

JOAN FEIGENBAUM

MAILING ADDRESS

Computer Science Department
Yale University
P.O. Box 208285
New Haven, CT 06520-8285 USA
URL: <http://www.cs.yale.edu/homes/jf/>

STREET ADDRESS

51 Prospect Street
New Haven, CT 06511 USA
Phone: +1 203 432-6432
Fax: +1 203 432-6373
Email: Joan.Feigenbaum@yale.edu

EMPLOYMENT HISTORY

Yale University, New Haven, CT	
<i>Grace Murray Hopper Professor of Computer Science</i>	04/2008 – present
<i>Henry Ford II Professor of Computer Science</i>	01/2006 – 03/2008
<i>Professor, Computer Science Department</i>	07/2000 – 12/2005
AT&T Labs – Research, Florham Park, NJ	
<i>Member of Research Staff</i>	1996 – 6/2000
<i>Head, Algorithms and Distributed Data</i>	1998 – 1999
AT&T Bell Laboratories, Murray Hill, NJ	
<i>Member of Technical Staff</i>	1986 – 1995

EDUCATION

Stanford University, Ph.D. in Computer Science	1986
Thesis Advisor: A. C. Yao	
Harvard University, B.A. in Mathematics	1981
Thesis Advisor: B. Mazur	
Yale University, M.A. Privatum	2001

CITIZENSHIP

United States

AWARDS

ACM Fellow	2001 – Present
AMS Winter Meeting Plenary Speaker	1999
ICM Invited Lecturer	1998

RESEARCH INTERESTS

Internet Algorithms, Security and Privacy, Computational Complexity,
Digital Copyright

EDITORIAL BOARDS

<i>ACM Trans. Economics and Computation</i> , Board Member	2011 – Present
<i>J. Cryptology</i> , Editor-in-Chief	1997 – 2002
<i>SIAM J. Computing</i> , Board Member	1993 – 2002

EDITORIAL BOARDS, Continued

<i>J. Algorithms</i> , Board Member	1992 – 1996
<i>J. Cryptology</i> , Board Member	1990 – 1996
<i>IEEE Trans. on Information Theory</i> , Guest Editor	1996
<i>J. Computing and System Sciences</i> , Guest Editor	1991, 1998
<i>J. Cryptology</i> , Guest Editor	1989 – 1990
<i>Communications of the ACM</i> , Guest Editor	1988 – 1989

PROGRAM-COMMITTEE CHAIR

<i>NetEcon</i> (Co-Chair with Y. R. Yang)	2008
<i>ACM Conference on Electronic Commerce</i> (Co-Chair with M. Seltzer)	2004
<i>ACM Workshop on Digital Rights Management</i>	2002
<i>IEEE Conference on Computational Complexity</i>	1998
<i>Crypto</i>	1991

PROGRAM-COMMITTEE MEMBER

<i>Crypto</i>	1989, 1993, 1996
<i>Eurocrypt</i>	1992, 1999
<i>Financial Cryptography</i>	1999, 2000
<i>ACM Conference on Computer and Communications Security</i>	1993, 1994, 2005
<i>IEEE Computer Security Foundations</i>	2000, 2012
<i>ACM Workshop on Security and Privacy in Digital Rights Management</i>	2001
<i>ACM Symposium on Theory of Computing</i>	1991, 1994, 1999, 2001, 2008
<i>IEEE Conference on Computation Complexity</i> (Then called “Structure in Complexity Theory”)	1993
<i>Intl. Colloquium on Automata, Languages, and Programming</i>	2011
<i>Intl. Computing and Combinatorics Conference</i>	1998
<i>ACM/SIAM Symposium on Discrete Algorithms</i>	1999
<i>ACM Symposium on Principles of Distributed Computing</i>	2004, 2009
<i>Workshop on Internet and Network Economics</i>	2005, 2008
<i>ACM Conference on Electronic Commerce</i>	2011
<i>ACM Web Science</i>	2012
<i>NetDB</i>	2007
<i>World Wide Web Conference</i>	2009

DIMACS-WORKSHOP CHAIR

Data Mining in the Internet Age (Co-chair with R. Agrawal, P. Raghavan, and J. Ullman)	2000
Management of Digital IP (Co-chair with D. Boneh and R. Venkatesan)	2000
Massive Data Sets in Telecommunications	1997

DIMACS-WORKSHOP CHAIR, Continued

Trust Management and Public-Key Infrastructure (Co-chair with E. Brickell and D. Maher)	1996
Complexity of Computer-Aided Verification (<i>Co-chair with R. Brayton and A. Emerson</i>)	1996
Structural Complexity and Cryptography (Co-chair with E. Allender and J.-Y. Cai)	1990
Distributed Computing and Cryptography (Co-chair with M. Merritt)	1989

ELECTED POSITIONS

ACM Sigecom Vice Chair	2005 – 2011
ACM Sigact Executive-Committee Member	2005 – 2009
Association for Women in Mathematics (AWM), Member at Large	2000 – 2004

OTHER PROFESSIONAL SERVICE

ACM Fellows, Selection-Committee Member	2012 – 2016
Knuth Prize, Selection-Committee Member	2009 – 2012
NSF Network Science and Engineering (NetSE), Council Member	2008 – 2009
NSF Cyber-Trust PI Meeting, Local Arrangements Chair	2008
Web Sciences Research Institute, Scientific Council Member	2006 – 2010
NetEcon, Steering Committee Member	2006 – Present
ACM Conference on Electronic Commerce, General Chair	2006
Member, SIGACT Committee for the Advancement of Theoretical Computer Science	2005 – 2007
DIMACS Special Focus on Computation and the Socio-Economic Sciences, Steering-Committee Member	2004 – 2007
International Association for Cryptologic Research, Fellows-Selection-Committee Member	2003 – 2006
American Association for the Advancement of Science Symposium, Session Organizer and Chair: <i>Incentive Compatibility in Internet Computation</i>	2003
Member, NAS Computer Science and Telecommunications Board	2002 – 2007
ACM Conference on Electronic Commerce, Tutorial Co-chair (with B. Grosz)	2003
ACM Workshop on Digital Rights Management, General Co-chair (with T. Sander)	2003
ACM Grace Murray Hopper Award, Selection-Committee Member	2001 – 2006
Institute for Mathematics and Its Applications (IMA), Member of Board of Directors	1999 – 2002
DIMACS Special Focus on Next-Generation Networks, Co-chair (with S. Muthukrishnan)	2000 – 2003
Advisory-Board Member, Johns Hopkins University Computer Science	1999 – 2000

OTHER PROFESSIONAL SERVICE, Continued

National Research Council Panel Member, Intellectual Property Protection in the Emerging Information Infrastructure	1998 – 1999
DIMACS Special Year on Massive Data Sets, Steering-Committee Member	1997 – 1998
DIMACS Research and Educational Institute (DREI '97): Three-week course and workshop on cryptology and security, Co-director (with S. Rudich)	1997
IEEE Conference on Computational Complexity, Steering-Committee Member	1994 – 1997
DIMACS Special Year on Logic and Algorithms, Steering-Committee Member	1995 – 1996
DIMACS Project-Committee Chair	1994 – 1996
National Academy of Sciences “Frontiers of Science” Symposium, Session organizer and chair: <i>Security and Privacy in the Information Economy</i>	1996
NSF Conference on Women in Science, Panel Member: <i>Past, Present, and Future Challenges</i>	1995
National Academy of Sciences “Frontiers of Science” Symposium, Participant	1995
American Association for the Advancement of Science Symposium, Session organizer and Chair: <i>Information Security: Principles and Public Policy</i>	1995
Computing Research Association Committee on the Status of Women, Charter Member	1991 – 1996
Grace Hopper Celebration of Women in Computing, Panel Member: <i>Science Policy</i>	1994
NSF, Member of Eleven Proposal-Evaluation Panels	1993 – 2011

GRANTS

NSF and ONR, N00014-980219 <i>ONR/NSF/AWM Workshops for Women Graduate Students and Postdoctoral Mathematicians</i> Co-PI (with S. Lenhart (PI) of Univ. Tennessee, C. Gordon of Dartmouth Univ., and G. Ratcliff of Univ. Missouri) \$230,000	01/97 – 12/99
Army Research Office, DAAG55-98-1-0393 <i>Checkers, Self-Testers, and Self-Correctors for Reactive Systems</i> Co-PI (with S. Kannan (PI) and I. Lee of Univ. Pennsylvania) \$270,000	07/98 – 07/01
DARPA, AF F39502-99-1-0512 <i>Scalable Trust of Next-Generation Management (STRONGMAN)</i> Co-PI (with J. Smith (PI) of Univ. Pennsylvania and M. Blaze and J. Ioannidis of AT&T) \$1,405,000	07/99 – 06/02

GRANTS, Continued

- ONR, N00014-01-1-0388 & AFOSR F49620-01-1-0157 01/01 – 12/03
Workshop Grant in support of AWM Workshops for Women Graduate students and Postdoctoral Mathematicians
Co-PI (with S. Lenhart (PI) of Univ. Tennessee, S.Geller of Texas A & M, E. Schaefer of Marymount Univ., and G. Ratcliff of Univ. Missouri)
\$259,000
- ONR, N00014-01-1-0795 05/01 – 04/06
Software Quality and Infrastructure Protection for Diffuse Computing
Co-PI (with A. Scedrov (PI) and J. Smith of Univ. Pennsylvania, J. Mitchell of Stanford Univ., J. Halpern of Cornell Univ., P. Lincoln of SRI, and C. Dwork of Microsoft)
\$5,000,000
- ONR, N00014-01-1-0447 06/01 – 12/01
A Game-Theoretic Treatment of Denial of Service
\$51,000
- NSF, CCR-0105337 06/01 – 05/04
Massive Data Streams: Algorithms and Complexity
PI (with S. Kannan of Univ. Pennsylvania)
\$256,300
- NSF, CCR-TC-0208972 07/02 – 07/05
GRIDLOCK: A New Scalable Approach to Unifying Computer and Communications Security
PI (with A. Keromytis of Columbia Univ. and J. Smith of Univ. Pennsylvania)
\$600,000
- NSF, ITR-0219018 08/02 – 07/05
Foundations of Distributed Algorithmic Mechanism Design
\$485,000
- NSF, ANIR-NR-0207399 08/02 – 08/05
Incentive-Compatible Designs for Distributed Systems
PI (with A. Krishnamurthy and R. Yang of Yale Univ. and S. Shenker of ICSI)
\$425,000
- NSF, ITR-0331548 10/03 – 09/10
Sensitive Information in a Wired World
Yale PI (with D. Boneh (PI), H. Garcia-Molina, J. Mitchell, and R. Motwani of Stanford; R. Kannan and A. Silberschatz of Yale; S. Forrest (PI) of Univ. New Mexico; H. Nissenbaum (PI) of NYU; and R. Wright (PI) of Rutgers)
\$12,500,000

GRANTS, Continued

US-Israel BSF, 2002065 <i>Decentralized Resource Allocation: Incentives and Computation</i> US PI (with N. Nisan (Israeli PI) of Hebrew University) \$120,000	10/03 – 09/07
ONR, N00014-04-1-0725 <i>Trustworthy Infrastructure, Mechanisms, and Experimentation for Diffuse Computing</i> Co-PI (with A. Scedrov (PI) and S. Zdancewic of Univ. of Pennsylvania, J. Mitchell of Stanford Univ., J. Halpern of Cornell Univ., and P. Lincoln of SRI) \$1,000,000	06/04 – 05/06
NSF, CNS-0428422 <i>An Economic Approach to Security</i> PI (with D. Bergemann of Yale Univ. and S. Shenker of ICSI) \$699,400	09/04 – 08/08
HSARPA, ARO-W911NF-05-1-0417 <i>Incrementally Deployable Security for Interdomain Routing</i> Co-PI (with J. Rexford (PI) of Princeton Univ.) \$407,483	08/05 – 04/08
NSF, IIS-0534052 and IIS-0534198 <i>New Privacy Frameworks for Collaborative Information Sharing</i> Co-PI (with V. Shmatikov (PI) of Univ. Texas) \$361,690	01/06 – 12/08
ARO, W911NF-06-1-0316 <i>Cyber-Threat Analytics</i> Yale PI (subcontract from SRI International, P. Porras (PI)) Yale budget: \$92,852	07/06 – 07/08
IARPA, FA8750-07-0031 <i>End-to-end, semantic accountability</i> Co-PI (with D. Weitzner (PI), H. Abelson, T. Berners-Lee, and G. Sussman of MIT, and J. Hendler of RPI) \$2,081,164	06/07 – 05/10
NSF, CCF-0728500 and CCF-0728443 <i>Foundations of Next-Generation Routing</i> Co-PI (with S. Shenker (PI) of ICSI) \$271,000	09/07 – 08/11
NSF, CNS-0716158, CNS-0716172, and CNS-0716223 <i>Massive-Dataset Algorithmics for Network Security</i> Co-PI (with V. Shmatikov (PI) of Univ. Texas and S. Kannan of Univ. Pennsylvania) \$250,000	10/07 – 09/10

GRANTS, Continued

ONR, N00014-09-10757 <i>Proactively Removing the Botnet Threat</i> PI (with S. Bellovin, A. Keromytis, and S. Stolfo of Columbia, V. Shmatikov and M. Walfish of Univ. Texas, and B. Ford of Yale) \$883,627	04/09 – 09/10
NSF, CNS-1016875 and CNS-1018557 <i>Accountability and Identifiability</i> Co-PI (with R. Wright (PI) and A. Jaggard of DIMACS) \$500,000	08/10 - 07/13
DARPA, N66001-11-C-4018 <i>DISSENT: Scalable and Disruption-Proof Anonymity for Interactive Internet Communication</i> Co-PI (with B. Ford (PI) of Yale and V. Shmatikov of Univ. Texas) \$2,078,695	10/10 - 09/14
IARPA, D11PC20198 <i>SPADE: Secure and Private Database Execution</i> Yale PI (subcontract from Applied Communication Sciences, T. Panagos (PI)) Yale budget: \$558,019	10/11 – 03/15

EDUCATION AND MENTORING

All are Yale University courses, postdocs, or students unless otherwise specified.

Classroom Teaching

<i>Computational Complexity</i>	Fall, 2010; Fall, 2009 Fall, 2008 Spring & Fall, 2007
<i>Mathematical Tools for Computer Science</i>	Fall, 2009
<i>Sensitive Information in a Wired World</i>	Fall, 2011 Spring, 2006 Fall, 2003
<i>The Internet: Co-Evolution of Technology and Society</i>	Spring, 2007 Fall, 2003
<i>Economics and Computation</i>	Fall, 2011; Fall, 2008 Spring, 2006 Spring, 2003 Spring, 2002
<i>E-commerce: Doing Business on the Internet</i>	Spring, 2003 Spring & Fall, 2001
<i>E-commerce Foundations</i>	Fall, 2000
<i>Number-Theoretic Algorithms and Cryptography</i> , Univ. of Pennsylvania	1996
<i>Cryptography and Security</i> , Columbia Univ.	1992
<i>Computability and Complexity Theory</i> , Columbia Univ.	1990

EDUCATION AND MENTORING, Continued

<i>Combinatorics and Discrete Math</i> , Columbia Univ.	1988
<u>Postdocs</u>	
Georgios Zervas	07/11 – present
Shaili Jain	10/10 – present
Michael Schapira	10/08 – 09/10
Fernando Esponda	01/06 – 06/07
Nimrod Kozlovski	07/04 – 06/05
Michael Elkin	09/03 – 08/04
<u>PhD Students</u>	
Debayan Gupta	Current
Raphael Ryger	Current
Hongda Xiao	Current
Felipe Saint-Jean	2010
Ramzi Dakdouk	2009
Aaron Johnson	2009
Vijay Ramachandran	2005
Jian Zhang	2005
Sheng Zhong	2004
Rahul Sami	2003
Ninghui Li, New York Univ.	2000
<u>PhD Thesis-Committee Memberships</u>	
Shaili Jain, Harvard Univ.	2010
Arvind Narayanan, Univ. of Texas	2009
Yinghua Wu	2009
Hao Wang	2008
Zheng Ma	2007
Zhiqiang Yang, Stevens Institute of Technology	2007
Kevin Chang	2006
Aleksandr Yampolskiy	2006
Kostas Anagnostakis, Univ. of Pennsylvania	2005
Dejing Dou	2004
Yael Gertner, Univ. of Pennsylvania	2003
Gauri Shah	2003
Xiaodong Sun, Rutgers Univ.	2003
Yehuda Lindell, Weizmann Institute of Science (external reader)	2002
Angelos Keromytis, Univ. of Pennsylvania	2001
Kobbi Nissim, Weizmann Institute of Science (external reader)	2001
Ashish Naik, SUNY Buffalo	1994
Nick Reingold	1992

EDUCATION AND MENTORING, Continued

Masters Students

Shu-Chun Weng	2011
Ashley Green	2004
Raghava Vellanki	2004
Pei-Wei Wu	2001
Yang-hua Chu, MIT	1997

Other

Women in Theory Symposium	2008
Panel Member: <i>Work-Life Balance</i>	
Panel Member: <i>Why Women Don't Ask</i>	
Association for Women in Mathematics "After-Tenure" Workshop	2004
Panel Speaker: <i>Leadership Roles outside of the University</i>	
Association for Women in Mathematics Workshop	1998
Invited Speaker: <i>Research Careers in Corporate Laboratories</i>	
Grace Hopper Celebration of Women in Computing	1997
Panel Member: <i>Building a Research Program</i>	
Julia Robinson Celebration of Women in Mathematics	1996
Panel Member: <i>Nonacademic Careers</i>	
ACM Federated Computing Research Conference	1996
Symposium on Academic Careers for Women	
Panel Member: <i>Building a Research Program</i>	
ACM Federated Computing Research Conference	1993
Symposium on Academic Careers for Women	
Panel Member: <i>Making Connections</i>	

SELECTED TALKS

Distinguished Lecture, Penn State University	12/2010
<i>The DISSENT Approach to Anonymous, Interactive Communication of the Internet</i>	
Keynote Lecture, IncoTrust Workshop	05/2010
<i>Accountability in International Data Exchange</i>	
Distinguished Lecture, Northwestern University	05/2009
<i>Approximate Privacy: Foundations and Quantification</i>	
Distinguished Lecture, UMASS Amherst	05/2009
<i>Approximate Privacy: Foundations and Quantification</i>	
Distinguished Lecture, Boston University	05/2009
<i>Approximate Privacy: Foundations and Quantification</i>	
NSF NetSE Informational Meeting	09/2008
Invited talk: <i>The SIGACT Community and the NetSE Program: A Match Made in Heaven</i>	
Women in Theory Symposium, Princeton NJ	06/2008
<i>Modeling and Analysis of Anonymous Communication Systems</i>	

SELECTED TALKS, Continued

Distinguished Lecture, Purdue University <i>Sensitive Information in a Networked World</i>	01/2008
FuDiCo III Keynote Speaker, Bertinoro, Italy <i>Theory of Networked Computing?</i>	06/2007
EECS/CASE Colloquium, Syracuse University <i>Sensitive Information in a Networked World</i>	11/2006
Computer Science Colloquium, Cornell University: <i>Incentive-Compatible Interdomain Routing</i>	10/2005
NYU Theory Day Invited Speaker: <i>Progress on the PORTIA Project</i>	11/2004
Radcliffe Institute Symposium on Privacy and Security Invited Speaker (with P. Swire): <i>Control of Personal Information</i>	04/2004
ACM Symposium on Principles of Distributed Computing Tutorial Speaker (with S. Shenker): <i>Incentives and Internet Algorithms</i>	07/2003
Stanford Institute for Theoretical Economics Invited Speaker: <i>Distributed Algorithmic Mechanism Design</i>	07/2002
Association for Symbolic Logic Annual Meeting Plenary Speaker: <i>Incentive-Compatible Distributed Algorithms</i>	03/2001
Computer Science Building Dedication, Harvard University Invited Speaker: <i>Research and Development on the Frontiers of E-Commerce</i>	10/1999
SIAM Annual Meeting Plenary Speaker: <i>Massive Graphs: Algorithms, Applications, and Open Problems</i>	05/1999
American Mathematical Society Winter Meeting Plenary Speaker: <i>Massive Graphs: Algorithms, Applications, and Open Problems</i>	01/1999
International Congress of Mathematicians Invited Speaker: <i>Games, Complexity Classes, and Approximation Algorithms</i>	08/1998
Grace Hopper Celebration of Women in Computing Plenary Lecturer: <i>Security and Privacy in the Information Economy</i>	09/1997
Julia Robinson Celebration of Women in Mathematics Plenary Lecturer: <i>Decentralized Trust Management</i>	07/1996
ACM Federated Computing Research Conference SIAM Symposium on Networks and Information Management Invited Speaker: <i>Decentralized Trust Management</i>	05/1996
University of Wisconsin Computer Sciences Department Distinguished Lecturer: <i>Decentralized Trust Management</i>	02/1996
American Mathematical Society Winter Meeting Invited Speaker: <i>The Role of Coding Theory in Computational Complexity</i>	01/1995

Updated: 01/17/12