VITA
Mikhail (Mike) J. Atallah

GENERAL INFORMATION

Contact Information

Mail: Purdue University, Department of Computer Science,
305 N. University Street, West Lafayette, IN 47907-2107
Phone: (765) 463-7310
Fax: 765-494-0739
Email: matallah@purdue.edu
Home Page: http://www.cs.purdue.edu/people/mja

Personal Data

Married, two children
U.S. Citizen (naturalized in 1984)

Education and Academic Career

2004–present	Distinguished Professor of Computer Science, Purdue Univ.
2003–present	Professor (courtesy) of Electr. and Comp. Eng., Purdue Univ.
1989–04	Professor of Computer Science, Purdue Univ.
1986–89	Associate Professor of Computer Science, Purdue Univ.
1982–86	Assistant Professor of Computer Science, Purdue Univ.
1982	Ph.D. in Electr. Eng. and Comp. Sci., Johns Hopkins Univ., Advisor: S. Rao Kosaraju (completed in 4 semesters, GPA = 4.0)
1980	M.S. in Electr. Eng. and Comp. Sci., Johns Hopkins Univ. (completed in 2 semesters, GPA = 4.0)
1975	B.E. in Electrical Engineering, American University in Beirut (after which I worked in industry until I went to graduate school in 1979)

Industry Experience

2007–9	Chief Technology Officer, Arxan Technologies Inc. Company was acquired in 2013 by private equity firm TA Associates: www.crunchbase.com/organization/arxan-technologies
2007–10	Chief Scientist, Arxan Defense Systems Inc. Company was acquired in 2010 by Microsemi Corporation: www.crunchbase.com/organization/arxan-defense-systems
2001–present	Technical Advisory Board, Arxan Technologies Inc.
2001	Co-Founder, Arxan Technologies Inc.
1988 (1 month)	Visiting Scientist, NASA Ames Research Center (RIACS Institute, Center for Advanced Architectures)
1975–78	Engineer, Siemens (1975–76), Wang (1977–78)

Academic Administration

2007–10	Associate Head	Computer Science, Purdue Univ.
2001–17	Associate Director	CERIAS, Purdue Univ. (Center for Education and Research in Information Assurance and Security)
1994–96	Associate Head	Computer Science, Purdue Univ.

Research Interests

Main current interest: Information security (protocols, watermarking, software security)
Other interests: Algorithms, parallel computation, computational geometry

PROFESSIONAL RECOGNITION

Awards, Honors

- Fellow of the ACM (2006)
- Fellow of the IEEE (1997) Life Fellow of the IEEE (2018)
- Presidential Young Investigator Award (1985)
  from then-President Ronald Reagan; awardee selections were made by the National Science Foundation (the PYI awards eventually morphed, in a much-expanded form, into the current CAREER awards)
- CCS Test of Time Award (2015)
  an award started in 2012 and given to particularly influential papers that appeared in CCS ten years earlier; CCS – www.sigsac.org/ccs.html – is one of the two "flagship" conferences in information security
- Arden L. Bement, Jr. Award (2017)
  the most prestigious award Purdue University bestows in pure and applied science and engineering
- Purdue Outstanding Commercialization Award (2013)
  for the technology that is the core of the products of Arxan Technologies Inc., that was developed jointly with my former doctoral student Hoi Chang; Arxan was co-founded by Hoi and myself and other Purdue colleagues and entrepreneurs, and was acquired in 2013 by Boston private equity firm TA Associates. Arxan Defense Systems Inc. used the technology for defense-related applications, and was acquired in 2010 by Microsemi Corporation.
- Purdue Sigma Xi Faculty Research Award (2016)
- Distinguished Alumnus Award, Faculty of Engineering, American University in Beirut (2007)
- Purdue College of Science Graduate Student Mentoring Award (2015)

- Selected (in 1999) as one of the best teachers in the history of Purdue University and included in Purdue's Book of Great Teachers, a permanent wall display of 200 (in 1999) Purdue teachers past and present – see

  `https://www.purdue.edu/provost/faculty/greatteachers.html`

- Selected (in 2004) as Fellow of the Purdue Teaching Academy. Approximately 6% of Purdue faculty have the rank of Fellow in the Teaching Academy. For more details see `http://www.teachingacademy.purdue.edu/`

- Selected as the Outstanding Teacher of the College of Science for 2004. Selected among the Top Ten Outstanding Teachers for the College of Science in 1994, 1995, 2006, 2007.

- Purdue ACM Outstanding CS Instructor Award (4 times)

Talks Given in Distinguished Lecture Series at Universities

2008 Univ. of Minnesota
(Distinguished Lecture Series)

2006 Northwestern Univ.
(Distinguished Lecture Series)

2006 Colorado State Univ.
(ISTeC Distinguished Lecture Series)

2003 Iowa State Univ.
(Distinguished Lecture Series)

2001 Ohio State Univ.
(Distinguished Lecture Series)

2001 Northwestern Univ.
(Distinguished Lecture Series)

1995 Univ. of Florida
(Barr Systems Distinguished Lecture Series)

1992 Johns Hopkins Univ.
(IBM Distinguished Lecture Series)

1988 Univ. of Virginia
(Distinguished Lecture Series)

Conference Talks Given as Keynote or Invited Speaker

2013 Workshop on Cloud Computing Security, Doha, Qatar
(Keynote Speaker)

2011 9th Annual Conference on Privacy, Security and Trust (PST '11), Montreal, Canada
(Keynote Speaker)

2011 KAUST Workshop on Hot trends in Computer Science, Saudi Arabia
(Invited Speaker)

2010 4th International Frontiers of Algorithmics Workshop (FAW '10), Wuhan, China
(One of three Invited Speakers)

2008 First International Workshop on Remote Entrusting (RE-TRUST '08), Trento, Italy
(Keynote Speaker)

2008 Workshop on Computer Privacy in Electronic Commerce, Montreal, Canada
(Invited Speaker)

2006 12th Annual International Computing and Combinatorics Conference (COCOON '06), Taipei, Taiwan
(Keynote Speaker)

2005 12th Annual IEEE/ACM International Conference on High Performance Computing (HiPC '05), Goa, India
(Keynote Speaker)

2005 Privacy Place Spring Workshop, Raleigh, NC
(Keynote Speaker)

2005 3rd Australasian Information Security Workshop (AISW '05), Newcastle, Australia
(Invited Speaker)

2005 10th Panhellenic Conference on Informatics (PCI '05), Volos, Greece
(Invited Speaker)

2004 2d International Conference on Advanced Technologies for Homeland Security, Storrs, CT
(Invited Speaker)

2002 National Cybercrime Conference, Chicago
(Invited Panelist)

2002 Indiana Venture Club, Indianapolis
(Keynote Speaker)

2002 Indiana Executive Forum, Indianapolis
(Invited Speaker)

2001 Workshop on Algorithms and Data Structures (WADS '01), Providence
(One of three Plenary Speakers)

1996 7th Workshop on Parallel Algorithms, Philadelphia
(Invited Speaker)

1996 7th International Symposium on Algorithms and Computation (ISAAC '96), Osaka, Japan
(One of two Invited Speakers)

1996 Summer Institute on Computational Geometry, Academia Sinica, Taiwan
(One of five Main Lecturers)

1996 IBM Tokyo Research Laboratory Workshop, Tokyo
(One of six Invited Speakers)

1994 TIMS XXXII International Meeting, Anchorage
(Invited Speaker)

1994 Algorithm Theory Day, Carleton Univ., Ottawa
(Invited Speaker)

1994 7th Int. Conference on Parallel and Distributed Computing Systems, Las Vegas
(Keynote Speaker)

1993 Workshop on Algorithms and Data Structures (WADS '93), Montreal
(Invited Speaker)

1993 DIMACS Workshop on Parallel Algorithms: From Solving Combinatorial Problems to Solving Grand Challenge Problems, Piscataway, NJ
(Invited Speaker)

1992 Leonardo Fibonacci Institute for Foundations of Computer Sci., Trento, Italy
(One of three Main Lecturers)

1992 4th Symp. on the Frontiers of Massively Parallel Computation (FRONTIERS '02), McLean
(Invited Panelist)

1991 2d Workshop on Parallel Algorithms, New Orleans
(Invited Speaker)

1989 Workshop on Algorithms and Data Structures (WADS '89), Ottawa
(Invited Speaker)

1987 IMA Workshop on Applications of Combinatorics and Graph Theory to VLSI, Minneapolis
(Invited Speaker)

1987 Computational Geometry Day at Courant Institute / New York Univ.
(Invited Speaker)

Journal Editorial Boards

- *IEEE Software* Guest co-Editor for Special Issue on Software Protection (2010–11)
- *Int. J. of Cyber Criminology* (2006–)
- *IEEE Trans. on Computers* (2003–07)
- *SIAM J. on Computing* (1988–98)
- *J. of Parallel and Distributed Computing* (1993–10)
- *Information Processing Letters* (1989–95)
- *Parallel Processing Letters* (1991–97)
- *Computational Geometry: Theory & Applications* (1990–2000)
- *Int. J. on Computational Geometry & Applications* (1990–2008)
- *Int. J. of Foundations of Computer Science* (1999–2006)
- *Methods of Logic in Computer Science* (1990–96)
- *Algorithmica* Guest Editor for a Special Issue on Computational Geometry (1990–91)

Journal Advisory Boards

- *Int. J. on Computational Geometry & Applications* (2008–)

Conference Committees

1. Member of Program Committee, *19th European Symposium on Research in Computer Security (ESORICS)* (2014, Wroclaw, Poland)
2. Member of Program Committee, *35th IEEE Symposium on Security and Privacy (S&P)* (2014, San Jose, California)
3. Co-Chair of Program Committee, *IEEE 22nd International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS)* (2014, Paris, France)
4. Member of Program Committee, *1st Workshop on LOng term Preservation for big Scientific data (LOPS)* (2014, Chicago, Illinois)
5. Member of Program Committee, *22nd ACM Conference on Computer and Communications Security (CCS)* (2013, Berlin, Germany)
6. Member of Program Committee, *17th European Symposium on Research in Computer Security (ESORICS)* (2012, Pisa, Italy)
7. Member of Program Committee, *16th International Conference on Financial Cryptography and Data Security* (2012, Bonaire, Netherlands Antilles)
8. Member of Program Committee, *30th ACM Symposium on Principles of Database Systems (PODS)* (2012, Tucson, Arizona)
9. Member of Program Committee, *16th European Symposium on Research in Computer Security (ESORICS)* (2011, Leuven, Belgium)
10. Member of Program Committee, *22nd Annual Symposium on Combinatorial Pattern Matching (CPM)* (2011, Palermo, Italy)
11. Member of Program Committee, *18th Annual Workshop on Selected Areas in Cryptography (SAC)* (2011, Toronto, Canada)
12. Member of Program Committee, *31st International Conference on Distributed Computing Systems (ICDCS)* (2011, Minneapolis, Minnesota)
13. Member of Program Committee, *10th ACM Workshop on Privacy in the Electronic Society (WPES)* (2011, Chicago, Illinois)
14. Member of Program Committee, *18th Annual IEEE/ACM International Conference on High Performance Computing (HiPC)* (2011, Bangalore, India)

15. Program Committee Co-Chair, *5th International Frontiers of Algorithmics Workshop (FAW)* (2011, Jinhua, China)

16. Member of Program Committee, *Web Intelligence for Information Security (WIISe)* (2011, Lyon, France)

17. Member of Program Committee, *13th International Conference on Information and Communication Security (ICICS)* (2011, Beijing, China)

18. Member of Program Committee, *36th International Conference on Very Large Databases (VLDB)* (2010, Singapore)

19. Member of Program Committee, *29th ACM Symposium on Principles of Database Systems (PODS)* (2010, Indianapolis, Indiana)

20. Member of Program Committee, *30th International Conference on Distributed Computing Systems (ICDCS)* (2010, Genoa, Italy)

21. Co-Chair of Program Committee, *10th Privacy Enhancing Technologies Symposium (PETS)* (2010, Berlin, Germany)

22. Member of Program Committee, *15th ACM Symposium on Access Control Models and Technologies (SACMAT)* (2010, Pittsburgh)

23. Member of Program Committee, *9th ACM Workshop on Privacy in the Electronic Society (WPES)* (2010, Chicago, Illinois)

24. Member of Program Committee, *17th Annual IEEE/ACM International Conference on High Performance Computing (HiPC)* (2010, Goa, India)

25. Member of Program Committee, *17th String Processing and Information Retrieval Symposium (SPIRE)* (2010, Los Cabos, Mexico)

26. Member of Program Committee, *16th Annual International Computing and Combinatorics Conference (COCOON)* (2010, Nha Trang, Vietnam)

27. Member of Program Committee, *12th International Conference on Information and Communications Security (ICICS)* (2010, Barcelona, Spain)

28. Member of Program Committee, *4th Annual International Conference on Combinatorial Optimization and Applications (COCOA)* (2010, Hawaii)

29. Member of Program Committee, *4th International Conference on Mathematical Methods, Models and Architectures for Computer Networks Security (MMMACNS)* (2010, St. Petersburg, Russia)

30. Member of Program Committee, *14th European Symposium on Research in Computer Security (ESORICS)* (2009, Saint Malo, France)

31. Co-Chair of Program Committee, *9th Privacy Enhancing Technologies Symposium (PETS)* (2009, Seattle, Washington)

32. Member of Program Committee, *29th International Conference on Distributed Computing Systems (ICDCS)* (2009, Montreal, Quebec)

33. Member of Program Committee, *4th ACM Symposium on Information, Computer and Communication Security (AsiaCCS)* (2009, Sydney, Australia)

34. Member of Program Committee, *16th Annual Workshop on Selected Areas in Cryptography (SAC)* (2009, Calgary, Canada)

35. Member of Program Committee, *14th ACM Symposium on Access Control Models and Technologies (SACMAT)* (2009, Stresa, Italy)

36. Member of Program Committee, *16th Annual IEEE/ACM International Conference on High Performance Computing (HiPC)* (2009, Cochin, India)

37. Member of Program Committee, *3d International Frontiers of Algorithmics Workshop (FAW)* (2009, Hefei, China)

38. Member of Program Committee, *15th Annual International Computing and Combinatorics Conference (COCOON)* (2009, Niagara Falls)

39. Member of Program Committee, *5th International Workshop on Security and Trust Management (STM)* (2009, Saint Malo, France)

40. Member of Program Committee, *2d International Workshop on Remote Entrusting (Re-Trust)* (2009, Riva del Garda, Italy)

41. Member of Program Committee, *11th International Conference on Information and Communications Security (ICICS)* (2009, Beijing, China)

42. Member of Program Committee, *7th Annual Conference on Privacy, Security and Trust (PST)* (2009, Saint John, New Brunswick, Canada)

43. Member of Program Committee, *15th ACM Conference on Computer and Communications Security (CCS)* (2008, Alexandria, Virginia)

44. Member of Program Committee, *8th Privacy Enhancing Technologies Symposium (PETS)* (2008, Leuven, Belgium)

45. Member of Program Committee, *13th ACM Symposium on Access Control Models and Technologies (SACMAT)* (2008, Estes Park, Colorado)

46. Member of Program Committee, *15th Symposium on String Processing and Information Retrieval (SPIRE)* (2008, Melbourne, Australia)

47. Member of Program Committee, *11th Annual Information Security Conference (ISC)* (2008, Taipei, Taiwan)

48. Member of Program Committee, *10th International Conference on Information and Communications Security (ICICS)* (2008, Birmingham, United Kingdom)

49. Member of Program Committee, *6th Annual Conference on Privacy, Security and Trust (PST)* (2008, Delta Fredericton Fredericton, New Brunswick, Canada)

50. Member of Program Committee, *2d International Frontiers of Algorithmics Workshop (FAW)* (2008, Changsha, China)

51. Member of Program Committee, *3d International Workshop on Dependability Aspects on Data Warehousing and Mining Applications (DAWAM)* (2008, Barcelona, Spain)

52. Member of Program Committee, *6th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA)* (2008, Doha, Qatar)

53. Member of Program Committee, *14th ACM Conference on Computer and Communications Security (CCS)* (2007, Alexandria, Virginia)

54. Member of Program Committee, *27th International Conference on Distributed Computing Systems (ICDCS)* (2007, Toronto, Canada)

55. Member of Program Committee, *7th ACM Digital Rights Management Workshop (ACM-DRM)* (2007, Alexandria, Virginia)

56. Member of Program Committee, *7th Privacy Enhancing Technologies Workshop (PET)* (2007, Ottawa, Canada)

57. Member of Program Committee, *10th Information Security Conference (ISC)* (2007, Valparaiso, Chile)

58. Member of Program Committee, *21st Annual International Parallel and Distributed Processing Symposium (IPDPS)* (2007, Long Beach, California)

59. Member of Program Committee, *10th Workshop on Algorithms and Data Structures (WADS)* (2007, Halifax, Canada)

60. Member of Program Committee, *9th International Conference on Information and Communications Security (ICICS)* (2007, ZhengZhou, China)

61. Member of Program Committee, *2d International Workshop on Dependability Aspects on Data WArehousing and Mining Applications (DAWAM)* (2007, Vienna, Austria)

62. Member of Program Committee, *25th ACM Symposium on Principles of Database Systems (PODS)* (2006, Chicago, Illinois)

63. Member of Program Committee, *5th ACM Workshop on Privacy in the Electronic Society (WPES)* (2006, Washington, DC)

64. Member of Program Committee, *6th Privacy Enhancing Technologies Workshop (PET)* (2006, Cambridge, U.K.)

65. Member of Program Committee, *11th ACM Symposium on Access Control Models and Technologies (SACMAT)* (2006, Lake tahoe, California)

66. Vice-Chair of Program Committee, *20th Annual International Parallel and Distributed Processing Symposium (IPDPS)* (2006, Rhodes, Greece)

67. Member of Program Committee, *17th Annual International Symposium on Algorithms and Computation (ISAAC)* (2006, Kolkata, India)

68. Member of Program Committee, *13th Annual IEEE/ACM International Conference on High Performance Computing (HiPC)* (2006, Bangalore, India)

69. Member of Program Committee, *8th International Conference on Information and Communications Security (ICICS)* (2006, Raleigh, NC)

70. Member of Program Committee, *1st ACM Workshop on Multimedia Content Protection and Security (MCPS)* (2006, Santa Barbara, CA)

71. Chair of Algorithms and Bioinformatics Track Program Committee, *4th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA)* (2006, Dubai, U.A.E.)

72. Member of Program Committee, *25th Foundations of Software Technology and Theoretical Computer Science (FSTTCS)* (2005, Hyderabad, India)

73. Member of Program Committee, *10th ACM Symposium on Access Control Models and Technologies (SACMAT)* (2005, Stockholm, Sweden)

74. Member of Program Committee, *14th International World Wide Web Conference (WWW)* (2005, Chiba, Japan)

75. Member of Program Committee, *3rd Australasian Information Security Workshop (AISW)* (2005, Newcastle, Australia)

76. Member of Program Committee, *3rd IEEE Conference on E-Commerce Technology (CEC)* (2005, Munich, Germany)

77. Member of Program Committee, *IEEE International Conference on Information Technology: Coding and Compression Track (ITCC)* (2005, Las Vegas, Nevada)

78. Member of Program Committee, *10th Panhellenic Conference on Informatics (PCI)* (2005, Volos, Greece)

79. Member of Program Committee, *4th ACM Workshop on Digital Rights Management (DRM)* (2004, Washington, DC)

80. Member of Program Committee, *9th ACM Symposium on Access Control Models and Technologies (SACMAT)* (2004, Yorktown Heights, New York)

81. Member of Program Committee, *2d IEEE Conference on E-Commerce Technology (CEC)* (2004, San Diego, California)

82. Member of Program Committee, *11th Annual IEEE/ACM International Conference on High Performance Computing (HiPC)* (2004, Bangalore, India)

83. Vice-Chair for Network Security, *International Conference on Parallel Processing (ICPP)* (2003, Kaohsiung, Taiwan)

84. Member of Program Committee, *10th Annual IEEE/ACM International Conference on High Performance Computing (HiPC)* (2003, Bangalore, India)

85. Member of Program Committee, *3rd IEEE/IPSJ Symposium on Applications and the Internet* (2003, Orlando, Florida)

86. Member of Program Committee, *8th Annual International Computing and Combinatorics Conference (COCOON)* (2002, Singapore)

87. Member of Program Committee, *Watermarking '2002* (2002, Paris, France)

88. Program Chair, *13th IEEE International Parallel Processing Symposium (IPPS)* (1999, San Juan, Puerto Rico)

89. Member of Program Committee, *12th Annual International Conference on Parallel and Distributed Computing and Systems (IPDCS)* (1999, Fort Lauderdale)

90. Vice-Chair of Program Committee, *5th Annual IEEE/ACM International Conference on High Performance Computing (HiPC)* (1998, India)

91. Member of Program Committee, *11th Annual IEEE International Parallel Processing Symposium (IPPS)* (1997, Geneva, Switzerland)

92. Member of Program Committee, *4th Annual International Workshop on Parallel Algorithms for Irregularly Structured Problems* (1997, Paderborn, Germany)

93. Member of Program Committee, *4th Annual IEEE/ACM International Conference on High Performance Computing (HiPC)* (1997, Bangalore, India)

94. Vice-Chair of Program Committee, *10th Annual IEEE International Parallel Processing Symposium (IPPS)* (1996, Hawaii)

95. Member of Program Committee, *8th Annual IEEE Symp. on Parallel and Distributed Processing (SPDP)* (1996, New Orleans)

96. Member of Program Committee, *3rd Annual IEEE/ACM International Conference on High Performance Computing (HiPC)* (1996, Trivandrum, India)

97. Member of Program Committee, *6th Annual ACM-SIAM Symp. on Discrete Algorithms (SODA)* (1995, San Francisco)

98. Member of Program Committee, *9th Annual IEEE International Parallel Processing Symposium (IPPS)* (1995, Santa Barbara)

99. Member of Program Committee, *6th Annual International Symposium on Algorithms and Computation (ISAAC)* (1995, Cairns, Australia)

100. Member of Program Committee, *2d Annual IEEE/ACM International Conference on High Performance Computing (HiPC)* (1995, Delhi, India)

101. Vice-Chair of Program Committee, *8th Annual IEEE International Parallel Processing Symposium (IPPS)* (1994, Cancun)

102. General Co-Chair, *7th Annual International Conference on Parallel and Distributed Computing and Systems (PDCS)* (1994, Las Vegas)

103. Member of Program Committee, *7th Annual IEEE International Parallel Processing Symposium (IPPS)* (1993, Newport Beach)

104. Member of Steering Committee, *5th Annual IEEE Symp. on Parallel and Distributed Processing (SPDP)* (1993, Dallas)

105. Co-Chair of Program Committee, *4th Annual IEEE Symp. on Parallel and Distributed Processing (SPDP)* (1992, Dallas)

106. Member of Program Committee, *2d Workshop on Algorithms and Data Structures (WADS)* (1991, Ottawa)

107. Member of Program Committee, *6th Annual ACM Symp. on Computational Geometry (SoCG)* (1990, Berkeley)

Other Editorial Activities

- *Handbook of Algorithms and Theory of Computation,* CRC Press (1st Edition: 1995–98; 2d Edition: 2006–).
- *Handbook of Parallel and Distributed Computing,* McGraw-Hill (1993–97).
- *Handbook of Computer Science and Engineering,* CRC Press (1994–97).
- *Computational Mathematics Series Editor* for Chapman & Hall / CRC (1999–2002).

PUBLICATIONS

Note on journal versions of conference papers: Conference papers marked by * have not appeared in journal version, and will not be submitted to journals unless the conference's page limitations constrained the presentation (journals will not publish papers that do not add substantially to a published conference version of a paper).

In Refereed Conferences

1. * Security and Privacy Risks in Electronic Communications: A User's Assessment (with Fariborz Farahmand, Joshua Ripple, and Robin L. Dillon-Merrill). *Proc. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON 2017)*, New York, October 2017, pp. 412–417. Won **Best Paper Award** in the track on "Big Data, Image Processing and Multimedia Technology" (best paper awards were given within tracks).

2. * Confidentiality Management in Collaborative Design (with Adam Dachowicz, Siva Chaitanya Chaduvula, and Jitesh H. Panchal). *Proc. of ASME 2016 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference (IDETC 2016)*, Charlotte, North Carolina, August 2016. 15 pages.

3. ErsatzPasswords: Ending Password Cracking and Detecting Password Leakage (with Mohammed H. Almeshekah, Chris Gutierrez, and Eugene H. Spafford). *Proc. 31st Annual Computer Security Applications Conference (ACSAC 15)*, Los Angeles, California, December 2015. Acceptance rate: 24% (47/193). Won **Outstanding Paper Award** from that conference.

4. * Enhancing Password Security using Deceptive Covert Communication (with Mohammed H. Almeshekah and Eugene H. Spafford). *Proc. 30th International Information Security and Privacy Conference*, Hamburg, Germany, May 2015, pp. 159–173.

5. Similarity Group-by Operators for Multi-dimensional Relational Data (with Ruby Y. Tahboub, Mingjie Tang, Walid G. Aref, Qutaibah M. Malluhi, Mourad Ouzzani, Yasin N. Silva). *Proc. 32d International Conference on Data Engineering (ICDE 2016)* Helsinki, Finland, May 2016, pp. 1448–1449.

6. Secure Collaborations in Engineering System Design (with Shumiao Wang, Siddharth Bhandari, Jitesh Panchal, and Karthik Ramani). *Proc. of ASME 2014 International Design and Engineering Technical Conference and Computers and Information in Engineering Conference (IDETC 2014)*, Buffalo, New York, August 2014. 13 pages.

7. * Back Channels Can Be Useful! – Layering Authentication Channels to Provide Covert Communication (with Mohammed H. Almeshekah and Eugene H. Spafford). *Proc. The 21st International Workshop in Security Protocols (SPW 2013)*, Cambridge, United Kingdom, March 2013.

8. * Secure and Private Outsourcing of Shape-Based Feature Extraction (with Shumiao Wang, Mohammed Nassar, and Qutaibah Malluhi) *Proc. 15th International Conference on Information and Communications Security (ICICS 13)*, Beijing, China, November 2013, pp. 90–99. Acceptance rate: 26% (29/113).

9. * Secure and Efficient Outsourcing of Sequence Comparisons (with Marina Blanton, Keith Frikken and Qutaibah Malluhi). *Proc. 17th European Symposium on Research in Computer Security (ESORICS 2012)*, Pisa, Italy, September 2012, pp. 505–522. Acceptance rate: 20% (50/148).

10. * Private Outsourcing of Matrix Multiplication over Closed Semi-Rings (with Keith Frikken and Shumiao Wang). *Proc. International Conference on Security and Cryptography (SECRYPT 2012)*, Rome, Italy, July 2012, pp. 136–144. Acceptance rate for full papers: 14% (22/160).

11. * Privacy-Preserving Business Process Outsourcing (with Mehdi Bentounsi and Salima Benbernou). *Proc. 19th IEEE International Conference on Web Services (ICWS 2012)*, Honolulu, Hawaii, June 2012, pp. 662-663.

12. * Anonyfrag: An Anonymization-Based Approach For Privacy-Preserving BPaaS (with Mehdi Bentounsi, Salima Benbernou, and Cheikh Deme). *Proc. 1st International Workshop on Cloud Intelligence (Cloud-I, a VLDB 2012 Workshop)*, Istanbul, Turkey, August 2012.

13. * Leakage-Free Redactable Signatures (with Elisa Bertino and Ashish Kundu). *Proc. ACM Conference on Data and Application Security and Privacy*, San Antonio, Texas, February 2012, pp. 307–316.

14. * Secure Authenticated Comparisons (with Keith Frikken and Hao Yuan). *Proc. 9th Conference on Applied Cryptography and Network Security (ACNS 11)*, Nerja, Spain, June 2011, pp. 514–531. Acceptance rate: 18% (31/172).

15. * Duress Detection for Authentication Attacks Against Multiple Administrators, (with Emil Stefanov), *Proc. 2010 ACM CCS Workshop on Insider Threats (WITS 10)*, Chicago, October 2010, pp. 37–46.

16. * Data Structures for Range Minimum Queries in Multidimensional Arrays (with Hao Yuan). *Proc. 21st ACM-SIAM Symp. on Discrete Algorithms (SODA 10)*, Austin, Texas, January 2010, pp. 150–160. Acceptance rate: 30% (136/445)

17. * Securely Outsourcing Linear Algebra Computations (with Keith Frikken). *Proc. of 5th ACM Symposium on Information, Computer and Communications Security (AsiaCCS 10)*, Beijing, China, April 2010, pp. 48–59.

18. * Identifying Interesting Instances for Probabilistic Skylines (with Yinian Qi). *Proc. 21st International Conference and Workshop on Database and Expert Systems Applications (DEXA 10)*, Bilbao, Spain, August 2010, pp. 300–314.

19. * Efficient and Secure Distribution of Massive Geo-Spatial Data (with Hao Yuan). *Proc. 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (GIS 2009)*, Seattle, Washington, November 2009, pp. 440–443.

20. * Robust Authentication Using Physically Unclonable Functions (with Marina V. Blanton and Keith B. Frikken). *Proc. 12th Information Security Conference (ISC 2009)*, Pisa, Italy, September 2009, pp. 262–277. Acceptance rate for full papers: 28% (29/105)

21. * Computing All Skyline Probabilities for Uncertain Data (with Yinian Qi). *Proc. 28th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS 09)*, Providence, Rhode Island, July 2009, pp. 279-287.

22. * Genuinity Signatures: Designing Signatures for Verifying 3D Object Genuinity (with Daniel Aliaga). *Proc. 30th Annual Conference of the European Association for Computer Graphics (Eurographics 09)*, Munich, Germany, pp. 437–446. Acceptance rate: 23% (56/243)

23. * Efficient Data Structures for Range-Aggregate Queries on Trees (with Hao Yuan). *Proc. of 12th International Conference on Database Theory (ICDT 09)*, Saint-Petersburg, Russia, pp. 111–120. Acceptance rate: 32% (25/77).

24. * Incentives and Perceptions of Information Security Risks (with Fariborz Farahmand and Benn Konsynski). *Proc. International Conference on Information Systems (ICIS 08)*, Paris, France, December 2008.

25. * Efficient Private Record Linkage (with Mohamed Yakout and Ahmed Elmagarmid). *Proc. 25th International Conference on Data Engineering (ICDE 09)*, Shanghai, China, April 2009, pp. 1283–1286.

26. * Private and Cheating-Free Outsourcing of Algebraic Computations (with David Benjamin). *Proc. of 6th Annual Conference on Privacy, Security and Trust (PST 08)*, Fredericton, New Brunswick, Canada, October 2008, pp. 240–245. Acceptance rate: 28% (25/71).

27. * Binding Software to Specific Native Hardware in a VM Environment: The PUF Challenge and Opportunity, (with Eric D. Bryant, John T. Korb, and John R. Rice). *Proc. of 1st Workshop on Virtual Machine Security (VMSec 08)*, Fairfax, Virginia, October 2008, pp. 45–48. Acceptance rate: 35% (7/20).

28. * Efficient Privacy-Preserving k-Nearest Neighbor Search (with Yinian Qi). *Proc. of 28th International Conference on Distributed Computing Systems (ICDCS 08)*, Beijing, China, June 2008, pp. 311–319. Acceptance rate: 16% (102/638).

29. * Efficient Distributed Third-Party Data Authentication for Tree Hierarchies (with Hao Yuan). *Proc. of 28th International Conference on Distributed Computing Systems (ICDCS 08)*, Beijing, China, June 2008, pp. 184–193. Acceptance rate: 16% (102/638).

30. * Private Combinatorial Group Testing (with Keith B. Frikken, Marina V. Blanton and YounSun Cho). *Proc. of 3d ACM Symposium on Information, Computer and Communications Security (AsiaCCS 08)*, Tokyo, March 2008, pp. 312–320. Acceptance rate: 18% (32/182 for regular papers).

31. * Efficient Data Authentication in an Environment of Untrusted Third-Party Distributors (with YounSun Cho and Ashish Kundu). *Proc. 24th International Conference on Data Engineering (ICDE 08)*, Cancun, Mexico, April 2008, pp. 696–704.

32. * Private Discovery of Shared Interests (with YounSun Cho). *Proc. 9th International Conference on Information and Communications Security (ICICS 07)*, Zhengzhou, China, December 2007.

33. * Incorporating Temporal Capabilities in Existing Key Management Schemes (with Marina V. Blanton and Keith B. Frikken). *Proc. 12th European Symposium on Research in Computer Security (ESORICS 07)*, Dresden, Germany, September 2007, pp. 515–530.

34. * Discrepancy-Sensitive Dynamic Fractional Cascading, Dominated Maxima Searching, and 2-d Nearest Neighbors in Any Minkowski Metric (with Marina V. Blanton, Michael T. Goodrich, and Stanislas Polu). *Proc. 2007 Workshop on Algorithms and Data Structures (WADS 07)*, Halifax, Nova Scotia, August 2007, pp. 114–126. Acceptance rate: 26% (40/150).

35. * Passwords for Everyone: Secure Mnemonic-based Accessible Authentication (with Mercan Topkara and Umut Topkara). *Proc. 2007 USENIX Annual Technical Conference (USENIX 07)*, Santa Clara, California, June 2007, pp. 369–374.

36. * Efficient Techniques for Realizing Geo-Spatial Access Control (with Marina V. Blanton and Keith B. Frikken). *Proc. of 2d ACM Symposium on Information, Computer and Communications Security (AsiaCCS 07)*, Singapore, March 2007, pp. 82–92. Accceptance rate: 18%.

37. * Passwords Decay, Words Endure: Secure and Re-usable Multiple Password Mnemonics (with Mercan Topkara and Umut Topkara). *Proc. 22d Annual ACM Symposium on Applied Computing (SAC 07)*, Seoul, Korea, March 2007, pp. 292–299.

38. * Information Hiding through Errors: A Confusing Approach (with Mercan Topkara and Umut Topkara). *Proc. SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents*, 2007, San Jose, CA, 12 pages.

39. * Secure and Private Collaborative Linear Programming (with Jiangtao Li). *Proc. 2nd International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 06)*, Atlanta, Georgia, November 2006, pp. 1–8.

40. Point-Based Trust: Define How Much Privacy Is Worth (with Danfeng Yao, Keith Frikken, and Roberto Tamassia). *Proc. 8th International Conference on Information and Communications Security (ICICS 06)*, Raleigh, North Carolina, December 2006, pp. 190–209. [Best Student Paper Award]

41. * Words Are Not Enough: Sentence Level Natural Language Watermarking (with Mercan Topkara and Umut Topkara). *Proc. 1st ACM Workshop on Multimedia Content Protection and Security (MCPS 06)*, Santa Barbara, California, October 2006, pp. 37–46.

42. * The Hiding Virtues of Ambiguity: Quantifiably Resilient Watermarking of Natural Language Text through Synonym Substitutions (with Mercan Topkara and Umut

Topkara). *Proc. ACM Multimedia and Security Workshop (MMSEC 06)*, Geneva, Switzerland, September 2006, pp. 164–174.

43. An Empirical Study of Automatic Event Reconstruction Systems (with Sundararaman Jeyaraman). *Proc. 6th Annual Digital Forensics Research Workshop (DFRWS 06)*, Lafayette, Indiana, August 2006.

44. * Key Management for Non-Tree Access Hierarchies (with Marina V. Blanton and Keith B. Frikken). *Proc. 11th ACM Symposium on Access Control Models and Technologies (SACMAT 06)*, Lake Tahoe, California, June 2006, pp. 11–18. Acceptance rate: 30% (25/82).

45. * Efficient Correlated Action Selection (with Marina V. Blanton, Keith B. Frikken, and Jiangtao Li). *Proc. 10th Financial Cryptography and Data Security Conference (FC 06)*, Anguilla, British West Indies, February 2006, pp. 296–310. Acceptance rate: 30% (19/64 for regular papers).

46. * Lost in Just the Translation (with Christian Grothoff, Krista Grothoff, and Ryan Stutsman). *Proc. 21st Annual ACM Symposium on Applied Computing (SAC 06)*, Dijon, France, April 2006, pp. 338–345. Acceptance rate: 32% (300/927).

47. * Trust Negotiation with Hidden Credentials, Hidden Policies, and Policy Cycles (with Keith B. Frikken and Jiangtao Li). *Proc. of the 13th Annual Network and Distributed System Security Symposium (NDSS 06)*, San Diego, California, February 2006, pp. 157–172. Acceptance rate: 13% (17/127).

48. * Natural Language Watermarking: Research Challenges and Applications (with Mercan Topkara, Giuseppe Riccardi, and Dilek Hakkani-Tur). *Proc. of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents VI*, January 2006, San Jose, California.

49. * Dynamic and Efficient Key Management for Access Hierarchies (with Marina V. Blanton and Keith B. Frikken). *Proc. of the 12th ACM Conference on Computer and Communications Security (CCS 05)*, Alexandra, Virginia, November 2005, pp. 190–202. Acceptance rate: 15% (38/249). This paper was given the **"CCS Test of Time Award"** in October 2015 (an award started in 2012 and given to particularly influential papers that appeared in CCS ten years earlier).

50. * ViWiD: Visible Watermarking-Based Defense Against Phishing (with Mercan Topkara, Ashish Kamra, and Cristina Nita-Rotaru). *Proc. of the Workshop on Digital Watermarking (IWDW 05)*, Lecture Notes in Computer Sciences, Springer Verlag, Siena, Italy, September 2005, pp. 470–482..

51. * Indexing Information for Data Forensics (with Michael T. Goodrich and Roberto Tamassia). *Proc. 3rd Conference on Applied Cryptography and Network Security (ACNS 05)*, New York, June 2005, pp. 206–221. Acceptance rate: 22% (35/156).

52. Translation-Based Steganography (with Christian Grothoff, Krista Grothoff, Ludmila Alkhutova, and Ryan Stutsman). *Proc. 7th International Information Hiding Workshop (IHW 05)*, Barcelona, Spain, June 2005, pp. 219–233.

53. * Provable Bounds for Portable and Flexible Privacy-Preserving Access Rights (with Marina V. Blanton). *Proc. 10th ACM Symposium on Access Control Models and Technologies (SACMAT 05)*, Stockholm, Sweden, June 2005, pp. 95–101. Acceptance rate: 21% (19/90).

54. * Privacy-Preserving Credit Checking (with Keith Frikken and Chen Zhang). *Proc. 6th ACM Conference on Electronic Commerce (EC 05)*, Vancouver, Canada, June 2005, pp. 147–154. Acceptance rate: 29% (33/113).

55. * Secure Collaborative Planning, Forecasting, and Replenishment (SCPFR) (with Marina Blanton, Vinayak Deshpande, Keith Frikken, Jiangtao Li, and Leroy Schwarz). *Multi-Echelon / Public Applications of Supply Chain Management Conference*, Atlanta, June 2006.

56. * Markov Models for Identification of Significant Episodes (with Robert Gwadera and Wojciech Szpankowski). *Proc. 5th SIAM International Conference on Data Mining (SDM 05)*, Newport Beach, California, April 2005, pp. 404–414. Acceptance rate: 18% (40/218).

57. * Secure Biometric Authentication for Weak Computational Devices (with Keith B. Frikken, Michael T. Goodrich, and Roberto Tamassia). *Proc. 9th International Conference on Financial Cryptography and Data Security (FC 05)*, Lecture Notes in Computer Sciences, Springer Verlag (LNCS 3570), Roseau, Dominica, February 2005, pp. 357–370. Acceptance rate: 24% (22/92).

58. * Achieving Fairness in Private Contract Negotiation (with Keith B. Frikken). *Proc. 9th International Conference on Financial Cryptography and Data Security (FC 05)*, Lecture Notes in Computer Sciences, Springer Verlag (LNCS 3570), Roseau, Dominica, February 2005, pp. 270-284. Acceptance rate: 24% (22/92).

59. * Remote Revocation of Smart Cards in a Private DRM system (with Keith B. Frikken and Marina V. Bykova). *Proc. Australasian Information Security Workshop (AISW 05)*, Newcastle, Australia, January 2005, pp. 169–177. Acceptance rate: 37% (13/35).

60. Verifying Data Integrity in Peer-to-Peer Media Streaming (with Ahsan Habib, Dongyan Xu, Bharat Bhargava, and John Chuang). *Proc. 12th Annual Multimedia Computing and Networking Workshop (MMCN 05)*, San Jose, California, January 2005, pp. 1–12. Acceptance rate: 16% (16/100 for regular papers).

61. * Detection of Significant Sets of Episodes in Event Sequences (with Robert Gwadera and Wojciech Szpankowski). *Proc. 4th IEEE International Conference on Data Mining (ICDM 04)*, Brighton, United Kingdom, November 2004, pp. 3–10. Acceptance rate: 9% (39/451).

62. * Private Collaborative Forecasting and Benchmarking (with Marina Bykova, Jiangtao Li, Keith B. Frikken, and Mercan Karahan). *Proc. 3rd ACM Workshop on Privacy in the Electronic Society (WPES 04)*, Washington, DC, October 2004, pp. 103–114. Acceptance rate: 22% (10/45 for regular papers).

63. * Privacy-Preserving Route Planning (with Keith B. Frikken). *Proc. 3rd ACM Workshop on Privacy in the Electronic Society (WPES 04)*, Washington, DC, October 2004, pp. 8–15. Acceptance rate: 22% (10/45 for regular papers).

64. * Hidden Access Control Policies with Hidden Credentials (with Keith B. Frikken and Jiangtao Li). *Proc. 3rd. ACM Workshop on Privacy in the Electronic Society (WPES 04)* (short paper), Washington, DC, October 2004, pp. 27–28. Acceptance rate: 45% (21/45 for short papers).

65. * A Hierarchical Protocol for Increasing the Stealthiness of Steganographic Methods (with Mercan Karahan, Umut Topkara, Cuneyt Taskiran, Eugene T. Lin, and Edward J. Delp). *Proc. ACM Multimedia and Security Workshop (MMSEC 04)*, Magdeburg, Germany, September 2004, pp. 16–24.

66. * wmdb.*: Rights Protection for Numeric Relational Data, (with Radu Sion and Sunil K. Prabhakar). *Proc. 20th International Conference on Data Engineering (ICDE 04)*, Boston, Massachusetts, 2004, p. 863.

67. * Privacy-Preserving Location-Dependent Query Processing (with Keith B. Frikken). *Proc. IEEE International Conference on Pervasive Services (ICPS 04)*, July 2004, pp. 9–17.

68. * Portable and Flexible Document Access Control Mechanisms (with Marina Bykova). *Proc. 9th European Symposium on Research in Computer Security (ESORICS 04)*, Lecture Notes in Computer Sciences, Springer Verlag (LNCS 3193), Sophia Antipolis, France, September 2004, pp. 193–208.

69. * Resilient Rights Protection for Sensor Streams (with Radu Sion and Sunil Prabhakar). *Proc. 30th International Conference on Very Large Data Bases (VLDB 04)*, Toronto, September 2004, pp. 732–743. Acceptance rate: 16% (81/504).

70. * Secure Outsourcing of Sequence Comparisons (with Jiangtao Li). *Proc. 4th Workshop on Privacy Enhancing Technologies (PET 04)*, Lecture Notes in Computer Sciences, Springer Verlag (LNCS 3424), Toronto, May 2004, pp. 63–78.

71. * Succinct Specifications of Portable Document Access Policies (with Marina Bykova). *Proc. 9th ACM Symposium on Access Control Models and Technologies (SACMAT 04)*, Yorktown Heights, June 2004, pp. 41–50.

72. * Private Fingerprint Verification without Local Storage (with Florian Kerschbaum, David Mraihi, and John R. Rice). *Proc. International Conference on Biometric Authentication (ICBA 04)* (short paper), Hong Kong, July 2004, pp. 387–394.

73. * Attacking Digital Watermarks (with Radu Sion). *Proc. Symposium on Electronic Imaging (SPIE 04)*, San Jose, California, January 2004, Vol. 5306, pp. 848–858.

74. * Adaptive Data Structures for IP Lookups (with Ananth Grama and Ioannis Ioannidis). *Proc. 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 03)*, San Francisco, California, April 2003, pp. 75–84. Acceptance ratio: 21% (224/1078).

75. Authentication of LZ-77 Compressed Data (with Stefano Lonardi). *Proc. 18th Annual ACM Symposium on Applied Computing (SAC 03)*, Melbourne, Florida, March 2003, pp. 282–287.

76. * On-the-fly Intrusion Detection for Web Portals (with Radu Sion and Sunil K. Prabhakar). *IEEE International Conference on Information Technology: Coding and Computing (ITCC 03)*, Las Vegas, Nevada, April 2003, pp. 325–330.

77. * Rights Protection for Relational Data (with Radu Sion and Sunil K. Prabhakar). *Proc. 2003 ACM International Conference on Management of Data (SIGMOD 03)*, San Diego, California, June 2003, pp. 98-109. Acceptance rate: 15% (52/342).

78. * Secure Supply-Chain Protocols (with Hicham G. Elmongui, Vinayak Deshpande, and Leroy B. Schwarz). *Proc. 2003 IEEE Conference on Electronic Commerce (CEC 03)*, Newport Beach, California, June 2003, pp. 293–302.

79. * Enhanced Smart-card Based License Management (with Jiangtao Li). *Proc. 2003 IEEE Conference on Electronic Commerce (CEC 03)*, Newport Beach, California, June 2003, pp. 111–119.

80. * Cropping-Resilient Segmented Multiple Watermarking (with Keith B. Frikken). *Proc. 2003 Workshop on Algorithms and Data Structures (WADS 03)*, Lecture Notes in Computer Sciences, Springer Verlag (LNCS 2748), Ottawa, Canada, August 2003, pp. 231–242. Acceptance rate: 32% (40/126).

81. * Replicated Parallel I/O without Additional Scheduling Costs (with Keith B. Frikken). *Proc. 14th International Conference and Workshop on Database and Expert Systems Applications (DEXA 03)*, Lecture Notes in Computer Sciences, Springer Verlag (LNCS 2736), Prague, Czech Republic, September 2003, pp. 223–232. Acceptance rate: 39% (91/236).

82. * Secure and Private Sequence Comparisons (with Florian Kerschbaum and Kevin Du). *Proc. 2d. ACM Workshop on Privacy in the Electronic Society (WPES 03)*, Washington, DC, October 2003, pp. 39–44. Acceptance rate: 32% (16/50).

83. * Privacy Preserving Electronic Surveillance (with Keith B. Frikken). *Proc. 2d. ACM Workshop on Privacy in the Electronic Society (WPES 03)*, Washington, DC, October 2003, pp. 45–54. Acceptance rate: 32% (16/50).

84. Reliable Detection of Episodes in Event Sequences (with Robert Gwadera and Wojciech Szpankowski). *Proc. 3rd IEEE International Conference on Data Mining (ICDM 03)*, Melbourne, Florida, November 2003, pp. 67–74. Acceptance rate: 12% (58/501).

85. * Resilient Information Hiding for Abstract Semi-Structures (with Radu Sion and Sunil Prabhakar), *Proc. of the Workshop on Digital Watermarking (IWDW 03)*, Lecture Notes in Computer Sciences, Springer Verlag (LNCS 2939), Seoul, Korea, October 2003, pp. 141–153.

86. * Power: A Metric for Evaluating Watermarking Algorithms (with Radu Sion and S. Prabhakar). *Proc. IEEE International Conference on Information Technology: Coding and Computing (ITCC 02)*, Las Vegas, Nevada, April 2002, pp. 95–100.

87. * On the Discovery of Weak Periodicities in Large Time Series (with Walid G. Aref, Christos Berberidis, Ioannis P. Vlahavas, and Ahmed K. Elmagarmid). *Proc. 6th European Conference on Principles and Practice of Knowledge Discovery in Databases (PKDD 02)*, August 2002, Helsinki, Finland. Lecture Notes in Computer Science, Vol. LNAI 2431, Springer Verlag, pp. 51–61.

88. * Optimal Parallel I/O for Range Queries through Replication (with Keith B. Frikken, Sunil K. Prabhakar, and Rei Safavi-Naini). *Proc. 13th International Conference and Workshop on Database and Expert Systems Applications (DEXA 02)*, Aix-en-Provence, France, September 2002. Lecture Notes in Computer Science, Vol. 2453, Springer Verlag, pp. 669–678. Acceptance rate: 37% (89/241).

89. * Multiple and Partial Periodicity Mining in Time Series Databases (with Christos Berberidis, Walid G. Aref, Ioannis P. Vlahavas, and Ahmed K. Elmagarmid). *Proc. 15th European Conference on Artificial Intelligence (ECAI 02)*, July 2002, Lyon, France. *IOS Press*, pp. 370–374.

90. * Natural Language Watermarking and Tamperproofing (with Victor Raskin, Christian F. Hempelmann, Mercan Karahan, Umut Topkara, Katrina E. Triezenberg, Radu Sion). *Proc. 5th International Information Hiding Workshop (IHW 02)*, Noordwijkerhout, The Netherlands, October 2002. Acceptance rate: 34% (27/78).

91. * On Watermarking Numeric Sets (with Radu Sion and Sunil K. Prabhakar). *Proc. 1st International Workshop on Digital Watermarking (IWDW 02)*, Seoul, South Korea, November 2002. Lecture Notes in Computer Science, 2613: Digital Watermarking, Springer-Verlag, New York, 2002, pp. 130–146.

92. * A Secure Protocol for Computing Dot-products in Clustered and Distributed Environments (with Ananth Grama and Ioannis Ioannidis). *Proc. 2002 Int. Conf. on Parallel Processing (ICPP 02)*, Vancouver, British Columbia, August 2002, pp. 79–384.

93. * Why NLP should move into IAS (with Victor Raskin, Sergei Nirenburg, Christian F. Hempelmann, and Katrina E. Triezenberg). *Proceedings of the Workshop on a Roadmap for Computational Linguistics (COLING),* Steven Krauwer (ed.), Taipei, Taiwan: Academia Sinica, 2002, pp. 1–7.

94. * Outsourcing Scientific Computations Securely, (with John R. Rice). *Proc. International NAISO (Natural & Artificial Intelligence Systems Organization) Congress on Information Science Innovations*, Dubai, U.A.E., March 2001.

95. * Natural Language Watermarking: Design, Analysis, and a Proof-of-Concept Implementation (with Victor Raskin; students: Michael C. Crogan, Christian Hempelmann, Florian Kerschbaum, Dina Mohamed, Sanket Naik). *Proc. 4th International Information Hiding Workshop (IHW 01)*, Pittsburgh, Pennsylvania, April 2001, pp. 185–199. Lecture Notes in Computer Science, Vol. 2137, Springer Verlag.

96. * Privacy-Preserving Cooperative Scientific Computations (with Kevin Du). *Proc. 14th IEEE Computer Security Foundations Workshop (CSFW 01)*, Cape Breton, Nova Scotia, Canada, June 2001, pp. 273–282.

97. * Secure Multi-Party Computational Geometry (with Kevin Du). *Proc. 2001 Workshop on Algorithms and Data Structures (WADS 01)*, Providence, Rhode Island, August 2001. Lecture Notes in Computer Science, Vol. 2125, Springer Verlag, pp. 165–179.

98. * Secure Multi-Party Computation Problems and their Applications: A Review and Open Problems (with Kevin Du). *Proc. 10th ACM/SIGSAC New Security Paradigms Workshop (NSPW 01)*, Cloudcroft, New Mexico, September 2001, pp. 11–20.

99. * Protecting Software Code by Guards (with Hoi Chang). *Proc. ACM Workshop on Security and Privacy in Digital Rights Management (SPDRM 01)*, Philadelphia, Pennsylvania, November 2001, pp. 160–175.

100. * Privacy-preserving Cooperative Statistical Analysis (with Kevin Du). *Proc. 17th Annual Computer Security Applications Conference (ACSAC 01)*, New Orleans, Louisiana, December 2001, pp. 102–110.

101. * (Almost) Optimal Parallel Block Access for Range Queries, (with Sunil K. Prabhakar). *Proc. 19th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS 00)*, Dallas, Texas, May 2000, pp. 205–215.

102. * Better Logging Through Formality: Applying Formal Specification Techniques to Improve Audit Logs and Audit Consumers, (with Chapman Flack). *Lecture Notes in Computer Science, Vol. 1907*, Springer Verlag, *Proc. 3rd International Workshop on the Recent Advances in Intrusion Detection (RAID 00)*, Toulouse, France, October 2000, pp. 1–16.

103. * Natural Language Processing for Information Assurance, (with Chris McDonough, Sergei Nirenburg, and Victor Raskin). *Proc. 9th ACM/SIGSAC New Security Paradigms Workshop (NSPW 00)*, Cork, Ireland, September 2000, pp. 51–65.

104. Protocols for Secure Remote Database Access with Approximate Matching, (with Kevin Du). *Proc. 1st ACM Workshop on Security and Privacy in E-Commerce,* Athens, Greece, November 2000, 25 pages.

105. * Watermarking Data Using Quadratic Residues, (with Samuel S. Wagstaff). *Proc. of SPIE Workshop on Electronic Imaging (SPIE 99)*, SPIE - The International Society for Optical Engineering, San Jose, January 1999, SPIE Vol. 3657, pp. 283–288.

106. * Disclosure Limitation of Sensitive Rules, (with Elisa Bertino, Ahmed K. Elmagarmid, M. Ibrahim, and Vassilis Verykios). *Proc. IEEE Knowledge and Data Engineering Exchange Workshop (KDEX 99)*, Chicago, November 1999, pp. 45–52.

107. * Parallel Geometric Algorithms in Coarse-Grain Network Models (with Danny Z. Chen). *Lecture Notes in Computer Science, Vol. 1449*, Springer Verlag, *Proc. of the Fourth Annual International Computing and Combinatorics Conference (COCOON 98)*, Taipei, Taiwan, August 1998, pp. 55–64.

108. Parallel Algorithms for Longest Increasing Chains in the Plane and Related Problems, (with Danny Z. Chen and K.S. Klenk). *Proc. Ninth Canadian Conference on Computational Geometry (CCG 97)*, Kingston, Canada, 1997, pp. 59–64.

109. Efficient Parallel Algorithms for Planar *st*-Graphs, (with Danny Z. Chen and Ovidiu Daescu). *Proc. of the Eighth Annual International Symposium on Algorithms and Computation (ISAAC 97)*, Singapore, December 1997, pp. 223–232. Lecture Notes in Computer Science, Vol. 1350, Springer Verlag,

110. * Static Matching of Ordered Program Segments to Dedicated Machines in a Heterogeneous Computing Environment, (with Dan W. Watson, John K. Antonio, H.J. Siegel, R. Gupta). *Proc. 5th IEEE Workshop on Heterogeneous Processing*, Honolulu, Hawaii, 1996, pp. 24–37.

111. Pattern Matching Image Compression (Abstract), (with Yann Genin and Wojciech Szpankowski). *Proc. IEEE Data Compression Conference (DCC 96)*, Snowbird, Utah, 1996, p. 421.

112. A Pattern Matching Approach to Image Compression, (with Yann Genin and Wojciech Szpankowski). *Proc. 3rd IEEE International Conference on Image Processing (ICIP 96)*, Lausanne, Switzerland, September 1996, pp. 349–356.

113. Applications of a Numbering Scheme for Polygonal Obstacles in the Plane, (with Danny Z. Chen). *Proc. 7th Annual International Symposium on Algorithms and Computation (ISAAC 96)*, Osaka, Japan, 1996, Springer Verlag Lecture Notes in Computer Sci.: 1178, December 1996, pp. 1–24.

114. * Internet, Education and the Web, (with Elias N. Houstis, Anupam Joshi, Sanjiva Weerawarana, and Ahmed K. Elmagarmid). *Proc. IEEE 5th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE 96)*, Stanford, California, 1996, pp. 27–32.

115. Parallel Algorithms for Maximum Matching in Interval Graphs, (with Marilyn G. Andrews, Danny Z. Chen, D.T. Lee). *Proc. 9th IEEE International Parallel Processing Symposium (IPPS 95)*, Santa Barbara, California, 1995, pp. 84–92.

116. * Static Program Decomposition Among Machines in an SIMD/SPMD Heterogeneous Environment with Non-Constant Mode Switching Costs, (with Dan W. Watson, H.J. Siegel, John K. Antonio). *Proc. 3d IEEE Workshop on Heterogeneous Processing*, Cancun, Mexico, 1994, pp. 58–65.

117. * Biased Finger Trees and Their Use in Dynamic Computational Geometry, (with Michael T. Goodrich and Kumar Ramaiyer). *Proc. 10th Annual ACM Symp. on Computational Geometry (SoCG 94)*, Stony Brook, New York, 1994, pp. 150–159.

118. On the Multisearching Problem for Hypercubes, (with Andreas Fabri). *Proc. 6th Parallel Architectures and Languages Europe Symp. (PARLE 94)*, Athens, Greece, 1994, Springer Verlag Lecture Notes in Computer Sci.: 817, 1994, pp. 159–166.

119. * A System for Drawing Graphs with Geometric Symmetry, (with Joseph B. Manning, K. Cudjoe, J. Lozito and R. Pacheco). *Proc. 1994 Workshop on Graph Drawing (GD 94)*, Princeton, New Jersey, 1994, Springer Verlag Lecture Notes in Computer Sci.: 894, 1994, pp. 262–265.

120. * A Framework for Compile-Time Selection of Parallel Modes in an SIMD/SPMD Heterogeneous Environment, (with Dan W. Watson, H.J. Siegel, John K. Antonio, Mark A. Nichols). *Proc. 2d IEEE Workshop on Heterogeneous Processing*, Newport Beach, California, 1993, pp. 57–64.

121. On Parallel Rectilinear Obstacle-Avoiding Paths, (with Danny Z. Chen). *Proc. 5th Canadian Conference on Computational Geometry (CCG 93)*, Waterloo, Canada, 1993, pp. 210–215.

122. Computing the All-Pairs Longest Chains in the Plane, (with Danny Z. Chen). *Proc. 1993 Workshop on Algorithms and Data Structures (WADS 93)*, Montreal, Canada, 1993. Springer Verlag Lecture Notes in Computer Sci.: 709, 1993, pp. 1–13.

123. An Optimal Algorithm for Shortest Paths on Interval and Circular-Arc Graphs, with Applications, (with Danny Z. Chen and D.T. Lee). *Proc. 1st Annual European Symposium on Algorithms (ESA 93)*, Bad Honnef, Germany, 1993. Springer Verlag Lecture Notes in Computer Sci.: 726, 1993, pp. 13–24.

124. Optimal Parallel Hypercube Algorithms for Polygon Problems, (with Danny Z. Chen). *Proc. 5th IEEE Symposium on Parallel and Distributed Processing (SPDP 93)*, Dallas, Texas, 1993, pp. 208–215.

125. Pattern Matching with Mismatches: A Probabilistic Analysis and a Randomized Algorithm, (with Philippe Jacquet and Wojciech Szpankowski). *Proc. 3rd Combinatorial Pattern Matching Symposium (CPM 92)*, Tucson, Arizona, 1992. Springer Verlag Lecture Notes in Computer Science: 644 (eds. Alberto Apostolico, Maxime Crochemore, Zvi Galil, Udi Manber), pp. 27–40, 1992.

126. An Efficient Parallel Algorithm for the Row Minima of a Totally Monotone Matrix, (with S. Rao Kosaraju). *Proc. 2d ACM-SIAM Symp. on Discrete Algorithms (SODA 91)*, San Francisco, California, 1991, pp. 394–403.

127. Co-Scheduling Compute-Intensive Tasks on a Network of Workstations: Models and Algorithms, (with Christina Lock, Dan C. Marinescu, H.J. Siegel, and Thomas L. Casavant). *Proc. 11th Int. Conf. on Distributed Computing Systems (ICDCS 91)*, Arlington, Texas, 1991, pp. 344–352.

128. Multisearch Techniques for Implementing Data Structures on a Mesh-Connected Computer, (with Frank Dehne, Russ Miller, Andrew Rau-Chaplin, Jyh-Jong Tsay). *Proc. 2d Annual ACM Symp. on Parallel Algorithms and Architectures (SPAA 91)*, Hilton Head, South Carolina, 1991, pp. 204–214.

129. An Input-Size/Output-Size Trade-Off in the Time-Complexity of Rectilinear Hidden Surface Removal, (with Michael T. Goodrich and Mark H. Overmars). *Proc. of the 17th Annual International Colloquium on Automata, Languages, and Programming (ICALP 90)*, Warwick, United Kingdom, 1990. Springer Verlag Lecture Notes in Computer Sci.: 443, 1990, pp. 689–702.

130. P-Complete Geometric Problems, (with Paul Callahan and Michael T. Goodrich). *Proc. 2d Annual ACM Symp. on Parallel Algorithms and Architectures (SPAA 90)*, Crete, Greece, 1990, pp. 317–326.

131. Parallel Rectilinear Shortest Paths with Rectangular Obstacles, (with Danny Z. Chen). *Proc. 2d Annual ACM Symp. on Parallel Algorithms and Architectures (SPAA 90)*, Crete, Greece, 1990, pp. 270–279.

132. A Faster Parallel Algorithm for a Matrix Searching Problem. *Proc. 2d Scandinavian Workshop on Algorithm Theory (SWAT 90)*, Bergen, Norway, 1990. Springer Verlag Lecture Notes in Computer Sci.: 447 1990, pp. 192–200.

133. On the Parallel-Decomposibility of Geometric Problems, (with Jyh-Jong Tsay). *Proc. 5th Annual ACM Symp. on Computational Geometry (SoCG 89)*, Saarbrucken, Federal Republic of Germany, 1989, pp. 104–113.

134. An Optimal Parallel Algorithm for the Visibility of a Simple Polygon from a Point, (with Danny Z. Chen). *Proc. 5th Annual ACM Symp. on Computational Geometry (SoCG 89)*, Saarbrucken, Federal Republic of Germany, 1989, pp. 114–123.

135. * Constructing Trees in Parallel, (with S. Rao Kosaraju, Lawrence L. Larmore, Gary L. Miller, and Shanghua Teng). *Proc. 1st Annual ACM Symp. on Parallel Algorithms and Architectures (SPAA 89)*, Santa Fe, New Mexico, 1989, pp. 421–431.

136. Optimal Channel Placement for Multi-Terminal Nets, (with Susanne E. Hambrusch). *Proc. 1989 Workshop on Algorithms and Data Structures (WADS 89)*, Ottawa, Canada, 1989, pp. 421–431.

137. * Fast Detection and Display of Symmetry in Embedded Planar Graphs, (with Joseph B. Manning). *Proc. 19th Southeastern Int. Conf. on Combinatorics, Graph Theory and Computing*, Baton Rouge, Louisiana, 1988.

138. On the Parallel Complexity of Evaluating Some Sequences of Set Manipulation Operations, (with S. Rao Kosaraju and Michael T. Goodrich). *Proc. 3rd Aegean Workshop on Computing (AWOC 88)*, Lecture Notes in Computer Science, 319: VLSI Algorithms and Architectures, Springer-Verlag, New York, 1988, pp. 1–10.

139. Efficient Parallel Algorithms for String Editing and Related Problems, (with Alberto Apostolico, Lawrence L. Larmore, and H. Scott McFaddin). *Proc. 26th Annual Allerton Conf. on Communication, Control, and Computing*, Monticello, Illinois, 1988, pp. 253–263.

140. Parallel Topological Sorting of Features in a Binary Image, (with Susanne E. Hambrusch and Lynn E. TeWinkel). *Proc. 26th Annual Allerton Conf. on Communication, Control, and Computing*, Monticello, Illinois, 1988, pp. 1114–1115.

141. Efficient Solutions to Some Maxdominance Problems, (with S. Rao Kosaraju). *Proc. 21st Annual Conf. on Info. Sciences and Systems (CISS 87)*, Baltimore, Maryland, 1987, pp. 600–610.

142. Cascading Divide-and-Conquer: A Technique for Designing Parallel Algorithms, (with Richard Cole and Michael T. Goodrich). *Proc. 28th Annual IEEE Symp. on Foundations of Computer Sci. (FOCS 87)*, Marina Del Rey, California, 1987, pp. 151–160.

143. Optimal Simulations Between Mesh-Connected Arrays of Processors, (with S. Rao Kosaraju). *Proc. 18th Annual ACM Symp. on Theory of Computing (STOC 86)*, Berkeley, California, 1986, pp. 264–271.

144. Efficient Plane Sweeping in Parallel, (with Michael T. Goodrich). *Proc. 2nd Annual ACM Symp. on Computational Geometry (SoCG 86)*, Yorktown Heights, New York, 1986, pp. 216–225.

145. Parallel Algorithms for Some Functions of Two Convex Polygons, (with Michael T. Goodrich). *Proc. 24th Annual Allerton Conf. on Communication, Control, and Computing*, Monticello, Illinois, 1986, pp. 758–767.

146. Efficient Solutions to a Class of Placement Problems, (with Susanne E. Hambrusch). *Proc. 11th Annual Workshop on Graph-Theoretic Concepts in Computer Sci. (WG 85)*, Wuerzburg, West Germany, 1985, pp. 11–21.

147. Parallel Solutions to Geometric Problems, (with Michael T. Goodrich). *Proc. 1985 Int. Conf. on Parallel Processing (ICPP 85)*, St. Charles, Illinois, 1985, pp. 411–417.

148. Solving Tree Problems on a Mesh-Connected Processor Array, (with Susanne E. Hambrusch). *Proc. 26th Annual IEEE Symp. on Foundations of Computer Sci. (FOCS 85)*, Portland, Oregon, 1985, pp. 222–231.

149. Simulations Between Mesh-Connected Processor Arrays. *Proc. 23nd Annual Allerton Conf. on Communication, Control, and Computing*, Monticello, Illinois, 1985, pp. 268–269.

150. Detecting Symmetry in a Planar Figure. *Proc. 22nd Annual Allerton Conf. on Communication, Control, and Computing*, Monticello, Illinois, 1984, pp. 101–102.

151. * Drawing Nonintersecting Segments Between Two Planar Sets. *Proc. 22nd Annual Allerton Conf. on Communication, Control, and Computing*, Monticello, Illinois, 1984, pp. 113–119.

152. Finding Euler Tours in Parallel. *Proc. 17th Annual Conf. on Info. Sciences and Systems (CISS 83)*, Baltimore, Maryland, 1983, pp. 685–689.

153. Dynamic Computational Geometry. *Proc. 24th Annual IEEE Symp. on Foundations of Computer Sci. (FOCS 83)*, Tucson, Arizona, 1983, pp. 92–99.

154. Graph Problems on a Mesh-Connected Processor Array, (with S.R. Kosaraju). *Proc. 14th Annual ACM Symp. on Theory of Computing (STOC 82)*, San Francisco, California, 1982, pp. 345–353.

155. An Adversary-Based Lower Bound for Sorting, (with S. Rao Kosaraju). *Proc. 15th Annual Conf. on Info. Sciences and Systems (CISS 81)*, Baltimore, Maryland, 1981, pp. 7–8.

In Refereed Journals

[Journal papers marked by * have not appeared in conference version.]

156. * Efficient and Secure Pattern Matching with Wildcards Using Lightweight Cryptography (with Javad Darivandpour). Accepted for publication in *Computers & Security*.

157. * Security in Cyber-Enabled Design and Manufacturing: A Survey (with Adam Dachowicz, Siva Chaitanya Chaduvula, and Jitesh H. Panchal). *ASME Journal of Computing and Information Science in Engineering*. Volume 18 No. 4, 4, July 2018, 15 pages.

158. * Secure Co-design: Achieving Optimality without Revealing (with Siva Chaitanya Chaduvula, and Jitesh Panchal). *Journal of Computing and Information Science in Engineering*. Vol. 18, No. 2, March 2018, 14 pages.

159. Secure Collaboration in Engineering Systems Design (with Shumiao Wang, Siddharth Bhandari, Siva Chaitanya Chaduvula, Jitesh Panchal, and Karthik Ramani). *ASME Journal of Computing and Information Science in Engineering (JCISE)*, Vol. 17, No. 4, June 2017, 11 pages.

160. * Microstructure-based Counterfeit Detection in Metal Part Manufacturing (with Adam Dachowicz, Siva Chaitanya Chaduvula, and Jitesh Panchal). *Journal of Materials (JOM)* (the main journal of The Minerals, Metals & Materials Society). November 2017, Volume 69, Issue 11, pp. 2390–2396.

161. * On Approximate Pattern Matching with Thresholds (with Peng Zhang). *Info. Processing Letters.* Vol. 123, 2017, pp. 21–26.

162. * Securing Aggregate Queries for DNA Databases (with Qutaibah Malluhi, Mohamed Nassar, and Abdullatif Shifka). *IEEE Transactions on Cloud Computing.* Volume PP, Issue 99, March 2017, 12 pages.

163. Inhibiting and Detecting Offline Password Cracking using ErsatzPasswords (with Mohammed H. Almeshekah, Chris Gutierrez, Eugene H. Spafford, and Jeff Avery). *ACM Transactions on Privacy and Security.* Volume 19 Issue 3, December 2016 Article No. 9.

164. Similarity Group-by Operators for Multi-dimensional Relational Data (with Ruby Y. Tahboub, Mingjie Tang, Walid G. Aref, Qutaibah M. Malluhi, Mourad Ouzzani, Yasin N. Silva). *IEEE Trans. on Knowledge and Data Engineering*, 28 (2), 2016, pp. 510–523.

165. Security-aware Business Process as a Service by hiding provenance (with Mehdi Bentounssi and Salima Benbernou). *Computer Standards & Interfaces*, 44, 2016, pp. 220–233.

166. * A Scheme for Collaboratively Processing Nearest Neighbor Queries in Oblivious Storage (with Keith Frikken and Shumiao Wang). *EAI Transactions on Collaborative Computing*, 14 (2), 2014.

167. * A Lower-Variance Randomized Algorithm for Approximate String Matching (with Elena Grigorescu and Yi Wu). *Info. Processing Letters*, 113 (18), 2013, pp. 690–692.

168. Incentive Alignment and Risk Perception: An Information Security Application (with Fariborz Farahmand and Eugene H. Spafford). *IEEE Transactions on Engineering Management*, 60 (2), 2013, pp. 238-246

169. * Efficient Relaxed Search in Hierarchically-Clustered Sequence Datasets (with Kai Bader and Christian Grothoff). *Journal of Experimental Algorithmics*, 17 (1), 2012, 18 pages.

170. * Efficient and Practical Approach for Private Record Linkage (with Mohamed Yakout and Ahmed Elmagarmid). *ACM Journal of Data and Information Quality*, 3 (3), 2012, 28 pages.

171. * Running Max/Min Filters using $1 + o(1)$ Comparisons per Sample (with Hao Yuan). *IEEE Transactions on Pattern Analysis and Machine Intelligence (IEEE-PAMI)*, 33 (12) (2011), pp. 2544-2548.

172. * Pattern Matching in the Hamming Distance with Thresholds (with Timothy W. Duket). *Info. Processing Letters*, 111 (14), (2011) pp. 674–677.

173. Asymptotically Efficient Algorithms for Skyline Probabilities of Uncertain Data (with Hao Yuan and Yinian Qi). *ACM Transactions on Database Systems*, 36 (2), (2011).

174. * On the Complexity of Authorization in RBAC under Qualification and Security Constraints (with Yuqing Sun, Qihua Wang, Ninghui Li, and Elisa Bertino). *IEEE Transactions on Dependable and Secure Computing*, 8 (6) (2011), pp. 883–897.

175. * Outsourcing Manufacturing: Secure Price Masking Mechanisms for Purchasing Component Parts (with Vinayak Deshpande, Leroy Schwarz, Marina Blanton, and Keith Frikken). *Production and Operations Management (POMS)*, 20 (2) (2011), pp. 165–180.

176. Dynamic and Efficient Key Management for Access Hierarchies (with Marina Blanton, Nelly Fazio, and Keith B. Frikken). *ACM Transactions on Information and System Security (TISSEC)*, 12 (2009).

177. * A Tree-Covering Problem Arising in Integrity of Tree-Structured Data (with Greg Frederickson and Ashish Kundu). *Info. Processing Letters*, 109 (2008), pp. 79–82.

178. Private Information: To Reveal Or Not To Reveal (with Danfeng Yao, Keith Frikken, and Roberto Tamassia). *ACM Transactions on Information and System Security (TISSEC)*, 12 (2008).

179. An Empirical Study of Automatic Event Reconstruction Systems (with Sundararaman Jeyaraman). *Digital Forensics*, 3(1) (2006), pp. 108–115.

180. Translation-Based Steganography (with Christian Grothoff, Krista Grothoff, Ludmila Alkhutova, and Ryan Stutsman). *Journal of Computer Security*, 17(3) (2009), pp. 269–303.

181. Attribute-Based Access Control with Hidden Policies and Hidden Credentials (with Keith B. Frikken and Jiangtao Li). *IEEE Transactions on Computers*, 55 (2006), pp. 1259–1270.

182. Succinct Representation of Flexible and Privacy-Preserving Access Rights (with Marina Blanton). *The VLDB Journal: The International Journal of Very Large Databases*, 15(4) (2006), pp. 334–354.

183. Rights Protection for Discrete Numeric Streams (with Radu Sion and Sunil Prabhakar). *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 18 (2006), pp. 699–714.

184. A Tree-based Forward Digest Protocol to Verify Data Integrity in Distributed Media Streaming (with Ahsan Habib, Dongyan Xu, Bharat Bhargava, and John Chuang). *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 17 (2005), pp. 1010–1014.

185. Rights Protection for Categorical Data (with Radu Sion and Sunil Prabhakar). *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 17 (2005), pp. 912–926.

186. Secure Outsourcing of Sequence Comparisons (with Jiangtao Li). *International Journal of Information Security*, 2005, pp. 277–287.

187. Adaptive Data Structures for IP Lookups (with Ananth Grama and Ioannis Ioannidis). *ACM Journal of Experimental Algorithmics (JEA)*, 10 (2005), pp. 1–24.

188. * A Survey of Anti-Tamper Technologies, (with Eric D. Bryant and Martin R. Stytz). *CrossTalk, The Journal of Defense Software Engineering*, 17 (2004), pp. 12–16.

189. Reliable Detection of Episodes in Event Sequences, (with Robert Gwadera and Wojciech Szpankowski). *Knowledge and Information Systems Journal (KAIS)*, 7 (2005), pp. 415–437.

190. Rights Protection for Relational Data, (with Radu Sion and Sunil Prabhakar). *IEEE Transactions on Knowledge and Data Engineering (TKDE)*, 16 (2004), pp. 1509–1525.

191. Augmenting LZ-77 with Authentication and Integrity Assurance Capabilities, (with Stefano Lonardi). *Concurrency: Practice and Experience*, 16 (2004), pp. 1063–1076.

192. * Digital Rights Protection, (with Sunil Prabhakar, Keith Frikken, Radu Sion). *IEEE Data Engineering Bulletin*, 27 (2004), pp. 19–26.

193. Efficient Parallel Algorithms for Planar st-Graphs, (with D.Z. Chen and O. Daescu). *Algorithmica*, 35 (2003), pp. 194–215.

194. (Almost) Optimal Parallel Block Access for Range Queries, (with Sunil K. Prabhakar). *Information Sciences*, 157 (2003), pp. 21–31.

195. * Compact Recognizers of Episode Sequences, (with Alberto Apostolico). *Information and Computation*, 174 (2002), pp. 180–192.

196. * Faster Image Template Matching in the Sum of the Absolute Value of Differences Measure. *IEEE Trans. on Image Processing*, 10 (2001), pp. 659–663.

197. * On Connecting Red and Blue Rectangles with Monotone Nonintersecting Rectilinear Paths, (with Danny Z. Chen). *Int. J. on Computational Geometry & Applications*, 11 (2001).

198. * A Randomized Algorithm for Approximate String Matching, (with Frederic Chyzac and Philippe Dumas). *Algorithmica*, 29 (2001), pp. 468–486.

199. Secure Outsourcing of Scientific Computations, (with K.N. Pantazopoulos, John R. Rice, Eugene H. Spafford). *Advances in Computers,* Vol 54, Chapter 6, 2001, pp. 215–272.

200. * On Estimating the Large Entries of a Convolution. *IEEE Trans. on Computers*, 50 (2001), pp. 193–196.

201. Parallel Algorithms for Maximum Matching in Complements of Interval Graphs and Related Problems, (with Marilyn G. Andrews, Danny Z. Chen, D.T. Lee). *Algorithmica*, 26 (2000), pp. 263–289.

202. Parallel Algorithms for Longest Increasing Chains in the Plane and Related Problems, (with Danny Z. Chen and K.S. Klenk). *Parallel Processing Letters*, 9 (1999), pp. 511–520.

203. * An Improved Hypercube Bound for Multi-searching and its Applications. *Int. J. on Computational Geometry & Applications*, 9 (1999), pp. 29–38.

204. Pattern Matching Image Compression: Algorithmic and Empirical Results, (with Yann Genin and Wojciech Szpankowski). *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 21 (1999), pp. 614–627.

205. * Algorithms for Variable Length Subnet Address Assignment, (with Douglas E. Comer). *IEEE Trans. on Computers*, C-47 (1998), pp. 693–699.

206. On the Multisearching Problem for Hypercubes, (with Andreas Fabri). *Computational Geometry: Theory and Applications*, 5 (1996), pp. 293–302.

207. Computing the All-Pairs Longest Chains in the Plane, (with Danny Z. Chen). *Int. J. on Computational Geometry & Applications*, 5 (1995), pp. 257–271.

208. Optimal Parallel Hypercube Algorithms for Polygon Problems, (with Danny Z. Chen). *IEEE Trans. on Computers*, C-44 (1995), pp. 914–922.

209. An Optimal Algorithm for Shortest Paths on Interval and Circular-Arc Graphs, with Applications, (with Danny Z. Chen and D.T. Lee). *Algorithmica*, 14 (1995), pp. 429–441.

210. On the Parallel Complexity of Evaluating Some Sequences of Set Manipulation Operations, (with Michael T. Goodrich and S. Rao Kosaraju). *J. of the ACM*, 41 (1994), pp. 1049–1088.

211. * A Block-Based Mode Selection Model for SIMD/SPMD Heterogeneous Parallel Environments, (with Dan W. Watson, H.J. Siegel, John K. Antonio, Mark A. Nichols). *J. of Parallel and Distributed Computing*, 21 (1994), pp. 271–288.

212. * New Clique and Independent Set Algorithms for Circle Graphs, (with Alberto Apostolico and Susanne E. Hambrusch). *Discrete Appl. Math.* 36 (1992), pp. 1–24. An Erratum by the same authors, correcting a proof, appeared in *Discrete Applied Mathematics*, 41 (1993), pp. 179–180.

213. A Faster Parallel Algorithm for a Matrix Searching Problem. *Algorithmica*, 9 (1993), pp. 156–167.

214. Output-Sensitive Hidden Surface Elimination for Rectangles, (with Michael T. Goodrich and Mark H. Overmars). *Info. and Computation*, 107 (1993), pp. 1–24.

215. Multisearch Techniques: Parallel Data Structures on Mesh-Connected Computers, (with Frank Dehne, Russ Miller, Andrew Rau-Chaplin, Jyh-Jong Tsay). *J. of Parallel and Distributed Computing*, 19 (1993), pp. 1–13.

216. * A Probabilistic Analysis of a Pattern Matching Problem, (with Philippe Jacquet and Wojciech Szpankowski). *Random Structures and Algorithms*, 4 (1993), pp. 191–213.

217. P-Complete Geometric Problems, (with Paul Callahan and Michael T. Goodrich). *Int. J. on Computational Geometry & Applications*, 3 (1993), pp. 443–462.

218. On Parallel Rectilinear Obstacle-Avoiding Paths, (with Danny Z. Chen). *Computational Geometry: Theory and Applications*, 3 (1993), pp. 307–313.

219. An Efficient Parallel Algorithm for the Row Minima of a Totally Monotone Matrix, (with S. Rao Kosaraju). *J. of Algorithms*, 13 (1992), pp. 394–413.

220. * Fast Detection and Display of Symmetry in Outerplanar Graphs, (with Joseph B. Manning). *Discrete Appl. Math.*, 39 (1992), pp. 13–35.

221. On the Parallel-Decomposibility of Geometric Problems, (with Jyh-Jong Tsay). *Algorithmica*, 8 (1992), pp. 209–231.

222. * Parallel Techniques for Computational Geometry. *Proc. of the IEEE*, 80 (1992), pp. 1425–1448. (Invited Paper.)

223. Models and Algorithms for Co-Scheduling Compute-Intensive Tasks on a Network of Workstations, (with Christina Black, Dan C. Marinescu, H.J. Siegel, and Thomas L. Casavant). *J. of Parallel and Distributed Computing*, 16 (1992), pp. 319–327. (Special Issue on Scheduling and Load-Balancing.)

224. Parallel Topological Sorting of Features on a Mesh, (with Susanne E. Hambrusch and Lynn E. TeWinkel). *Algorithmica*, 6 (1991), pp. 762–769. (Special Issue on Parallel Algorithms for Geometric Problems on Digitized Pictures.)

225. An Optimal Parallel Algorithm for the Visibility of a Simple Polygon from a Point, (with Danny Z. Chen and Hubert Wagener). *J. of the ACM*, 38 (1991), pp. 516–533.

226. * Sequence Comparison on the Connection Machine, (with H. Scott McFaddin). *Concurrency: Practice and Experience*, 3 (1991), pp. 89–107.

227. * A Linear Time Algorithm for the Computation of Some Distance Functions between Convex Polygons, (with Celso Ribeiro and Sergio Lifschitz). *RAIRO J. Oper. Res.*, 25 (1991), pp. 413–424.

228. * Computing Some Distance Functions Between Polygons, (with Celso Ribeiro and Sergio Lifschitz). *Pattern Recognition*, 24 (1991), pp. 775–781.

229. Parallel Rectilinear Shortest Paths with Rectangular Obstacles, (with Danny Z. Chen). *Computational Geometry: Theory and Applications*, 1 (1991), pp. 79–113.

230. * On Performing Robust Order Statistics on Tree-Structured Dictionary Machines, (with Michael T. Goodrich). *J. of Parallel and Distributed Computing*, 9 (1990), pp. 69–76.

231. Efficient Parallel Algorithms for String Editing and Related Problems, (with A. Apostolico, L. Larmore, and H.S. McFaddin). *SIAM J. on Computing*, 19 (1990), pp. 968–988.

232. An Efficient Algorithm for Maxdominance, With Applications, (with S. Rao Kosaraju). *Algorithmica*, 4 (1989), pp. 221–236.

233. Cascading Divide-and-Conquer: A Technique for Designing Parallel Algorithms, (with R. Cole and Michael T. Goodrich). *SIAM J. on Computing*, 18 (1989), pp. 499–532.

234. * An Optimal Parallel Algorithm for the Minimum Circle-Cover Problem, (with Danny Z. Chen). *Info. Processing Letters*, 32 (1989), pp. 159–165.

235. Optimal Simulations Between Mesh-Connected Arrays of Processors, (with S. Rao Kosaraju). *J. of the ACM*, 35 (1988), pp. 635–650.

236. On Multidimensional Arrays of Processors. *IEEE Trans. on Computers*, C-37 (1988), pp. 1306–1309. Reprinted in 1994 in *Interconnection Networks for High-Performance Parallel Computers*, I.D. Scherson and A.S. Youssef (Ed.), IEEE Computer Society Press.

237. * Finding a Minimum Independent Dominating Set in a Permutation Graph, (with G.K. Manacher and J. Urrutia). *Discrete Appl. Math.*, 21 (1988), pp. 177–183.

238. Fast Detection and Display of Symmetry in Trees, (with J.B. Manning). *Congressus Numerantium*, 64 (1988), pp. 159–169.

239. Parallel Algorithms for Some Functions of Two Convex Polygons, (with Michael T. Goodrich). *Algorithmica*, 3 (1988), pp. 535–548.

240. Efficient Solutions to Some Transportation Problems, With Applications to Minimizing Robot Arm Travel, (with S. Rao Kosaraju). *SIAM J. on Computing*, 17 (1988), pp. 849–869.

241. Sorting With Efficient Use of Special-Purpose Sorters, (with Greg N. Frederickson and S. Rao Kosaraju). *Info. Processing Letters*, 27 (1988), pp. 13–15.

242. Efficient Algorithms for Common Transversals, (with C. Bajaj). *Info. Processing Letters*, 25 (1987), pp. 87–91.

243. On Bipartite Matchings of Minimum Density, (with Susanne E. Hambrusch). *J. of Algorithms*, 8 (1987), pp. 480–502.

244. A Note on Finding a Maximum Empty Rectangle, (with Greg N. Frederickson). *Discrete Appl. Math.*, 13 (1986), pp. 87–91.

245. Solving Tree Problems on a Mesh-Connected Processor Array, (with Susanne E. Hambrusch). *Info. and Control*, 69 (1986), pp. 168–187.

246. Computing the Convex Hull of Line Intersections. *J. of Algorithms*, 7 (1986), pp. 285–288.

247. Optimal Rotation Problems in Channel Routing, (with Susanne E. Hambrusch). *IEEE Trans. on Computers*, C-35 (1986), pp. 843–847.

248. Efficient Parallel Solutions to Some Geometric Problems, (with M.T. Goodrich). *J. of Parallel and Distributed Computing*, 3 (1986), pp. 492–507.

249. An Assignment Algorithm With Applications to Integrated Circuit Layout, (with Susanne E. Hambrusch). *Discrete Appl. Math.*, 13 (1986), pp. 9–22.

250. A Generalized Dictionary Machine for VLSI, (with S. Rao Kosaraju). *IEEE Trans. on Computers*, C-34 (1985), pp. 151–155.

251. Some Dynamic Computational Geometry Problems. *Computers and Math. w. Appl.*, 11 (1985), pp. 1171–1181.

252. A Matching Problem in the Plane. *J. of Computer and System Sciences*, 31 (1985), pp. 63–70.

253. On Symmetry Detection. *IEEE Trans. on Computers*, C-34 (1985), pp. 663–666.

254. Graph Problems on a Mesh-Connected Processor Array, (with S. Rao Kosaraju). *J. of the ACM*, 31 (1984), pp. 649–667.

255. Checking Similarity of Planar Figures. *Int. J. of Computer and Info. Sciences*, 13 (1984), pp. 279–290.

256. Finding Euler Tours in Parallel, (with Uzi Vishkin). *J. of Computer and System Sciences*, 29 (1984), pp. 330–337.

257. Parallel Strong Orientation of an Undirected Graph. *Info. Proc. Letters*, 18 (1984), pp. 37–39.

258. A Linear Time Algorithm for the Hausdorff Distance Between Convex Polygons. *Info. Processing Letters*, 17 (1983), pp. 207–209.

259. Finding the Cyclic index of an Irreducible, Nonnegative Matrix. *SIAM J. on Computing*, 11 (1982), pp. 567–570.

260. An Adversary-Based Lower Bound for Sorting, (with S. Rao Kosaraju). *Info. Processing Letters*, 13 (1981), pp. 55–57.

Books, Book Chapters:

261. Algorithms and Theory of Computation Handbook, Volume 1: General Concepts and Techniques (Ed. with Marina Blanton), Chapman and Hall/CRC press, 2009, 1938 pages.

262. Algorithms and Theory of Computation Handbook, Volume 2: Special Topics and Techniques (Ed. with Marina Blanton), Chapman and Hall/CRC press, 2009.

263. Privacy-Preserving Cryptographic Protocols (with Keith B. Frikken). *Digital Privacy Theories, Technologies, and Practices*, Alessandro Acquisiti, Stefanos Gritzalis, Costas Lambrinoudakis, and Sabrina e Capitani di Vimercati (eds), Auerbach, 2008.

264. Digital Rights Management, (with Keith Frikken, Carrie Black, Susan Overstreet, Pooja Bhatia). *Practical Handbook of Internet Computing*, Munindar P. Singh (Ed.), CRC Press, 2004.

265. Protocols for Secure Remote Database Access with Approximate Matching, (with Kevin Du). *Recent Advances in Secure and Private E-Commerce*, Kluwer Academic Publishers, 2001.

266. Deterministic Parallel Computational Geometry, (with Danny Z. Chen). *Computational Geometry*, Joerg-Rudiger Sack and Jorge Urrutia (Eds.), 1999.

267. Handbook of Algorithms and Theory of Computation (Ed.), CRC Press, 1999, 1296 pages.

268. Parallel Computations of Levenshtein Distances, (with Alberto Apostolico). *Pattern Matching Algorithms and Applications*, Alberto Apostolico and Zvi Galil (Eds.), Oxford University Press, 1997, pp. 143–184.

269. Parallel Computational Geometry. *Handbook of Parallel and Distributed Computing*, Albert Zomaya (Ed.), McGraw-Hill, 1996, pp. 404–428.

270. Mixed-mode System Heterogeneous Computing, (with H. J. Siegel, Muthucumaru Maheswaran, Dan Watson, John Antonio). *Heterogeneous Computing*. Mary M. Eshaghian (Ed.), Artech House, 1996, pp. 19–66.

271. Parallel Computational Geometry, (with Danny Z. Chen). *Parallel Computing: Paradigms and Applications*, Albert Zomaya (Ed.), International Thomson, 1996, pp. 162–197.

272. Deterministic Parallel Computational Geometry, (with Michael T. Goodrich). *Synthesis of Parallel Algorithms*, John H. Reif (Ed.), Morgan Kaufmann, 1993, pp. 497–536.

Other Publications

273. Security Issues in Collaborative Computing (abstract of keynote talk). *Lecture Notes in Computer Science, Vol. 4112*, Springer Verlag, *Proc. of the 12th Annual International Computing and Combinatorics Conference (COCOON 06)*, Taipei, Taiwan, August 2006, p. 2.

274. A Survey of Watermarking Techniques for Non-Media Digital Objects (abstract of keynote talk). *Proc. Australasian Information Security Workshop (AISW 05)*, Newcastle, Australia, January 2005, p. 73.

275. Extreme Events Involving Computer Systems and Networks, *Report of the Workshop on Extreme Events*, National Center for Atmospheric Research, Boulder, Colorado, 2000, pp. 27–28.

276. Program Chair's Message. *Proc. Second Merged IPPS/SPDP Symposium*, San Juan, Puerto Rico, 1999, p. xvii.

277. Section Advisor's Introduction. *Handbook of Computer Science and Engineering,* CRC Press, 1997, pp. 29–31.

278. Issues on the Algorithm-Software Continuum (position statement as panel member). *Proc. 4th Symposium on the Frontiers of Massively Parallel Computation*, McLean, Virginia, 1992, p. 212.

279. Editor's Foreword. *Algorithmica* Special Issue on Computational Geometry, **8** (1992), pp. 343–344.

280. La Multiplication en Parallele des Matrices Concaves et ses Applications, *Actes des Journees du Laboratoire d'Informatique de Paris-Nord*, Villetaneuse, France, 1989, pp. 179–198.

Patents Issued

281. U.S. Patent 7,870,399, issued on January 11, 2011; titled: Software trusted platform module and application security wrapper (with Eric D. Bryant, Avni Harilal Rambhia, and John R. Rice)

282. U.S. Patent 7,853,018, issued on December 14, 2010; titled: Method and Apparatus for Hiding a Private Key (with Eric D. Bryant)

283. U.S. Patent 7,757,097 B2, issued on July 13, 2010; titled: Method and system for tamperproofing software (with Hoi Chang)

284. U.S. Patent 7,539,872, issued on May 26, 2009; titled: Method and System for Rights Assessment over Digital Data through Watermarking (with Radu Sion and Sunil Prabhakar)

285. U.S. Patent 7,287,166, issued on October 23, 2007; titled: Guards for Application in Software Tamperproofing (with Hoi Chang and John R. Rice)

286. U.S. Patent 2007/0244693 A1, issued on October 18, 2007; titled: Natural Language Watermarking (with Srinivas Bangalore, Dilek Z. Hakkani-Tur, Giuseppe Riccardi, Mercan Topkara, Umut Topkara)

287. U.S. Patent 6,941,463, issued on September 9, 2005; titled: Secure Computational Outsourcing Techniques (with John R. Rice, Eugene H. Spafford, and Kostas N. Pantazopoulos)

288. U.S. Patent 6,957,341, issued on October 18, 2005; titled: Method and System for Secure Computational Outsourcing and Disguise (with John R. Rice)

RESEARCH CONTRACTS AND GRANTS RECEIVED

2017–18	$120,000	Naval Postgraduate School, Grant NPS-FOA-16-001 Title: Computing without Revealing: A Cryptographic Approach to eProcurement (with J. Panchal)
2016–18	$154,327	Qatar National Research Fund, Grant NPRP X-063-1-014 Title: The Garbled Computer: Towards Computing without Seeing (the above amount is Atallah's share of budget – project has many other co-PIs, involves multiple universities)
2013–18	$1,000,000	National Science Foundation, Grant CPS-1329979 Title: Foundations of Cyber-Physical Infrastructure for Creative Design and Making of Cyber-physical Products (with J. Panchal and K. Ramani)
2010–15	$25,000,000	National Science Foundation, STC Grant Title: Emerging Frontiers of Science of Information (with W. Szpankowski as PI, and many other co-PIs)
2010–14	$350,124	Qatar National Research Fund, Grant NPRP 096221090 Title: Trusted Computation-intensive Services in Cloud Computing Environments (the above amount is Atallah's share of budget – another $700,000 is budgeted for Qatar University partners Q. Malluhi and K. Khan)
2009–12	$499,883	National Science Foundation, Grant CNS-0913875 Title: A Computational Framework for Marking Physical Objects against Counterfeiting and Tampering (with Daniel Aliaga)
2009–12	$267,816	National Science Foundation, Grant CNS-0915436 Title: Privacy Constrained Searching (with Keith B. Frikken)
2009–12	$377,000	Air Force Office of Scientific Research, Contract FA9550-09-1-0223 Title: Techniques for Secure and Reliable Computational Outsourcing (with Marina V. Blanton)
2006–09	$400,000	National Science Foundation, CyberTrust Grant CNS-0627488 Title: Improving the Privacy and Security of Online Survey Data Collection, Storage, and Processing (with J. Mills)
2003–07	$800,000	National Science Foundation, ITR Grant 0325345-IIS Title: Secure Supply-Chain Protocols (with V. Deshpande and L. Schwarz)
2003–06	$276,274	National Science Foundation, ITR Grant 0312357-IIS Title: Distributed Data Mining to Protect Information Privacy (with C. Clifton)
2003–05	$150,000	National Science Foundation, ITR Grant 0242421-IIS Title: Watermarking Relational Databases (with S. Prabhakar)

2002–05	$273,791	Office of Naval Research, Contract N00014-02-1-0364 Title: General Paradigms for Watermarking and Tamperproofing Multi-Type/Media Documents
2004–	$20,000	Motorola Title: Secure Supply-Chain Collaborations (with V. Deshpande and L. Schwarz)
2002–03	$29,500	Discovery Park e-Enterprise Center Title: Secure Supply-Chain Collaboration (with L. Schwarz and V. Deshpande)
2002–05	$55,423	National Science Foundation, Grant 0219560-IIS Title: Private Prediction Using Selective Models
2001–02	$100,000	Trask Trust Fund Title: Software Tamperproofing (with J.T. Korb and J.R. Rice)
2001–02	$40,118	Lilly Endowment Inc. Title: Watermarking Semi-Structured Content: XML and DBMS (with S.K. Prabhakar)
2001–02	$36,688	Lilly Endowment Inc. Title: Natural Language Watermarking: Watermarking Text-Meaning Representation Trees (with V. Raskin)
2001–02	$119,860	Hewlett Packard Title: Curriculum in Mobile Communications Projects (with J.O. Allebach–PI, C.A. Bouman, G.T.C. Chiu, E.J. Coyle, E.J. Delp, L. Jamieson, J. Krogmeier, C. Rosenberg)
2000–01	$25,623	Lilly Endowment Inc. Title: Protocols for Secure Remote Database Access
2000–01	$21,113	Lilly Endowment Inc. Title: Randomness in Computer Security (with S.S. Wagstaff)
2000–01	$24,507	Lilly Endowment Inc. Title: Natural Language Watermarking: Enhancing Resilience and Implementation (with V. Raskin)
2000–01	$36,702	Lilly Endowment Inc. Title: Privacy-Enhancing Audit and Intrusion Detection (with S.K. Prabhakar)
1999–00	$21,685	Lilly Endowment Inc. Title: A New Approach for Tamperproofing Software
1999–00	$36,685	Lilly Endowment Inc. Title: Watermarking and Quadratic Residues (with S.S. Wagstaff)

1999–00	$39,000	Lilly Endowment Inc. Title: Database Support for Information Security (with S.K. Prabhakar)
1999–00	$36,685	Lilly Endowment Inc. Title: Natural Language Processing Techniques for Information Security (with V. Raskin)
1999–03	$360,844	National Science Foundation, Grant EIA-9903545 Title: Audit Trails: Content, Storage and Processing (with E.H. Spafford)
1999–02	$5,000	National Science Foundation, REU supplement to Grant 9903545-EIA Title: Audit Trails: Content, Storage and Processing (with E.H. Spafford)
1997	$5,000	Microsoft
1996–99	$799,348	DARPA, Contract F30602-96-1-0334 Title: Software Tools for Enhanced Computer Security (with E.H. Spafford–PI, S.S. Wagstaff, A.L. Hosking, and C.E. Brodley)
1996–98	$111,222	National Security Agency, Contract MDA904-96-1-0116 Title: Pattern Matching Techniques for Computer Misuse and Anomaly Detection (with E.H. Spafford)
1996–98	$40,598	Office for Research and Development, Contract 96-F152200-000 Title: Audit Data Reduction and Misuse Detection: A Pattern Matching Approach (with E.H. Spafford)
1995–96	$150,000	IBM Title: Project Purdue On-Line (with A. K. Elmagarmid, A. Joshi, E. N. Houstis, S. Weerawarana A. P. Mathur, J. R. Rice)
1992–96	$212,457	National Science Foundation, Grant 9202807-CCR Title: Parallel Algorithms for Geometric Problems
1990–93	$256,216	Air Force Office of Scientific Research, Contract AFOSR-90-0107 Title: Efficient Algorithmic Techniques for Combinatorial Problems (with A. Apostolico, W. Szpankowski)
1989–92	$373,000	National Library of Medicine, Grant R01-LM05118 Title: Algorithms for Macromolecular Structure Analysis (with A. Apostolico, P.T. Gilham, W. Szpankowski, H.L. Weith)
1988–92	$320,000	Office of Naval Research, Contract N00014-84-K-0502 Title: Parallel Algorithms: Design, Analysis, and Implementation (with Susanne E. Hambrusch)

1986–88	$67,763	National Science Foundation, Grant DCR-8602385 Title: High-Level Systems for Scientific Computing (with W.R. Dyksen)
1986–88	$144,583	Office of Naval Research, Grant N00014-84-K-0502 Title: Parallel Algorithms: Design, Analysis, and Implementation (with Susanne E. Hambrusch)
1986–88	$14,700	Purdue Research Foundation XR Grant
1986–87	$60,000	Sperry Title: Parallel Processing of Database Operations (with B. Bhargava)
1986	$25,000	SUN Microsystems
1986–87	$117,084	National Science Foundation, Grant DCR-8612590 Title: A Laboratory for Electronic Prototyping (with C. Bajaj and C. M. Hoffmann)
1986–91	$4,246,350	Office of Naval Research, URI N00014-86-K-0689 Title: Computational Combinatorics (with T. Morin, S. Abhyankar, V. Chandru, C. Coullard, G. N. Frederickson, S. E. Hambrusch, R. Rardin, D. Wagner, R. Wong)
1985	$65,970	Tektronics
1985–90	$312,500	National Science Foundation, Grant DCR-8451393 Title: Presidential Young Investigator
1985–90	$187,500	AT&T Information Systems Title: Design and Analysis of Algorithms (matching funds for the above NSF PYI grant)
1985–86	$60,000	Sperry Title: Parallel Processing of Database Operations (with B. Bhargava)
1984	$3,500	Purdue Research Foundation XL Grant (I declined to accept the award because the above Sperry grant funded the project)
1984–86	$100,573	Office of Naval Research, Grant N00014-84-K-0502 Title: Parallel Algorithms and VLSI Computation (with Susanne E. Hambrusch)
1984–85	$45,000	Sperry Title: Parallel Computation (with D.B. Gannon)

OTHER PROFESSIONAL SERVICE / RECOGNITION

Panels, Proposal Reviews

- Served on External Review Committee for the Department of Computer Science and Engineering of the American University in Beirut (2013)
- Served on National Academies Panel on Digitization and Communications Science (2007–8)
- Served on External Review Committee for SUNY Buffalo's Department of Computer Science and Engineering (2008)
- Served on NSF Committee of Visitors for the oversight of the programs in the CISE Division of Computer and Computation Research (1993)
- Served on many NSF panels – both for proposal reviews and for direction-setting workshops
- Served New York State's Education Dept. in a 3-member Site Visit Committee to SUNY Buffalo, in the framework of the State's Statewide Doctoral Program Review (1990).
- Served as Consultant to the Ohio Board of Regents Investment Fund (1995)
- Served on a Canadian NSERC Expert Committee for a Site Visit to University of Ottawa (1996)
- Reviewed research proposals for
  - American Mathematical Society
  - Army Research Office
  - National Science Foundation
  - Natural Sciences and Engineering Research Council of Canada
  - National Security Agency Mathematical Sciences Program
  - Swedish Research Council for Engineering Sciences
  - Ohio Board of Regents
  - Idaho Board of Education

Other Invited Talks

[Does not include those listed earlier under "Distinguished Lecture Series at Universities" or under "Conference Talks Given as Keynote or Invited Speaker"]

2015 Goldman Sachs
2013 Qatar University
2012 Univ. of Paris 5
2011 Tech. Univ. Munich
2011 Rome Laboratory
2011 King Abdullah Univ. of Science and Technology
2011 Qatar University

2009 Shandong Univ.
2009 Rose-Hulman Inst. of Tech.
2009 American Univ. of Beirut
2008 Northrop Grumman Corp.
2008 Univ. of Montreal
2008 Syracuse Univ.
2007 Lockheed Martin Corp.
2006 SUNY at Buffalo
2006 American Univ. of Beirut
2006 Notre Dame Univ., Lebanon
2006 Univ. of Sharjah, UAE
2006 IUPUI
2005 Ecole Polytechnique, France
2004 Univ. of Illinois at Urbana-Champaign
2003 Univ. of Arizona
2001 Univ. of Illinois at Urbana-Champaign
2001 Univ. of Notre Dame
2001 Johns Hopkins Univ.
2001 Univ. of New Mexico
2000 Case Western Reserve Univ.
2000 Johns Hopkins Univ.
2000 Univ. of Maryland at College Park
2000 Computer Security Institute
1999 American Univ. of Beirut
1999 Computer Security Institute
1998 Schlumberger
1998 DARPA
1998 NSA
1998 MITRE
1996 Institut National de Recherche en Informatique et en Automatique (INRIA), France
1993 Georgia Inst. of Technology
1993 National Chung Cheng Univ., Taiwan
1992 Institut National de Recherche en Informatique et en Automatique (INRIA), France
1992 Univ. of North Texas
1991 Univ. of Maryland at College Park
1990 Univ. of Paris 7 Advanced School on Combinatorial Pattern Matching
1989 Univ. of Paris 13
1988 Northwestern Univ.
1988 SUNY at Stony Brook
1988 Rensselaer Polytechnic Institute
1988 Univ. of Pittsburgh
1988 Univ. of California at Davis
1988 Kestrel Institute
1988 RIACS Institute, NASA Ames Research Center
1988 Univ. of Tennessee

1988 Johns Hopkins Univ.
1988 SUNY at Buffalo
1988 AT&T Bell Laboratories
1986 Univ. of Maryland at College Park
1986 Washington Univ. in St. Louis
1984 Johns Hopkins Univ.
1982 AT&T Bell Laboratories
1982 Columbia Univ.
1982 Ohio State Univ.
1982 Purdue Univ.
1982 Rensselaer Polytechnic Institute

Refereeing for Journals and Conferences

ACM Trans. on Computer Systems
ACM Symp. on Computational Geometry
ACM-SIAM Symp. on Discrete Algorithms
Acta Informatica
Advances in Computing Research
Advances in Engineering Software
Algorithmica
Combinatorica
Computational Geometry: Theory & Applications
Discrete and Computational Geometry
IEEE Computer
IEEE Security and Privacy
IEEE Trans. on Biomedical Engineering
IEEE Trans. on Circuits and Systems
IEEE Trans. on Computers
IEEE Trans. on Pattern Analysis and Machine Intelligence
IEEE Trans. on Software Engineering
IEEE Trans. on Software Engineering and Methodology
IEEE Distributed Computing Systems Conf.
IEEE Int. Parallel Processing Symp.
IEEE Symp. on Parallel and Distributed Processing
Info. Processing Letters
Int. Colloq. on Automata, Languages, and Programming
Int. Conf. on Computing and Information
Int. Conf. on Distributed Computing Systems
Int. Conf. on Parallel Processing
Int. Conf. on Supercomputing
Int. J. on Computational Geometry & Applications
Int. J. of Computer Aided VLSI Design
Int. J. of Computer and Info. Sciences
Int. J. of Modeling and Simulation
Int. J. of Parallel Programming

J. of Algorithms
J. of the ACM
J. of Computer and System Sciences
J. of Intelligent and Fuzzy Systems
J. of Parallel and Distributed Computing
Mathematical Programming
Operations Research Letters
Parallel Processing Letters
Proceedings of the IEEE
SIAM J. on Computing
SIAM J. on Discrete Mathematics
Software Practice and Experience
Supercomputing Conf.
Symp. on Parallel Algorithms and Architectures
Symp. on Theoretical Aspects of Computer Science
Workshop on Algorithms and Data Structures
... and all the journals/conferences I served as editor or PC member

Reviewing of Books and Proposals for

Mathematics of Computation
Morgan Kaufmann Publishers
M.I.T. Press
Oxford University Press
John Wiley & Sons
Zentralblatt fuer Mathematik

STUDENTS

Note: All Theses are Ph.D. unless it is explicitly specified that they are M.S.

Ph.D. Student Thesis Supervision

- Michael T. Goodrich (1987). Currently Chancelor's Professor of Computer Science, University of California, Irvine, formerly Professor of Computer Science at Johns Hopkins University
- Jyh-Jong Tsay (1990). Currently Associate Professor at the Institute of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan.
- Joseph B. Manning (1990). Currently Permanent College Lecturer, Computer Science, University College, Cork, Ireland.
- Danny Z. Chen (1992). Currently Professor of Computer Science and Engineering, University of Notre Dame, South Bend, Indiana.
- Wenliang (Kevin) Du (2001). (Co-advisor: E.H. Spafford.) Currently Professor of Computer Science at Syracuse University

- Hoi Chang (2003). Independent software entrepreneur, formerly Chief Software Architect, Arxan Technologies Inc
- Radu Sion (2004). (Co-advisor: S. Prabhakar.) Currently Associate Professor of Computer Science at SUNY Stony Brook
- Keith B. Frikken (2005). Currently with Google, formerly Associate Professor of Computer Science at Miami University in Ohio
- Robert Gwadera (2005). (Co-advisor: W. Szpankowski). Currently Postdoc at the University of Lugano, Switzerland
- Jiangtao Li (2006). (Co-advisor: N. Li.) Currently with Facebook, formerly Security Architect at Intel
- Marina Blanton (2007). Currently Assistant Professor of Computer Science and Engineering, Uni versity of Notre Dame, South Bend, Indiana
- Mercan Topkara (2007). (Co-advisor: Cristina Nita-Rotaru.) Currently Research Engineer at JW Player, formerly Research Staff Member at IBM Thomas J. Watson Research Center
- Umut Topkara (2007). Currently Research Engineer at JW Player, formerly Research Scientist at IBM Thomas J. Watson Research Center
- Hao Yuan (2010). Currently Assistant Professor of Computer Science at City University in Hong Kong
- Sundararaman Jeyaraman (2011). Currently Principal Engineer at FireEye, Inc, formerly Senior Software Architect at Cisco Systems Inc
- Shumiao Wang (2014). Currently Reliability Engineer, Google, Mountain View, California
- Mohammed Almeshekah (2015). Currently Assistant Professor, King Saud University, Riyadh, Saudi Arabia
- Siva Chaitanya Chaduvula
- Adam Dachowicz
- Javad Darivandpour
- Duc V Le
- Shoaib Amjad Khan

Other Student Thesis Committees:

In Computer Science:

Andre Bondi, David Mount, Teemu Kerola, Bhasker Parthasarathy, Shuhshen Pan, Ravi Janardan, Y-Huei Wang, Stefan Bechtolsheim, Ko-Yang Wang, Susan Rodger, John Riedl, Ajay Gupta, Lynn TeWinkel, Tamal Dey, Bonita Rais, Yungho Leu, Malcom C. Fields, Brian L. Stuart, Carl R. Gritter, Hyung-Yi T. Tu, Hiram Hunt, Po Ting Wu, Kuei Yu Wang, Fausto Bernardini, Hong Wang, Houzhi Xu, Praerit Garg, Evaggelia Pitoura, Mihai G. Sirbu, Ioana M. Boier Martin, Constantine C. Pantazopoulos, Bozhidar D. Dimitrov, Katherine E. Price (M.S. thesis), Jincheng Chen, Reuben Pasquini, Diego Zamboni, Tom Daniels, Stefano Lonardi, Young Jun Kim, Dow-Yung Yang, Chuan-Ming Liu, Joao Cangussu, Tian Zhao, Vanessa Cangussu (MS), Stephanie Miller (MS Thesis), Ravishankar Ithal (MS Thesis), Kyungkoo Jun, Benjamin Kuperman, Murat Kantarcioglu, Baskar Sridharan, Jaideep Vaidya, Weichao Wang, Ioannis Ioannidis, Mohamed Hefeeda, Wei Jiang, Yang Yu, Reynold Cheng, Paul Williams, Yuni Xia, Yuhui Zhong, Ossama Younis, Florian Buchholtz, James Early, Paul Ruth, Mahesh Tripunitara, Rajeev Gopalakrishna, Ji-Won Byun, Xuxian Jiang, Ethan Blanton, Tomek Czajka, Mummoorthy Murugesan Maleq Khan, Barry Wittman, Yongwook Choi, Jing Dong, Omar Alrawi (MS Thesis) Zhen Zhu, Yinian Qi, Sael Lee, Samuel Kerr (MS), Tyler Wykoff, Rohit Jain Brendan Saltaformaggio, Hasini Gunasinghe, Mohammad-Mohsen Minaei-Bidgoli, Shagufta Mehnaz Yudong Cao, Shuxian Jiang, Debajyoti Das, Alexandre Block, Eman Alnabati, Tamalika Mukherjee Mingyuan Wang

In Industrial Engr:

Chin-Wen Lin, Widodo Sulistyono

In Electrical and Computer Engr:

Hyun S. Yang, Robert J. Safranek, Pradeep K. Dubey, Daniel W. Watson, Dennis M. Hawver, Ray A. Kamin III, Chao-Chun Wang, Allan D. Knies, Min Tan, Muthucumaru Maheswaran, Mitch Theys, Tracy Braun Richard Kennell, Hilmi Ozdoganoglu (MS Thesis), Issa Khalil

In Linguistics:

Craig J. McDonough, Dina Mohamed (M.A. Thesis) Christian F. Hempelmann, Katrina Triezenberg, Whitney Vandiver Simon Slobodnik (M.A. Thesis)

Outside Purdue:

Andreas Fabri, Ecole Nationale Superieure des Mines de Paris Katrin Dobrindt, Ecole Nationale Superieure des Mines de Paris

Nou Dadoun, Univ. of British-Columbia
Weifa Liang, Australian National Univ.
Paulina Wegrowicz, McGill Univ. (MS thesis)
Nathan Evans, Tech. U. Munich
Charles Helou, U. of Montreal

Courses Taught

[All at Purdue University]

Regular courses:

CS 158 Programming
CS 182 Foundations of Computer Science
CS 251 Data Structures
CS 381 Intro. to the Analysis of Algorithms
CS 440 Intro. to File and Database Systems
CS 426 Computer Security
CS 555 Cryptography and Data Security
CS 572 Heuristic Problem Solving
CS 580 Algorithm Design, Analysis and Implementation
CS 650 Computational Aspects of Parallel Processing

Independent study courses (1 or 2 students per course):

CS 490 Image Template Matching
CS 590 Parallel Algorithms
CS 590 Expert System Buiding
CS 590 Computer Vision
CS 590 Parallel Computation I
CS 590 Parallel Computation II
CS 590 Security Techniques for Electronic Commerce
CS 590 Outsourcing Data Storage Securely
CS 590 Topics in Computer Security
CS 590 Watermarking Multimedia
CS 590 Audit Trail Data Compression
CS 590 Intrusion Detection
CS 590 Database Support for Audit Trails and Intrusion Detection
CS 590 Issues in Browser Security
CS 590 Internet Platform Architectures
CS 590 Watermarking Natural Language Text
CS 590 Stepping Stone Detection
CS 590 Code Obfuscation Techniques
CS 590 Secure P2P Networking
CS 590 Secure Multi-party Computing
CS 590 Confidential Data Outsourcing
CS 590 Secure Computations In Cloud

Note: Excellent teaching evaluations. Selected among Top Ten Outstanding Teachers for the College of Science in 1994, 1995, and the Outstanding Teacher for 2004 and 2006. Advisor to Purdue UPE student organization (2003–04), Purdue ACM student organization (1995–97) and to WICS (Women in Computer Science) student organization (1982–84).

Purdue Continuing-Education Short-Course Lectures on Information Security

- Risk Analysis
- Detecting Computer Crime
- Legislation and Standards
- Threats from Malicious Software

UNIVERSITY COMMITTEE DUTIES

[All at Purdue University]

Computer Science Department Committees:

Undergraduate (1982–83, 83–84, 86–99)
Colloquia (1984–85)
Industrial Relations (1984–85, 85–86)
5-Year Plan (1985–86)
Faculty Recruiting (1987–88, 90–95 as Chair, 97–99, 02–03, 03–05 as Chair, 11–12)
Graduate (1988–90, 95–96 as Chair, 96–97, 98–00, 05–06)
Promotions (1989–)
Upsilon Pi Epsilon Membership committee (many times)
690S Coordinator (many times)
Halstead Award selection committee (many times)
Purdue Research Foundation grants selection committee (many times)
ECE Liaison (many times)
Departmental Advisory Committee (00–01)
Head Search Committee (many times, often as Chair)
CS Dept. Executive Committee (many times)
Mentoring Committee (many times)
Awards Committee (many times)
Strategic Planning Steering Committee (2017)

College of Science Committees:

International Travel Ranking
XR Grants
XL Grants
Representative of Computer Science Dept on Faculty Council (1990–96,2016–2017)
Faculty Affairs Committee (1990–93)
Promotions (1991–93, 03–05, 18–20)

Distinguished Professor Ad-Hoc Committee (as Chair: 1994–95; as member: 96–97, 99–00, 06, 15, 18)

Educational Policy and Curriculum Committee (1994–95)

University Faculty Scholar Committee (2000–01)

Grade appeals (2005–6)

Co-chair of Engagement group in strategic planning committee

Strategic Plan Oversight Committee (2009–10)

College of Science Faculty Council Committee (2016–17)

University Committees:

Agriculture and Artificial Intelligence (1984–85)

University Senate Member (1991–92)

Library Committee (1998)

Computing Research Institute Director Search Committee (1999–00)

Research Computing and Communications Advisory Committee (1999–00)

Trask Venture Fund Committee (2001–2003)

Homeland Security Institute Executive Committee (2003–5)

Distinguished Professor Nomination Committee (1994)

Commitee on Research Integrity (2009–)

Co-Chair of Task Force on Retirement Benefits (2008–2010)

Faculty Awards and Recognition Committee (2015–16)

Provost's Standing Committee on Reputational Stewardship (2016–2019)

Provost Search Committee (2017)

Other Duties:

Member of Internal Advisory Board of Center for Education and Research in Information Assurance and Security (1998-)

Member of Executive Committee of Discovery Park's e-Enterprise Center (2002-)

Member of Discovery Park Strategic Plan Task Force (2002)

Member of Internal Advisory Board for Purdue's Homeland Security Institute (2002)