

Cynthia Dwork

Gordon McKay Professor of Computer Science, Harvard University
Professor by Affiliation, Harvard Law School
Professor by Affiliation, Department of Statistics, Harvard University

Education:

1983: Ph.D. in Computer Science, Cornell University
1981: M.Sc. in Computer Science, Cornell University
1979: BSE (with Honors), in Electrical Engineering and Computer Science, Princeton University

Employment

January, 2017 – present: Gordon McKay Professor of Computer Science at the Harvard Paulson School of Engineering
October, 2001 – 2023 : Microsoft Research, Silicon Valley Campus; Title on resignation: Distinguished Scientist
January, 2017 – June 2022: Radcliffe Alumnae Professor at the Radcliffe Institute for Advanced Study
June, 2000 – October, 2001: Compaq Systems Research Center; Staff Fellow
August, 1985 – June, 2000: IBM Almaden Research Center, Research Staff Member
May, 1983 - May, 1985 Post-Doctoral Research Fellow, MIT Laboratory for Computer Science
Host: Nancy Lynch

Other Professional Affiliations

Consulting Professor, Stanford University, 1997 – 2006
1989-1990: Visiting Scientist, MIT Laboratory for Computer Science
Bantrell Post-Doctoral Fellowship (at MIT), 1983-1985

Honors and Awards:

Test-of-Time Award, ICML 2023, for *Learning Fair Representations*, R. Zemel, Y. Wu, K. Swersky, T. Pitassi, and C. Dwork
30-Year Test-of-Time Award, STOC 2022, for *Non-Malleable Cryptography*, Dolev, Dwork, and Naor

2022 ACM Paris Kanellakis Theory and Practice Award, for fundamental contributions to the development of differential privacy, with Blum, Dinur, McSherry, Nissim, and Smith

RSA Conference 2022 Award for Excellence in Mathematics, co-sponsored by the International Association of Cryptologic Research (IACR)

Donald E. Knuth Prize, 2020

Institute of Electrical and Electronics Engineers (IEEE) Richard W. Hamming Medal, 2020

Gödel Prize, 2017, for *Calibrating Noise to Sensitivity in Private Data Analysis*, by Dwork, McSherry, Nissim, and Smith

Theory of Cryptography Conference Test of Time Award, 2016, for *Calibrating Noise to Sensitivity in Private Data Analysis*, by Dwork, McSherry, Nissim, and Smith

PET Award for Outstanding Research in Privacy Enhancing Technologies, 2009

Edsger W. Dijkstra Prize, 2007, for *Consensus in the Presence of Partial Synchrony*, by Dwork, Lynch, and Stockmeyer

Fellow of the American Philosophical Society, elected 2016

Fellow of the Association for Computing Machinery, elected 2016

Member of the National Academy of Sciences, elected 2014

Fellow of the American Academy of Arts and Sciences, elected 2008

Member of the National Academy of Engineering, elected 2008

Fellow of the Association for Computing Machinery, elevated 2015

Charles Ira Young Tablet and Medal for Excellence in Independent Research, Department of Electrical Engineering and Computer Science, Princeton University, 1979

Grants

Alfred P. Sloan Foundation, “Towards Practicing Privacy,” (with J. Mitchell and D. Nekipelov)
“Collaborative Proposal: Foundations of Adaptive Data Analysis,” NSF CCF-1763665, Algorithmic Foundations (medium) award, with Aaron Roth, Adam Smith, and James Zou, 2018

“Representation via Representations,” with Giovanni Parmigiani (Dana Farber), Harvard Data Science Initiative, 2018

Alfred P. Sloan Foundation, “Pseudo-Randomness and the Crystal Ball,” (with O. Reingold), G-2020-13941, 2020

“The Theory of Algorithmic Fairness,” a Simons Collaboration Project, with Avrim Blum, Constantinos Daskalakis, Shafi Goldwasser, Jon Kleinberg, Katrina Liett, Huijia (Rachel) Lin, Jamie Morgenstern, Moni Naor, Toni Pitassi, Omer Reingold (collaboration director), Aaron Roth, and Guy Rothblum, Simons Foundation 733782

Books and Book Chapters

Federal Statistics, Multiple Data Sources, and Privacy Protection: Next Steps. Panel on Improving Federal Statistics for Policy and Social Science Research Using Multiple Data Sources and State-of-the-Art Estimation Methods, National Academies of Sciences, Engineering, and Medicine, The National Academies Press, 2017.

Innovations in Federal Statistics: Combining Data Sources While Protecting Privacy. Panel on Improving Federal Statistics for Policy and Social Science Research Using Multiple Data Sources and State-of-the-Art Estimation Methods, National Academies of Sciences, Engineering, and Medicine, The National Academies Press, 2017.

Strengthening Data Science Methods for Department of Defense Personnel and Readiness Missions, Committee on Strengthening Data Science Methods for Department of Defense Personnel and Readiness Missions, National Academies of Sciences, Engineering, and Medicine, National Academies Press (2016)

The Algorithmic Foundations of Differential Privacy, with Aaron Roth, NOW Publishers, 2014

Differential Privacy: A Cryptographic Approach to Private Data Analysis, concluding chapter of *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, Lane, Stoddard, Bender, and Nissenbaum, editors, Cambridge University Press, 2014

Protecting Individual Privacy in the Struggle Against Terrorism, Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals (National Research Council), National Academies Press (2008)

Professional Activities:

Co-founder (with Omer Reingold) of Symposium on Foundations of Responsible Computing
Member-at-Large of the 2016, 2017, and 2018 Class Membership Committee, National Academy of Sciences

Member of the National Academies Panel on Improving Federal Statistics for Policy and Social Science Research Using Multiple Data Sources and State-of-the-Art Estimation Methods, 2015 – present

Member of the National Research Council Committee on Strengthening Data Science Methods for Department of Defense Personnel and Readiness Missions, 2014 – 2016

Member of the National Research Council Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals (National Research Council), 2006-2008.

Member-at-Large, Executive Committee of ACM SIGACT, 2009-2011

SIGACT Committee for the Advancement of Theoretical Computer Science, 2008-2013

Founding Editor, *Journal of Privacy and Confidentiality*, 2008 – present; Editor-in-Chief since 2017

Member, Computing Community Consortium, 2016-2018

Editorial Boards. *Journal of Algorithms* (1990 - 2006), *Information and Computation* (1991(?) - 2010), *J. Cryptology* (1999-2010)

Advisory Boards.

Institute for Quantitative Social Sciences (IQSS), April 2020–present

Center of Mathematical Sciences and Applications (CMSA), September 2019–present
Advisory Board, AI Now, 2017–2021

Advisory Board, Harvard Data Science Initiative, 2017–present

Inaugural Chair, Scientific Advisory Board, Alan Turing Institute, 2016–2019

Advisory Board, Berkman Klein Assembly for Internet and Society, Harvard, 2016–present

Science Advisory Board, Institute for Pure and Applied Mathematics (IPAM), 2015–present

Advisory Board, Advisory Board, Electronic Privacy Information Center (EPIC), 2015(?)–present

External Advisory Board, Simons Institute (at UC Berkeley), 2012 - 2015

Member of External Review Committee, Computer Science at IST Austria, 2013

External Advisory Board, Integrating Data for Analysis, Anonymization, and Sharing (iDASH; a National Center for Biomedical Computing), 2011 - 2015

External Advisory Board of DIMACS (1996 – 2008)

Scientific Advisory Board, Bertinoro International Center for Informatics (2004 – 2008)

IACR Fellows Committee (2004 – 2009)

Chair of the Steering Committee of the Symposium on Principles of Distributed Computing, 1993-1995;

Workshops, Programs, Conferences, &c.

1. Organized and taught the Graduate Summer School on Algorithmic Fairness (with Guy Rothblum) at the Institute for Pure and Applied Mathematics (IPAM), UCLA, 2022
2. “Who Counts? Sex and Gender Bias in Data,” (with Ruha Benjamin and Patricia Williams), cross-disciplinary workshop held at the Institute for Pure and Applied Mathematics (IPAM), UCLA, 2022
3. Co-Organized the Workshop on the Analysis of Census Noisy Measurement Files and Differential Privacy (with Ruobin Gong, Weijie Su, and Linjun Zhang), at DIMACS (Rutgers), 2022
4. co-founded the Symposium on Foundations of Responsible Computing (FORC), an annual conference dedicated to mathematically strong research in computation and society writ large; inaugural meeting will be at Harvard Center of Mathematical Sciences and Applications, June, 2020
5. Wrong at the Root: Racial Bias and the Tension Between Numbers and Words in Non-Internet Data (with Patricia Williams), cross-disciplinary workshop, part of Simons Institute Summer Cluster on Algorithmic Fairness, June, 2019
6. Simons Institute Summer Cluster on Algorithmic Fairness (with Sampath Kannan and Jamie Morgenstern), May-June, 2019
7. DP Deployed (with Abhishek Bhowmick, David O’Brien, and Abhradeep Thakurta), held at the American Academy of Arts and Sciences with funding from the Sloan Foundation, September, 2018
8. Adaptive Data Analysis, held at the Simons Institute with funding from the Sloan Foundation, July, 2018
9. Simons Institute Short Summer Cluster on Algorithmic Fairness (with Sampath Kannan and Guy Rothblum), July 2018
10. Algorithmic Fairness (with Guy Rothblum), workshop at STOC, June, 2018
11. Mathematical Foundations of Data Science (with Mark Bun, Toni Pitassi, Guy Rothblum, Thomas Steinke, and Kunal Talwar), Banff (Banff International Research Station), April-May, 2018
12. Algorithmic challenges in protecting privacy for biomedical data, with Anand Sarwate, Sriram Sankararaman, and James Zou, IPAM, January, 2018

13. Four Facets of Differential Privacy, Institute for Advanced Study and Sloan Foundation, Princeton, November 2016
14. Defining Fairness, with Urs Gasser and Alexandra Wood, Harvard University, November 2016
15. Session on Differential Privacy and Statistics, IMS/Bernoulli World Congress of Probability and Statistics 2016
16. Differential Privacy: Analyzing Sensitive Data and Implications, AAAS 2015 Annual Meeting (with S. Vadhan), February 2015
17. Big Data and Differential Privacy, Simons Institute (UC Berkeley) (with K. Talwar, A. Blum, K. Chaudhuri, and M. Jordan), December, 2013.
18. New Directions in the Science of Privacy, March 2013, Simons Foundation (with M. Naor)
19. Differential Privacy and Law and Policy, March 2013, funded by Sloan Foundation, Benjamin Cardozo School of Law (with M. Naor, P. Ohm, and F. Wu)
20. Differential Privacy and Economics and Social Sciences, March 2013, funded by Sloan Foundation, hosted at Simons Foundation (with M. Naor and D. Nekipelov)
21. Statistical and Learning-Theoretic Challenges in Data Privacy, February 2010, Institute of Pure and Applied Mathematics, UCLA (with A. Smith, S. Fienberg, and A. Slavkovic)
22. Microsoft Research, Asia, Theory Workshop, April, 2008 (with A. Bogdanov, W. Chan, and S. Teng)
23. Microsoft Research / Carnegie-Mellon Center for Computational Thinking Mindswap on Privacy, October, 2007 (with L. Cranor, K. Talwar, and R. Williams)
24. NSF/Microsoft/IBM-Sponsored Workshop on Data Confidentiality, September, 2007 (with S. Fienberg, E. Bertino, E. Viegas, and L. Zayatz)
25. BICI workshop (Bertinoro): Computer Science / Statistics Workshop On Privacy and Confidentiality, July, 2005 (with S. Fienberg)
26. BICI and DIMACS workshop on Mathematics of Web Search and Meta-Search, Bertinoro, June 2004 (with A. Gelman and D. Sivakumar)
27. DIMACS workshop on Privacy-Preserving Data Mining, March, 2004 (with B. Pinkas and R. Wright)
28. IPAM Workshop on Cryptography, Los Angeles, CA, Jan 2002
29. MSRI Workshop on Number-Theoretic Aspects of Cryptography, Berkeley, CA, October, 2000
30. Workshop on Parallel and Distributed Computing, Dagstuhl, 1995
31. SIAM Minisymposium on Theory of Distributed Computing, 1992

Miscellaneous:

1. Hold first, second, and third Black Belt degrees in Chun do Kwon style of Tae Kwon Do (Korean Karate).
2. Instructor, Mountain View - Los Altos Adult School, Tae Kwon Do class, 1990 - 1995
3. Designed and Taught Seminar on Women's Self-Protection, a four-hour workshop teaching physical and non-physical avoidance of and defense against assault.

Selected Lectures

1. Ding Shum Lecture, Center of Mathematical Sciences and Applications, Harvard, planned, March 2023
2. Simons Lectures (3 lectures), MIT Department of Mathematics, September 2022
3. Green Family Lecture Series (3 lectures), Institute for Pure and Applied Mathematics, UCLA, July 2022
4. Special Sectional Lecture, International Congress of Mathematicians, June 2022
5. Keynote Talk, Beijing Academy of Artificial Intelligence Conference (BAAI), June, 2022
6. Simons Foundation Presidential Lecture, February 2022
7. Keynote talk, International Symposium on Artificial Intelligence and Mathematics (ISAIM), January 2022
8. Keynote talk, CCS 2021
9. Turing Lecture, Alan Turing Institute, September 30, 2021
10. Keynote talk, 40th ACM Conference on Principles of Distributed Computing (PODC), 2021
11. Inspirational Talk, TCS Women Workshop, STOC 2021
12. Differential Privacy: the Mathematical Bulwark against Reidentification and Reconstruction, Keynote talk, First SIAM Conference on Mathematics of Data Science (MDS), 2020
13. Outcome Indistinguishability, Knuth Prize Lecture, delivered at the IEEE Foundations of Computer Science (FOCS) conference, November, 2020
14. Differential Privacy and the US Census, Keynote talk, ACM Symposium on Principles of Database Systems (PODS) 2019
15. Differential Privacy and the US Census, Keynote talk, ACM Federated Computing Research Conference (FCRC) 2019
16. Differential Privacy and the People's Data, International Association for Cryptologic Research (IACR) Distinguished Lecture, 2019
17. Recent Developments in Algorithmic Fairness, Keynote talk, International Conference on Learning Representations (ICLR) 2019
18. Science briefing on Differential Privacy, Invited Lecture, National Association of Science Writers annual meeting, October 2018
19. "The Emerging Theory of Algorithmic Fairness," Keynote talk, ACM Symposium on Theory of Computing (STOC), June 2108

20. “Making Algorithms Play Fair,” You and AI, flagship lecture series of the Royal Society, June 2018
21. “Fair Questions,” Keynote talk, AAAI Conference on Artificial Intelligence, 2018
22. “Privacy in the Land of Plenty,” AMS Josiah Willard Gibbs Lecture, AMS Joint Mathematics Meetings, January 2018
23. “Differential Privacy: Gateway Theory,” Plenary talk, SIAM Symposium on Discrete Algorithms (SODA), 2018
24. “Theory for Society: Fairness in Classification,” Invited talk, Theory of Cryptography Conference, 2017
25. “What’s Fair?” Keynote talk, ACM Conference on Knowledge Discovery and Data Mining (KDD) 2017
26. “The Promise of Differential Privacy,” Rothschild Lecture, Isaac Newton Institute, November 2016
27. “Theory for Society,” Snowbird, July 2016
28. “Privacy in the Land of Plenty,” SIAM General Meeting, July 2016
29. “Accuracy, Privacy, and Validity: When Right is Wrong and Wrong is Right,” SIAM Meeting on Discrete Mathematics, June 2016
30. “The Mete and Measure of Privacy,” Class III (Engineering and Applied Sciences) Research Briefing, National Academy of Sciences Annual Meeting, April 2015 (session highlighting the research of new members)
31. Plenary Lecture, “Differential Privacy and False Discovery Control,” Information Theory and Applications (ITA), February 2015
32. Plenary Lecture, “Privacy in the Land of Plenty,” NIPS, December 2014
33. “A Surprising Application of Differential Privacy,” Celebration of the 50th Anniversary of Computer Science at Cornell, October, 2014
34. Plenary Lecture, “Pleasures, Pressures, and Surprises of Differential Privacy,” Society of Epidemeologic Research, June 2014
35. “The State of the Art of Privacy Protection,” Big Data Privacy Workshop Advancing the State of the Art in Technology and Practice, co-hosted by the White House Office of Science and Technology Policy and MIT, March 2014
36. “Differential Privacy Dreams and Nightmares,” Celebration of the 70th Birthday of Butler Lampson, February, 2014

37. “Natural Differential Privacy,” Verification, Model Checking, and Abstract Interpretation (VMCAI), January 2014
38. “The Mete and Measure of Privacy,” Future of Statistical Sciences Workshop, (the Statistics2013 Capstone Event), November 2013
39. Keynote talk, “Privacy-Preserving Data Analysis: From Fallacious to Felicitous ... and to Fruition!” Very Large Databases (VLDB), August, 2013
40. Plenary Lecture, “Differential Privacy and the Power of (Formalizing) Negative Thinking,” European Joint Conferences on Theory and Practice of Software (ETAPS), March, 2012
41. “The Promise of Differential Privacy,” Keynote talk, International Conference on Data Mining (ICDM), 2011
42. “Privacy against many arbitrary low-sensitivity queries,” International Congress of Mathematicians, 2010
43. ”New Directions In Private Data Analysis,” Plenary Lecture, SODA 2010
44. “Rethinking privacy and disclosure limitation from a cryptographic perspective,” in invited session, “Oh privacy where art thou? Mapping the landscape of data confidentiality,” Joint Statistics Meeting (JSM) 2009
45. “The Differential Privacy Frontier,” Theory of Cryptography Conference (TCC) 2009
46. “Differential Privacy: A Survey of Results,” Keynote talk, Theory and Applications of Models of Computation (TAMC) 2008, Xian, China, 4/2008.
47. “An *Ad Omnia* Approach to Defining and Achieving Private Data Analysis,” Keynote talk, First ACM SIGKDD Workshop on Privacy, Security, and Trsut in KDD (PinKDD), 2007.
48. “Differential Privacy,” Plenary Lecture, ICALP, 2006.
49. “Sub-Linear Queries (SuLQ) Statistical Databases: Privacy with Power,” RSA, 2005
50. “Fighting Spam: The Science,” LATIN 2004.
51. “Positive Applications of Lattices to Cryptography,” Mathematical Foundations of Computer Science (MFCS’97), Bratislava, Slovakia, 8/1997.
52. “Copyright? Protection?” Plenary Lecture, Federated Computing Research Conference, 5/1996.
53. 25th Congress of the Mexican Mathematical Association, plenary lecture, Xalapa, Mexico, 1992
54. “Zero-Knowledge with Finite State Verifiers,” CRYPTO ’88, Santa Barbara, California, 1988

Publications

Publications in Journals

1. C. Dwork, P. Kanellakis, and J. Mitchell, "On the Sequential Nature of Unification," *J. of Logic Programming* 1(1), 1985
2. S. Cook, C. Dwork, and R. Reischuk, "Upper and Lower Time Bounds for Parallel RAMS Without Simultaneous Writes", *SIAM J. Computing* 15(1), 1986
3. D. Dolev, C. Dwork, and L. Stockmeyer, "On the Minimal Synchronism Needed for Distributed Consensus," *JACM* 34(1), 1987
4. C. Dwork and Y. Moses, "Knowledge and Common Knowledge in a Byzantine Environment: Crash Failures," *Information and Computation* 88(2) (1990)
5. B. Chor and C. Dwork, "Randomization in Byzantine Agreement" *Advances in Computing Research, Volume 4*, JAI Press Inc (1989)
6. C. Dwork, N. Lynch, and L. Stockmeyer, "Consensus in the presence of Partial Synchrony," *JACM*, 35(2), 1988
7. C. Dwork, P. Kanellakis, and L. Stockmeyer, "Parallel Algorithms for Term Matching," *SIAM J. Computing* 17(4), 1988
8. C. Dwork, D. Peleg, N. Pippenger, and E. Upfal, "Fault Tolerance in Networks of Bounded Degree," *SIAM J. Computing* 17(5), 1988
9. B. Coan, D. Dolev, C. Dwork, and L. Stockmeyer, "The Distributed Firing Squad Problem," *SIAM J. Computing* 18(5), 1989
10. C. Dwork, D. Shmoys, and L. Stockmeyer, Flipping persuasively in constant time, *SIAM J. Computing* 19 (1990), 472–499.
11. C. Dwork and L. Stockmeyer, "A Gap Theorem for 2-Way Probabilistic Finite State Automata," *SIAM J. Computing* 19(6) (1990).
12. B. Coan, and C. Dwork, "Simultaneity is Harder Than Agreement," *Information and Computation* 91(2), 1991
13. A. Bar-Noy, D. Dolev, C. Dwork, and R. Strong, "Shifting Gears: Changing Algorithms on the Fly to Expedite Byzantine Agreement," *Information and Computation* 97 (2), 1992, pp. 205-233
14. C. Dwork and L. Stockmeyer, "Finite State Verifiers I: The Power of Interaction" *JACM* 39(4), 1992, pp. 800–828

15. C. Dwork and L. Stockmeyer, “Finite State Verifiers II: Zero Knowledge” *JACM* 39(4), 1992, pp. 829–858
16. D. Dolev, C. Dwork, O. Waarts, and M. Yung, “Perfectly Secure Message Transmission,” *JACM* 40(1), 1993, pp. 17–47
17. H. Attiya, D. Dwork, N. Lynch, and L. Stockmeyer, “Bounds on the Time to Reach Agreement in the Presence of Timing Uncertainty,” *JACM* 41(1), pp. 122 – 152 (1994)
18. C. Dwork and M. Naor, “Efficient Existentially Unforgeable Signatures,” *J. Cryptology* 11(3), pp. 187 – 208, 1998
19. C. Dwork, M. Herlihy, and O. Waarts, “Contention in Shared-Memory Algorithms,” *JACM* 44(6), 1997
20. C. Dwork “Copyright? Protection?” *The Mathematics of Coding, Extraction, and Distribution, The IMA Volumes in Mathematics and its Applications 107* Editors: G. Cybenko, D. O’Leary, and J. Rissanen, Springer Verlag
21. C. Dwork and O. Waarts, “Simple and Efficient Bounded Concurrent Timestamping and the Traceable Use Abstraction” *JACM* 46(5), pp. 633 – 666, 1999.
22. C. Dwork, J. Halpern, and O. Waarts, “Accomplishing Work in the Presence of Failures,” *SIAM J. Computing* 27(5), pp. 1457 – 1491 (1998)
23. C. Dwork, M. Herlihy, S. Plotkin, and O. Waarts, “Time-Lapse Snapshots,” *SIAM J. Computing* 28(5), pp. 1848 – 1874, 1999.
24. D. Dolev, C. Dwork, and M. Naor, “Non-Malleable Cryptography” *SIAM J. Computing* 30(2), pp. 391–437, 2000.
25. C. Dwork, M. Naor, O. Reingold, and L. Stockmeyer, “Magic Functions,” *JACM* 50(6), pp. 852–921, 2003.
26. C. Dwork, M. Naor, and A. Sahai, “Concurrent Zero Knowledge,” *JACM* 51(6), pp. 851–898, 2004
27. D. Dolev, C. Dwork, and M. Naor, “Non-Malleable Cryptography” to be reprinted by SIAM with a “pre-introduction” describing progress during the 13 years 1991–2003, in *SIAM Review*, 2003.
28. S. Chien, C. Dwork, S. Chien, C. Dwork, R. Kumar, D. Simon, and D. Sivakumar, Towards Exploiting Link Evolution, *Internet Mathematics* 1 (3), 2003.
29. C. Dwork and M. Naor, Zaps and Their Applications, *SIAM J. Comput.* 36(6), pp. 1513–1543, 2007.

30. C. Dwork, A Firm Foundation for Private Data Analysis, *Communications of the ACM* 54(1), 2011.
31. C. Dwork and M. Noar, On the Difficulties of Disclosure Prevention in Statistical Databases or The Case for Differential Privacy, *Journal of Privacy and Confidentiality* 2(1), 2010.
32. C. Dwork, A firm foundation for private data analysis. *CACM* 54(1), 2011
33. L. Backstrom, C. Dwork, J.M. Kleinberg, Wherefore art thou R3579X?: anonymized social networks, hidden patterns, and structural steganography, *CACM* 54(12), 2011
34. C. Dwork and R. Pottenger, Toward practicing privacy, *JAMIA* 20(1), (2013)
35. C. Dwork, V. Feldman, M. Hardt, T. Pitassi, O. Reingold, and A. Roth, The reusable holdout: Preserving validity in adaptive data analysis, *Science*, 349(6248), 636-638. Winner of the 2015 Pat Goldberg Memorial Best Paper Award
36. C. Dwork, F. McSherry, K. Nissim, and A. Smith, Calibrating Noise to Sensitivity in Private Data Analysis, *J. Privacy and Confidentiality*, 2016
37. C. Dwork, A. Smith, T. Steinke, and J. Ullman, Exposed! A Survey of Attacks on Private Data, *Annual Reviews of Statistics and its Application*, 2016
38. C. Dwork, V. Feldman, M. Hardt, T. Pitassi, O. Reingold, and A. Roth, Guilt-Free Data Reuse, *CACM*, 2017
39. C. Dwork and J. Ullman, The Fienberg Problem, *J. Privacy and Confidentiality*, 2018
40. C. Dwork, N. Kohli, and D. Mulligan, Differential Privacy in Practice: Expose Your Epsilons!, *J. Privacy and Confidentiality*, 9(2), 2019
41. C. Dwork, W. Su, and L. Zhang, Differentially Private False Discovery Rate Control, *J. Privacy and Confidentiality*, 2021

Papers in Conference Proceedings

1. S. Cook and C. Dwork, "Bounds on the Time for Parallel RAMs to Compute Simple Functions," *Proceedings of the 14th Symposium on Theory of Computing*, 1982
2. D. Dolev, C. Dwork, N. Pippenger, and A. Wigderson, "Superconcentrators, Generalizers, and Generalized Connectors with Limited Depth," *Proceedings of the 15th Symposium on Theory of Computing*, 1983
3. C. Dwork and D. Skeen, "The Inherent Cost of Nonblocking Commitment," *Proceedings of the 2nd Symposium on Principles of Distributed Computing*, 1983
4. "D. Dolev, C. Dwork, and L. Stockmeyer, "On the Minimal Synchronism needed for Distributed Consensus," *Proceedings of the 24th Symposium on the Foundations of Computer Science*, 1983
5. C. Dwork, N. Lynch, and L. Stockmeyer, "Consensus in the presence of Partial Synchrony," *Proceedings of the 3rd Symposium on the Principles of Distributed Computing*, 1984
6. C. Dwork and D. Skeen, "Patterns of Communication in Consensus Protocols," *Proceedings of the 3rd Symposium on the Principles of Distributed Systems*, 1984
7. B. Coan, D. Dolev, C. Dwork, and L. Stockmeyer, "The Distributed Firing Squad Problem," *Proceedings of the 17th Symposium on Theory of Computing*, 1985
8. B. Coan and C. Dwork, "Simultaneity is Harder than Agreement", *Proceedings of the 5th IEEE Symposium on Reliability in Distributed Software and Database Systems*, 1986
9. C. Dwork and Y. Moses, "Knowledge and Common Knowledge in a Byzantine Environment I: Crash Failures," *Proceedings of the Conference on Theoretical Aspects of Reasoning About Knowledge*, 1986
10. C. Dwork, P. Kanellakis, and L. Stockmeyer, "Parallel Algorithms for Term Matching," *Proceedings of the 8th International Conference on Automated Deduction*, 1986
11. C. Dwork, D. Peleg, N. Pippenger, and E. Upfal, "Fault Tolerance in Networks of Bounded Degree," *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, 1986
12. C. Dwork, D. Shmoys, and L. Stockmeyer, "Flipping Persuasively in Constant Expected Time," *Proceedings of the 27th Annual Symposium on Foundations of Computer Science*, 1986
13. A. Bar-Noy, D. Dolev, C. Dwork, and R. Strong, "Shifting Gears: Changing Algorithms on the Fly to Expedite Byzantine Agreement," *Proceedings of the 6th Annual ACM Symposium on Principles of Distributed Computing*, 1987
14. C. Dwork and L. Stockmeyer, "Zero Knowledge with Finite State Verifiers," *Invited Paper, CRYPTO'88*

15. C. Dwork and L. Stockmeyer, "A Gap Theorem for 2-Way Probabilistic Finite State Automata," *Proceedings of the 30th Annual Symposium on Foundations of Computer Science*, 1989
16. D. Dolev, C. Dwork, O. Waarts, and M. Yung, "Perfectly Secure Message Transmission," *Proceedings of the 31st Annual Symposium on Foundations of Computer Science*, 1990
17. C. Dwork, "Strong Verifiable Secret Sharing," *Proceedings of the 4th International Workshop on Distributed Algorithms*, 1990
18. D. Dolev, C. Dwork, and M. Naor, "Non-Malleable Cryptography," *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, 1991
19. H. Attiya, D. Dwork, N. Lynch, and L. Stockmeyer, "Bounds on the Time to Reach Agreement in the Presence of Timing Uncertainty," *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, 1991
20. C. Dwork, "On Verification in Secret Sharing," *Proc. CRYPTO '91*, Springer Verlag LNCS Vol. 576, 1992
21. C. Dwork and O. Waarts, "Simple and Efficient Bounded Concurrent Timestamping, or, Bounded Concurrent Timestamp Systems are Comprehensible!" *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, 1992, pp. 655–666
22. C. Dwork, M. Herlihy, S. Plotkin, and O. Waarts, "Time-Lapse Snapshots," *Proceedings of the Israel Symposium on the Theory of Computing and Systems*, 1992, pp. 154–170
23. C. Dwork, J. Halpern, and O. Waarts, "Accomplishing Work in the Presence of Failures," *Proceedings of the 11th Annual ACM on Principles of Distributed Computing*, 1992, pp. 91–102
24. C. Dwork and M. Naor, "Pricing via Processing," *Proc. CRYPTO '92*
25. C. Dwork, U. Feige, J. Kilian, M. Naor, S. Safra, "Low Communication 2-Prover Zero-Knowledge Proofs for NP," *Proc. CRYPTO '92*
26. C. Dwork, M. Herlihy, and O. Waarts, "Contention in Shared-Memory Algorithms," *Proc. 25th Annual Symposium on Theory of Computing*, 1993
27. C. Dwork, M. Herlihy, and O. Waarts, "Bounded Round Numbers," *Proc. 12th Annual Symposium on Principles of Distributed Computing*, 1993, pp. 53–64
28. C. Dwork and M. Naor, "Efficient Existentially Unforgeable Signatures," February, 1994, CRYPTO '94
29. M. Ajtai, J. Aspnes, C. Dwork, O. Waarts, "The Competitive Analysis of Wait-Free Algorithms and its Application to the Cooperative Collect Problem," *35th IEEE Symposium on Foundations of Computer Science*, 1994

30. D. Choy, R. Dievendorf, C. Dwork, J. Lotspiech, R. Morris, L. Anderson, A. Bell, T. Griffin, B. Hoenig, J. McCrossin, A. Miller, N. Pass, F. Pestoni, D. Picciano, "The Almaden Distributed Digital Library System," ADL'95, 1995
31. C. Dwork, J. Lotspiech, and M. Naor, "Digital Signets for Protection of Digital Information," *Proc. 28th Annual Symposium on Theory of Computing*, 1996
32. C. Dwork, C-T. Ho, H. R. Strong, "Collective Consistency," *Proc. 10th Workshop on Distributed Algorithms*, 1996
33. D. Choy, C. Dwork, J. Lotspiech, L. Anderson, J. Boyer, R. Dievendorf, T. Griffin, B. Hoenig, M. Jackson, W. Kaka, J. McCrossin, A. Miller, R. Morris, N. Pass, A Digital Library System for Periodicals Distribution, ADL'96 (Advances in Digital Libraries '96)
34. R. Canetti, C. Dwork, M. Naor, R. Ostrovsky, Deniable Encryption, "Security in Communication Networks" workshop, Amalfi, Italy 1996 and CRYPTO'97
35. M. Ajtai and C. Dwork, "A Public-key Cryptosystem with Worst-case/Average-case Equivalence," STOC'97
36. C. Dwork, M. Naor, and A. Sahai, "Concurrent Zero-Knowledge," STOC'98
37. C. Dwork and A. Sahai, "Concurrent Zero-Knowledge: Reducing the Need for Timing Constraints," CRYPTO'98
38. C. Dwork, M. Naor, O. Reingold, and L. Stockmeyer, "Magic Functions," FOCS'99
39. C. Dwork and M. Naor, "Zaps and Their Applications" STOC 2000
40. C. Dwork, R. Kumar, M. Naor, D. Sivakumar, "Rank Aggregation Methods for the Web," WWW10; selected as *Web Search Area highlight* and one three best IBM research papers for 2001 in the CS/EE/Math categories.
41. C. Dwork and L. Stockmeyer, 2-Round Zero Knowledge and Proof Auditors, STOC 2002.
42. S. Chien, C. Dwork, R. Kumar, D. Simon, and D. Sivakumar, Towards Exploiting Link Evolution, Workshop on Algorithms for the Web, November, 2002.
43. C. Dwork, A. Goldberg, and M. Naor, On Memory-Bound Functions for Combating Spam, CRYPTO 2003.
44. C. Dwork, R. Shaltiel, A. Smith, L. Trevisan, Analysis of a 2-Round Zero-Knowledge Argument, Theory of Cryptography Conference, 2004.
45. C. Dwork, M. Naor, and O. Reingold, Immunizing Encryption Schemes from Decryption Errors, EUROCRYPT 2004.
46. C. Dwork and K. Nissim, Privacy-Preserving Datamining on Vertically Partitioned Databases, CRYPTO 2004

47. C. Dwork, Fighting Spam: The Science, (invited talk), LATIN, 2004.
48. S. Chawla, C. Dwork, F. McSherry, A. Smith, and H. Wee, Towards Privacy in Public Databases, Theory of Cryptography Conference, 2005.
49. A. Blum, C. Dwork, F. McSherry, and K. Nissim, Practical Privacy: The SuLQ Framework, Principals of Database Systems, 2005.
50. C. Dwork, Sub-linear Queries Statistical Databases: Privacy with Power, Cryptography Track, RSA, (invited talk), 2005.
51. S. Chawla, C. Dwork, F. McSherry, and K. Talwar, On Privacy-Preserving Histograms, Uncertainty in Artificial Intelligence, 2005.
52. C. Dwork, M. Naor, and H. Wee, Pebbling and Proofs of Work, CRYPTO 2005.
53. M. Ajtai, C. Dwork, and L. Stockmeyer, Architecture for Secure Computing, by Ajtai, Dwork, and Stockmeyer Latin American Theory of Informatics Conference (LATIN), 2006.
54. N. Ailon, S. Chien, and C. Dwork, On Clusters in Markov Chains, Latin American Theory of Informatics Conference (LATIN), 2006.
55. C. Dwork, F. McSherry, K. Nissim, and A. Smith, Calibrating Noise to Sensitivity in Private Data Analysis, Theory of Cryptography Conference, 2006.
56. C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, Our Data, Ourselves: Privacy via Distributed Noise Generation, Eurocrypt, 2006.
57. C. Dwork, Differential Privacy, ICALP 2006 (invited talk).
58. C. Dwork, Ask a Better Question, Get a Better Answer: A New Approach to Private Data Analysis, International Conference on Database Theory (invited talk), 2007.
59. B. Barak, K. Chaudhuri, C. Dwork, S. Kale, F. McSherry, K. Talwar, Privacy, accuracy, and consistency too: a holistic solution to contingency table release, PODS 2007.
60. C. Dwork, F. McSherry, K. Talwar, The price of privacy and the limits of LP decoding, STOC 2007. L. Backstrom, C. Dwork, J. Kleinberg, Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. WWW (Best Paper), 2007.
61. C. Dwork, F. McSherry, and K. Talwar, Differentially Private Marginals Release with Mutual Consistency and Error Independent of Sample Size, Proceedings of the Joint UNECE-EuroSTAT Work Session on Statistical Data Confidentiality (invited paper), 2007.
62. C. Dwork, An Ad Omnia Approach to Defining and Achieving Private Data Analysis, Proceedings of the First SIGKDD International Workshop on Privacy, Security, and Trust in KDD (PinKDD'07), Lecture Notes in Computer Science, Volume 4890, Springer, (invited paper) 2008; received the 2009 PET Award for Outstanding Research in Privacy Enhancing Technologies.

63. C. Dwork, Differential Privacy: A Survey of Results, Proceedings of The 5th Annual Conference on Theory and Applications of Models of Computation, (invited talk), 2008.
64. C. Dwork and S. Yekhanin, New Efficient Attacks on Statistical Disclosure Control Mechanisms, CRYPTO 2008.
65. C. Dwork, Differential Privacy: A Survey of Results, *Proc. TAMC 2008*.
66. C. Dwork, M. Naor, G. Rothblum, and V. Vaikuntanathan, How Efficient Can Memory Checking Be?, *Proc. TCC 2009*.
67. C. Dwork, The Differential Privacy Frontier (Extended Abstract), *TCC 2009* (invited paper).
68. C. Dwork, M. Naor, O. Reingold, G. Rothblum, and S. Vadhan, On the complexity of differentially private data release: efficient algorithms and hardness results, *Proc. STOC 2009*.
69. C. Dwork and J. Lei, Differential privacy and robust statistics, *Proc. STOC 2009*
70. C. Dwork, Differential Privacy in New Settings (invited talk), *Proc. SODA*, 2010
71. C. Dwork, M. Naor, T. Pitassi, G. Rothblum, and S. Yekhanin, Pan-Private Streaming Algorithms, *Proc. First Innovations in Computer Science Conference*, 2010
72. C. Dwork, M. Naor, T. Pitassi, and G. Rothblum, Differential Privacy Under Cointinual Observation, *Proc. STOC 2010*
73. C. Dwork, G. Rothblum, and S. Vadhan, Boosting and Differential Privacy, *Proc. FOCS, 2010*
74. C. Dwork, M. Hardt, T. Pitassi, O. Reingold, and R. Zemel, Fairness through awareness, *Proc. ITCS, 2012*
75. C. Dwork, M. Naor, and S. Vadhan, The Privacy of the Analyst and the Power of the State, *Proc. FOCS, 2012*
76. R. Zemel, Y. Wu, K. Swersky, T. Pitassi, and C. Dwork, Learning Fair Representations, *Proc. ICML*, 2013; winner of 2023 ICML Test-of-Time award
77. C. Dwork, K. Talwar, A. Thakurta, and L. Zhang, Analyze Gauss: Optimal Bounds for Privacy-Preserving PCA, *Proc. STOC*, 2014
78. C. Dwork, A. Nikolov, and K. Talwar, Using Convex Relaxations for Efficiently and Privately Releasing Marginals, *Proc. SoCG*, 2014
79. C. Dwork, V. Feldman, M. Hardt, T. Pitassi, O. Reingold, and A. Roth, Preserving Statistical Validity in Adaptive Data Analysis, *Proc. STOC*, 2015
80. C. Dwork, A. Smith, T. Steinke, J. Ullman, and S. Vadhan, Robust Traceability from Trace Amounts, *Proc. FOCS*, 2015

81. C. Dwork, M. Naor, O. Reingold, and G. Rothblum, Pure Differential Privacy for Rectangle Queries via Private Partitions, *Proc. Asiacrypt*, 2015
82. C. Dwork, V. Feldman, M. Hardt, T. Pitassi, O. Reingold, and A. Roth, Generalization in Adaptive Data Analysis and Holdout Reuse, *proc NIPS*, 2015
83. C. Dwork, M. Naor, and G. Rothblum, Spooky Interaction and Its Discontents: Compilers for Succinct Two-Message Argument Systems. *CRYPTO*, 2016
84. C. Dwork, N. Immorlica, A. Kalai, and M. Leiserson, Decoupled Classifiers for Group-Fair and Efficient Machine Learning, *FAT* 2018* (and *FATML* workshop poster, 2017)
85. M. Bun, C. Dwork, G. Rothblum, and T. Steinke, Composable and Versatile Privacy via Truncated CDP, *Theory and Practice of Differential Privacy (TPDP; poster)*, 2017, and *STOC 2018*
86. V. Feldman and C. Dwork, Privacy-preserving Prediction, *COLT*, 2018
87. C. Dwork and C. Ilvento, Fairness Under Composition, *ITCS 2019*
88. Z. Deng, C. Dwork, and A. Smith, Differential Privacy After the Fact: The Case of Congressional Reapportionment, *Theory and Practice of Differential Privacy (TPDP; refereed workshop)*, 2019
89. C. Dwork, M. Kim, O. Reingold, N. Rothblum, and G. Yona, Learning from Outcomes: Evidence-Based Rankings, *FOCS 2019*
90. C. Dwork, C. Ilvento, and M. Jagadeesan, Individual Fairness in Pipelines, *First Symposium on Foundations of Responsible Computing, FORC 2020*
91. C. Dwork, C. Ilvento, P. Sur, and G. Rothblum, Abstracting Fairness: Oracles, Metrics, and Interpretability, *First Symposium on Foundations of Responsible Computing, FORC 2020*
92. M. Neunhoffer, Z. Steven Wu and C. Dwork, Private Post-GAN Boosting, *ICLR*, 2020 (also appeared in *TPDP* (poster), 2020)
93. C. Dwork and C. Ilvento, Consistent Integer, Non-Negative, Hierarchical Histograms without Integer Programming, *TPDP* (poster), 2020
94. Z. Deng, C. Dwork, J. Wang, L. Zhang, Interpreting Robust Optimization via Adversarial Influence Functions *ICML*, July 2020
95. C. Dwork, M. Kim, O. Reingold, N. Rothblum, and G. Yona, Outcome Indistinguishability, *STOC 2021*; also appeared in non-archival track of 2nd Symposium on Foundations of Responsible Computing (*FORC 2021*)
96. E. Du and C. Dwork, Improved Generalization Guarantees in Restricted Data Models, *Symposium on Foundations of Responsible Computing (FORC)*, 2022

97. C. Dwork, M.P. Kim, O. Reingold, G. Rothblum, and G. Yona, Beyond Bernoulli: Generating Random Outcomes that cannot be Distinguished from Nature, *Proc. International Conference on Algorithmic Learning Theory (ALT)*, 2022
98. C. Dwork and M. Minow, Distrust of Artificial Intelligence: Sources & Responses from Computer Science & Law. *Daedalus*, 151(2), 2022
99. Z. Deng, C. Dwork, and L. Zhang, HappyMap: A Generalized Multicalibration Method; Sufficient Conditions and Applications, *Proc. ITCS*, 2022
100. C. Dwork, Differential Privacy: Getting More for Less, *Proc. International Congress of Mathematicians 2022 (ICM 2022)*
101. T. Dick, C. Dwork, M. Kearns, T. Liu, A. Roth, G. Vietri, and Z.S. Wu, Confidence-ranked reconstruction of census microdata from published statistics, *Proc. National Academy of Sciences (PNAS)*, 120(8), 2023
102. C. Dwork, O. Reingold, and G. Rothblum, From the Real Towards the Ideal: Risk Prediction in a Better World, *Proc. 4th Symposium on Foundations of Responsible Computing (FORC)*, 2023 (Best Paper Award)
103. C. Dwork, D. Lee, R. Lin, and P. Tankala, From Pseudorandomness to Multi-Group Fairness and Back, *COLT*, 2023

Other Venues

1. C. Dwork and G. Rothblum, Concentrated Differential Privacy, <https://arxiv.org/pdf/1603.01887.pdf>
2. Deng, Z., Ding, F., Dwork, C., Hong, R., Parmigiani, G., Patil, P. and Sur, P., 2020. Representation via representations: Domain generalization via adversarially learned invariant representations. arXiv preprint arXiv:2006.11478
3. M. Burhanpurkar, Z. Deng, C. Dwork, and L. Zhang, Scaffolding sets. arXiv preprint arXiv:2111.03135, 2021
4. J. Abowd, L. Alvisi, C. Dwork, S. Kannan, A. Machanavajjhala, and J. Reiter, Privacy-Preserving Data Analysis for the Federal Statistical Agencies, Transition Document 2017, website of the Computing Community Consortium (CCC), available at <https://cra.org/ccc/wp-content/uploads/sites/2/2015/01/CCCPrivacyTaskForcePaperRevised-FINAL.pdf> (accessed 5/24/2018)

Patents

1. Dolev, Danny (Jerusalem, IL) Dwork, Cynthia (Palo Alto, CA) System for secure and private communication in a triple-connected network, US Pat. No. 5,161,186 (Nov. 3, 1992).
2. Dwork, Cynthia (Palo Alto, CA) Halpern, Joseph Y. (Cupertino, CA) Strong Jr., Hovey R. (San Jose, CA) Fault-Tolerant Load Management System and Method, US Pat. No. 5,513,354 (Apr. 30, 1996).
3. Dwork, Cynthia (Palo Alto, CA) Naor, Simeon (Tel-Aviv, IL) Method for message authentication from non-malleable cryptosystems, US Pat. No. 5,539,826 (Jul 23, 1996).
4. Dwork, Cynthia (Palo Alto, CA) Ho, Ching-tien (San Jose, CA) Strong Jr., Hovey Raymond (San Jose, CA) Method and System for Achieving Collective Consistency in Detecting Failures in a Distributed Computing System, US Pat. No. 5,682,470 (Oct. 28, 1997)
5. Dwork, Cynthia (Palo Alto, CA) Halpern, Joseph Y. (Cupertino, CA) Strong Jr., Hovey R. (San Jose, CA) Fault tolerant load management system and method United States Patent 5727210 03/10/1998
6. Dwork, Cynthia (Palo Alto, CA) Naor, Moni (Tel Aviv, IL) Pestoni, Florian (Buenos Aires, AR) System and method for certifying content of hard-copy documents, US Pat. No. 5,926,551 (Jul. 20, 1999)
7. Dwork, Cynthia (Palo Alto, CA) Halpern, Joseph Y. (Cupertino, CA) Lotspiech, Jeffrey Bruce (San Jose, CA) Method and System for Protection of Digital Information, US Pat. No. 5,978,482 (Nov. 2, 1999)
8. Dwork, Cynthia (Palo Alto, CA) Halpern, Joseph Y. (Cupertino, CA) Lotspiech, Jeffrey Bruce (San Jose, CA) Method and System for Protection of Digital Information, US Pat. No. 6,038,316 (Mar. 14, 2000)
9. C. Dwork, M. Naor and F. Pestoni, *System and method for verifying signatures on documents*, US Patent No. 6,081,610 (June 27, 2000)
10. Dwork, Cynthia (Palo Alto, CA) Naor, Moni (Tel Aviv, IL) Pestoni, Florian (Buenos Aires, AR) Machine-readable checks United States Patent 6126203 10/03/2000
11. Dwork, Cynthia (San Francisco, CA, US) Naor, Simeon (Tel-Aviv, IL) Ravikumar, Shanmugasundaram (San Jose, CA, US) Sivakumar, Dandapani (Cupertino, CA, US) System and method for aggregating ranking results from various sources to improve the results of web searching United States Patent 20030037074 02/20/2003
12. Dwork, Cynthia (San Francisco, CA, US) Naor, Simeon (Matam, IL) Ravikumar, Shanmugasundaram (San Jose, CA, US) Sivakumar, Dandapani (Cupertino, CA, US) System and method for aggregating ranking results from various sources to improve the results of web searching United States Patent 7,188,106 03/06/2007

13. Atkinson, Robert George (Woodinville, WA, US) Goodman, Joshua T. (Redwood, WA, US) Lyon, James M. (Redwood, WA, US) Williams, Roy (Woodinville, WA, US) Ahmed, Khaja E. (Bellevue, WA, US) Katz, Harry Simon (Bellevue, WA, US) Rounthwaite, Robert L. (Fall City, WA, US) Goldberg, Andrew V. (Redwood City, WA, US) Dwork, Cynthia (San Francisco, CA, US) Reducing unwanted and unsolicited electronic messages by exchanging electronic message transmission policies and solving and verifying solutions to computational puzzles United States Patent 20040181585 09/16/2004
14. Dwork, Cynthia (San Francisco, CA, US) Naor, Moni (Tel-Aviv, IL) Low communication complexity memory-bound function United States Patent 20060161567 07/20/2006
15. Dwork, Cynthia (San Francisco, CA, US) Kobliner, Yaacov Nissim (Beer Sheva, IL) Preserving privacy when statistically analyzing a large database United States Patent 20060161527 07/20/2006
16. Dwork, Cynthia (San Francisco, CA, US) Mcsherry, Frank David (San Francisco, CA, US) Nissim Kobliner, Yaacov (Beer-Sheva, IL) Blum, Avrim L. (Pittsburgh, PA, US) Private clustering and statistical queries while analyzing a large database United States Patent 20060200431 09/07/2006
17. Dwork, Cynthia (San Francisco, CA, US) Mcsherry, Frank D. (San Francisco, CA, US) Noise in secure function evaluation United States Patent 20070083493 04/12/2007
18. Dwork, Cynthia (San Francisco, CA, US) Mcsherry, Frank D. (San Francisco, CA, US) Data diameter privacy policies United States Patent 20070124268 05/31/2007
19. Dwork, Cynthia (San Francisco, CA, US) Mcsherry, Frank D. (San Francisco, CA, US) Exponential noise distribution to optimize database privacy and output utility United States Patent 20070130147 06/07/2007
20. Dwork, Cynthia (San Francisco, CA, US) Mcsherry, Frank D. (San Francisco, CA, US) Noisy histograms United States Patent 20070136027 06/14/2007
21. Dwork, Cynthia (San Francisco, CA, US) Mcsherry, Frank D. (San Francisco, CA, US) Differential data privacy United States Patent 20070143289 Publication Date:06/21/2007
22. Dwork, Cynthia (San Francisco, CA, US) Ravikumar, Shanmugasundaram (San Jose, CA, US) Sahai, Amit (Cambridge, MA, US) Digital signature system and method based on hard lattice problem United States Patent 7237116 06/26/2007
23. Protection against timing and resource consumption attacks Publication Date:06/28/2007 United States Patent 20070150437 Dwork, Cynthia (San Francisco, CA, US) Mcsherry, Frank D. (San Francisco, CA, US) Mironov, Ilya (Mountain View, CA, US)
24. Dwork, Cynthia (San Francisco, CA, US) Mcsherry, Frank D. (San Francisco, CA, US) Selective privacy guarantees United States Patent 20070147606 06/28/2007