Theory conference, Warsaw, Poland, 2000.

Program Committee, Cryptography and Lattices Conference, Providence, RI, 2001.

Program Committee, Ninth International Workshop on Quality of Service, Karlsruhe, Germany, 2001 and Tenth International Workshop on Quality of Service, Miami Beach, Florida, 2002.

Program Committee, Conference on Technologies, Protocols and Services for NGI (part of SPIE's ITCOM 2001), Denver, 2001.

Organizing Committee, Network Dynamics workshop, IMA, Minneapolis, 2001.

Program Committee, 14th Biannual ITS Conference, Seoul, Korea, 2002.

Program Committee, Second International Workshop on Internet Charging and QoS Technology (ICQT'02), Zurich, Switzerland, 2002.

Organizing Committee, 1st Workshop on Economics and Information Security, Berkeley, California, 2002 and 2nd, College Park, Maryland, 2003..

Steering Committee, SIAM International Conferences on Data Mining, 2002–2005.

Program Committee, IEEE International Security in Storage Workshop, Greenbelt, Maryland, 2002, Washington, DC, 2003, and San Francisco, California, 2005.

Program Committee, Financial Cryptography 2003, Guadeloupe, Financial Cryptography 2005, Dominica, and Financial Cryptography 2006, Anguilla.

Program Committee, Fifth International Conference on Electronic Commerce, Pittsburgh, 2003.

Program Committee, Third International Workshop on Internet Charging and QoS Technology (ICQT'03), Munich, Germany, 2003.

Program Committee, International Network Optimization Conference (INOC 2003), Paris, France, 2003 and INOC 2005, Lisbon, Portugal, 2005.

Program Committee, Fourth International Workshop on Internet Charging and QoS Technology (ICQT'04), Barcelona, Spain, 2004.

Program Committee, Sixth ACM Conference on Electronic Commerce (ACM EC 2005).

Program Committee, International Conference on Cryptology in Malaysia (Mycrypt 2005), Kuala Lumpur, Malaysia, 2005.

Program Committee, CoNEXT, Toulouse, France, 2005.

Program Committee, 3rd Workshop on the Economics of Peer-to-Peer Systems, Philadelphia, 2005.

Program Committee, 33rd and 34th Telecommunications Policy Research Conference, Arlington, VA, 2005 and 2006.

Program Committee, 9th Information Security Conference, Samos Island, Greece, 2006.

Program Committee, Workshop on the Economics of Securing the Information Infrastructure, Arlington, VA, 2006.

Program Committee, FM10 Openness: Code, Science, and Content, Chicago, IL, 2006.

Technical Program Committee, 20th International Teletraffic Congress, Ottawa, Canada, 2007.

AMERICAN MATHEMATICAL SOCIETY

AMS-IMS Committee on Translations, 1981-1984.

AMS Committee on the Publication Program, 1985-1993.

AMS Committee on Electronic Exchange of Information, 1988-1989.

Chair, Copyright Subcommittee of the AMS Committee on the Publication Program, 1993-1994.

AMS Committee on Publication Policy, 1994-1996.

AMS Abstracts Revision Task Force, 1995.

AMS Committee to select the Gibbs Lecturers for 1995-6.

Member-at-large, Council of the AMS, 1996-1998.

Executive Committee of the Council of the AMS, 1996-1999.

AMS Committee on Committees, 1997-98.

AMS Fulkerson Prize Selection Committee, 2002-2004.

OTHER COMMITTEES

Selection Panel for NSF Post-doctoral Fellowships, 1981–1983.

NSF Panel on Future Directions in Computational Mathematics, Algorithms, and Scientific Software (Rheinboldt Panel), 1984–5.

NSF Advisory Committee for Mathematical Sciences, 1987–1990.

Advisory Panel for the NSA Mathematical Sciences Program, 1990–1994.

NIST Panel for Computing and Applied Mathematics of the National Research Council, 1992–4.

Electronic Publishing Committee of the European Mathematical Society, 1995–2004.

AAAS Task Force on Transition from Paper, 1996–97.

International Mathematical Union Committee on Electronic Publishing, 1996–97.

arXiv Mathematics Preprint Archive Committee, 1997–2002.

ACM preprint database (CoRR) committee, 1997–.

SIAM Task Force for Computing, 1998–99.

MAA Committee on Industrial and Government Mathematicians, 2001–04.

SIAM selection committee for the 2002 George Pólya Prize.

The Economist Innovation Awards selection committee, 2002–2004.

Minnesota High Tech Association TEKNE Awards selection committee, 2005.

ADVISORY AND SUPERVISORY BOARDS

Scientific Advisory Council of the Berkeley Mathematical Sciences Research Institute, 1992–1995.

Executive Advisory Board, Mathematical Sciences Institute at Cornell/SUNY–Stony Brook, 1992–5.

Dean’s Advisory Council, School of Science, Purdue Univ., 1993–6.

Board of Governors, Institute of Mathematics and its Applications, Minneapolis, 1994–6. Chair, 1996.

Board of Trustees, Mathematical Sciences Research Institute, Berkeley, 1996–2000. Vice-chairman, 1997–2001.

Executive Committee of the Council of the AMS, 1996–2000.

Chairman of the Scientific Advisory Board of Cylink Corp., 1997–2000.

Scientific Advisory Committee for CRM, Centre de Recherches Mathématiques, Univ. Montréal, 1997–2002.

Mathematics Visiting Committee, Lehigh University, 1997–2000.

Mathematics Visiting Committee, Harvard, 1998–2004.

Scientific Advisory Board, Centre for Applied Cryptographic Research, University of Waterloo, 1998–.

Advisory Board of GlobeArc, Inc., 1999.

Advisory Board, Illinois Center for Cryptography and Information Protection, 2000–.

Scientific Research Board, American Institute for Mathematics, 2000–2001.

Merrill Lynch TechBrains Board, 2001–2005.

Advisory Board, Institute for New Media Studies, 2001–.

Scientific Research Board, American Institute for Mathematics and AIM Research Conference Center, 2002–2004.

Advisory Council, inCode Telecom Group, 2002–.

Ingenta Advisory Board, 2002–2003.

TrueDisk Technical Advisory Board, 2002.

Signal Lake Advisory Board, 2004–.

Board on Mathematical Sciences and Their Applications, National Academies, 2005–2008.

Coburn Ventures Change Fellow, 2005–.

MEMBERSHIP IN PROFESSIONAL SOCIETIES

American Mathematical Society

Association for Computing (ACM)

European Association for Theoretical Computer Science

Institute of Electrical and Electronic Engineers

International Association for Cryptologic Research

Mathematical Association of America

Society for Industrial and Applied Mathematics