

PUBLICATIONS

Joan Feigenbaum

March 6, 2017

Journal and Book Articles

1. J. Feigenbaum and B. Ford, “Seeking Anonymity in an Internet Panopticon,” *Communications of the ACM* **58:10** (Oct. 2015), pp. 58 – 69.
2. D. Jaggard, A. Johnson, S. Cortes, P. Syverson, and J. Feigenbaum, “20,000 In League Under the Sea: Anonymous Communication, Trust, MLATs, and Undersea Cables,” *Proceedings on Privacy Enhancing Technologies* **1** (2015), pp. 4 – 24.
3. J. Feigenbaum, A. D. Jaggard, and M. Schapira, “Approximate Privacy: Foundations and Quantification,” *ACM Transactions on Algorithms*, Volume 10, Issue 3, Article 11 (June 2014). Extended abstract appears in *Proceedings of the 2010 ACM Conference on Electronic Commerce*; related material appears in DIMACS Technical Reports 2009-14 and 2010-01.
4. J. Feigenbaum, A. Johnson, and P. Syverson, “A Probabilistic Analysis of Onion Routing in a Black-Box Model,” *ACM Transactions on Information and System Security*, Volume 15, Issue 3, Article 14 (November 2012). Preliminary version appears in *Proceedings of the 2007 Workshop on Privacy in the Electronic Society*.
5. J. Feigenbaum, V. Ramachandran, and M. Schapira, “Incentive-Compatible Interdomain Routing,” *Distributed Computing* **23** (2011), pp. 301 – 319. Preliminary version appears in *Proceedings of the 2006 ACM Conference on Electronic Commerce*.
6. J. Feigenbaum, D. Parkes, and D. Pennock, “Computational Challenges in Electronic Commerce,” *Communications of the ACM* **52:1** (Jan. 2009), pp. 70 – 74.
7. J. Feigenbaum, S. Kannan, A. McGregor, S. Suri, and J. Zhang, “Graph Distances in the Data-Stream Model,” *SIAM Journal on Computing* **38** (2008), pp. 1709 – 1727. Extended abstract appears in *Proceedings of the 2005 ACM/SIAM Symposium on Discrete Algorithms*.
8. D. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G. Sussman, “Information Accountability,” *Communications of the ACM* **51:6** (June 2008), pp. 82 – 88.
9. J. Feigenbaum, J. Halpern, P. Lincoln, J. Mitchell, A. Scedrov, J. Smith, and P. Syverson, “Software Quality and Infrastructure Protection for Diffuse Computing,” in **Information Security Research**, Wiley, 2007, pp. 559 – 566.

10. J. Feigenbaum, M. Schapira, and S. Shenker, “Distributed Algorithmic Mechanism Design,” Chapter 14 in **Algorithmic Game Theory**, Cambridge University Press, 2007, pp. 363 – 384.
11. J. Aspnes, J. Feigenbaum, A. Yampolskiy, and S. Zhong, “Towards a Theory of Data Entanglement,” *Theoretical Computer Science* **389** (2007), pp. 26 – 43. Extended abstract appears in *Proceedings of the 2004 European Symposium on Research in Computer Security*.
12. J. Feigenbaum, D. Karger, V. Mirrokni, and R. Sami, “Subjective-Cost Policy Routing,” *Theoretical Computer Science* **378** (2007), pp. 175 – 189. Special issue of selected papers from the 2005 *Workshop on Internet and Network Economics*.
13. J. Feigenbaum, Y. Ishai, T. Malkin, K. Nissim, M. Strauss, and R. Wright, “Secure Multiparty Computation of Approximations,” *ACM Transactions on Algorithms* **2** (2006), pp. 435 – 472. Extended abstract appears in *Proceedings of the 2001 International Colloquium on Automata, Languages, and Programming*.
14. J. Feigenbaum, R. Sami, and S. Shenker, “Mechanism Design for Policy Routing,” *Distributed Computing* **18** (2006), pp. 293 - 305. Special issue of selected papers from the 2004 *ACM Symposium on Principles of Distributed Computing*.
15. J. Feigenbaum, S. Kannan, A. McGregor, S. Suri, and J. Zhang, “On Graph Problems in a Semi-Streaming Model,” *Theoretical Computer Science* **348** (2005), pp. 207 - 216. Special issue of selected papers from the 2004 *International Colloquium on Automata, Languages, and Programming*.
16. J. Feigenbaum, L. Fortnow, D. Pennock, and R. Sami, “Computation in a Distributed Information Market,” *Theoretical Computer Science* **343** (2005), pp. 114 - 132. Preliminary version appears in *Proceedings of the 2003 ACM Conference on Electronic Commerce*.
17. J. Feigenbaum, C. Papadimitriou, R. Sami, and S. Shenker, “A BGP-based Mechanism for Lowest-Cost Routing,” *Distributed Computing* **18** (2005), pp. 61 - 72. Special issue of selected papers from the 2002 *ACM Symposium on Principles of Distributed Computing*.
18. J. Feigenbaum, S. Kannan, and J. Zhang, “Computing Diameter in the Streaming and Sliding-Window Models,” *Algorithmica* **41** (2005), pp. 25 - 41.
19. Archer, J. Feigenbaum, A. Krishnamurthy, R. Sami, and S. Shenker, “Approximation and Collusion in Multicast Cost Sharing,” *Games and Economic Behavior* **47** (2004), pp. 36 - 71. Abstract appears in *Proceedings of the 2001 ACM Conference on Electronic Commerce*.

20. N. Li, B. Grosz, and J. Feigenbaum, "Delegation Logic: A Logic-Based Approach to Distributed Authorization," *ACM Transactions on Information and Systems Security* **6** (2003), pp. 128 - 171. Parts of this paper appear in preliminary form in the 1999 *IEEE Computer Security Foundations Workshop* and the 2000 *IEEE Symposium on Security and Privacy*.
21. J. Feigenbaum, A. Krishnamurthy, R. Sami, and S. Shenker, "Hardness Results for Multicast Cost Sharing," *Theoretical Computer Science* **304** (2003), pp. 215 - 236. Extended abstract appears in *Proceedings of the 2002 Conference on Foundations of Software Technology and Theoretical Computer Science*.
22. J. Feigenbaum, S. Kannan, M. Strauss, and M. Viswanathan, "Testing and Spot-Checking of Data Streams," *Algorithmica* **34** (2002), pp. 67 - 80. Extended abstract appears in *Proceedings of the 2000 ACM/SIAM Symposium on Discrete Algorithms*.
23. J. Feigenbaum, S. Kannan, M. Strauss, and M. Viswanathan, "An Approximate L^1 -Difference Algorithm for Massive Data Streams," *SIAM Journal on Computing* **32** (2002), pp. 131 - 151. Extended abstract appears in *Proceedings of the 1999 IEEE Symposium on Foundations of Computer Science*.
24. J. Feigenbaum, C. Papadimitriou, and S. Shenker, "Sharing the Cost of Multicast Transmissions," *Journal of Computer and System Sciences* **63** (2001), pp. 21 - 41 (Special issue on Internet Algorithms). Preliminary version appears in *Proceedings of the 2000 ACM Symposium on Theory of Computing*.
25. J. Feigenbaum and S. Kannan, "Dynamic Graph Algorithms," in **Handbook of Discrete and Combinatorial Mathematics**, K. Rosen (ed.), CRC Press, Boca Raton, 2000, pp. 1142 - 1151.
26. J. Feigenbaum, S. Kannan, M. Vardi, and M. Viswanathan, "The Complexity of Problems on Graphs Represented by OBDDs," *Chicago Journal of Theoretical Computer Science*, vol. 1999, number 5.
<http://www.cs.uchicago.edu/publications/cjtc/articles/1999/5/contents.html>.
Extended Abstract appears in *Proceedings of the 1998 Symposium on Theoretical Aspects of Computer Science*.
27. M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis, "The Role of Trust Management in Distributed System Security," in **Secure Internet Programming: Security Issues for Distributed and Mobile Objects**, J. Vitek and C. Jensen (eds.), Lecture Notes in Computer Science, vol. 1603, Springer, Berlin, 1999, pp. 185 - 210.
28. J. Feigenbaum, L. Fortnow, S. Laplante, and A. Naik, "On Coherence, Random-Self Reducibility, and Self-Correction," *Computational Complexity* **7** (1998), pp. 174 - 191. Extended abstract appears in *Proceedings of the 1996 IEEE Conference on Computational Complexity*. (The first ten in this series of conferences were called *Structure in Complexity Theory*.)

29. J. Feigenbaum, "Games, Complexity Classes, and Approximation Algorithms," in **Proceedings of the International Congress of Mathematicians, volume III: Invited Lectures**, *Documenta Mathematica, Journal der Deutschen Mathematiker-Vereinigung*, 1998, pp. 429 - 439.
30. L. Cowen, J. Feigenbaum, and S. Kannan, "A Formal Framework for Evaluating Heuristic Programs," *Annals of Mathematics and Artificial Intelligence* **22** (1998), pp. 193 - 206. Extended abstract appears in *Proceedings of the 1996 International Colloquium on Automata, Languages, and Programming*.
31. M. Blaze, J. Feigenbaum, P. Resnick, and M. Strauss, "Managing Trust in an Information-Labeling System," *European Transactions on Telecommunications* **8** (1997), pp. 491 - 501. Special issue of selected papers from the 1996 *Amalfi Conference on Secure Communication in Networks*.
32. Y.-H. Chu, J. Feigenbaum, B. LaMacchia, P. Resnick, and M. Strauss, "REFEREE: Trust Management for Web Applications," *Computer Networks and ISDN Systems* **29** (1997), pp. 953 - 964. Reprinted from *Proceedings of the 1997 International World Wide Web Conference*.
33. J. Feigenbaum, S. Rudich, M. Blaze, and K. McCurley, "Security and Privacy in the Information Economy," *Proceedings of the National Academy of Sciences* **94** (1997), pp. 2789 - 2792. Erratum for bibliography: **94** (1997), p. 6577.
34. Condon, J. Feigenbaum, C. Lund, and P. Shor, "Random Debaters and the Hardness of Approximating Stochastic Functions," *SIAM Journal on Computing* **26** (1997), pp. 369 - 400. Extended abstract appears in *Proceedings of the 1994 IEEE Conference on Structure in Complexity Theory*.
35. D. Beaver, J. Feigenbaum, J. Kilian, and P. Rogaway, "Locally Random Reductions: Improvements and Applications," *Journal of Cryptology* **10** (1997), pp. 17 - 36.
36. J. Feigenbaum, G. D. Forney, Jr., B. H. Marcus, R. J. McEliece, and A. Vardy, "Introduction to the Special Issue on Codes and Complexity," *IEEE Transactions on Information Theory* **42** (1996), pp. 1649 - 1659.
37. Condon, J. Feigenbaum, C. Lund, and P. Shor, "Probabilistically Checkable Debate Systems and Nonapproximability Results for PSPACE-Hard Functions," *Chicago Journal of Theoretical Computer Science*, vol. 1995, number 4. <http://www.cs.uchicago.edu/publications/cjtc/articles/1995/4/contents.html>. Extended abstract appears in *Proceedings of the 1993 ACM Symposium on Theory of Computing*.

38. J. Feigenbaum, "The Use of Coding Theory in Computational Complexity," in **Different Aspects of Coding Theory**, *Proceedings of Symposia on Applied Mathematics*, R. Calderbank (ed.), American Mathematical Society, Providence, 1995, pp. 207 - 233.
39. J. Feigenbaum, L. Fortnow, C. Lund, and D. Spielman, "The Power of Adaptiveness and Additional Queries in Random-Self-Reductions," *Computational Complexity* **4** (1994), pp. 158 - 174. Extended abstract appears in *Proceedings of the 1992 IEEE Conference on Structure in Complexity Theory*.
40. J. Feigenbaum and N. Reingold, "Universal Traversal Sequences," *American Mathematical Monthly* **101** (1994), pp. 262 - 265.
41. J. Feigenbaum, "Locally Random Reductions in Interactive Complexity Theory," in **Advances in Computational Complexity Theory**, *DIMACS Series on Discrete Mathematics and Theoretical Computer Science*, J.-y. Cai (ed.), vol. 13, American Mathematical Society, Providence, 1993, pp. 73 - 98.
42. J. Feigenbaum, J. A. Kahn, and C. Lund, "Complexity Results for POMSET Languages," *SIAM Journal on Discrete Mathematics* **6** (1993), pp. 432 - 442. Extended abstract appears in *Proceedings of the 1991 Workshop on Computer-Aided Verification*.
43. J. Feigenbaum and L. Fortnow, "Random-Self-Reducibility of Complete Sets," *SIAM Journal on Computing* **22** (1993), pp. 994 - 1005. Extended abstract appears in *Proceedings of the 1991 IEEE Conference on Structure in Complexity Theory*.
44. J. Feigenbaum, E. Grosse, and J. Reeds, "Cryptographic Protection of Membership Lists," *Newsletter of the International Association for Cryptologic Research* **9** (1992), pp. 16 - 20.
45. J. Feigenbaum and J. Lagarias, "Probabilistic Algorithms for Speed-Up," in **Probability and Algorithms**, M. Steele (ed.), National Academy Press, Washington DC, 1992, pp. 39 - 51. Reprinted by invitation in *Statistical Sciences* **8** (1993), pp. 20 - 25.
46. J. Feigenbaum, "Probabilistic Algorithms for Defeating Adversaries," in **Probability and Algorithms**, M. Steele (ed.), National Academy Press, Washington DC, 1992, pp. 53 - 63. Reprinted by invitation in *Statistical Sciences* **8** (1993), pp. 26 - 30.
47. J. Feigenbaum, "Overview of Interactive Proof Systems and Zero-Knowledge," in **Contemporary Cryptology: The Science of Information Integrity**, G. Simmons (ed.), IEEE Press, New York, 1992, pp. 423 - 439.
48. J. Feigenbaum and A. A. Schaffer, "Finding the Prime Factors of Strong Direct Product Graphs in Polynomial Time," *Discrete Mathematics* **109** (1992), pp. 77 - 102.

49. R. Beigel and J. Feigenbaum, "On Being Incoherent Without Being Very Hard," *Computational Complexity* **2** (1992), pp. 1 - 17.
50. J. Feigenbaum, M. Liberman, and R. Wright, "Cryptographic Protection of Databases and Software," in **Distributed Computing and Cryptography**, *DIMACS Series on Discrete Mathematics and Theoretical Computer Science*, J. Feigenbaum and M. Merritt (eds.), vol. 2, American Mathematical Society, Providence, 1991, pp. 161 - 172.
51. J. Feigenbaum and M. Merritt, "Open Questions, Talk Abstracts, and Summary of Discussions," in **Distributed Computing and Cryptography**, *DIMACS Series on Discrete Mathematics and Theoretical Computer Science*, J. Feigenbaum and M. Merritt (eds.), vol. 2, American Mathematical Society, Providence, 1991, pp. 1 - 45.
52. J. Feigenbaum, "Lexicographically Factorable Extensions of Irreducible Graphs," in **Graph Theory, Combinatorics, and Applications: vol. 1**, John Wiley and Sons, New York, 1991, pp. 481 - 492.
53. D. Eppstein, J. Feigenbaum, and C.-L. Li, "Equipartitions of Graphs," *Discrete Mathematics* **91** (1991), pp. 239 - 248.
54. M. Abadi and J. Feigenbaum, "Secure Circuit Evaluation: A Protocol Based on Hiding Information from an Oracle," *Journal of Cryptology* **2** (1990), pp. 1 - 12. Extended abstract appears in *Proceedings of the 1988 Symposium on Theoretical Aspects of Computer Science*.
55. M. Abadi, J. Feigenbaum, and J. Kilian, "On Hiding Information from an Oracle," *Journal of Computer and System Sciences* **39** (1989), pp. 21 - 50. (Special issue of selected papers from the 1987 IEEE Conference on Structure in Complexity Theory.) Extended abstract appears in *Proceedings of the 1987 ACM Symposium on Theory of Computing* and of the 1987 IEEE Conference on Structure in Complexity Theory.
56. J. Feigenbaum and R. Haddad, "On Factorable Extensions and Subgraphs of Prime Graphs," *SIAM Journal on Discrete Mathematics* **2** (1989), pp. 197 - 218.
57. J. Feigenbaum, "Directed Cartesian Product Graphs Have Unique Factorizations that Can be Computed in Polynomial Time," *Discrete Applied Mathematics* **15** (1986), pp. 105 - 110.
58. J. Feigenbaum and A. A. Schäffer, "Recognizing Composite Graphs is Equivalent to Testing Graph Isomorphism," *SIAM Journal on Computing* **15** (1986), pp. 619 - 627.
59. J. Feigenbaum, J. Hershberger, and A. A. Schäffer, "A Polynomial-Time Algorithm for Finding the Prime Factors of Cartesian-Product Graphs," *Discrete Applied Mathematics* **12** (1985), pp. 123 - 138.

60. H. F. Korth, G. M. Kuper, J. Feigenbaum, J. D. Ullman, and A. Van Gelder, "System/U: A Database System Based on the Universal Relation Assumption," *ACM Transactions on Database Systems* **9** (1984), pp. 331 - 347.
61. J. Feigenbaum and R. E. Tarjan, "Two New Kinds of Biased Search Trees," *Bell System Technical Journal* **62** (1983), pp. 3139 - 3158.

Proceedings Articles and Technical Reports

62. J. Feigenbaum and B. Ford, "Multiple Objectives of Lawful-Surveillance Protocols," to appear in *Proceedings of the 25th International Workshop on Security Protocols*, 2017.
63. A. Johnson, R. Jansen, A. D. Jaggard, J. Feigenbaum, and P. Syverson, "Avoiding The Man on the Wire: Improving Tor's Security with Trust-Aware Path Selection," in *Proceedings of the 24th Symposium on Network and Distributed System Security (NDSS)*, 2017.
64. A. Segal, J. Feigenbaum, and B. Ford, "Privacy-Preserving Lawful Contact Chaining (Preliminary Report)," in *Proceedings of the 15th Workshop on Privacy in the Electronic Society (WPES)*, ACM Press, New York, 2016, pp. 185 - 188.
65. L. Barman, M. Zamani, I. Dacosta, J. Feigenbaum, B. Ford, J-P Hubaux, and D. Wolinsky, "PriFi: A Low-Latency and Tracking-Resistant Protocol for Local-Area Anonymous Communication," in *Proceedings of the 15th Workshop on Privacy in the Electronic Society (WPES)*, ACM Press, New York, 2016, pp. 181 - 184.
66. A. Segal, J. Feigenbaum, and B. Ford, "Open, Privacy-Preserving Protocols for Lawful Surveillance," <http://arxiv.org/abs/1607.03659>. Also available as Technical Report YALEU/DCS/TR-1526, Yale University, New Haven, CT, July 2016.
67. D. Gupta, B. Mood, J. Feigenbaum, K. Butler, and P. Traynor, "Using Intel Software Guard Extensions for Efficient Two-Party Secure Function Evaluation," in *Proceedings of the 4th FC Workshop on Encrypted Computing and Applied Homomorphic Cryptography*, Lecture Notes in Computer Science, vol. 9604, Springer, Berlin, 2016, pp. 302 - 318.
68. J. Feigenbaum and R. N. Wright, "Systemization of Secure Computation," Technical Report AFRL-RI-RS-TR-2015-241, November 2015.
69. J. Feigenbaum and B. Rosen, "On the use of security and privacy technology as a plot device," in *Proceedings of the 23rd International Workshop on Security Protocols*, Lecture Notes in Computer Science, vol. 9379, Springer, Berlin, 2015, pp. 261 - 275. The appendix of this paper is the short story "Drive Me Crazy" listed in the Fiction section below.

70. B. Mood, D. Gupta, K. Butler, and J. Feigenbaum, "Reuse It or Lose It: More Efficient Secure Computation Through Reuse of Encrypted Values," in *Proceedings of the 21st Conference on Computer and Communications Security (CCS)*, ACM Press, New York, 2014, pp. 582 - 596. Expanded version available at <http://arxiv.org/abs/1506.02954>.
71. Segal, B. Ford, and J. Feigenbaum, "Catching Bandits and *Only* Bandits: Privacy-Preserving Intersection Warrants for Lawful Surveillance," in *Proceedings of the 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI)*, 2014.
72. J. Perry, D. Gupta, J. Feigenbaum, and R. N. Wright, "Systematizing Secure Computation for Research and Decision Support," in *Proceedings of the 9th Conference on Security and Cryptography for Networks (SCN)*, Lecture Notes in Computer Science, vol. 8642, Springer, Berlin, 2014, pp. 380 - 397.
73. A.D. Jaggard, A. Johnson, P. Syverson, and J. Feigenbaum, "Representing Network Trust and Using It to Improve Anonymous Communication," in *7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs)*, 2014.
74. J. Feigenbaum, A. D. Jaggard, and R. N. Wright, "Open vs. Closed Systems for Accountability," in *HotSoS'14: Proceedings of the 2014 ACM Symposium and Boot Camp on the Science of Security*, Article No. 4.
75. J. Feigenbaum and J. Koenig. "On the Feasibility of a Technological Response to the Surveillance Morass," in *Proceedings of the 22nd International Workshop on Security Protocols*, Lecture Notes in Computer Science, vol. 8809, Springer, Berlin, 2014, pp. 239 - 252.
76. G. DiCrescenzo, J. Feigenbaum, D. Gupta, T. Panagos, J. Perry, and R. N. Wright, "Practical and Privacy-Preserving Policy Compliance for Outsourced Data," in *Proceedings of the 2nd Workshop on Encrypted Computing and Applied Homomorphic Cryptography and Encrypted Computing (WAHC)*, FC 2014 Workshops, Lecture Notes in Computer Science, vol. 8438, Springer, Berlin, 2014, pp. 181 - 194.
77. J. Feigenbaum, "How Useful are Formal Models of Accountability?," in *2nd International Workshop on Accountability: Science, Technology, and Policy*, Cambridge MA, January 2014.
78. H. Xiao, B. Ford, and J. Feigenbaum, "Structural Cloud Audits that Protect Private Information," in *Proceedings of the 5th Cloud Computing Security Workshop (CCSW)*, ACM Press, New York, 2013, pp. 101 - 112.

79. J. Feigenbaum, A. D. Jaggard, and R. N. Wright, "Accountability as an Interface between Cybersecurity and Social Science," in *Proceedings of the Workshop to Explore Social Science Contributions to Understanding Cyber Security*, Orlando FL, April 2013.
80. D. Gupta, A. Segal, A. Panda, G. Segev, M. Schapira, J. Feigenbaum, J. Rexford, and S. Shenker, "A New Approach to Interdomain Routing Based on Secure Multi-Party Computation," in *Proceedings of the 2012 ACM Workshop on Hot Topics in Networks (HotNets)*.
81. J. Feigenbaum, M. Mitzenmacher, and G. Zervas, "An Economic Analysis of User-Privacy Options in Ad-Supported Services," in *Proceedings of the 8th Workshop on Internet and Network Economics (WINE)*, Lecture Notes in Computer Science, vol. 7695, Springer, Berlin, 2012, pp. 30 - 43.
82. J. Feigenbaum, A. Johnson, and P. Syverson, "Anonymity Analysis of Onion Routing in the Universally Composable Framework," in *Proceedings of the 2012 Workshop on Provable Privacy*.
83. J. Feigenbaum, B. Godfrey, A. Panda, M. Schapira, S. Shenker, and A. Singla, "Brief Announcement: On the Resilience of Routing Tables," in *Proceedings of the 2012 ACM Symposium on Principles of Distributed Computing (PODC)*. Expanded version is available as YALEU/DCS/TR-1454, Yale University, New Haven, CT, August 2012.
84. J. Feigenbaum, "Privacy, Anonymity, and Accountability in Ad-Supported Services," in *Proceedings of the 2012 ACM/IEEE Symposium on Logic in Computer Science (LICS)*, IEEE Computer Society Press, Los Alamitos, 2012, pp. 9 - 10.
85. J. Feigenbaum, A. D. Jaggard, R. N. Wright, and H. Xiao, "Systematizing 'Accountability' in Computer Science (Version of Feb. 17, 2012)," YALEU/DCS/TR-1452, Yale University, New Haven, CT, February 2012.
86. J. Feigenbaum, "Defining 'Anonymity' in Networked Communication, version 1," YALEU/DCS/TR-1448, Yale University, New Haven, CT, December 2011.
87. J. Feigenbaum, A. D. Jaggard, and R. N. Wright, "Towards a Formal Model of Accountability," in *Proceedings of the 14th New Security Paradigms Workshop (NSPW)*, ACM Press, New York, 2011, pp. 45 - 56.
88. J. Feigenbaum, J. A. Hendler, A. D. Jaggard, D. J. Weitzner, and R. N. Wright, "Accountability and Deterrence in Online Life (Extended Abstract)," in *Proceedings of the 3rd International Conference on Web Science*, ACM Press, New York, 2011.

89. F. Saint-Jean, J. Zhang, J. Feigenbaum, and P. Porras, "Privacy-Preserving Discovery of Consensus Signatures," YALEU/DCS/TR-1429, Yale University, New Haven CT, July 2010.
90. F. Saint-Jean and J. Feigenbaum, "Usability of Browser-Based Tools for Web-Search Privacy," YALEU/DCS/TR-1424, Yale University, New Haven CT, March 2010.
91. J. Feigenbaum, A. Johnson, and P. Syverson, "Preventing Active Timing Attacks in Low- Latency Anonymous Communication," in *Proceedings of the 10th Privacy-Enhancing Technologies Symposium (PETS)*, Lecture Notes in Computer Science, vol. 6205, Springer, Berlin, 2010, pp. 166 - 183.
92. J. Rexford and J. Feigenbaum, "Incrementally-deployable security for interdomain routing (extended abstract)" in *Proceedings of the Conference on Cybersecurity Applications and Technologies for Homeland Security (CATCH)*, IEEE Computer Society Press, Los Alamitos, 2009, pp. 130-134.
93. J. Feigenbaum, A. Johnson, and P. Syverson, "A Model of Onion Routing with Provable Anonymity," in *Proceedings of the 2007 Financial Crypto Conference (FC)*, Lecture Notes in Computer Science, vol. 4886, Springer, Berlin, 2008, pp. 57-71.
94. F. Saint-Jean, A. Johnson, D. Boneh, and J. Feigenbaum, "Private Web Search," in *Proceedings of the 6th Workshop on Privacy in the Electronic Society (WPES)*, ACM Press, New York, 2007, pp. 84-90.
95. D. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G. Sussman, "Information Accountability," MIT-CSAIL-TR-2007-034, June 2007.
96. J. Zhang and J. Feigenbaum, "Finding Highly Correlated Pairs Efficiently with Powerful Pruning," in *Proceedings of the 15th Conference on Information and Knowledge Management (CIKM)*, ACM Press, New York, 2006, pp. 152-161.
97. O. Kardes, R. Ryger, R. Wright, and J. Feigenbaum, "Implementing Privacy-Preserving Bayesian-Net Discovery for Vertically Partitioned Data," in *Proceedings of the ICDM Workshop on Privacy and Security Aspects of Data Mining*, IEEE Computer Society, Los Alamitos, 2005, pp. 26 - 34.
98. J. Zhang, J. Rexford, and J. Feigenbaum, "Learning-Based Anomaly Detection in BGP Updates," YALEU/DCS/TR-1318, Yale University, New Haven, April 2005. Abstract in *Proceedings of the Sigcomm Workshop on Mining Network Data (MineNet)*, ACM Press, New York, 2005, pp. 219 - 220.
99. D. Bergemann, T. Eisenbach, J. Feigenbaum, and S. Shenker, "Flexibility as an Instrument in Digital Rights Management," *2005 Workshop on Economics of Information Security (WEIS)*.

100. J. Feigenbaum, B. Pinkas, R. Ryger, and F. Saint-Jean, "Secure Computation of Surveys," *2004 EU Workshop on Secure Multiparty Protocol (SMP)*.
101. J. Feigenbaum, S. Kannan, and J. Zhang, "Annotation and Computational Geometry in the Streaming Model," YALEU/DCS/TR-1249, Yale University, New Haven CT, March 2003.
102. J. Feigenbaum and S. Shenker, "Distributed Algorithmic Mechanism Design: Recent Results and Future Directions," in *Proceedings of the 6th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communication (DIALM)*, ACM Press, New York, 2002, pp. 1 - 13. Reprinted by invitation in *Current Trends in Theoretical Computer Science: The Challenge of the New Century, Algorithms and Complexity*, vol. 1, World Scientific, Singapore, 2004, pp. 403-434.
103. J. Feigenbaum, M. Freedman, T. Sander, and A. Shostack, "Privacy Engineering for DRM Systems," in *Proceedings of the 1st ACM Workshop on Security and Privacy in Digital Rights Management (DRM)*, Lecture Notes in Computer Science, vol. 2320, Springer, Berlin, 2002, pp. 76 - 105.
104. E. Miller and J. Feigenbaum, "Taking the Copy out of Copyright," in *Proceedings of the 1st ACM Workshop on Security and Privacy in Digital Rights Management (DRM)*, Lecture Notes in Computer Science, vol. 2320, Springer, Berlin, 2002, pp. 233 - 244.
105. J. Feigenbaum, J. Fong, M. Strauss, and R. Wright, "Secure Multiparty Computation of Approximations," <http://eprint.iacr.org/2000/30/>
106. N. Li, B. Grosf, and J. Feigenbaum, "A Practically Implementable and Tractable Delegation Logic," *Proceedings of the 21st Symposium on Security and Privacy*, IEEE Computer Society Press, Los Alamitos, 2000, pp. 27 - 42.
107. N. Li, J. Feigenbaum, and B. Grosf, "A Logic-based Knowledge Representation for Authorization with Delegation," *IBM Research Report RC21492(96966)*. Extended abstract appears in *Proceedings of the 12th Computer Security Foundations Workshop (CSFW)*, IEEE Computer Society Press, Los Alamitos, pp. 162 - 174.
108. M. Blaze, J. Feigenbaum, and M. Naor, "A Formal Treatment of Remotely Keyed Encryption (Extended Abstract)," in *Advances in Cryptology - Eurocrypt '98*, Lecture Notes in Computer Science, vol. 1403, Springer, Berlin, 1998, pp. 251 - 265.
109. M. Blaze, J. Feigenbaum, and M. Strauss, "Compliance Checking in the PolicyMaker Trust Management System," in *Proceedings of the 2nd Financial Crypto Conference (FC)*, Lecture Notes in Computer Science, vol. 1465, Springer, Berlin, 1998, pp. 254 - 274.

110. J. Feigenbaum, "Talk Abstracts: DIMACS Research and Educational Institute on Cryptography and Network Security (DREI '97)," *DIMACS Technical Report 97-80*, Rutgers University, Piscataway NJ, 1998.
111. J. Feigenbaum and M. Strauss, "An Information-Theoretic Treatment of Random-Self-Reducibility," in *Proceedings of the 14th Symposium on Theoretical Aspects of Computer Science (STACS)*, Lecture Notes in Computer Science, vol. 1200, Springer, Berlin, 1997, pp. 523 - 534.
112. M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," in *Proceedings of the 17th Symposium on Security and Privacy*, IEEE Computer Society Press, Los Alamitos, 1996, pp. 164 - 173.
113. M. Blaze, J. Feigenbaum, and F. T. Leighton, "Master-Key Cryptosystems," *DIMACS Technical Report 96-02*, Rutgers University, Piscataway, 1996. Presented at *Crypto '95 Rump Session*, Santa Barbara CA, August 1995.
114. M. Blaze, J. Feigenbaum, and J. Lacy, "Managing Trust in Medical Information Systems," *AT&T Laboratories Technical Report 96.14.1*.
115. R. Brayton, A. Emerson, and J. Feigenbaum, "Workshop Summary: Computational and Complexity Issues in Automated Verification," *DIMACS Technical Report 96-15*, Rutgers University, Piscataway, 1996.
116. J. Feigenbaum, D. Koller, and P. Shor, "A Game-Theoretic Classification of Interactive Complexity Classes," in *Proceedings of the 10th Conference on Structure in Complexity Theory*, IEEE Computer Society Press, Los Alamitos, 1995, pp. 227-237.
117. J. Feigenbaum, L. Fortnow, and A. Naik, "Two Remarks on Self-Correctability versus Random-Self-Reducibility," *DIMACS Technical Report 94-45*, Rutgers University, Piscataway, 1994.
118. D. Beaver, J. Feigenbaum, R. Ostrovsky, and V. Shoup, "Instance-Hiding Proof Systems," *DIMACS Technical Report 93-65*, Rutgers University, Piscataway, 1993.
119. J. Feigenbaum and R. Ostrovsky, "A Note on One-Prover, Instance-Hiding, Zero-Knowledge Proof Systems," in *Advances in Cryptology - Asiacrypt '91*, Lecture Notes in Computer Science, vol. 739, Springer, Berlin, 1993, pp. 352 - 359.
120. D. Beaver, J. Feigenbaum, and V. Shoup, "Hiding Instances in Zero-Knowledge Proof Systems," in *Advances in Cryptology - Crypto '90*, Lecture Notes in Computer Science, vol. 537, Springer, Berlin, 1991, pp. 326 - 338.

121. D. Beaver, J. Feigenbaum, J. Kilian, and P. Rogaway, "Security with Low Communication Overhead," in *Advances in Cryptology - Crypto '90*, Lecture Notes in Computer Science, vol. 537, Springer, Berlin, 1991, pp. 62 - 76.
122. R. Beigel, M. Bellare, J. Feigenbaum, and S. Goldwasser, "Languages that are Easier than their Proofs," in *Proceedings of the 32nd Symposium on Foundations of Computer Science (FOCS)*, IEEE Computer Society Press, Los Alamitos, 1991, pp. 19 - 28.
123. E. Allender, J. Cai, and J. Feigenbaum, "Workshop Summary: Structural Complexity And Cryptography," *DIMACS Technical Report 91-36*, Rutgers University, Piscataway, 1991.
124. D. Beaver and J. Feigenbaum, "Hiding Instances in Multioracle Queries," in *Proceedings of the 7th Symposium on Theoretical Aspects of Computer Science (STACS)*, Lecture Notes in Computer Science, vol. 415, Springer, Berlin, 1990, pp. 37 - 48.
125. M. Abadi, E. Allender, A. Broder, J. Feigenbaum, and L. Hemachandra, "Generating Hard, Certified Elements of NP-Complete Sets," in *Advances in Cryptology - Crypto '88*, Lecture Notes in Computer Science, vol. 403, Springer, Berlin, 1990, pp. 297 - 310.
126. J. Feigenbaum, S. Kannan, and N. Nisan, "Lower Bounds on Random-Self-Reducibility," in *Proceedings of the 5th Structure in Complexity Theory Conference*, IEEE Computer Society Press, Los Alamitos, 1990, pp. 100 - 109.
127. J. Feigenbaum, R. J. Lipton, and S. R. Mahaney, "A Completeness Theorem for Almost-Everywhere Invulnerable Generators," *AT&T Bell Laboratories Technical Memorandum*, Murray Hill, February 3, 1989.
128. J. Feigenbaum, "A Note on the Cycle Structure of Cartesian-Product Graphs," *AT&T Bell Laboratories Technical Memorandum*, Murray Hill, October 7, 1987.
129. J. Feigenbaum, "Encrypting Problem Instances, or, Can You Take Advantage of Someone Without Having to Trust Him," in *Advances in Cryptology - Crypto '85*, Lecture Notes in Computer Science, vol. 218, Springer, Berlin, 1986, pp. 477 - 488.
130. J. Feigenbaum, "Product Graphs: Some Algorithmic and Combinatorial Results," *Stanford University Technical Report STAN-CS-86-1121*, PhD Thesis, 1986.
131. J. Feigenbaum and D. Subramanian, "Factorization in Experiment Generation," in *Proceedings of AAAI '86*, Morgan Kaufman Publishers, Philadelphia, 1986, pp. 518 - 522.

132. D. Coppersmith and J. Feigenbaum, "Finite Graphs with Two Inequivalent Factorizations under the Composition Operator," *IBM Research Report RC11149*, Yorktown Heights, 1985.
133. J. Feigenbaum and A. A. Schaffer, "Recognizing Corona Graphs," *AT&T Bell Laboratories Technical Memorandum*, Murray Hill, August 23, 1985.

Committee Reports, Position Papers, RFCs, and News Articles

134. B. Ford and J. Feigenbaum, "Technology Can Make Lawful Surveillance Both Open and Effective," *MIT Technology Review*, August 18, 2014.
135. J. Feigenbaum and B. Ford, "Is Data Hoarding Necessary for Lawful Surveillance?," *Huffington Post*, April 19, 2014.
136. J. Feigenbaum and B. Ford, "Lead out of YBB+," *Yale Daily News*, January 29, 2014.
137. J. Feigenbaum, "Accountability as a Driver of Innovative Privacy Solutions," *Privacy and Innovation Symposium*, Yale Law School Information Society Project, October 2010, <http://www.law.yale.edu/intellecualife/Privacy%20Symposium.htm>
138. J. Feigenbaum and M. Mitzenmacher, "Towards a Theory of Networked Computation," Report on NSF-Sponsored ToNC workshops, July 2009. <http://www.cs.yale.edu/homes/jf/Report2009.pdf>
139. J. Feigenbaum, "Workshop Report: NetEcon '08," *ACM SIGecom Exchanges*, Vol. 7, No. 3, November 2008.
140. J. Feigenbaum and D. J. Weitzner (eds.), "Report on the 2006 PORTIA/TAMI Workshop on Privacy and Accountability," June 2006, <http://dig.csail.mit.edu/2006/tami-portia-accountability-ws/summary>
141. J. Feigenbaum, "Towards Better Support for Copyright Compliance and for Privacy," *British Computer Society Workshop on Web Science*, London UK, September, 2005.
142. J. Feigenbaum, B. Pinkas, R. Ryger, and F. Saint-Jean, "Some Requirements for Adoption of Privacy-Preserving Data Mining," *PORTIA Project White Paper*, April 2005.
143. J. Feigenbaum, Untitled White Paper on "Malevolence in the Cyberinfrastructure," *NSF Workshop on Cyberinfrastructure for the Social Sciences*, Warrenton VA, March 2005.

144. D. Bergemann, J. Feigenbaum, S. Shenker, and J. M. Smith, "Towards an Economic Analysis of Trusted Systems (Position Paper)," *Third Workshop on Economics and Information Security (WEIS)*, Minneapolis MN, May 2004.
145. D. Boneh, J. Feigenbaum, A. Silberschatz, and R. Wright, "PORTIA: Privacy, Obligations, and Rights in Technologies of Information Assessment," *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering* **27** (2004), pp. 10 - 18.
146. J. Aspnes, J. Feigenbaum, M. Mitzenmacher, and D. Parkes, "Towards Better Definitions and Measures of Internet Security (Position Paper)," *Workshop on Research Needs in Large-Scale Network Security*, Landsdowne VA, March 2003.
147. J. Feigenbaum and S. Shenker, "Incentives and Internet Computation," *Distributed Computing Column #9, SIGACT News* **33** (2002), pp. 37 - 54.
148. J. Feigenbaum, N. Nisan, V. Ramachandran, R. Sami, and S. Shenker, "Agents' Privacy In Distributed Algorithmic Mechanisms (Position Paper)," *First Workshop on Economics and Information Security (WEIS)*, Berkeley CA, May 2002.
149. J. Feigenbaum, M. Freedman, T. Sander, and A. Shostack, "Economic Barriers to the Deployment of Existing Privacy Technology (Position Paper)," *First Workshop on Economics and Information Security (WEIS)*, Berkeley CA, May 2002.
150. J. Feigenbaum, "Toward Realistic Assumptions, Models, and Goals for Security Research (Position Paper)," *NSF Workshop on Security Research*, Berkeley CA, February 2002.
151. N. Li and J. Feigenbaum, "Nonmonotonicity, User Interfaces, and Risk Assessment in Certificate Revocation (Position Paper)," in *Proceedings of the 5th Financial Crypto conference*, Lecture Notes in Computer Science, vol. 2339, Springer, Berlin, 2002, pp. 166 - 177.
152. National Research Council Committee on Intellectual Property Rights in the Emerging Information Infrastructure (Chair: R. Davis), **The Digital Dilemma: Intellectual Property in the Information Age**, National Academy Press, Washington DC, 2000.
153. J. Callas, J. Feigenbaum, D. Goldschlag, and E. Sawyer, "Fair Use, Intellectual Property, and the Information Economy (Panel Session Summary)," in *Proceedings of the 3rd Financial Crypto Conference*, Lecture Notes in Computer Science, vol. 1648, Springer, Berlin, 1999, pp. 173 - 183.
154. M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis, "The KeyNote Trust-Management System, Version 2," *Internet RFC 2704*, September 1999. <http://ftp.isi.edu/in-notes/rfc2704.txt>.

155. J. Feigenbaum, "Overview of the AT&T Labs Trust Management Project (Position Paper)," in *Proceedings of the 1998 Cambridge University Security Protocol International Workshop*, Lecture Notes in Computer Science, vol. 1550, Springer, Berlin, 1999, pp. 45 - 58.
156. M. Blaze, J. Feigenbaum, and A. Keromytis, "KeyNote: Trust Management for Public-Key Infrastructure (Position Paper)" in *Proceedings of the 1998 Cambridge University Security Protocols International Workshop*, Lecture Notes in Computer Science, vol. 1550, Springer, Berlin, 1999, pp. 59 - 63.
157. J. Feigenbaum, "Towards an Infrastructure for Authorization (Position Paper)," 1998 *USENIX Ecommerce Conference - Invited Talks Supplement*, pp. 15 - 19.
158. J. Feigenbaum, "In Defense of Metadata Platforms (Position Paper)," in *Proceedings of the DIMACS Workshop on "Design for Values: Ethical, Social, and Political Dimensions of Information Technology,"* February 1998, pp. 20 - 24.
159. J. Feigenbaum and P. Lee, "Trust Management and Proof-Carrying Code in Secure Mobile-Code Applications (Position Paper)," in *Proceedings of the DARPA Workshop on Foundations for Secure Mobile Code*, March 1997, pp. 48 - 55.
160. J. Feigenbaum, E. Hargittai, and J. O'Rourke, "Statistical Analysis of the CRA Women's Database," *Computing Research News* **6(4)**, 1994, pp. 3 - 4.
161. J. Feigenbaum, "CRA Committee is Creating a Database of Women Scientists," *Computing Research News* **4(2)**, 1992, pp. 4 - 5.
162. J. Feigenbaum, "DIMACS Update," *SIGACT News* **22(1)**, 1991, pp. 24 - 25.
163. J. Feigenbaum, "DIMACS Update," *SIGACT News* **21(4)**, 1990, pp. 49 - 52.
164. J. Feigenbaum, "Report on DIMACS Seminar Series," *SIGACT News* **21(2)**, 1990, pp. 25 - 27.
165. J. Feigenbaum, "Report on DIMACS Seminar Series," *SIGACT News* **20(4)**, 1989, pp. 48 - 49.
166. J. Feigenbaum, "Report on DIMACS Seminar Series," *SIGACT News* **20(3)**, 1989, pp. 34 - 35.

Fiction

167. “Eventually, the World Intrudes,” a **How to Get Away with Murder** fanfiction story published under the pseudonym LadiesMile, March 6, 2016.
<https://www.fanfiction.net/s/11827960/1/Eventually-the-World-Intrudes>
168. “I’ll Take Care of You,” a **How to Get Away with Murder** fanfiction story published under the pseudonym LadiesMile, February 27, 2016.
<https://www.fanfiction.net/s/11813590/1/I-ll-Take-Care-of-You>
169. “Lunch in LOVE Park,” a **How to Get Away with Murder** fanfiction story published under the pseudonym LadiesMile, February 12, 2016.
<https://www.fanfiction.net/s/11785238/1/Lunch-in-LOVE-Park>
170. “This Isn’t The Job I Signed Up For,” a **How to Get Away with Murder** fanfiction story published under the pseudonym LadiesMile, November 2015.
<https://www.fanfiction.net/s/11641511/1/This-Isn-t-the-Job-I-Signed-Up-For>
171. “It Doesn’t Work That Way,” a **How to Get Away with Murder** fanfiction story published under the pseudonym LadiesMile, October 2015.
<https://www.fanfiction.net/s/11580724/1/It-Doesn-t-Work-That-Way>
172. J. Feigenbaum and B. Rosen, “Drive Me Crazy,” in *Proceedings of the 23rd International Workshop on Security Protocols*, Lecture Notes in Computer Science, vol. 9379, Springer, Berlin, 2015, pp. 263 - 275. This story is the appendix of the paper “On the use of security and privacy technology as a plot device” listed in the Proceedings Articles and Technical Reports section above.
173. “It’s Time to Move On,” a **Covert Affairs** fanfiction story published under the pseudonym LadiesMile, October 2014. <https://www.fanfiction.net/s/10780629/1/It-s-Time-To-Move-On>
174. “Heart to Hearts Require Talking,” a **Covert Affairs** fanfiction story published under the pseudonym LadiesMile, May 2014.
<https://www.fanfiction.net/s/10369659/1/Heart-to-Hearts-Require-Talking>