ERIC BACH

Computer Sciences Department
University of Wisconsin
Madison, WI 53706
608-262-7997

EDUCATION

A.B. in Mathematics, University of Michigan, Ann Arbor, 1974 (Highest Honors and High Distinction).

Ph.D. in Computer Science, University of California, Berkeley, 1984 (supervised by Manuel Blum).

POSITIONS HELD

1984 – 1989: Assistant Professor, Computer Sciences Department, University of Wisconsin, Madison.

1989 – 1995: Associate Professor, Computer Sciences Department, University of Wisconsin, Madison.

1995 – present: Professor, Computer Sciences Department, University of Wisconsin, Madison.

Visiting positions at U. California (Berkeley), U. Paris-Sud (Orsay), U. Waterloo, U. Chile (Santiago).

Affiliate appointments in Mathematics and Electrical & Computer Engineering, UW-Madison.

HONORS AND AWARDS

James B. Angell Scholar, University of Michigan (all years).

Phi Beta Kappa, Nominated 1974.

Anthony and Gee Graduate Fellowship, UC Berkeley Computer Sciences Division, 1978.

California Microelectronics Fellowship, UC Berkeley Computer Sciences Division, 1983.

Friedman Memorial Dissertation Prize, UC Berkeley Mathematics Department, 1984.

Distinguished Dissertation Award, ACM, 1984.

Professor of the Year, UW Madison Computer Sciences Department, 1986.

Presidential Young Investigator, NSF, 1986.

Vilas Associate Research Award, UW Madison, 2006.

Carolyn Rosner Award for Excellence in Teaching, UW Computer Sciences Department, 2009.

BIOGRAPHICAL LISTINGS

Who's Who in America

Who's Who in Science and Engineering

American Men and Women of Science

Wikipedia

PUBLICATIONS

[Books]

1. E. Bach, Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms, MIT Press, 1985. [ACM Distinguished Dissertation Series.]

2. E. Bach and J. Shallit, Algorithmic Number Theory: Volume 1, Efficient Algorithms, MIT Press, 1996.

[Patents]

3. M. Hellman and C.E. Bach, Method and Apparatus for Use in Public-Key Data Encryption System, United States Patent # 4,633,036 (1986).

[Refereed Journal and Conference Papers]

4. E. Bach, Fast Algorithms Under the Extended Riemann Hypothesis: A Concrete Estimate, Proceedings of the Fourteenth Annual ACM Symposium on Theory of Computing, 1982, 290-295.

5. E. Bach, G. Miller, and J. Shallit, Sums of Divisors, Perfect Numbers, and Factoring, SIAM Journal on Computing 15 (1986), 1143-1154. [Preliminary version in Proceedings of the Sixteenth Annual ACM Symposium on Theory of Computing, 1984, 183-190.]

6. E. Bach, How to Generate Factored Random Numbers, SIAM Journal on Computing 17 (1988), 179-193. **Invited to Special Issue on Cryptography**. [Preliminary version: How to Generate Random Integers with Known Factorization, Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing, 1983, 184-188.]

7. E. Bach and J. Shallit, Factoring with Cyclotomic Polynomials, Mathematics of Computation 52, (1989), 201-219. [Preliminary version in Proceedings of the 26th Annual Symposium on Foundations of Computer Science, 1985, 443-450.]

8. E. Bach, Intractable Problems in Number Theory (**invited paper**), in Advances in Cryptology: Proceedings of CRYPTO 88, ed. S. Goldwasser, Springer-Verlag, 1990, 77-93.

9. E. Bach, Explicit Bounds for Primality Testing and Related Problems, Mathematics of Computation 55 (1990), 355-380.

10. E. Bach and V. Shoup, Factoring Polynomials Using Fewer Random Bits, Journal of Symbolic Computation 9 (1990), 229-239. [**Reprinted** in Computational Algebraic Complexity, ed. E. Kaltofen, Academic Press, 1990, 1-11.]

11. E. Bach, A Note on Square Roots in Finite Fields, IEEE Transactions on Information Theory 36 (1990), 1494-1498.

12. E. Bach, Realistic Analysis of Some Randomized Algorithms, Journal of Computer and System Sciences 42 (1991), 30-52. [Preliminary version in Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing, 1987, 453-461.] **Invited to (stillborn) special issue of best STOC 87 papers.**

13. E. Bach, Toward a Theory of Pollard's Rho-Method, Information and Computation 90 (1991), 139-155.

14. E. Bach and J. Sorenson, Sieve Algorithms for Perfect Power Testing, Algorithmica 9 (1993), 313-328.

15. E. Bach and L. Huelsbergen, Statistical Evidence for Small Generating Sets, Mathematics of Computation 61 (1993), 69-82. **Invited to special issue in memory of D.H. Lehmer.**

16. E. Bach, J. Driscoll, and J. Shallit, Factor Refinement, Journal of Algorithms 15 (1993) 199-222. [Preliminary version in Proceedings of the First Annual ACM-SIAM Symposium on Discrete Algorithms, 1990, 201-211.]

17. E. Bach, Timing the Blind Watchmaker: Comments on an Evolution Model of Richard Dawkins, UMAP Journal 14 (1993), 295-308.

18. E. Bach, Exact Analysis of a Priority Queue Algorithm for Random Variate Generation, Proceedings of the Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, 1994, 48-56.

19. E. Bach, Tensor Products and Computability, Journal of Symbolic Computation 18 (1994), 585-593.

20. E. Bach, Improved Approximations for Euler Products (**invited paper**), in Number Theory: Fourth Conference of the Canadian Number Theory Association, 1995, 13-28.

21. G. Lewandowski, A. Condon, and E. Bach, Asynchronous Analysis of Dynamic Programming Algorithms, IEEE Transactions on Parallel and Distributed Systems 7 (1996), 425-438. [Abstract in Proceedings of the 1993 ACM SIGMETRICS Conference on Measurement and Modeling of Computer Systems, 1993, 268-269.]

22. E. Bach, Weil Bounds for Singular Curves, Applicable Algebra in Engineering, Communication, and Computing, 7 (1996), 289-298.

23. E. Bach, R. Mansharamani, and J. Strikwerda, Estimating Completion Time Ratios of a Fork-Join Barrier Synchronization, Performance Evaluation 26 (1996), 145-154.

24. E. Bach and R. Peralta, Asymptotic Semismoothness Probabilities, Mathematics of Computation 65 (1996), 1701-1715.

25. E. Bach and J. Sorenson, Explicit Bounds for Primes in Residue Classes, Mathematics of Computation 65 (1996), 1717-1735. [Abstract in Proceedings of AMS Symposia in Applied Mathematics (Mathematics of Computation Conference), v. 48, 1993, 535-539.]

26. E. Bach, R. Lukes, J. Shallit, and H. Williams, Results and Estimates on Pseudopowers, Mathematics of Computation 65 (1996) 1737-1747.

27. E. Bach, The Complexity of Number-Theoretic Constants, Information Processing Letters 62 (1997), 145-152.

28. E. Bach, Comments on Search Procedures for Primitive Roots, Mathematics of Computation 66 (1997), 1719-1727.

29. E. Bach, Energy Arguments in the Theory of Algorithms, American Mathematical Monthly 104 (1997), 831-837.

30. E. Bach, Moments in the Duration of Play, Statistics and Probability Letters 36 (1997), 1-7.

31. E. Bach, Efficient Prediction of Marsaglia-Zaman Random Number Generators, IEEE Transactions on Information Theory 44 (1998), 1253-1257.

32. E. Bach, Fugitives from the Law of Averages, UMAP Journal 19 (1998), 171-174.

33. E. Bach, A. Condon, E. Glaser, and C. Tanguay, DNA Models and Algorithms for NP-complete Problems, Journal of Computer and System Sciences 57 (1998), 172-186. [Preliminary version in Proc. 11th Annual IEEE Conf. on Computational Complexity, 1996, pp. 290-300.] **Invited to special issue of best papers from 1996 IEEE Complexity.**

34. E. Bach and K. Huber, Note on Square Roots Mod N. IEEE Transactions on Information Theory 45 (1999), 807-809.

35. E. Bach, Sheaf Cohomology is #P-hard, Journal of Symbolic Computation 27 (1999), 429-433.

36. E. Bach, J. Boyar, T. Jiang, K.S. Larsen, and G.-H. Lin, Better Bounds on the Accomodating Ratio for the Seat Reservation Problem, in Computing and Combinatorics (Proc. COCOON 2000), Springer-Verlag, 2000, pp. 223-231. [Full version: PP-2000-8, Department of Mathematics and Computer Science, University of Southern Denmark.]

37. E. Bach and M. Kiwi, Threshold Data Structures and Coding Theory, Theoretical Computer Science 235 (2000), 3-23. **Invited to special issue of papers from Blum Festschrift.**

38. A. Ambainis, E. Bach, A. Nayak, A. Vishwanath, and J. Watrous, One-dimensional Quantum Walks, Proc. 30th Annual ACM Symp. on Theory of Computing, pp. 37-49. ACM Press, 2001.

39. E. Bach, J. von zur Gathen, and H. W. Lenstra, Jr., Factoring Polynomials over Special Finite Fields, Finite Fields and Their Applications 7 (2001), 5-28.

40. E. Bach, Random Bisection and Evolutionary Walks, Journal of Applied Probability 38 (2001), 582-596.

41. J.-Y. Cai and E. Bach, On Testing for Zero Polynomials by a Set of Points with Bounded Precision, Theoretical Computer Science 296 (2003), 15-25. [Preliminary version in Computing and Combinatorics (Proc. COCOON 2001), Springer-Verlag, 2001, pp. 473-482.] **Invited to special issue of best papers from COCOON 2001.**

42. E. Bach, J. Boyar, L. Epstein, L. M. Favrholdt, T. Jiang, K. S. Larsen, G.-H. Lin, and R. van Stee, Tight Bounds on the Competitive Ratio on Accommodating Sequences for the Seat Reservation Problem, Journal of Scheduling 6 (2003), 131-147.

43. E. Bach, S. Coppersmith, M. Paz Goldschen, R. Joynt, and J. Watrous, One-dimensional Quantum Walks with Absorbing Boundaries, J. Computer and System Sciences 69 (2004), 562-592.

44. E. Bach, Bounds for the Expected Duration of the Monopolist Game, Information Processing Letters 101 (2007), 86-92.

45. E. Bach and N. C. Ryan, Efficient Verification of Tunnell's Criterion, Japan Journal of Industrial and Applied Mathematics 24 (2007), 229-239. **Invited to special issue on Algorithmic Number Theory.**

46. E. Bach, Sums over primes (**invited paper**), Proc. of Conference on Algorithmic Number Theory (ANT-2007), ed. A.-M. Ernvall-Hytonen, et al., General Publications No. 46, Turku Centre for Computer Science, 2007.

47. E. Bach and D. X. Charles, The Hardness of Computing an Eigenform, Contemporary Mathematics 463 (2008), 9-16. **Invited from AMS Special Session on Computational Arithmetic Geometry, 2006.**

48. G. Fusco and E. Bach, Phase Transition of Multivariate Polynomial Systems, Mathematical Structures in Computer Science 19 (2009), 9-23. [Preliminary version in Proc. 4th Annual Conference on Theory and Applications of Models of Computation, Shanghai, 2007, pp. 632-645.] **Invited to special issue of best papers from TAMC 2007.**

49. E. Bach, D. Klyve, and J. Sorenson, Computing Prime Harmonic Sums, Mathematics of Computation 78 (2009), 2283-2305.

50. L. Hellerstein, B. Rosell, E. Bach, S. Ray, D. Page, Exploiting Product Distributions to Identify Relevant Variables of Correlation Immune Functions, Journal of Machine Learning Research 10 (2009), 2374-2411.

51. E. Bach, Improved Asymptotic Formulas for Counting Correlation Immune Boolean Functions, SIAM Journal on Discrete Mathematics 23 (2009), 1525-1538.

52. E. Bach, Iterative Root Approximation Methods in p-adic Numerical Analysis, J. Complexity 25 (2009), 511-529.

53. E. Bach and J.-Y. Cai, A Novel Information Transmission Problem and its Optimal Solution, Communications in Information and Systems 9 (2009), 141-162. [Preliminary version: Proc. 16th International Symposium on Fundamentals of Computation Theory, Budapest, 2007, pp. 64-75.]

54. E. Bach, S. Chawla, and S. Umboh, Threshold Rules for On-Line Sample Selection, Discrete Mathematics, Algorithms and Applications 2 (2010), 625-642. [Preliminary version: Proc. 2010 Computing and Combinatorics (COCOON), Springer-Verlag Lecture Notes in Computer Science v. 6196, 2010, pp. 489-499.] **Invited to special issue of best papers from COCOON 2010.**

55. K. Rudinger, J.K. Gamble, M. Wellons, M. Friesen, E. Bach, R. Joynt, and S. Coppersmith, Noninteracting Multiparticle Quantum Random Walks Applied to the Graph Isomorphism Problem for Strongly Regular Graphs. Phys. Rev. A 85, 2012, 022334.

56. K. Rudinger, J. K. Gamble, E. Bach, M. Friesen, R. Joynt, and S. N. Coppersmith, Comparing Algorithms for Graph Isomorphism Using Discrete- and Continuous-time Quantum Random Walks, J. Comput. Theor. Nanoscience 10 (2013), 1653-1661.

57. E. Bach and J. Sorenson, Approximately Counting Semismooth Integers, Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation, ACM Press, 2013, pp. 23-30.

58. E. Bach and A. Bridy, On the Number of Distinct Functional Graphs of Affine-Linear Transformations over Finite Fields, Linear Algebra and its Applications 439 (2013), 1312-1320.

59. A. Frees, J. Gamble, K. Rudinger, E. Bach, M. Friesen, R. Joynt, and S. Coppersmith, Power-law scaling for the adiabatic algorithm for search-engine ranking, Phys. Rev. A 88 (2013), 032307.

60. D. Luchaup, L. De Carli, S. Jha, and E. Bach, Deep packet inspection with DFA-trees and parameterized language overapproximation, Proc. 2014 IEEE Conf. Computer Communications (INFOCOM), IEEE Press, 2014, pp. 531-539.

61. E. Bach and A. Shallue, Counting Composites with Exactly Two Strong Liars. Mathematics of Computation, to appear.

[Book Chapters, Encyclopedia Articles (all invited)]

62. E. Bach, Number-Theoretic Algorithms, Annual Review of Computer Science 4 (1990), 119-172.

63. E. Bach, Carmichael Numbers, in Encyclopaedia of Mathematics, Supplement I, ed. M. Hazewinkel, Kluwer, Dordrecht, 1997, p. 178.

64. E. Bach, Probabilistic Primality Tests, in Encyclopaedia of Mathematics Supplement Volume I, ed. M. Hazewinkel, Kluwer, Dordrecht, 1997, pp. 419-420.

65. E. Bach, Pseudoprimes, in Encyclopaedia of Mathematics Supplement Volume I, ed. M. Hazewinkel, Kluwer, Dordrecht, 1997, pp. 421-422.

[Technical Reports (not appearing elsewhere)]

66. E. Bach, Discrete Logarithms and Factoring, University of California at Berkeley Computer Science Division, Report UCB/CSD/84/186, 1984.

67. E. Bach, Matching Modulo Divisors, and a Simple $N^{1/4}$ Factoring Algorithm, University of California at Berkeley Computer Science Division, Report UCB/CSD/84/187, 1984.

68. E. Bach and J. Shallit, A Class of Functions Equivalent to Factoring, University of Chicago Computer Science Department, Report 84-008, 1984.

69. E. Bach and J. von zur Gathen, Deterministic Factorization of Polynomials over Special Finite Fields, University of Wisconsin Computer Sciences Department Report #799, 1988.

70. E. Bach, Carmichael Functions, University of Wisconsin Computer Sciences Department Report #939, 1990.

71. E. Bach, M. Giesbrecht, and J. McInnes, The Complexity of Number Theoretic Problems, ITRC Lecture Series, Technical Report 247/91, University of Toronto, 1991.

72. E. Bach, Algorithmic Number Theory, ICR Distinguished Visitor Series, University of Waterloo, 1991.

73. E. Bach, J. Boyar, and K. S. Larsen, The Accomodating Ratio for the Seat Reservation Problem, Institut for Matematik og Datalogi, Odense University, Preprint No. 25, 1997.

[In Preparation]

74. E. Bach and L. Borisov, Absorption Probabilities for the Two-Barrier Quantum Walk. Quantum Information and Computation, submitted.

75. E. Bach, S. Barman, and S. Umboh, Computational Aspects of Non-Uniform Coupon Collection. In preparation. Plan to submit to SIAM Review.

76. E. Bach, Permutation sensitive signatures. In preparation, to be submitted to IEEE Trans. Information Theory.

77. E. Bach, Lectures on Algorithmic Number Theory.

78. E. Bach, Exact Formulas for an Urn Model Related to Chained Hashing.

79. E. Bach, Asynchronous Combination and the Branching Random Walk.

GRANTS

[PI or co-PI]

NSF, Computational Number Theory, $81,022, 1985-88.

NSF, Presidential Young Investigator Award, $235,311, 1986-1991.

WARF, Support for Shallit/Lubiw Sabbatical Visit, $5,750, 1989.

NSF, Algorithms in Number Theory, $195,813, 1992-1995.

NSERC Canada, Foreign Researcher Award, $6800, 1995.

NSF, Algorithmic Number Theory, $232,948, 1996-2000.

Department of Education, Graduate Assistance in Areas of National Need (MaCE Program), $458,457 (includes 25% matching from UW Graduate School), 1997-2002.

University of Waterloo, ORCCA Visiting Research Chair, $3000, 2003.

NSF, Algorithmic Number Theory, $290,127, 2000-2005.

AT&T Foundation, Public Key Infrastructure Laboratory, $200,000, 2001-2003. (Co-PI.)

NSF, Connecting the Quantum Dots: Theory of Quantum Computing in a Solid-State Implementation, $499,939, 2001-2005. (Co-PI.)

WARF, Aspects of Algorithmic Number Theory, $19,593, 2004-2005.

NSF, Quantum Algorithms for NP-Intermediate Problems, $300,000, 2005-2009. (Co-PI.)

WARF, Vilas Associate Award, $86,000, 2006-2008.

NSF, Aspects of Algorithmic Number Theory, $330,072, 2007-2012.

ARO, Quantum Algorithms Based on Physical Processes, $510,000, 2009-2013. (Co-PI.)

WARF, Problems in Algorithmic Number Theory, $34,635, 2013-2014.

NSF, Algorithmic Number Theory, $450,000, 2014-2017.

[Major Participant]

NSF, Workshop on Algorithmic Number Theory, $28,920, 1992. (PI was Rudy Najar, Cal State – Fresno.)

NSF, Traineeships in Mathematics and Computation in Engineering (MaCE), $444,000, 1993-1998. (I served as MaCE Director 1996-1998. PI was Tom Kurtz.)

NSF, Internships in Probability and Stochastic Processes, $259,017, 1998-2000. (Organized one of three summer programs. PI was Tom Kurtz.)

NSF, Vertical Integration of Research and Education, $2,782,000, 1999-2004. (One of six Steering Committee members. PI was Richard Brualdi.)

[Participating Faculty Member]

NSF, TOPAZ – A Laboratory for Research in Parallel Computing, $3,400,000, 1986-1991. (PI was David DeWitt.)

NSF, PRISM: A Laboratory for Research in Future High-Performance Parallel Computing, $1,985,000 (with $900,000 matching funds from UW-Madison), 1991-1996. (PI was Mary Vernon.)

NSF, Research Training Grant: Algebraic Geometry and Number Theory at UW, $ 1,629,274, 2009-2014. (PIs are Jordan Ellenberg and Ken Ono.)

STUDENTS ADVISED

[PhD]

Victor Shoup, Removing Randomness from Computational Number Theory, 1989.

Marty Wolf, Limited Nondeterminism in Parallel Models of Computation, 1990.

Jonathan Sorenson, Algorithms in Number Theory, 1991

João Meidanis (co-advised with D. Joseph), Algorithms for Problems in Computational Genetics, 1992.

Walter Ludwig, Algorithms for Scheduling Malleable and Nonmalleable Parallel Tasks, 1995.

Scott Lindhurst, Computing Roots in Finite Fields and Groups, with a Jaunt Through Sums of Digits, 1997.

John Watrous, Space-bounded Quantum Computation, 1998.

Denis Charles, Computational Aspects of Modular Forms and Elliptic Curves, 2005. **Won Outstanding Graduate Research Award, UW CS Dept.**

Andrew Shallue, Two Number-Theoretic Problems that Illustrate the Power and Limitations of Randomness, 2007.

Andrew Bridy, in progress.

[MS]

Kim-Ee Yeoh, 1999.

Mark Ward, 2003.

Jang-Woo Park, 2003.

Diwakar Ramachandran, 2004.

[BS]

Jason Franklin, 2003.

Yael Peled, 2003.

MAJOR INVITED LECTURES

[Short Courses and Distinguished Lecture Series]

Algorithms in Number Theory, ITRC Lecture Series, University of Toronto, June 1988.

Algorithmic Number Theory, ICR Distingished Visitor Lectures, University of Waterloo, July 1991.

NSF Faculty Enhancement Workshop on Algorithmic Number Theory (10 lectures). California State University – Fresno, June 1992.

Mini-Course on Algorithmic Number Theory (l0 Lectures) Universidad de Chile, Santiago, December 1997 - January 1998.

Five Lectures on Algorithmic Number Theory, Rocky Mountain Mathematics Consortium Summer Institute on Number Theory and Cryptography, Laramie, June 2006.

[Plenary Lectures at Conferences]

Intractable Problems in Number Theory, IACR CRYPTO Conference, Santa Barbara, August 1988.

Using Deterministic Sequences in Randomized Algorithms, AMS Summer Meeting on Computational Number Theory, Bowdoin, July 1988.

The State of the Art in Algorithmic Number Theory, Opening Address at Center for Cryptography, Computer, and Network Security, UW-Milwaukee, November 1996.

The Algorithmic Approach to the Theory of Numbers, Jornadas de Matemáticas, Caracas, Venezuela, March 1999.

Is the Riemann Hypothesis Necessary?, Plenary Lecture at Symposium on Number Theory in Memory of Kustaa Inkeri, Turku, Finland, June 1999.

p-adic Numerical Analysis, Plenary Lecture at Conference on the Mathematics of Public-Key Cryptography, Toronto, June 1999.

Random Bisection and its Applications, Two Plenary Lectures at Com2MAC Conference on Cryptography, Pohang Inst. Sci. Tech., Korea, July 2000.

The Random Bisection Model and its Applications, Presidential Invited Address at 2002 Meeting of the Classification Society of North America, Madison, June 2002.

Sums over Primes, Main Lecture at Conference on Algorithmic Number Theory (ANT 2007), Turku, Finland, May 2007.

Two Lectures on Cryptography: A Mathematical Prologue to the Study of Electronic Encryption and Exemplary Designs from the Golden Age of Shift Register Cryptography, NTACC, Warsaw, October 2010.

[Other Invited Talks at Meetings]

Factoring With Cyclotomic Polynomials, AMS Special Session on Mathematical Computer Science, Chicago, March 1985.

Some Polynomials Associated with Pollard's Rho Method, Mathematisches Forschungsinstitut Oberwolfach, May 1988.

Deterministic Factorization of Polynomials over Special Finite Fields, 850th meeting of the AMS, Boulder, August 1989.

Statistical Evidence for Small Generating Sets. Mathematisches Forschungsinstitut Oberwolfach, November 1992.

Improved Approximations for Euler Products, 1994 Canadian Number Theory Conference, Halifax, July 1994.

Threshold Data Structures and Coding Theory, Conference on Theoretical Computer Science in Honour of Manuel Blum's 60th Birthday, City University of Hong Kong, April 1998.

p-adic Secant Algorithms, Invited talk at DIMACS Workshop on Unusual Applications of Number Theory, January 2000.

Travels Beyond Arithmetic, Conference in Honour of Hugh Williams's 60th Birthday, Banff, July 2003.

Permutation-Sensitive Signatures, AMS Sectional Meeting, Bloomington, April 2003.

Computing Prime Harmonic Sums, AMS Sectional Meeting, Notre Dame, May 2006.

Correlation Immunity: What, Why, and How Often? 40th Birthday Conference, Department of Combinatorics and Optimization, University of Waterloo, June 2007.

Reductions Among Number-Theoretic Problems, Festschrift for Joachim von zur Gathen's 60th Birthday, Bonn, May 2010.

Probability, Number Theory, and Computation, Workshop on Mathematical Aspects of P versus NP and Variants, Brown University, August 2011.

Counting Affine Maps, Workshop on The Art of Iterating Rational Functions over Finite Fields, Banff, May 2013.

OTHER PUBLIC LECTURES

Computers, Number Theory, and Secret Codes. Beloit College (1985); Valparasio U. (1992); Butler U. (1993).

How to Generate Factored Random Numbers. U. Toronto (1983); IBM San Jose (1983); MIT (1984); Kent State U. (1985).

Toward a Theory of Pollard's Rho-Method. U. California, Berkeley (1987); U. Washington (1987); INRIA, Paris (1989).

Sieve Algorithms for Perfect Power Testing. U. Paris-Sud, Orsay (1989).

Deterministic Factorization of Polynomials over Special Finite Fields. École Normale Supèrieure, Paris (1989).

Realistic Analysis of Some Randomized Algorithms. U. Chicago (1986); U. Southern California (1986); U. Wisconsin – Milwaukee (1989); Howard University (1991).

Probabilistic Ideas in Number Theory. U. Waterloo (1992); Beloit College (1992).

Comments on an Evolution Model of Richard Dawkins. Valparasio U. (1992); U. Waterloo (1992); U. Wisconsin – Milwaukee (1993); Northwestern U. (1994).

Statistical Evidence for Small Generating Sets. ICSI, Berkeley (1992); Princeton (1992).

Average-case Analysis of Algorithms for Linear Algebra mod N. U. Saarbrücken (1992); U. Manitoba (1997).

Search Procedures for Primitive Roots, U. Waterloo (1995).

Heuristic Models in Algorithmic Number Theory, Carnegie-Mellon U. (1996); Bell Laboratories (1997); U. Chile (1998); Montreal Math. Colloquium (1998).

Threshold Data Structures and Algebraic Coding Theory, U. Chile (1997); Georgia Tech (1999).

The Extended Riemann Hypothesis and its Algorithmic Applications. U. Illinois (2003).

Combinatorial Analysis of Quantum Random Walks. Beloit College (2002); U. Illinois (2002); U. Waterloo (2003); U. Aarhus (2005).

Permutation-Sensitive Signatures. U. Waterloo (2003).

PROFESSIONAL ACTIVITES

[Editorial Boards]

Journal of Algorithms, 1994-2004.

ACM Transactions on Algorithms, 2005-2008.

Computational Complexity, 1991-2013.

Chicago Journal of Theoretical Computer Science, 1994-present.

[Organizer or Program Chair]

Special Session on Number Theory and Cryptography, Milwaukee AMS Meeting, 1997.

Research and Education Institute, DIMACS, 1997.

Probability Intern Program, UW-Madison, 1998.

Special Session on Number Theory and Cryptography, Notre Dame AMS Meeting, April 2000.

Special Session on Cryptography and Number Theory, Columbus AMS Meeting, October 2001.

[Program Committee Member]

1988 IACR CRYPTO Conference.

1989 IEEE Symposium on Foundations of Computer Science (FOCS).

1994 ACM Symposium on Theory of Computing (STOC).

1994 Symposium on Algorithmic Number Theory (ANTS).

1997 ACM-SIAM Symposium on Discrete Algorithms (SODA).

1998 Algorithmic Number Theory Symposium (ANTS-III).

2000 MSRI Workshop on Cryptography, Berkeley.

2004 Algorithmic Number Theory Symposium (ANTS-VI)

2007 Conference on Theory and Applications of Models of Computation (TAMC).

[Other Service Activities]

AIM Working Group on Computational Opportunities in Algebra, Number Theory, and Combinatorics, NSF, 2002.

Panelist, NSF Minority Graduate Fellowships (1990-92), NSF Proposal Reviews (2000, 2005, 2013, 2014).

External Examiner for Hamilton College (Senior Fellowship Thesis, 1999); Aarhus University (PhD, 2005); Lahore University of Education (PhD, 2009).

Reviewer for Mathematical Reviews.

Proposal referee for National Science Foundation (USA), National Security Agency (USA), National Science and Engineering Research Council (Canada), Fields Institute (Canada), Australian Research Council, Fondo Nacional de Desarrollo Cientifico y Tecnologico (Chile).

Journal paper referee for: Acta Arithmetica, ACM Transactions on Algorithms, ACM Transactions on Mathematical Software, ACM Crossroads, Algorithmica, American Mathematical Monthly, Computers and Mathematics with Applications, Computing Surveys, Computational Complexity, Designs, Codes, and Cryptography, Electronic Journal on Combinatorics, Finite Fields and Applications, 4OR, Houston Journal of Mathematics, IEEE Transactions on Computers, IEEE Transactions on Information Theory, IEEE Transactions on Parallel and Distributed Processing, Information and Computation, Information Processing Letters, International Journal of Number Theory, Journal of the ACM, Journal of Algorithms, Journal of Combinatorics and Number Theory, Journal of Computer and System Sciences, Journal of Cryptology, Journal of Integer Sequences, Journal of Mathematical Cryptology, Journal of Symbolic Logic, Journal de la Thèorie des Nombres (Bordeaux), Mathematics of Computation, New Zealand Journal of Mathematics, Parallel Processing Letters, Parallel Computing, Proceedings of the AMS, SIAM Journal on Computing, SIAM Journal on Discrete Mathematics, Software Practice and Experience, Statistics and Probability Letters, Theoretical Computer Science, Undergraduate Mathematics and Applications.

Paper reviewer for many conferences, including STOC, FOCS, SODA, ICALP, ISSAC, etc.

Event Coordinator, 2014 Badger Invitational Science Olympiad.

Member of American Mathematical Society, ACM Special Interest Groups on Automata and Computability Theory and on Symbolic and Algebraic Manipulation, Mathematics Association of America.

COURSES TAUGHT

[Graduate]

Topics in Computational Number Theory and Cryptography

Topics in Theoretical Computer Science: Computational Learning Theory

Topics in Theoretical Computer Science: Parallel Algorithms
Arithmetic Algorithms
Mathematical Techniques for the Analysis of Algorithms
Advanced Algorithms and Data Structures
Abstract and Concrete Complexity Theory

[Undergraduate]
A Physical Introduction to Computer Science
Introduction to Cryptography
Introduction to Algorithms
Models of Computation
Numerical Methods
Problem Solving Using Computers
Data Structures
Discrete Mathematics

TECHNICAL INTERESTS

I am primarily interested in the computational complexity of number-theoretic problems, especially primality testing and factoring. My other interests include cryptography, quantum computing, analysis of algorithms and discrete probability theory, complexity theory, and six-string automata.