PUBLICATIONS

Joan Feigenbaum

June 1, 2023

1. J. Feigenbaum, M. Movahedi, and P. Newton, "Computing on private data," *Amazon.science*, June 1, 2023.

2. C. Malchik and J. Feigenbaum, "Toward User Control over Information Access: A Sociotechnical Approach," *Proceedings of the 2022 New Security Paradigms Workshop*, October 24–27, 2022, North Conway NH, USA, ACM Press, 2023, pp. 117–129. .

3. J. Feigenbaum, "A Gift that Keeps on Giving: The Impact of Public-Key Cryptography on Theoretical Computer Science," Chapter 5 of **Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman**, R. Slayton (ed.), ACM, New York, 2022, pp. 157–184.

4. L. Idan and J. Feigenbaum, "PRShare: A Framework for Privacy-Preserving, Interorganizational Data Sharing," *ACM Transactions on Privacy and Security*, Volume 25, Issue 4, Article 29, November 2022. (Final version of [10, 11].)

5. C. Malchik and J. Feigenbaum, "From Data Leverage to Data Co-Ops: An Institutional Model for User Control over Information Access," `https://arxiv.org/pdf/2201.10677.pdf`.

6. S. Judson and J. Feigenbaum, "On Heuristic Models, Assumptions, and Parameters," `https://arxiv.org/pdf/2201.07413.pdf`.

7. D. Jetchev and J. Feigenbaum, "Privacy challenges in extreme gradient boosting," *Amazon.science*, June 22, 2021.

8. J. Feigenbaum, A. D. Jaggard, and R. N. Wright, *Accountability in Computing: Concepts and Mechanisms*, **Foundations and Trends in Privacy and Security 2(4)** (2020), pp. 247–399.

9. X. Meng and J. Feigenbaum, "Privacy-Preserving XGBoost Inference," in *Privacy-Preserving Machine Learning – PriML and PPML Joint Edition*, NeurIPS Workshop, 2020.

10. L. Idan and J. Feigenbaum, "PRShare: A Framework for Privacy-Preserving, Interorganizational Data Sharing," Technical Report YALEU/DCS/TR-1554, Yale University, New Haven CT, September 2020. (Expanded version of [11].)

11. L. Idan and J. Feigenbaum, "PRShare: A Framework for Privacy-Preserving, Interorganizational Data Sharing," in *Proceedings of the 19^{th} ACM Workshop on Privacy in the Electronic Society*, 2020, pp. 137–149. (Preliminary version of [4].)

12. L. Barman, I. Dacosta, M. Zamani, E. Zhai, A. Pyrgelis, B. Ford, J. Feigenbaum, and J.-P. Hubaux, "PriFi: Low-Latency Anonymity for Organizational Networks," *Proceedings on Privacy Enhancing Technologies* **2020**(4), pp. 24–47. (Final version of [22].)

13. J. Feigenbaum, "Cryptographic computing can accelerate the adoption of cloud computing," *Amazon.science*, February 11, 2020.

14. L. Idan and J. Feigenbaum, "Show me your friends, and I will tell you whom you vote for: Predicting voting behavior in social networks," in *Proceedings of the IEEE/ACM International Conference on Advances in Social-Network Analysis and Mining*, 2019, pp. 816–824.

15. J. Feigenbaum, "Encryption and Surveillance: Why the law-enforcement access question will not just go away," *Communications of the ACM* **62:5** (May 2019), pp. 27–29.

16. J. Feigenbaum and D. Weitzner, "On the incommensurability of laws and technical mechanisms: Or, what cryptography can't do," in *Proceedings of the 26^{th} International Workshop on Security Protocols*, Lecture Notes in Computer Science, volume 11286, Springer, 2018, pp. 266–279.

17. J. Feigenbaum, "PriFi Networking for Tracking-Resistant Mobile Computing," Technical Report AFRL-RI-RS-TR-2017-230, Air Force Research Laboratory, Rome NY, November 2017.

18. L. Barman, I. Dacosta, M. Zamani, E. Zhai, B. Ford, J.-P. Hubaux, and J. Feigenbaum, "PriFi: A Low-Latency Local-Area Anonymous Communication Network," `https://arxiv.org/abs/1710.10237`.

19. J. Feigenbaum and B. Ford, "Multiple Objectives of Lawful-Surveillance Protocols," in *Proceedings of the 25th International Workshop on Security Protocols*, Lecture Notes in Computer Science, volume 10476, Springer, 2017, pp. 1–8.

20. J. Feigenbaum, "Multiple Objectives of Lawful-Surveillance Protocols (Transcript of Discussion)," in *Proceedings of the 25th International Workshop on Security Protocols*, Lecture Notes in Computer Science, volume 10476, Springer, 2017, pp. 9–17.

21. 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*, 2017.

22. 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 ACM Workshop on Privacy in the Electronic Society*, 2016, pp. 181–184. (Preliminary version of [12].)

23. A. Segal, J. Feigenbaum, and B. Ford, "Privacy-Preserving Lawful Contact Chaining (Preliminary Report)," in *Proceedings of the 15th ACM Workshop on Privacy in the Electronic Society*, 2016, pp. 185–188.

24. 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.

25. 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, volume 9604, Springer, 2016, pp. 302–318.

26. J. Feigenbaum and R. Wright, "Systemization of Secure Computation," Technical Report AFRL-RI-RS-TR-2015-241, Air Force Research Laboratory, Rome NY, November 2015.

27. J. Feigenbaum and B. Ford, "Seeking Anonymity in an Internet Panopticon," *Communications of the ACM* **58:10** (October 2015), pp. 58–69.

28. B. Mood, D. Gupta, K. Butler, and J. Feigenbaum, "Reuse It or Lose It: More Efficient Secure Computation Through Reuse of Encrypted Values," `http://arxiv.org/abs/1506.02954`. (Expanded version of [40].)

29. J. Feigenbaum and B. Rosen, "On the Use of Security and Privacy as a Plot Device," in *Proceedings of the 23rd International Workshop on Security Protocols*, Lecture Notes in Computer Science, volume 9379, Springer, 2015, pp. 261–275.

30. J. Feigenbaum, "On the Use of Security and Privacy Technology as a Plot Device (Transcript of Discussion)," in *Proceedings of the 23rd International Workshop on Security Protocols*, Lecture Notes in Computer Science, volume 9379, Springer, 2015, pp. 276–282.

31. A. 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* **2015**(1):4–24.

32. B. Ford and J. Feigenbaum, "Technology Can Make Lawful Surveillance Both Open and Effective," *MIT Technology Review*, August 18, 2014.

33. A. 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*, 2014.

34. J. Perry, D. Gupta, J. Feigenbaum, and R. Wright, "Systematizing Secure Computation for Research and Decision Support," in *Proceedings of the 9th Conference on Security and Cryptography for Networks*, Lecture Notes in Computer Science, volume 8642, Springer, 2014, pp. 380–397.

35. 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*, 2014.

36. J. Feigenbaum, A. D. Jaggard, and R. Wright, "Open vs. Closed Systems for Accountability," in *Proceedings of HotSoS'14: Symposium and Boot Camp on Science of Security*, ACM, 2014, Article number 4.

37. 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, volume 8809, Springer, 2014, pp. 239–252.

38. J. Feigenbaum and J. Koenig, "On the Feasibility of a Technological Response to the Surveillance Morass (Transcript of Discussion)," in *Proceedings of the 22nd International Workshop on Security Protocols*, Lecture Notes in Computer Science, volume 8809, Springer, 2014, pp. 253–262.

39. G. DiCrescenzo, J. Feigenbaum, D. Gupta, T. Panagos, J. Perry, and R. Wright, "Practical and Privacy-Preserving Policy Compliance for Outsourced Data," in *Proceedings of the 2nd FC Workshop on Encrypted Computing and Applied Homomorphic Cryptography*, Lecture Notes in Computer Science, volume 8438, Springer, 2014, pp. 181–194.

40. 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 ACM Conference on Computer and Communication Security*, 2014, pp. 582–596. (Preliminary version of [28].)

41. J. Feigenbaum, A. D. Jaggard, and M. Schapira, "Approximate Privacy: Foundations and Quantification," *ACM Transactions on Algorithms* **10:3** (June 2014), Article 11. (Final version of [59]; related material appears in [62] and [68].)

42. J. Feigenbaum and B. Ford, "Is Data Hoarding Necessary for Lawful Surveillance?," *Huffington Post*, April 19, 2014.

43. J. Feigenbaum and B. Ford, "Lead out of YBB+," *Yale Daily News*, January 29, 2014.

44. J. Feigenbaum, "How Useful are Formal Models of Accountability?," in *2nd International Workshop on Accountability: Science, Technology, and Policy*, January 2014.

45. H. Xiao, B. Ford, and J. Feigenbaum, "Structural Cloud Audits that Protect Private Information," in *Proceedings of the 5th ACM Cloud Computing Security Workshop*, 2013, pp. 101–112.

46. J. Feigenbaum, A. D. Jaggard, and R. 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.

47. J. Feigenbaum, B. Godfrey, A. Panda, M. Schapira, S. Shenker, and A. Singla, "On the Resilience of Routing Tables," `http://arxiv.org/abs/1207.3732`. Also available as YALEU/DCS/TR-1454, Yale University, New Haven, CT, August 2012. (Expanded version of [54].)

48. J. Feigenbaum, A. Johnson, and P. Syverson, "Probabilistic Analysis of Onion Routing in a Black-Box Model," *ACM Transactions on Information and System Security* **15:3** (November 2012), Article 14. (Final version of [78].)

49. 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 11th ACM Workshop on Hot Topics in Networks*, 2012, pp. 37–42.

50. J. Feigenbaum, M. Mitzenmacher, and G. Zervas, "An Economic Analysis of User-Privacy Options in Ad-Supported Services," in *Proceedings of the 8^{th} Workshop on Internet and Network Economics*, Lecture Notes in Computer Science, volume 7695, Springer, 2012, pp. 30–43.

51. J. Feigenbaum, Aaron Johnson, and Paul Syverson, "Anonymity Analysis of Onion Routing in the Universally Composable Framework," in *Provable Privacy Workshop*, 2012.

52. J. Feigenbaum, "Privacy, Anonymity, and Accountability in Ad-Supported Services," in *Proceedings of the 27^{th} ACM/IEEE Symposium on Logic in Computer Science*, 2012, pp. 9–10.

53. J. Feigenbaum, A. D. Jaggard, R. 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.

54. 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 31^{st} ACM Symposium on Principles of Distributed Computing*, 2012, pp. 237–238. (Preliminary version of [47].)

55. J. Feigenbaum, V. Ramachandran, and M. Schapira, "Incentive-Compatible Interdomain Routing," *Distributed Computing* **23** (2011), pp. 301–319. (Final version of [85].)

56. J. Feigenbaum, "Defining 'Anonymity' in Networked Communication, version 1," YALEU/DCS-TR-1448, Yale University, New Haven CT, December 2011.

57. J. Feigenbaum, A. D. Jaggard, and R. Wright, "Towards a Formal Model of Accountability," in *Proceedings of the 14^{th} ACM New Security Paradigms Workshop*, 2011, pp. 45–56.

58. J. Feigenbaum, J. Hendler, A. D. Jaggard, D. Weitzner, and R. Wright, "Accountability and Deterrence in Online Life (Extended Abstract)," in *Proceedings of the 3^{rd} International ACM Conference on Web Science*, 2011.

59. J. Feigenbaum, A. D. Jaggard, and M. Schapira, "Approximate Privacy: Foundations and Quantification (Extended Abstract)," in *Proceedings of the 11^{th} ACM Conference on Electronic Commerce*, 2010, pp. 167–178. (Preliminary version of [41].)

60. J. Feigenbaum, "Accountability as a Driver of Innovative Privacy Solution," in *Privacy and Innovation Symposium*, Yale Law School Information Society Project, October 2010.

61. 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.

62. J. Feigenbaum, A. D. Jaggard, and M. Schapira, "Approximate Privacy: PARs for Set Problems," DIMACS Technical Report 2010-01, Rutgers University, Piscataway NJ, June 2010. (Final version of some but not all of the material in this report appears in [41].)

63. J. Feigenbaum, A. Johnson, and P. Syverson, "Preventing Active Timing Attacks in Low-Latency Anonymous Communication," UTCS/TR-10-15, University of Texas, Austin TX, April 2010. (Expanded version of [65].)

64. 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.

65. J. Feigenbaum, A. Johnson, and P. Syverson, "Preventing Active Timing Attacks in Low-Latency Anonymous Communication (Extended Abstract)," in *Proceedings of the 10^{th} Privacy Enhancing Technologies Symposium*, Lecture Notes in Computer Science, volume 6205, Springer, 2010, pp. 166–183. (Condensed version of [63].)

66. J Feigenbaum and M. Mitzenmacher, "Towards a Theory of Networked Computation," Report on NSF-Sponsored ToNC Workshop, July 2009.

67. J. Rexford and J. Feigenbaum, "Incrementally-deployable security for interdomain routing (extended abstract)," in *Proceedings of the IEEE Conference on Cybersecurity Applications and Technologies for Homeland Security*, 2009, pp. 130–134.

68. J. Feigenbaum, A. D. Jaggard, and M. Schapira, "Approximate Privacy: Foundations and Quantification," DIMACS Technical Report 2009-14, Rutgers University, Piscataway NJ, October 2009. (Final version of some but not all of the material in this report appears in [41].)

69. J. Feigenbaum, D. Parkes, and D. Pennock, "Computational Challenges in Electronic Commerce," *Communications of the ACM* **52:1** (January 2009), pp. 70–74.

70. J. Feigenbaum, "Workshop Report: NetEcon '08," *ACM SIGecom Exchanges* **7:3**, November 2008.

71. 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. (Final version of [91].)

72. 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.

73. 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.

74. J.Feigenbaum, M. Schapira, and S. Shenker, "Distributed Algorithmic Mechanism Design," Chapter 14 in **Algorithmic Game Theory**, Cambridge University Press, 2007, pp. 363–384.

75. J. Aspnes, J. Feigenbaum, A. Yampoliskiy, and S. Zhong, "Toward a Theory of Data Entanglement," *Theoretical Computer Science* **389** (2007), pp. 26–43. (Final version of [103].)

76. J. Feigenbaum, D. Karger, V. Mirrokni, and R. Sami, "Subjective-Cost Policy Routing," *Theoretical Computer Science* **378** (2007), pp. 175–189. (Final version of [92]. Special issue of selected papers from WINE 2005.)

77. J. Feigenbaum, A. Johnson, and P. Syversion, "A Model of Onion Routing with Provable Anonymity," in *Proceedings of the 11th International Conference on Financial Cryptology and Data Security*, Lecture Notes in Computer Science, volume 4886, Springer, 2007, pp. 57–71.

78. J. Feigenbaum, A. Johnson, and P. Syverson, "Probabilistic Analysis of Onion Routing in a Black-Box Model," in *Proceedings of the 6th ACM Workshop on Privacy in Electronic Society*, 2007, pp. 1–10. (Preliminary version of [48].)

79. F. Saint-Jean, A. Johnson, D. Boneh, and J. Feigenbaum, "Private Web Search," in *Proceedings of the 6th ACM Workshop on Privacy in the Electronic Society*, 2007, pp. 84–90.

80. D. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G. Sussman, "Information Accountability," MIT-CSAIL-TR-2007-034, Cambridge MA, June 2007.

81. J. Zhang and J. Feigenbaum, "Finding Highly Correlated Pairs Efficiently with Powerful Pruning," in *Proceedings of the 15th ACM Conference on Information and Knowledge Management*, 2006, pp. 152–161.

82. J. Feigenbaum and D. Weitzner, "Report on the 2006 PORTIA/TAMI Workshop on Privacy and Accountability," June 2006.

83. 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. (Final version of [124].)

84. J. Feigenbaum, R. Sami, and S. Shenker, "Mechanism Design for Policy Routing," *Distributed Computing* **18** (2006), pp. 293–305. (Final version of [104]. Special issue of selected papers from PODC 2004.)

85. J. Feigenbaum, V. Ramachandra, and M. Schapira, "Incentive-Compatible Interdomain Routing," in *Proceedings of the 7th ACM Conference on Electronic Commerce*, 2006, pp. 130–139. (Preliminary version of [55].)

86. J. Feigenbaum, "Towards Better Support for Copyright Compliance and for Privacy," in *British Computer Society Workshop on Web Science*, September 2005.

87. 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.

88. J. Zhang, J. Rexford, and J. Feigenbaum, "Learning-Based Anomaly Detection in BGP Updates," YALEU/DCS/TR-1318, Yale University, New Haven CT, April 2005. (Expanded version of [98].)

89. J. Feigenbaum, Untitled White Paper on "Malevolence in the Cyberinfrastructure," in *NSF Workshop on Cyberinfrastructure for the Social Sciences*, March 2005.

90. 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, 2005, pp. 26–34.

91. J. Feigenbaum, S. Kannan, A. McGregor, S. Suri, and J. Zhang, "Graph Distances in the Streaming Model: The Value of Space," in *Proceedings of the 16^{th} ACM-SIAM Symposium on Discrete Algorithms*, 2005, pp. 745–754. (Preliminary version of [71].)

92. J. Feigenbaum, D. Karger, V. Mirrokni, and R. Sami, "Subjective-Cost Policy Routing," in *Proceedings of the 1^{st} Workshop on Internet and Network Economics*, Lecture Notes in Computer Science, volume 3828, Springer, 2005, pp. 174–183. (Preliminary version of [76].)

93. 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. (Final version of [105]. Special issue of selected papers from ICALP 2004.)

94. J. Feigenbaum, L. Fortnow, D. Pennock, and R. Sami, "Computation in a Distributed Information Market," *Theoretical Computer Science* **343** (2005), pp. 114–132. (Final version of [108].)

95. J. Feigenbaum, C. Papadimitriou, R. Sami, and S. Shenker, "A BGP-based Mechanism for Lowest-Cost Routing," *Distributed Computing* **18** (2005), pp. 61–72. (Final version of [117]. Special issue of selected papers from PODC 2002.)

96. J. Feigenbaum, S. Kannan, and J. Zhang, "Computing Diameter in the Streaming and Sliding-Window Models," *Algorithmica* **41** (2005), pp. 25–41.

97. D. Bergemann, T. Eisenbach, J. Feigenbaum, and S. Shenker, "Flexibility as an Instrument in Digital Rights Management," in *Fourth Workshop on the Economics of Information Security*, June 2005.

98. J. Zhang, J. Rexford, and J. Feigenbaum, "Learning-Based Anomaly Detection in BGP Updates," in *Proceedings of the Sigcomm Workshop on Mining Network Data*, ACM, 2005, pp. 219–220. (Preliminary version of [88].)

99. J. Feigenbaum, B. Pinkas, R. Ryger, and F. Saint-Jean, "Secure Computation of Surveys," in *EU Workshop on Secure Multiparty Protocols*, October 2004. `https://cachin.com/cc/smp2004/program.html`

100. D. Bergemann, J. Feigenbaum, S. Shenker, and J. Smith, "Towards an Economic Analysis of Trusted Systems (Position Paper)," in *Third Workshop on Economics and Information Security*, May 2004.

101. 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.

102. A. 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. (Final version of [125].)

103. J. Aspnes, J. Feigenbaum, A. Yampolskiy, and S. Zhong, "Toward a Theory of Data Entanglement," in *Proceedings of the 9^{th} European Symposium on Research in Computer Security*, Lecture Notes in Computer Science, volume 3193, Springer, 2004, pp. 177–192. (Preliminary version of [75].)

104. J. Feigenbaum, R. Sami, and S. Shenker, "Mechanism Design for Policy Routing," in *Proceedings of the 23^{rd} ACM Symposium on Principles of Distributed Computing*, 2004, pp. 11–20. (Preliminary version of [84].)

105. J. Feigenbaum, S. Kannan, A. McGregor, S. Suri, and J. Zhang, "On Graph Problems in a Semi-Streaming Model," in *Proceedings of the 31^{th} International Colloquium on Automata, Languages, and Programming*, Lecture Notes in Computer Science, volume 3142, Springer, 2004, pp. 531–543. (Preliminary version of [93].)

106. J. Aspnes, J. Feigenbaum, M. Mitzenmacher, and D. Parkes, "Towards Better Definitions and Measures of Internet Security (Position Paper)," in *Workshop on Research Needs in Large-Scale Network Security*, March 2003.

107. 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.

108. J. Feigenbaum, L. Fortnow, D. Pennock, and R. Sami, "Computation in a Distributed Information Market," in *Proceedings of the 4^{th} ACM Conference on Electronic Commerce*, 2003, pp. 156–165. (Preliminary version of [94].)

109. N. Li, B. Grosof, and J. Feigenbaum, "Delegation Logic: A Logic-Based Approach to Distributed Authorization," *ACM Transactions on Information and System Security* **5** (2003), pp. 128–171. (Final version of [127] and [135].)

110. J. Feigenbaum, A. Krishnamurthy, R. Sami, and S. Shenker, "Hardness Results for Multicast Cost Sharing," *Theoretical Computer Science* **304** (2003), pp. 215–236. (Final version of [118].)

111. J. Feigenbaum and S. Shenker, "Distributed Computing Column #9: Incentives and Internet Computation," *SIGACT News* **33:4** (2002), pp. 37–54.

112. J. Feigenbaum, N. Nisan, V. Ramachandran, R. Sami, and S. Shenker, "Agents' Privacy in Distributed Algorithmic Mechanism Design (Position Paper)," in *First Workshop on Economics and Information Security*, May 2002.

113. J. Feigenbaum, M. Freedman, T. Sander, and A. Shostak, "Economic Barriers to the Deployment of Existing Privacy Technologies (Position Paper)," in *First Workshop on Economics and Information Security*, May 2002.

114. J. Feigenbaum and S. Shenker, "Distributed Algorithmic Mechanism Design: Recent Results and Future Directions," in *Proceedings of the 6^{th} ACM International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communication*, 2002, pp. 1–13. (Reprinted in **Current Trends in Theoretical Computer Science: The Challenge of the New Century**, *Algorithms and Complexity*, volume 1, World Scientific, 2004, pp. 403–434.)

115. J. Feigenbaum, S. Kannan, M. Strauss, and M. Viswanathan, "Testing and Spot-Checking of Data Streams," *Algorithmica* **304** (2002), pp. 67–80. (Final version of [129].)

116. 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. (Final version of [134].)

117. J. Feigenbaum, C. Papadimitriou, R. Sami, and S. Shenker, "A BGP-based Mechanism for Lowest-Cost Routing," in *Proceedings of the 21^{st} ACM Symposium on Distributed Computing*, 2002, pp. 173–182. (Preliminary version of [95].)

118. J. Feigenbaum, A. Krishnamurthy, R. Sami, and S. Shenker, "Hardness Results for Multicast Cost Sharing," in *Proceedings of the 22^{nd} Conference on Foundations of Software Technology and Theoretical Computer Science*, Lecture Notes in Computer Science, volume 2556, Springer, 2002, pp. 133–144. (Preliminary verion of [110].)

119. J. Feigenbaum, M. Freedman, T. Sander, and A. Shostack, "Privacy Engineering for DRM Systems," in *Proceedings of the 1th ACM Workshop on Security and Privacy in Digital Rights Management (2001)*, Lecture Notes in Computer Science, volume 2320, Springer, 2002, pp. 76–105.

120. E. Miller and J. Feigenbaum, "Taking the Copy out of Copyright," in *Proceedings of the 1th ACM Workshop on Security and Privacy in Digital Rights Management (2001)*, Lecture Notes in Computer Science, volume 2320, Springer, 2002, pp. 233–244.

121. J. Feigenbaum, "Toward Realistic Assumptions, Models, and Goals for Security Research (Position Paper)," in *NSF Workshop on Security Research*, February 2002.

122. N. Li and J. Feigenbaum, "Nonmonotonicity, User Interfaces, and Risk Assessment in Certificate Revocation (Position Paper)," in *Proceedings of the 5th International Conference on Financial Cryptography (2001)*, Lecture Notes in Computer Science, volume 2339, Springer, 2002, pp. 166–177.

123. J. Feigenbaum, C. Papadimitriou, and S. Shenker, "Sharing the Cost of Multicast Transmission," *Journal of Computer and System Sciences* **63** (2001), pp. 21–41. (Final version of [130].)

124. J. Feigenbaum, Y. Ishai, T. Malkin, K. Nissim, M. Strauss, and R. Wright, "Secure Multiparty Computation of Approximations," in *Proceedings of the 28th International Colloquium on Automata, Languages, and Programming*, Lecture Notes in Computer Science, volume 2076, Springer, 2001, pp. 927–938. (Preliminary version of [83].)

125. J. Feigenbaum, A. Krishnamurthy, R. Sami, and S. Shenker, "Approximation and Collusion in Multicast Cost Sharing (Abstract)," in *Proceedings of the 3rd ACM Conference on Electronic Commerce*, 2001, pp. 253–255. (Preliminary version of [102].)

126. 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.

127. N. Li, B. Grosof, and J. Feigenbaum, "A Practically Implementable and Tractable Delegation Logic," in *Proceedings of the 21st IEEE Symposium on Security and Privacy*, 2000, pp. 27–42. (This and [135] are preliminary versions of [109].)

128. J. Feigenbaum and S. Kannan, "Dynamic Graph Algorithms," in **Handbook of Discrete and Combinatorial Mathematics**, CRC Press, 2000, pp. 1142-1151.

129. J. Feigenbaum, S. Kannan, M. Strauss, and M. Viswanathan, "Testing and Spot-Checking of Data Streams (Extended Abstract)," in *Proceedings of the 11th ACM-SIAM Symposium on Discrete Algorithms*, 2000, pp. 165–174. (Preliminary version of [115].)

130. J. Feigenbaum, C. Papadimitriou, and S. Shenker, "Sharing the Cost of Multicast Transmission (preliminary version)," in *Proceedings of the 32nd ACM Symposium on Theory of Computing*, 2000, pp. 218–227. (Preliminary version of [123].)

131. J. Feigenbaum, J. Fong, M. Strauss, and R. Wright, "Secure Multiparty Computation of Approximations," `http://eprint.iacr.org/2000/30`.

132. J. Feigenbaum, S. Kannan, M. Vardi, and M. Viswanathan, "The Complexity of Problems on Graphs Represented by OBDDs," *Chicago Journal of Theoretical Computer Science*, volume 1999, Article 5. (Final version of [147].)

133. 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 International Conference on Financial Cryptography*, Lecture Notes in Computer Science, volume 1648, Springer, 1999, pp. 173–183.

134. J. Feigenbaum, S. Kannan, M. Strauss, and M. Viswanathan, "An Approximate L^1-Difference Algorithm for Massive Data Streams," in *Proceedings of the 40th IEEE Symposium on Foundations of Computer Science*, 1999, pp. 501–511. (Preliminary version of [116].)

135. N. Li, J. Feigenbaum, and B. Grosof, "A Logic-based Knowledge Representation for Authorization and Delegation," in *Proceedings of the 12th IEEE Computer Security Foundations Workshop*, 1999, pp. 162–174. (This and [127] are preliminary versions of [109].)

136. 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**, Lecture Notes in Computer Science, volume 1603, Springer, 1999, pp. 185–210.

137. M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis, "The KeyNote Trust-Management System, Version 2," *Internet RFC 2704*, September 1999. `https://tools.ietf.org/html/rfc2704`

138. J. Feigenbaum, "Overview of the AT&T Labs Trust-Management Project," in *Proceedings of the 6th International Workshop on Security Protocols (1998)*, Lecture Notes in Computer Science, volume 1550, Springer, 1999, pp. 45–50.

139. J. Feigenbaum, "Overview of the AT&T Labs Trust-Management Project (Transcript of Discussion)," in *Proceedings of the 6th International Workshop on Security Protocols (1998)*, Lecture Notes in Computer Science, volume 1550, Springer, 1999, pp. 51–58.

140. M. Blaze, J. Feigenbaum, and A. Keromytis, "KeyNote: Trust Management for Public-Key Infrastructures," in *Proceedings of the 6th International Workshop on Security Protocols (1998)*, Lecture Notes in Computer Science, volume 1550, Springer, 1999, pp. 59–63.

141. M. Blaze, J. Feigenbaum, and M. Strauss, "Compliance Checking in the PolicyMaker Trust Management System," in *Proceedings of the 2nd International Conference on Financial Cryptography*, Lecture Notes in Computer Science, volume 1465, Springer, 1998, pp. 254–274.

142. 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, volume 1403, Springer, 1998, pp. 251–265.

143. J. Feigenbaum, "Towards an Infrastructure for Authorization (Position Paper)," in *Third USENIX Workshop on Electronic Commerce, Invited Presentations Supplement*, September 1998. `https://www.usenix.org/legacy/publications/library/proceedings/ec98/`

144. 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.

145. J. Feigenbaum, L. Fortnow, S. Laplante, and A. Naik, "On Coherence, Random-Self-Reducibility, and Self-Correction," *Computational Complexity* **7** (1998), pp. 174–191. (Final version of [159].)

146. 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. (Final version of [160].)

147. J. Feigenbaum, S. Kannan, M. Vardi, and M. Viswanathan, "The Complexity of Problems on Graphs Represented by OBDDs (Extended Abstract)," in *Proceedings of the 15th Symposium on Theoretical Aspects of Computer Science*, Lecture Notes in Computer Science, volume 1373, Springer, 1998, pp. 216–226. (Preliminary version of [132].)

148. J. Feigenbaum, "In Defense of Metadata Platforms (Position Paper)," in *DIMACS Workshop on Design for Values: Ethical, Social, and Political Dimensions of Information Technology*, February 1998.

149. 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, January 1998.

150. 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*, Lecture Notes in Computer Science, volume 1200, Springer, 1997, pp. 523–534.

151. 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. (Special issue of papers presented at WWW 1997.)

152. A. 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. (Final version of [168].)

153. 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.

154. D. Beaver, J. Feigenbaum, J. Kilian, and P. Rogaway, "Locally Random Reductions: Improvements and Applications," *Journal of Cryptology* **10** (1997), pp. 17–36.

155. M. Blaze, J. Feigenbaum, P. Resnick, and M. Struass, "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.*)

156. J. Feigenbaum and P. Lee, "Trust Management and Proof-Carrying Code in Secure Mobile-Code Applications (Position Paper)," in *DARPA Workshop on Foundations for Secure Mobile Code*, March 1997.

157. M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," in *Proceedings of the 17^{th} IEEE Symposium on Security and Privacy*, 1996, pp. 164–173.

158. 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.

159. J. Feigenbaum, L. Fortnow, S. Laplante, and A. Naik, "On Coherence, Random-Self-Reducibility, and Self-Correction," in *Proceedings of the 11^{th} IEEE Conference on Computational Complexity*, 1996, pp. 59–67. (Preliminary version of [145].)

160. L. Cowen, J. Feigenbaum, and S. Kannan, "A Formal Framework for Evaluating Heuristic Programs," in *Proceedings of the 23^{rd} International Colloquium on Automata, Languages, and Programming*, Lecture Notes in Computer Science, volume 1099, Springer, 1996, pp. 634–645. (Preliminary version of [146.])

161. R. Brayton, A. Emerson, and J. Feigenbaum, "Workshop Summary: Computational and Complexity Issues in Automated Verification," DIMACS Technical Report 96-15, Rutgers University, Piscataway NJ, June 1996.

162. M. Blaze, J. Feigenbaum, and J. Lacy, "Managing Trust in Medical Information Systems," AT&T Labs Technical Report 96.14.1, Murray Hill, NJ, May 1996.

163. M. Blaze, J. Feigenbaum, and F. T. Leighton, "Master-Key Cryptosystems," DIMACS Technical Report 96-02, Rutgers University, Piscataway NJ, February 1996. (Presented at the Crypto '95 Rump Session.)

164. J. Feigenbaum, D. Koller, and P. Shor, "A Game-Theoretic Classification of Interactive Complexity Classes," in *Proceedings of the 10^{th} IEEE Structure in Complexity Theory Conference,* 1995, pp. 227–237.

165. A. 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*, volume 1995, number 4. (Final version of [177].)

166. J. Feigenbaum, "The Use of Coding Theory in Computational Complexity," in **Different Aspects of Coding Theory**, *Proceedings of Symposia on Applied Mathematics*, American Mathematical Society, 1995, pp. 207–233.

167. J. Feigenbaum, L. Fortnow, and A. Naik, "Two Remarks on Self-Correctability versus Random-Self-Reducibility," DIMACS Technical Report 94-45, Rutgers University, Piscataway NJ, 1994.

168. A. Condon, J. Feigenbaum, C. Lund, and P. Shor, "Random Debaters and the Hardness of Approximating Stochastic Functions," in *Proceedings of the 9th IEEE Structure in Complexity Theory Conference*, 1994, pp. 280–293. (Preliminary version of [152].)

169. 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. (Final version of [184].)

170. J. Feigenbaum and N. Reingold, "Universal Traversal Sequences," *American Mathematical Monthly* **101** (1994), pp. 262–265.

171. J. Feigenbaum, E. Hargittai, and J. O'Rourke, "CRA Database aids academic recruiters," *Computing Research News* **6:4** (1994), pp. 3–4.

172. 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, volume 739, Springer, 1993, pp. 352–359.

173. D. Beaver, J. Feigenbaum, R. Ostrovsky, and V. Shoup, "Instance-Hiding Proof Systems," DIMACS Technical Report 93-65, Rutgers University, Piscataway NJ, September 1993.

174. J. Feigenbaum, "Locally Random Reductions in Interactive Complexity Theory," in **Advances in Computational Complexity Theory**, *DIMACS Series on Discrete Mathematics and Theoretical Computer Science*, volume 13, American Mathematical Society, 1993, pp. 73–98.

175. J. Feigenbaum, J. A. Kahn, and C. Lund, "Complexity Results for POMSET Languages," *SIAM Journal on Discrete Mathematics* **6** (1993), pp. 432–442. (Final version of [185].)

176. J. Feigenbaum and L. Fortnow, "Random-Self-Reducibility of Complete Sets," *SIAM Journal on Computing* **22** (1993), pp. 994–1005. (Final version of [195].)

177. A. Condon, J. Feigenbaum, C. Lund, and P. Shor, "Probabilistically Checkable Debate Systems and Nonapproximability Results for PSPACE-Hard Functions," *Proceedings of the 25th ACM Symposium on Theory of Computing*, 1993, pp. 305–314. (Preliminary version of [165].)

178. J. Feigenbaum and J. Lagarias, "Probabilistic Algorithms for Speed-Up," *Statistical Science* **8** (1993), pp. 20–25. (Reprinted from **Probability and Algorithms**, National Academy Press, 1992, pp. 39–51.)

179. J. Feigenbaum, "Probabilistic Algorithms for Defeating Adversaries," *Statistical Science* **8** (1993), pp. 26–30. (Reprinted from **Probability and Algorithms**, National Academy Press, 1992, pp. 53–63.)

180. J. Feigenbaum, "Overview of Interactive Proof Systems and Zero-Knowledge," in **Contemporary Cryptology: The Science of Information Integrity**, IEEE Press, 1992, pp. 423–439.

181. J. Feigenbaum and A. A. Schäffer, "Finding the Prime Factors of Strong Direct Product Graphs in Polynomial Time," *Discrete Mathematics* **109** (1992), pp. 77–102.

182. R. Beigel and J. Feigenbaum, "On Being Incoherent Without Being Very Hard," *Computational Complexity* **2** (1992), pp. 1–17.

183. 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.

184. J. Feigenbaum, L. Fortnow, C. Lund, and D. Spielman, "The Power of Adaptiveness and Additional Queries in Random-Self-Reductions," in *Proceedings of the 7th IEEE Structure in Complexity Theory Conference*, 1992, pp. 338–346. (Preliminary version of [169].)

185. J. Feigenbaum, J. A. Kahn, and C. Lund, "Complexity Results for POMSET Languages," in *Proceedings of the 3^{rd} International Workshop on Computer-Aided Verification (1991)*, Lecture Notes in Computer Science, volume 575, Springer, 1992, pp. 343–353. (Preliminary version of [175].)

186. J. Feigenbaum, "CRA Committee is Creating a Database of Women Scientists," *Computing Research News* **4:2** (1992), pp. 4–5.

187. 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, volume 537, Springer, 1991, pp. 62–76.

188. 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, volume 537, Springer, 1991, pp. 326–338.

189. E. Allender, J. Cai, and J. Feigenbaum, "Workshop Summary: Structural Complexity and Cryptography," DIMACS Technical Report 91-36, Rutgers University, Piscataway NJ, 1991.

190. R. Beigel, M. Bellare, J. Feigenbaum, and S. Goldwasser, "Languages that are Easier than their Proofs," in *Proceedings of the 32^{nd} IEEE Symposium on Foundations of Computer Science*, 1991, pp. 19–28.

191. 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*, volume 2, American Mathematical Society, 1991, pp. 161–172.

192. 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*, volume 2, American Mathematical Society, 1991, pp. 1–45.

193. J. Feigenbaum, "Lexicographically Factorable Extensions of Irreducible Graphs," in **Graph Theory, Combinatorics, and Applications: Volume 1**, John Wiley and Sons, 1991, pp. 481–492.

194. D. Eppstein, J. Feigenbaum, and C.-L. Li, "Equipartitions of Graphs," *Discrete Mathematics* **91** (1991), pp. 239–248.

195. J. Feigenbaum and L. Fortnow, "Random-Self-Reducibility of Complete Sets," in *Proceedings of the 6^{th} IEEE Structure in Complexity Theory Conference*, 1991, pp. 124–132. (Preliminary version of [176].)

196. D. Beaver and J. Feigenbaum, "Hiding Instances in Multioracle Queries," in *Proceedings of the 7^{th} Symposium on Theoretical Aspects of Computer Science*, Lecture Notes in Computer Science, volume 415, Springer, 1990, pp. 37–48.

197. M. Abadi and J. Feigenbaum, "Secure Circuit Evaluation: A Protocol Based on Hiding Information from and Oracle," *Journal of Cryptology* **2** (1990), pp. 1–12. (Final version of [208].)

198. J. Feigenbaum, "DIMACS Update," *SIGACT News* **22:1** (1991), pp. 24–25.

199. 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, volume 403, Springer, 1990, pp. 297–310.

200. J. Feigenbaum, S. Kannan, and N. Nisan, "Lower Bounds on Random-Self-Reducibility," in *Proceedings of the 5^{th} IEEE Structure in Complexity Theory Conference*, 1990, pp. 100–109.

201. J. Feigenbaum, "DIMACS Update," *SIGACT News* **21:4** (1990), pp. 49–52.

202. J. Feigenbaum, "Report on DIMACS Seminar Series," *SIGACT News* **21:2** (1990), pp. 25–27.

203. J. Feigenbaum, R. Lipton, and S. Mahaney, "A Completeness Theorem for Almost-Everywhere Invulnerable Generators," AT&T Bell Laboratories Technical Memorandum, Murray Hill, NJ, February 1989.

204. M. Abadi, J. Feigenbaum, and J. Kilian, "On Hiding Information from an Oracle," *Journal of Computer and System Sciences* **39** (1989), pp. 21–50. (Final version of [209] and [210]. Special issue of selected papers from Structures 1987.)

205. J. Feigenbaum and R. Haddad, "On Factorable Extensions and Subgraphs of Prime Graphs," *SIAM Journal on Discrete Mathematics* **2** (1989), pp. 197–218.

206. J. Feigenbaum, "Report on DIMACS Seminar Series," *SIGACT News* **20:4** (1989), pp. 48–49.

207. J. Feigenbaum, "Report on DIMACS Seminar Series," *SIGACT News* **20:3** (1989), pp. 34–35.

208. M. Abadi and J. Feigenbaum, "A Simple Protocol for Secure Circuit Evaluation," in *Proceedings of the 5^{th} Symposium on Theoretical Aspects of Computer Science*, Lecture Notes in Computer Science, volume 294, Springer, 1988, pp. 264–272. (Preliminary version of [197].)

209. M. Abadi, J. Feigenbaum, and J. Kilian, "On Hiding Information from an Oracle (Extended Abstract)," in *Proceedings of the 19^{th} ACM Symposium on Theory of Computing*, 1987, pp. 195–203. (This and [210] are preliminary versions of [204].)

210. M. Abadi, J. Feigenbaum, and J. Kilian, "On Hiding Information from an Oracle," in *Proceedings of the 2^{nd} IEEE Structure in Complexity Theory Conference*, p. 9, 1987. (This and [209] are preliminary versions of [204].)

211. J. Feigenbaum, "A Note on the Cycle Structure of Cartesian-Product Graphs," AT&T Bell Laboratories Technical Memorandum, Murray Hill, NJ, October 1987.

212. J. Feigenbaum, "Directed Cartesian Product Graphs have Unique Factorizations that Can be Computed in Polynomial Time," *Discrete Applied Mathematics* **15** (1986), pp. 105–110.

213. J. Feigenbaum and A. A. Schäffer, "Recognizing Composite Graphs is Equivalent to Testing Graph Isomorphism," *SIAM Journal on Computing* **15** (1986), pp. 619–627.

214. J. Feigenbaum, "Encrypting Problem Instances," in *Advances in Cryptology – Crypto '85*, Lecture Notes in Computer Science, volume 218, Springer 1986, pp. 477–488.

215. J. Feigenbaum, "Product Graphs: Some Algorithmic and Combinatorial Results," PhD Thesis, Technical Report STAN-CS-86-1121, Stanford University, Stanford CA, June 1986.

216. D. Subramanian and J. Feigenbaum, "Factorization in Experiment Generation," in *Proceedings of the 5^{th} National Conference on Articial Intelligence*, AAAI, 1986, pp. 518–522.

217. J. Feigenbaum, J. Hershberger, and A. A. Schäffer, "A Polynomial-Time Algorithm for Finding the Prime Factors of Cartesian-Product Graph," *Discrete Applied Mathematics* **12** (1985), pp. 123–138.

218. D. Coppersmith and J. Feigenbaum, "Finite Graphs with Two Inequivalent Factorizations under the Composition Operator," IBM Research Report RC11149, Yorktown Heights, NY, 1985.

219. J. Feigenbaum and A. Schäffer, "Recognizing Corona Graphs," AT&T Bell Laboratories Technical Memorandum, Murray Hill, NJ, August 1985.

220. 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.

221. J. Feigenbaum and R. E. Tarjan, "Two New Kinds of Biased Search Trees," *Bell System Technical Journal* **62** (1983), pp. 3139–3158.