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	
Grace Murray Hopper Professor of Computer Science	04/2008 – present
Professor (Adjunct) of Law	07/2016 – 06/2017
Department Chair, Computer Science	07/2014 – 06/2017
Henry Ford II Professor of Computer Science	01/2006 – 03/2008
Professor of Computer Science	07/2000 – 12/2005
AT&T Labs – Research, Florham Park, NJ	
Member of Research Staff	1996 – 6/2000
Department Head, Algorithms and Distributed Data	1998 – 1999
AT&T Bell Laboratories, Murray Hill, NJ	1986 – 1995
Member of Technical Staff	

EDUCATION

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

CITIZENSHIP: United States

AWARDS

Member, Connecticut Academy of Science and Engineering	2013 – Present
AAAS Fellow	2012 – Present
Connecticut Technology Council "Women of Innovation" Award	2012
ACM Fellow	2001 – Present
AMS Winter Meeting Plenary Speaker	1999
ICM Invited Lecturer	1998

RESEARCH INTERESTS

Security, Privacy, Anonymity, and Accountability
Internet Algorithmics
Computational Complexity

EDITORIAL BOARDS

PeerJ, Computer Science, Board Member	2015 – Present
ACM Trans. Economics and Computation, Board Member	2011 – 2016
J. Cryptology, Editor-in-Chief	1997 – 2002
SIAM J. Computing, Board Member	1993 – 2002
J. Algorithms, Board Member	1992 – 1996
J. Cryptology, Board Member	1990 – 1996
IEEE Trans. on Information Theory, Guest Editor	1996
J. Computing and System Sciences, Guest Editor	1991, 1998
J. Cryptology, Guest Editor	1989 – 1990
Communications of the ACM, Guest Editor	1988 – 1989

PROGRAM-COMMITTEE CHAIR

ACM Symposium on Theory of Computing	2013
NetEcon (Co-Chair with Y. R. Yang)	2008
ACM Conference on Electronic Commerce (Co-Chair with M. Seltzer)	2004
ACM Workshop on Digital Rights Management	2002
IEEE Conference on Computational Complexity	1998
Crypto	1991

PROGRAM-COMMITTEE MEMBER

Crypto	1989, 1993, 1996
Eurocrypt	1992, 1999
Financial Cryptography	1999, 2000
Workshop on Applied Homomorphic Cryptography	2016
ACM Conference on Computer and Communications Security	1993, 1994, 2005
IEEE Computer Security Foundations	2000, 2012
ACM Workshop on Security and Privacy in Digital Rights Management	2001
PETS Workshop on Surveillance and Technology	2015
ACM Symposium on Theory of Computing	1991, 1994, 1999, 2001, 2008
IEEE Conference on Computational Complexity *(Then called "Structure in Complexity Theory")*	1993
Intl. Colloquium on Automata, Languages, and Programming	2011
Intl. Computing and Combinatorics Conference	1998
ACM/SIAM Symposium on Discrete Algorithms	1999
ACM Symposium on Principles of Distributed Computing	2004, 2009
Workshop on Internet and Network Economics	2005, 2008
ACM Conference on Electronic Commerce	2011
ACM Conference on Economics and Computation	2014
ACM Web Science	2012
NetDB	2007
World Wide Web Conference	2009

PROGRAM-COMMITTEE MEMBER, Continued

USENIX Workshop on Free and Open Communication on the Internet	2013
ACM "Turing 50" Celebration	2017

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
Trust Management and Public-Key Infrastructure (Co-chair with E. Brickell and D. Maher)	1996
Complexity of Computer-Aided Verification *(Co-chair with R. Brayton* and A. Emerson)	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 SIGEcom Test of Time Award, Selection-Committee Member	2014 – 2016
ACM Fellows, Selection-Committee Member	2012 – 2015
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: *Incentive Compatibility in Internet Computation*	2003
Member, NAS Computer Science and Telecommunications Board	2002 – 2007

OTHER PROFESSIONAL SERVICE, Continued

ACM Conference on Electronic Commerce, Tutorial Co-chair (with B. Grosof)	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
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: *Security and Privacy in the Information Economy*	1996
NSF Conference on Women in Science, Panel Member: *Past, Present, and Future Challenges*	1995
National Academy of Sciences "Frontiers of Science" Symposium, Participant	1995
American Association for the Advancement of Science Symposium, Session organizer and Chair: *Information Security: Principles and Public Policy*	1995
Computing Research Association Committee on the Status of Women, Charter Member	1991 – 1996
Grace Hopper Celebration of Women in Computing, Panel Member: *Science Policy*	1994
NSF, Member of Twelve Proposal-Evaluation Panels	1993 – 2015

GRANTS

NSF and ONR, N00014-980219 01/97 – 12/99
ONR/NSF/AWM Workshops for Women Graduate Students and Postdoctoral Mathematicians
Co-PI (with S. Lenhart (PI) of Univ. Tennessee, C. Gordon of Dartmouth Univ., and G. Ratcliff of Univ. Missouri)
$230,000

Army Research Office, DAAG55-98-1-0393 07/98 – 07/01
Checkers, Self-Testers, and Self-Correctors for Reactive Systems
Co-PI (with S. Kannan (PI) and I. Lee of Univ. Pennsylvania)
$270,000

DARPA, AF F39502-99-1-0512 07/99 – 06/02
Scalable Trust of Next-Generation Management (STRONGMAN)
Co-PI (with J. Smith (PI) of Univ. Pennsylvania and M. Blaze and J. Ioannidis of AT&T)
$1,405,000

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

US-Israel BSF, 2002065 10/03 – 09/07
Decentralized Resource Allocation: Incentives and Computation
US PI (with N. Nisan (Israeli PI) of Hebrew University)
$120,000

ONR, N00014-04-1-0725 06/04 – 05/06
Trustworthy Infrastructure, Mechanisms, and Experimentation for Diffuse Computing
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

NSF, CNS-0428422 09/04 – 08/08
An Economic Approach to Security
PI (with D. Bergemann of Yale Univ. and S. Shenker of ICSI)
$699,400

HSARPA, ARO-W911NF-05-1-0417 08/05 – 04/08
Incrementally Deployable Security for Interdomain Routing
Co-PI (with J. Rexford (PI) of Princeton Univ.)
$407,483

NSF, IIS-0534052 and IIS-0534198 01/06 – 12/08
New Privacy Frameworks for Collaborative Information Sharing
Co-PI (with V. Shmatikov (PI) of Univ. Texas)
$361,690

ARO, W911NF-06-1-0316 07/06 – 07/08
Cyber-Threat Analytics
Yale PI (subcontract from SRI International, P. Porras (PI))
Yale budget: $92,852

IARPA, FA8750-07-0031 06/07 – 05/10
End-to-end, semantic accountability
Co-PI (with D. Weitzner (PI), H. Abelson, T. Berners-Lee, and G. Sussman of MIT, and J. Hendler of RPI)
$2,081,164

NSF, CCF-0728500 and CCF-0728443 09/07 – 08/11
Foundations of Next-Generation Routing
Co-PI (with S. Shenker (PI) of ICSI)
$271,000

NSF, CNS-0716158, CNS-0716172, and CNS-0716223 10/07 – 09/10
Massive-Dataset Algorithmics for Network Security
Co-PI (with V. Shmatikov (PI) of Univ. Texas and
S. Kannan of Univ. Pennsylvania)
$250,000

ONR, N00014-09-10757 04/09 – 09/10
Proactively Removing the Botnet Threat
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

NSF, CNS-1016875 and CNS-1018557 08/10 - 07/13
Accountability and Identifiability
Co-PI (with R. Wright (PI) and A. Jaggard of DIMACS)
$500,000

DARPA, N66001-11-C-4018 10/10 - 09/14
DISSENT: Scalable and Disruption-Proof Anonymity for
Interactive Internet Communication
Co-PI (with B. Ford (PI) of Yale and V. Shmatikov of Univ. Texas)
$2,078,695

IARPA, D11PC20198 10/11 – 03/15
SPADE: Secure and Private Database Execution
Yale PI (subcontract from Applied Communication Sciences,
T. Panagos (PI))
Yale budget: $558,019

ONR, N00014-12-10478 04/12 – 09/15
Reasoning Infrastructure for Secure-Aware Software Development
Co-PI (with B. Ford (PI) and Z. Shao of Yale)
$750,000

ONR, N000014-12-10522 07/12 – 06/15
Optimal Design of Peer Production and Crowdsourcing Systems
PI (with S. Jain (postdoc) of Yale)
$350,000

Google Faculty Research Award 09/12 – 02/13
Accountability and Choice in Online Consumer Feedback
PI (with G. Zervas (postdoc) of Yale and J. Byers of Boston Univ.)
$53,000

DARPA, FA8750-13-2-0058 01/13 – 05/15
Systematization of Secure Computation
PI (with R. Wright of DIMACS)
$678,093

GRANTS, Continued

NSF CNS-1409599 09/14 – 08/18
Hiding Hay in a Haystack: Integrating Censorship Resistance into the Mainstream Internet
PI
$600,000

NSF CNS-1407454 09/14 – 08/18
An App-Centric Transport Architecture for the Internet
PI
$400,000

Google Faculty Research Award 03/15 – 08/16
Privacy and Accountability in Lawful Surveillance
PI
$54,500

DHS grant FA8750-16-2-0034 02/16 – 02/19
PriFi Networking for Tracking-Resistant Mobile Computing
PI (with B. Ford of EPFL)
$1,727,334

William and Flora Hewlett Foundation grant 2016-3834 03/16 – 03/18
Law and Technology of Cyber Conflict
Co-PI (with O. Hathaway (PI) and Scott Shapiro of Yale Law School)
$406,000

EDUCATION AND MENTORING

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

Classroom Teaching

Law and Technology of Cyber Conflict	Fall, 2016
Law and Technology of Cyber Conflict: Practicum	Spring, 2017
Computational Complexity	Spring, 2016 Spring, 2015 Fall, 2012; Fall, 2010 Fall, 2009; Fall, 2008 Spring & Fall, 2007
Mathematical Tools for Computer Science	Fall, 2012; Fall, 2009
Sensitive Information in a Wired World	Fall, 2013; Fall, 2011 Spring, 2006 Fall, 2003
The Internet: Co-Evolution of Technology and Society	Spring, 2007 Fall, 2003
Economics and Computation	Fall, 2011; Fall, 2008 Spring, 2006 Spring, 2003 Spring, 2002

EDUCATION AND MENTORING, Continued

Classroom Teaching, Continued

E-commerce: Doing Business on the Internet	Spring, 2003 Spring & Fall, 2001
E-commerce Foundations	Fall, 2000
Number-Theoretic Algorithms and Cryptography, Univ. of Pennsylvania	1996
Cryptography and Security, Columbia Univ.	1992
Computability and Complexity Theory, Columbia Univ.	1990
Combinatorics and Discrete Math, Columbia Univ.	1988

Postdocs

Mahdi Zamani	02/16 – 12/16
Georgios Zervas	07/11 – 06/13
Shaili Jain	10/10 – 04/13
Michael Schapira	10/08 – 09/10
Fernando Esponda	01/06 – 06/07
Nimrod Kozlovski	07/04 – 06/05
Michael Elkin	09/03 – 08/04

PhD Students

Lihi Idan	Current
Raphael Ryger	Current
Debayan Gupta	2016
Aaron Segal (co-advised with Bryan Ford)	2016
Hongda Xiao	2014
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

PhD Thesis-Committee Memberships

John Maheswaran	2015
Ewa Syta	2015
Ennan Zhai	2015
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

EDUCATION AND MENTORING, Continued

PhD Thesis-Committee Memberships, Continued

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

Masters Students

Swara Kopparty	2015
Aditi Jain	2012
Ran Zhao	2012
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: *Work-Life Balance*	
Panel Member: *Why Women Don't Ask*	
Association for Women in Mathematics "After-Tenure" Workshop	2004
Panel Speaker: *Leadership Roles outside of the University*	
Association for Women in Mathematics Workshop	1998
Invited Speaker*: Research Careers in Corporate Laboratories*	
Grace Hopper Celebration of Women in Computing	1997
Panel Member: *Building a Research Program*	
Julia Robinson Celebration of Women in Mathematics	1996
Panel Member: *Nonacademic Careers*	
ACM Federated Computing Research Conference	1996
Symposium on Academic Careers for Women	
Panel Member: *Building a Research Program*	
ACM Federated Computing Research Conference	1993
Symposium on Academic Careers for Women	
Panel Member: *Making Connections*	

SELECTED TALKS

Project Overview, DARPA PROCEED PI Meeting	03/2015
Where We Stand with Respect to SMPC	

SELECTED TALKS, Continued

Invited Lecture, Pitney Bowes Security and Privacy Symposium 06/2013
Accountability and Deterrence in Online Life
Distinguished Lecture, University of Michigan 01/2013
The DISSENT Approach to Anonymous, Interactive Communication on the Internet
Invited Lecture, ACM/IEEE Symp. on Logic in Computer Science 06/2012
Privacy, Anonymity, and Accountability in Ad-Supported Services
Distinguished Lecture, University of Illinois 04/2011
The DISSENT Approach to Anonymous, Interactive Communication on the Internet
Distinguished Lecture, Penn State University 12/2010
The DISSENT Approach to Anonymous, Interactive Communication on the Internet
Keynote Lecture, IncoTrust Workshop 05/2010
Accountability in International Data Exchange
Distinguished Lecture, Northwestern University 05/2009
Approximate Privacy: Foundations and Quantification
Distinguished Lecture, UMASS Amherst 05/2009
Approximate Privacy: Foundations and Quantification
Distinguished Lecture, Boston University 05/2009
Approximate Privacy: Foundations and Quantification
NSF NetSE Informational Meeting 09/2008
Invited talk: *The SIGACT Community and the NetSE Program: A Match Made in Heaven*
Women in Theory Symposium, Princeton NJ 06/2008
Modeling and Analysis of Anonymous Communication Systems
Distinguished Lecture, Purdue University 01/2008
Sensitive Information in a Networked World
FuDiCo III Keynote Speaker, Bertinoro, Italy 06/2007
Theory of Networked Computing?
EECS/CASE Colloquium, Syracuse University 11/2006
Sensitive Information in a Networked World
Computer Science Colloquium, Cornell University: 10/2005
Incentive-Compatible Interdomain Routing
NYU Theory Day Invited Speaker: *Progress on the PORTIA Project* 11/2004
Radcliffe Institute Symposium on Privacy and Security 04/2004
Invited Speaker (with P. Swire): *Control of Personal Information*
ACM Symposium on Principles of Distributed Computing 07/2003
Tutorial Speaker (with S. Shenker): *Incentives and Internet Algorithms*
Stanford Institute for Theoretical Economics 07/2002
Invited Speaker: *Distributed Algorithmic Mechanism Design*
Association for Symbolic Logic Annual Meeting 03/2001
Plenary Speaker: *Incentive-Compatible Distributed Algorithms*

SELECTED TALKS, Continued

Computer Science Building Dedication, Harvard University 10/1999
Invited Speaker: *Research and Development on the Frontiers of E-Commerce*

SIAM Annual Meeting 05/1999
Plenary Speaker: *Massive Graphs: Algorithms, Applications, and Open Problems*

American Mathematical Society Winter Meeting 01/1999
Plenary Speaker: *Massive Graphs: Algorithms, Applications, and Open Problems*

International Congress of Mathematicians 08/1998
Invited Speaker: *Games, Complexity Classes, and Approximation Algorithms*

Grace Hopper Celebration of Women in Computing 09/1997
Plenary Lecturer: *Security and Privacy in the Information Economy*

Julia Robinson Celebration of Women in Mathematics 07/1996
Plenary Lecturer: *Decentralized Trust Management*

ACM Federated Computing Research Conference SIAM Symposium on 05/1996
Networks and Information Management
Invited Speaker: *Decentralized Trust Management*

University of Wisconsin Computer Sciences Department 02/1996
Distinguished Lecturer: *Decentralized Trust Management*

American Mathematical Society Winter Meeting 01/1995
Invited Speaker: *The Role of Coding Theory in Computational Complexity*

Updated: June 26, 2017