

Rebecca N. Wright

DIMACS and Department of Computer Science
Rutgers University
CoRE Building, Room 404
Piscataway, NJ 08854 USA

Phone: +1 (732) 445-5931
Fax: +1 (732) 445-5932
E-mail: rebecca.wright@rutgers.edu
Web: www.cs.rutgers.edu/~rebecca.wright

Research Interests

Computer and communications security, particularly in the areas of privacy, cryptographic protocols, and networked computing. Designing protocols, systems, and services that perform their specified computational or communication functions even if some of the participants or underlying components behave maliciously.

Education

Yale University

New Haven, CT

Ph.D. in Computer Science, December 1994.

Dissertation: *Achieving Perfect Secrecy Using Correlated Random Variables*.

Advisor: Professor Michael J. Fischer.

M.S. in Computer Science, May 1992.

Columbia University

New York, NY

A.B., May 1988.

Double major in Computer Science and Mathematics.

Professional Experience

Rutgers University

Piscataway, NJ

Professor

July 2010 – present

Director, DIMACS

September 2011 – present

Deputy Director, DIMACS

September 2007 – August 2011

Associate Professor

September 2007 – June 2010

Engaged in research in security and privacy with a focus on privacy-preserving distributed protocols, foundations of networked computing, and voter registration databases. Setting direction for DIMACS, running programs, and obtaining funding.

Stevens Institute of Technology
Hoboken, NJ

Professor
September 2006 – July 2007

Associate Professor
September 2002 – August 2006

Conducted research in privacy and security with a focus on privacy-preserving data mining and other technologies that balance individual needs such as privacy with collective needs such as network survivability and public safety. Introduced privacy-preserving solutions for Bayesian networks, clustering, frequency mining, and k -anonymization. Co-developed a new cybersecurity undergraduate degree program.

DIMACS, Rutgers University
Piscataway, NJ

Visiting Research Associate
March–August 2002

Conducted research in privacy-preserving data mining and in shared-memory protocols resilient to malicious process behavior.

AT&T Labs—Research
Florham Park, NJ

Principal Technical Staff Member
1999 – 2002

Senior Technical Staff Member
1996 – 1999

Developed a broad research program in computer and communications security for distributed computer networks, spanning mathematical and empirical analysis of secure communication and fault-tolerant distributed computing. Specific topics include secure multiparty computation, Byzantine fault tolerance, and public-key infrastructures. Extended the notion of secure multiparty computation to approximation algorithms. Developed efficient solutions for privacy-protecting statistical analysis. Introduced probabilistic quorum systems.

AT&T Bell Laboratories
Murray Hill, NJ

Member of Technical Staff
1994 – 1996

Key contributor in the design and development of the Omega key management service, both as a research project and as a potential AT&T certificate authority (CA) service. Negotiated with Netscape to have Omega recognized as a CA in version 1.1 of Netscape's Web browser, one of the first to support public-key authentication. Developed a formal logic to extend reasoning about cryptographic protocols to include revocation, authentication, and security policies.

Teaching, Advising, and Mentoring

Rutgers University
Piscataway, NJ

2007 – Present

Courses taught:

- 16:198:500 Light Seminar on Accountability in Online Life — Fall 2011
- 16:198:500 Light Seminar on Economics of Cybersecurity — Fall 2009
- 16:198:671 Privacy in a Networked World — Fall 2008
- 16:198:500 Light Seminar on Readings in Differential Privacy — Fall 2008
- 16:198:672 Theory of Distributed Computation — Fall 2007

Ph.D. student thesis advising:

Geetha Jagannathan, Ph.D., 2010.
Dissertation title: *Data Privacy in Knowledge Discovery*

Darakhshan Mir. Expected completion 2012.
Dissertation topic: *Differential Privacy*

Ph.D. student independent study advising:

Syeda Arzoo Zehra, Spring 2009, Fall 2009.
Aleksander Nikolov, Fall 2009.
Imdadullah Khan, Winter 2008.

Additional doctoral committees:

Andre Madeira, Rutgers University, 2009.
Justin Brickell, University of Texas at Austin, 2009.
Antonio Nicolosi, New York University, 2007.

Additional qualifying exam committees:

Chris Mansley, Rutgers University, 2010.
Brian Thompson, Rutgers University, 2009.

August 2003

Organizer and lecturer for *DIMACS Tutorial on Applied Cryptography and Network Security*, August 4–7, 2003, held as part of the *DIMACS 2003–2006 Special Focus on Communication Security and Information Privacy*.

Summer 2002

Mentor for student Ursula Witcher (now a postdoctoral fellow at Harvey Mudd College) in the DIMACS *Research Experience for Undergraduates* program.

Summer 1995

Research project leader for the DIMACS *Young Scholars Program* for high school students.

Courses taught:

CS465 Privacy in a Networked World — Spring 2005
CS601 Algorithmic Complexity — Spring 2003, Spring 2004, Fall 2005, Spring 2007
CS625 Foundations of Distributed Computing — Fall 2002, Spring 2006
CS668 Foundations of Cryptography — Fall 2003, Fall 2004
CS693 Cryptographic Protocols — Spring 2005

Ph.D. students advised:

Michael de Mare, Ph. D., 2010.
Co-advisor: Stephen Bloom
Dissertation title: *Set Membership Using 3SAT*

Zhiqiang Yang, Ph.D., 2007.
Dissertation title: *Efficient Distributed Protocols for Privacy and Anonymity*
Awarded Outstanding Graduate Student Award, 2005

Geetha Jagannathan. Transferred to Rutgers Fall 2007.
Awarded Outstanding Graduate Student Award, 2006

Masters students advised:

Hiranmayee Subramaniam (M.S., 2003).
M.S. project: *Experimental Analysis of Privacy-Preserving Statistics*

Undergraduate research students advised:

Kelsey Livingston (Smith College) and Jennifer Tam (Tufts University)
Stevens/DIMACS REU project for Summer 2006
Project: *Authentication and Encryption for RFID Technology*

Christopher Guarino, Stevens Undergraduate Scholars' Project, Spring 2003
Project: *Economics and Incentives in Computer Security*

Postdocs supervised:

Sheng Zhong (DIMACS/Stevens postdoc, September 2004 – July 2005)
Sotiris Ioannidis (co-supervised with Susanne Wetzels, February 2005 – June 2007)
Vijay Ramachandran (February 2006 – July 2007)

Lecturer for the UC Berkeley TRUST Center's *Women's Institute in Summer Enrichment* program for graduate students, post-doctoral fellows and professors from all disciplines that are interested in ubiquitous secure technology and the social, political, and economical ramifications that are associated with this technology.

AT&T

1994–2002

Maintained a strong commitment to students. Supervised undergraduate students Elizabeth Belding (now a Professor at UC Santa Barbara) and Sara Spalding in summer research projects at AT&T. Member of AT&T's Undergraduate Research Program Committee, 1998–2000. Participated in AT&T's Student Research Day.

Institute for Advanced Studies

Summer 2000

Princeton, NJ

Lecturer for *Cryptographic Complexity Theory*, IAS/Park City Mathematics Institute Mentoring Program for Women in Mathematics, a program for undergraduate and graduate students and postdoctoral researchers in mathematics.

Polytechnic University

Adjunct Faculty

Brooklyn, NY

Spring 1996

Taught *Information, Privacy, and Security*, a graduate course on practical and theoretical aspects of computer security.

Awards and Honors

National Academy of Engineering, *Armstrong Endowment for Young Engineers – Gilbreth Lectureship*, 2008.

Association for Computing Machinery, *Recognition of Service Award*, 2006.

Stevens Institute of Technology, *Master of Engineering, Honoris Causa*, 2006.

Stevens Institute of Technology, *Research Recognition Award*, 2004.

National Science Foundation, *University–Industry Postdoctoral Research Associateship in the Mathematical Sciences*, March 1994. (Although this was awarded, I did not actually take the associateship, instead taking a full-time position at AT&T Bell Laboratories.)

Yale University, *John F. Enders Fellowship*, Summer 1993.

Yale University, *Theres and Dennis M. Rohan Fellowship*, September 1992 – May 1993.

Yale University, *University Fellowship*, September 1989 – May 1992.

National Science Foundation, *Graduate Research Fellowship, Honorable Mention*, 1989.

Grants

National Science Foundation, *Three New DIMACS Special Focus Programs*, NSF CCF-1144502, September 2011–August 2015, Principal Investigator, \$698,995.

National Science Foundation, *Distributed Computing with Adaptive Heuristics*, NSF CCF-1101690, September 2011–August 2014, Principal Investigator, \$398,267.

National Science Foundation, *Efficient Privacy Methods using Linear Programming*, NSF CCF-1018445, September 2010–August 2013, Co-Principal Investigator, \$499,274.

National Science Foundation, *CMISS: DIMACS Project on CS/Math in Service to Society*, NSF CCF-1032010, September 2010–August 2014, Co-Principal Investigator, \$800,000.

National Science Foundation, *Accountability and Identifiability*, NSF CNS-1018557, August 2010–July 2013, Principal Investigator, \$249,991. (This is a collaborative project with another NSF grant awarded simultaneously to Yale, for a total, including Rutgers, of \$499,991.)

National Science Foundation, *The Value of Computational Thinking Across Grade Levels*, NSF DRL-1020201, July 2010–June 2014, Co-Principal Investigator, \$1,856,219.

National Science Foundation, *Second INCO-TRUST Workshop*, NSF CNS-1040356, July 2010–June 2011, Principal Investigator, \$90,907.

National Science Foundation, *First INCO-TRUST Workshop*, NSF CNS-0925990, October 2009–September 2010, Principal Investigator, \$49,121.

National Science Foundation, *AUSTIN – An Initiative to Assure Software Radios have Trusted Interactions*, NSF CNS-0910557, September 2009–August 2011, Co-Principal Investigator, \$410,000. (This is a collaborative project with NSF grants awarded simultaneously to U. Mass–Amherst and Virginia Polytechnic Institute, for a total, including Rutgers, of \$1,000,000.)

National Science Foundation, *Computer Science and Decision Making*, NSF CCF-0916782, September 2009–August 2012, Co-Principal Investigator, \$300,000.

Rutgers University Academic Excellence Fund, *The Rutgers University Research Initiative on Cybersecurity Economics*, July 2009–June 2010, Principal Investigator, \$60,000.

United States – Israel Binational Science Foundation. *Interdisciplinary Workshop on Data Privacy*, 20080208-00004698, February 2008–January 2009, Co-Principal Investigator, \$30,000.

National Science Foundation, *DIMACS Special Focus on Algorithmic Foundations of the Internet*, NSF CNS-0721113, October 2007–September 2011, Co-Principal Investigator, \$311,867.

National Science Foundation, *Mitigating Exploits of the Current Interdomain Routing Infrastructure*, NSF CNS-0716511 (to Stevens) and NSF CNS-0753061 (to Rutgers), September 2007–August 2011, Principal Investigator, \$259,035. (This award was transferred from Stevens to Rutgers in 2008. This is a collaborative project with another NSF grant awarded simultaneously to Tulane and also transferred to Rutgers, for a total, including Rutgers, of \$422,800.)

Galois Connections, Inc., *Automated Wide-Area Network Configuration from High-Level Specifications*, subcontract on *Phase-1 DARPA-STTR contract*, September 2006–September 2007, Principal Investigator, \$8,735.

Sun Microsystems, *Sun Academic Excellence Award*, T-US-837331-B, July 2006, Co-Principal Investigator, \$24,658.

National Science Foundation, *Incentive-Compatible Protocols*, NSF CNS-0524139 (to Stevens) and NSF CNS-0751674 (to Rutgers), September 2005–August 2009, Principal Investigator, \$212,500. (This award was transferred from Stevens to Rutgers in 2007. This is a collaborative project with another NSF grant awarded simultaneously to SUNY Buffalo, for a total, including Rutgers, of \$425,000.)

National Science Foundation, *Cybersecurity Laboratory: Translating Theory into Practice*, NSF DUE-0516788, September 2005–August 2008, Co-Principal Investigator, \$125,001.

Stevens Wireless Network Security Center, *Prototyping of Privacy-Preserving Bayes Network Structure*, August 2004–August 2005, Principal Investigator, \$90,000.

National Science Foundation, *Capacity Building through Interdisciplinary Degrees in Cybersecurity*, NSF DUE-0417085, July 2004–June 2007, Co-Principal Investigator, \$297,003.

National Science Foundation, *Sensitive Information in a Wired World*, NSF CNS-0331584 (to Stevens) and NSF CNS-0822269 (to Rutgers), October 2003–September 2009, Principal Investigator, \$888,001. (This award was transferred from Stevens to Rutgers in 2008. This is a collaborative project with four other NSF grants awarded simultaneously to Stanford, Yale, NYU and University of New Mexico, for a total, including Stevens, of \$12,500,000. Jointly these grants form *the PORTIA project*. More information about the PORTIA project, including a list of all PIs and coPIs, industrial partners, graduate students, and postdoctoral associates is available at www.cs.rutgers.edu/~rebecca.wright/PORTIA.)

New Jersey Institute of Technology Center for Wireless Networking and Internet Security, *Practical Optimizations to Privacy-Preserving Statistics Computation*, subcontract on grant from **New Jersey Commission on Science and Technology**, September 2003–December 2003, Principal Investigator, \$13,640.

Stevens Wireless Network Security Center, *Privacy-Preserving Data Mining for Homeland Security*, August 2002–August 2004, Principal Investigator, \$205,851.

Professional Activities

Committee on State Voter Registration Databases, *The National Academies*, 2007–2010.

Computing Innovations Fellows Selection Committee, *a project of the Computing Community Consortium and the Computing Research Association*, 2009.

Board of Directors, *International Association for Cryptologic Research (IACR)*, 2001–2005. (2001–2002, appointed position. 2002–2005, elected position.)

Advisory Board, Columbia University Computer Science Department, 2008–2010.

Founder and Moderator, *ProfessHers mailing list*, 2008–present. Sponsored by the Committee on the Status of Women in Computing Research of the Computing Research Association (CRA-W).

Founder, *ny-sec mailing list*. **Moderator**, 2003–2007.

Editorial Boards:

- **Editorial Board**, *Journal of Computer Security*, 2001-2011.
- **Editorial and Advisory Board**, *International Journal of Information and Computer Security*, 2004–present.
- **Editorial Board**, *Transactions on Data Privacy* (sponsored by the Artificial Intelligence Research Institute of the Spanish Higher Research Council, the UNESCO Chair in Data Privacy, and the Catalan Association of Artificial Intelligence), 2008–present.
- **Editorial Board**, *The Handbook of Information Security*, Wiley, Hossein Bidgoli, editor, 2005.

Conference Organization:

- **U.S. Chair**, *INCO-TRUST Workshop on International Cooperation in Security and Privacy: International Data Exchange with Security and Privacy—Applications, Policy, Technology, and Use*, May 3–5, 2010. Sponsored by the National Science Foundation and the European Commission.
- **U.S. Chair**, *INCO-TRUST Workshop on International Co-operation in Trustworthy Systems: Security, Privacy and Trust in Large-Scale Global Networks and Services as Part of the Future Internet*, March 31–April 1, 2009. Sponsored by the National Science Foundation and the European Commission.
- **Steering Committee**, *Information Security Conference*, 2006–2010.
- **Tutorials Chair**, *12th ACM Conference on Computer and Communications Security*, 2005.
- **U. S. Chair**, *2nd Japan/US Workshop on Critical Information Infrastructure Protection*, June 26–27, 2005. Sponsored by the National Science Foundation and the Japan Science and Technology Agency.
- **General Chair**, *Crypto 2002*.
- **Rump Session Chair**, *Financial Cryptography 2001*.
- **Invited session organizer**, “Computer Security,” *Grace Murray Hopper Celebration of Women in Computing*, Cape Cod, MA, September 14–16, 2000.

Program Committees:

- *6th Workshop on the Economics of Networks, Systems, and Computation*, San Jose, CA, June 6, 2011.
- *9th International Conference on Cryptology and Network Security*, Kuala Lumpur, Malaysia, December 12–14, 2010. **Program Co-Chair**.
- *12th International Symposium on Stabilization, Safety, and Security of Distributed Systems*, New York, NY, September 20–22, 2010. **Track Co-Chair**, Security.
- *The World Wide Web Conference*, Raleigh, NC, April 26–30, 2010. **Area Chair**, Security and Privacy.

- *Engaging Data: First International Forum on the Application and Management of Personal Electronic Information*, Cambridge, MA, October 12–13, 2009.
- *30th IEEE Symposium on Security and Privacy*, Oakland, CA, May 17–19, 2009.
- *15th ACM Conference on Computer and Communications Security*, Alexandria, VA, October 27–31, 2008.
- *17th ACM Conference on Information and Knowledge Management*, Napa, CA, October 26–30, 2008. **Track Chair.**
- *2nd ACM SIGKDD International Workshop on Privacy, Security, and Trust in KDD*, Las Vegas, NV, August 24, 2008.
- *8th Privacy Enhancing Technologies Symposium*, Leuven, Belgium, July 23–25, 2008.
- *28th International Conference on Distributed Computing Systems*, Beijing, China, June 17–20, 2008.
- *Interdisciplinary Studies in Privacy and Security*, New Brunswick, NJ, May 12, 2008.
- *International Workshop on Practical Privacy-Preserving Data Mining*, Atlanta, GA, April 26, 2008.
- *16th Usenix Security Symposium*, Boston, MA, August 6–10, 2007.
- *11th Pacific-Asia Conference on Knowledge Discovery and Data Mining*, Nanjing, China, May 22–25, 2007.
- *13th ACM Conference on Computer and Communications Security*, Alexandria, VA, October 30 – November 3, 2006. **Program Chair.**
- *2006 IEEE Symposium on Security and Privacy*, Oakland, CA, May 21–24, 2006.
- *15th International World Wide Web Conference*, Edinburgh, Scotland, May 2006.
- *12th ACM Conference on Computer and Communications Security*, Alexandria, VA, November 7–11, 2005.
- *11th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, Chicago, IL, August 21–24, 2005.
- *Crypto 2005*, Santa Barbara, CA, August 14–18, 2005.
- *Fifth SIAM International Conference on Data Mining*, Newport Beach, April 21–23, 2005. **Vice Program Chair.**
- *13th Usenix Security Symposium*, San Diego, CA, August 9–13, 2004.
- *Eurocrypt 2004*, Interlaken, Switzerland, May 2–May 6, 2004.
- *Eighth International Financial Cryptography Conference*, Key West, FL, February 9–12, 2004.
- *ACM Workshop on Privacy in the Electronic Society*, Washington DC, October 30, 2003.
- *Seventh International Financial Cryptography Conference*, Guadeloupe, French West Indies, January 27–30, 2003. **Program Co-Chair.**
- *ACM Workshop on Privacy in the Electronic Society*, Washington DC, November 21, 2002.
- *ACM Workshop on Scientific Aspects of Cyber Terrorism*, Washington DC, November 21, 2002.

- *15th IEEE Computer Security Foundations Workshop*, Nova Scotia, June 24–26, 2002.
- *Eurocrypt 2002*, Amsterdam, Netherlands, April 28–May 2, 2002.
- *Sixth International Financial Cryptography Conference*, Bermuda, March 11–14, 2002.
- *Eighth Annual ACM Conference on Computer and Communications Security*, Philadelphia, PA, November 5–8, 2001.
- *14th IEEE Computer Security Foundations Workshop*, Nova Scotia, June 11–13, 2001.
- *Tenth International World Wide Web Conference*, Hong Kong, May 2001.
- *Crypto 2000*, Santa Barbara, CA, August 20–24, 2000.
- *Seventh Annual ACM Conference on Computer and Communications Security*, Athens, Greece, November 1–4, 2000.
- *Crypto '97*, Santa Barbara, CA, August 17–21, 1997.
- *Third ACM Conference on Computer and Communications Security*, New Delhi, India, March 14–16, 1996.

Workshop Organizing Committees:

- *Security and Privacy Day*, Rutgers University, Piscataway, NJ, May 15, 2009.
- *BSF/DIMACS/DyDAn Workshop and Working Group on Data Privacy*, Rutgers University, Piscataway, NJ, February 4–7, 2008.
- *DIMACS/DyDAn Workshop on Mathematical and Computational Methods for Information Security*, Texas Southern University, Houston, TX, December 7, 2007.
- *Workshop on Privacy Aspects of Data Mining*, Omaha, NE, October 28, 2007. Held in conjunction with the Seventh IEEE International Conference on Data Mining.
- *AIM Workshop on Generic Case Complexity*, American Institute of Mathematics, Palo Alto, CA, August 13–17, 2007.
- *IBM Research / Stevens Institute of Technology / Columbia University Security and Privacy Day*, IBM Research, Hawthorne, NY, November 13, 2006.
- *Stevens / Columbia / IBM Research Security and Privacy Day*, Stevens Institute of Technology, Hoboken, NJ, November 14, 2005.
- *Workshop on Privacy and Security Aspects of Data Mining*, Houston, TX, November 27, 2005. Held in conjunction with the Fifth IEEE International Conference on Data Mining.
- *DIMACS/PORTIA Workshop and Working Group on Privacy-Preserving Data Mining*, Rutgers University, Piscataway, NJ, March 15–17, 2004.
- *3rd Stevens Symposium on Cybersecurity and Trustworthy Software*, Stevens Institute of Technology, Hoboken, NJ, March 26, 2004.
- *Workshop on Foundations of Computer Security*, Copenhagen, Denmark, July 25–26, 2002. Held in conjunction with the 17th IEEE Symposium on Logic in Computer Science.
- *DIMACS Workshop on Networks Threats*, Rutgers University, Piscataway, NJ, December 4–6, 1996.

Grant Proposal Review:

- *National Science Foundation*, ten grant proposal review panels and several ad hoc reviews, 2002–present.
- *Lawrence Livermore National Labs*, Strategic Initiative review, 2008.
- *Austrian Science Fund*, 2007.
- *American Mathematical Society* for *National Security Agency*, Mathematical Sciences Program, 2006, 2008.
- *Israel Science Foundation*, 2006.
- *Canada Foundation for Innovation*, 2004.
- *Oak Ridge Institute for Science and Education*, 2002.
- *Hong Kong Research Grants Council*, 2001.

Referee for various journals, including *Journal of Cryptology*, *Data and Knowledge Engineering*, *Distributed Computing*, *International Journal of Information Security*, *IEEE Transactions on Engineering Management*, and *Journal of the ACM*.

Rutgers Committees:

- *Computer Science Department committees*
 - Executive Committee, 2009–present. (Elected position.)
 - Faculty Search Committee, 2010–2011. (Co-chair.)
 - Publicity Committee, 2008–2009.
 - Peer Evaluation Committee, 2007–2008. (Elected position.)
 - Teaching Effectiveness Committee, 2007–2008.
- *DIMACS committees*
 - Executive Committee, 2005–present.
 - Organizing Committee, *DIMACS Special Focus on Algorithmic Foundations of the Internet*, 2007–2010.
 - Projects Committee, 1996–2002.
- *Other Rutgers committees*
 - Computing Coordination Council, 2009–present.
 - SAS Committee on Faculty Development, 2011.
 - Dean Search Committee, School of Engineering, 2008–2009.

Stevens Institute Committees:

- *Computer Science Department committees*
 - Faculty Search Committee, 2006–2007. (Chair).
 - PhD Committee, 2003–2007. (Chair, 2006–2007).
 - Quals Committee, 2003–2007.
 - Web Coordinator, 2002–2006.
- *Standing Institute committees*

Faculty Council, 2006–2007. (Elected position.)
Board of Trustees Strategy Committee, 2006–2007. (Elected position.)
Committee on Committees, 2004–2006. (Elected position. Chair, 2005–2006.)
Undergraduate Academic Standards Committee, 2003–2005. (Elected position.
Chair, 2004–2005.)
Board of Trustees Faculty Development Committee, 2004–2005.

Selected Invited Talks

Secure Knowledge Management Workshop, *Strategic Policies for Cyberdeterrence: A Game-Theoretic Framework*, Rutgers University, Piscataway, NJ, October 21–22, 2010.

China Computer Federation Conference on Future Computing, *Economics of Cybersecurity*, **Keynote Speaker**, Changsha, China, June 17–18, 2010.

Security and Privacy Day, *Strategic Policies for Cyberdeterrence: A Game-Theoretic Framework*, Stevens Institute of Technology, Hoboken, NJ, May 28, 2010.

Workshop on Cryptographic Protocols and Public-Key Cryptography, *Rationality and Traffic Attraction: Incentives for Honest Path Announcements in BGP*, Bertinoro, Italy, May 24–29, 2009.

Dagstuhl Workshop on Model-Based Design of Trustworthy Health Information Systems, *The Cancer Institute of New Jersey’s Tissue Repository: A Privacy and Security Case Study*, Schloss Dagstuhl, Germany, February 11–14, 2009.

Columbia University Security Seminar, *Privacy-Preserving Data Mining: Extending the Boundary*, Columbia University, New York, NY, April 23, 2008.

Gilbreth Lectures for Young Engineers, National Meeting of the National Academy of Engineering, *Privacy in a Networked World*, Irvine, CA, February 7, 2008.

Frontiers of Engineering Symposium of the National Academy of Engineering, *Privacy in a Networked World*, Redmond, WA, September 24–26, 2007.

Workshop on Cryptographic Protocols, *Privacy-Preserving Imputation of Missing Data*, Bertinoro, Italy, March 4–9, 2007.

IPAM Workshop on Locally Decodable Codes, Private Information Retrieval, Privacy-Preserving Data-Mining, and Public Key Encryption with Special Properties, *Privacy-Preserving Bayesian Network Learning and Other Recent Results in Privacy-Preserving Data Mining*, University of California, Los Angeles, CA, October 25–28, 2006.

Workshop on Computational Methods for Security in a Web Environment, *Privacy-Preserving Data Mining*, Universidad de Tarapacá, Arica, Chile, July 23–27, 2006.

TAMI/Portia Privacy and Accountability Workshop, *Accountability in Privacy-Preserving Data Mining*, Massachusetts Institute of Technology, Cambridge, MA, June 28–29, 2006.

Workshop on Data Surveillance and Privacy Protection, *Progress on the PORTIA Project in Privacy-Preserving Data Mining*, Harvard University Center for Research on Computation and Society, Cambridge, MA, June 3, 2006.

Five-College Speaker Series on Information Assurance, *Privacy-Preserving Data Mining in the Fully Distributed Model*, University of Massachusetts, Amherst, MA, October 17, 2005.

MADNES Workshop on Secure Mobile Ad-Hoc Networks and Sensors, *Privacy-Preserving Data Mining in the Fully Distributed Model*, **Keynote Speaker**, Singapore, September 21–22, 2005.

CS-Statistics Workshop on Privacy and Confidentiality, *Privacy-Enhancing k -Anonymization of Customer Data*, Bertinoro, Italy, July 9–15, 2005.

University of Tsukuba Laboratory of Cryptography and Information Security, *Privacy-Enhancing k -Anonymization of Customer Data*, University of Tsukuba, Tsukuba, Japan, June 24, 2005.

1st International Interdisciplinary Congress of Scientific Research, *The PORTIA project: Privacy, Obligations, and Rights in Technologies of Information Assessment*, Boca Chica, Dominican Republic, June 8–9, 2005.

10th Meeting of the Science, Technology, and Law Panel of the National Academies, *The Use of Commercial Databases for National Security: Privacy, Evaluation, and Accuracy*, Washington DC, 18 March, 2005.

U.S.–Japan Experts Workshop on Critical Information Infrastructure Protection, *Privacy-Preserving Bayesian Network Structure Computation on Distributed Heterogeneous Data*, National Science Foundation, Washington, DC, September 28–29, 2004.

Stanford University Crypto and Database Privacy Group Meetings, *Privacy-Preserving Bayesian Network Structure Computation on Distributed Heterogeneous Data*, Stanford University, Palo Alto, CA, August 13, 2004.

Polytechnic University Computer and Information Science Department, *Privacy-Protecting Statistics Computation: Theory and Practice*, Polytechnic University, Brooklyn, NY, April 2, 2004.

Responding to Terror and Ensuring Privacy: Can We Design Technologies and Policies That Do Both?, *Cryptographic Methods for Privacy-Preserving Computation on Data*, co-hosted by the Heritage Foundation and the Center for Democracy and Technology, Washington, DC, December 1, 2003.

New Jersey Institute of Technology Electrical and Computer Engineering Department, *Privacy-Protecting Statistics Computation: Theory and Practice*, New Jersey Institute of Technology, Newark, NJ, November 24, 2003.

IEEE LICS'03 Workshop on Foundations of Computer Security, *Privacy in Today's World: Solutions and Challenges*, Ottawa, Canada, June 26–27, 2003.

Carnegie Mellon University Privacy in DATA Workshop, *Privacy-Protecting Statistics Computation: Theory and Practice*, Carnegie Mellon University, Pittsburgh, PA, March 27–28, 2003.

New Jersey Institute of Technology Workshop on Homeland and Cyber Security, *Privacy-Preserving Data Mining*, Newark, NJ, April 16–17, 2003.

U. Penn Computer Security Seminar, *Privacy in Today's World: Solutions and Challenges*, University of Pennsylvania, Philadelphia, PA, March 18, 2003.

CUNY Graduate Center Computer Science Department, *Privacy in Today's World: Solutions and Challenges*, CUNY Graduate Center, New York, NY, February 20, 2003.

Yale Computer Science Department, *Tight Bounds for Shared Memory Systems Accessed by Byzantine Processes*, Yale University, New Haven, CT, October 10, 2002.

Dagstuhl Workshop on Cryptography, *Tight Bounds for Shared Memory Systems Accessed by Byzantine Processes*, Schloss Dagstuhl, Germany, September 22–27, 2002.

CCR/DIMACS Workshop on Mining Massive Data Sets and Streams: Mathematical Methods and Algorithms for Homeland Defense, *Protecting Privacy in Data-Mining Applications*, Institute for Defense Analysis, Princeton, NJ, June 20–22, 2002.

Mathematical Foundations of Programming Semantics XVIII, *Reasoning about Trust and Insurance in a Public Key Infrastructure*, Special session on Security, New Orleans, LA, March 23–26, 2002.

Monte Verita Workshop on Cryptographic Protocols, *Private Function Evaluation with Sublinear Communication*, Monte Verita, Switzerland, March 18–23, 2001.

IBM T.J. Watson Research, *Efficient Fault-Tolerant Certificate Revocation and Reasoning about Trust and Insurance in a Public Key Infrastructure*, IBM Watson Research Center, Hawthorne, NY, December 7, 2000.

SRI International, *Secure Multiparty Computation of Approximations*, SRI International, Palo Alto, CA, May 25, 2000.

Florida State University Computer Science Department, *Secure Multiparty Computation of Approximations*, Florida State University, Tallahassee, FL, April 11, 2000.

Third Annual Algebra Weekend, *Secure Multiparty Computation*, **Plenary Speaker**, University of Missouri, Columbia, MO, October 2–3, 1999.

Joint Seminar of the Amherst College Mathematics and Computer Science Departments, the U. Mass Computer Science Department, and the Five College Theory Seminar, *Experimental Performance of Shared RSA Modulus Generation*, Amherst College, Amherst, MA, September 29, 1998.

Hong Kong University of Science and Technology Computer Science Department Theory Seminar, *Secure Communication in Minimal Connectivity Models*, Hong Kong University of Science and Technology, Hong Kong, February 1998.

Dagstuhl Workshop on Cryptography, *Secure Communications over Echo Lines*, Schloss Dagstuhl, Germany, September 22–26, 1997.

DIMACS Special Year on Networks Seminar, *Probabilistic Quorum Systems*, AT&T Labs, Murray Hill, NJ, February 21, 1997.

Hong Kong University of Science and Technology Department of Computer Science, *The Omega Key Management Service*, Hong Kong University of Science and Technology, Hong Kong, November 10, 1995.

Columbia University Theory Seminar, *Achieving Perfect Secrecy Using Correlated Random Variables*, Columbia University, New York, NY, October 20, 1994.

IBM Communication in Distributed Systems Seminar, *Achieving Perfect Secrecy Using Correlated Random Variables*, IBM Watson Research Center, Hawthorne, NY, May 6, 1994.

Princeton University Computer Science Department, *Achieving Perfect Secrecy Using Correlated Random Variables*, Princeton University, Princeton, NJ, April 6, 1994.

Harvard University Computer Science Department, *Achieving Perfect Secrecy Using Correlated Random Variables*, Harvard University, Cambridge, MA, March 21, 1994.

Yale University Computer Science Liaison Program, *Applying Game Theory to Cryptography*, Yale University, New Haven, CT, October 15–16, 1992.

IBM Communication in Distributed Systems Seminar, *Secret Communication Among Friends*, IBM Watson Research Center, Hawthorne, NY, January 21, 1991.

DIMACS Workshop in Structural Complexity and Cryptography, *Secret Key Exchange Using a Random Deal of Cards*, Rutgers University, Piscataway, NJ, December 3–6, 1990.

DIMACS Workshop on Distributed Computing and Cryptography, *Experimental Work on Database Encryption*, Princeton, NJ, October 4–6, 1989.

Panel Participation

INET NY 2011 – It’s Your Call: What Kind of Internet Do You Want?, *New Privacy Models*, New York, NY, June 14, 2011. Panelist.

Engaging Data: First International Forum on the Application and Management of Personal Electronic Information, *Ensuring Data Protection: Technical Methods*, Massachusetts Institute of Technology, Cambridge, MA, October 12–13, 2009. Panelist.

Privacy Workshop: Implementing Privacy Protections in Government Data Mining, Technologies for Privacy-Protective Data Mining, Department of Homeland Security Privacy Office, Washington, DC, July 24–25, 2008. Panelist.

NY Systems/Networking Summit, Hot Research Topics in Security, New York University, New York, NY, November 17, 2006. Panelist.

Privacy and Technology Workshop: Exploring Government Use of Commercial Data for Homeland Security, How Can Technology Help Protect Individual Privacy While Enabling Government Agencies to Analyze Data?, Department of Homeland Security Privacy Office, Washington, DC, September 8–9, 2005. Panelist.

New Jersey Statewide Symposium on Homeland Security, Large-Scale Cyber Attacks, Rutgers University, Newark, NJ, October 12, 2004. Panelist and panel moderator.

DIMACS Workshop on Design and Formal Verification of Security Protocols, Design vs. Verification: Is Verification the Wrong Approach?, Rutgers University, Piscataway, NJ, September 3–5, 1997. Panelist.

McGraw-Hill Companies, On-Line Privacy Forum, McGraw-Hill Companies, New York, NY, November 4, 1996. Panelist.

Publications: Journal papers

- [1] “A Practical Differentially Private Random Decision Tree Classifier,” (with G. Jagannathan and K. Pillaipakkamnatt), *Transactions on Data Privacy*, to appear.
- [2] “Communication-Efficient Privacy-Preserving Clustering,” (with G. Jagannathan*, K. Pillaipakkamnatt, and D. Umamo[†]), *Transactions on Data Privacy*, Vol. 3, No. 1, 2010, pp. 1–25.
- [3] “Private Multiparty Sampling and Approximation of Vector Combinations,” (with Y. Ishai, T. Malkin, and M. Strauss), *Theoretical Computer Science*, Vol. 410, No. 18, 2009, pp. 1730–1745.
- [4] “Privacy-Preserving Imputation of Missing Data,” (with G. Jagannathan*), *Data & Knowledge Engineering*, Vol. 65, No. 1, 2008, pp. 40–56.
- [5] “Secure Multiparty Computation of Approximations,” (with J. Feigenbaum, Y. Ishai, T. Malkin, K. Nissim, and M. Strauss), *ACM Transactions on Algorithms*, Vol. 2, No. 3, 2006, pp. 435–472.
- [6] “Privacy-Preserving Bayesian Network Computation on Vertically Partitioned Data,” (with

*Ph.D. student at the time work was performed.

†M.S. student at the time work was performed.

‡Undergraduate student at the time work was performed.

§Postdoctoral researcher at the time work was performed.

- Z. Yang*), *IEEE Transactions on Knowledge and Data Engineering*, Vol. 18, No. 9, 2006, pp. 1253–1264.
- [7] “Experimental Analysis of a Privacy-Preserving Scalar Product Protocol,” (with Z. Yang* and H. Subramaniam[†]), *International Journal of Computer Systems Science and Engineering*, Vol. 21, No. 1, 2006, pp. 47–52.
- [8] “Tight Bounds for Shared Memory Systems Accessed by Byzantine Processes,” (with N. Alon, M. Merritt, O. Reingold, and G. Taubenfeld), *Distributed Computing*, Vol. 18, No. 2, 2005, pp. 99–109.
- [9] “PORTIA: Privacy, Obligations, and Rights in Technologies of Information Assessment,” (with D. Boneh, J. Feigenbaum, and A. Silberschatz), *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering*, Vol. 27, No. 1, 2004, pp. 10–18.
- [10] “An Authentication Logic with Formal Semantics Supporting Synchronization, Revocation, and Recency,” (with S. Stubblebine), *IEEE Transactions on Software Engineering*, Vol. 28, No. 3, 2002, pp. 256–285.
- [11] “Experimental Performance of Shared RSA Modulus Generation,” (with S. Spalding[‡]), *Algorithmica*, Vol. 33, No. 1, 2002, pp. 89–103.
- [12] “Depender Graphs: A Method of Efficient Fault-Tolerant Certificate Distribution,” (with P. Lincoln and J. Millen), *Journal of Computer Security*, Vol. 9, No. 4, 2001, pp. 323–338.
- [13] “Probabilistic Quorum Systems,” (with D. Malkhi, M. Reiter, and A. Wool), *Information and Computation*, Vol. 170, No. 2, 2001, pp. 184–206.
- [14] “Secure Communication in Minimal Connectivity Models,” (with M. Franklin), *Journal of Cryptology*, Vol. 13, No. 1, 2000, pp. 9–30.
- [15] “The Ω Key Management Service,” (with M. Reiter, M. Franklin, and J. Lacy), *Journal of Computer Security*, Vol. 4, No. 4, 1996, pp. 267–287.
- [16] “Bounds on Secret Key Exchange Using a Random Deal of Cards,” (with M. Fischer), *Journal of Cryptology*, Vol. 9, No. 2, 1996, pp. 71–99.

Publications: Book chapters

- [17] “Privacy in a Networked World,” *Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2007 Symposium*, The National Academies Press, (2008), pp. 5–12.
- [18] “Cryptography,” *Encyclopedia of Physical Science and Technology (Third Edition)*, Elsevier Academic Press, (2001), Robert A. Myers, editor, pp. 61–77.

*Ph.D. student at the time work was performed.

†M.S. student at the time work was performed.

‡Undergraduate student at the time work was performed.

§Postdoctoral researcher at the time work was performed.

- [19] “Finite-State Approximation of Phrase-Structure Grammars,” (with F. Pereira), *Finite-State Language Processing*, (1997), MIT Press, Cambridge, MA, Emmanuel Roche and Yves Schabes, editors, pp. 149–173.
- [20] “An Application of Game-Theoretic Techniques to Cryptography,” (with M. Fischer), *Advances in Computational Complexity Theory*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Volume 13, American Mathematical Society, (1993), Jin-Yi Cai, editor, pp. 99–118.
- [21] “Cryptographic Protection of Databases and Software,” (with J. Feigenbaum and M. Liberman), *Distributed Computing and Cryptography*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Volume 2, American Mathematical Society, (1991), Joan Feigenbaum and Michael Merritt, eds, pp. 161–172.

Publications: Books and journal special issues edited

- [22] *Cryptology and Network Security – 9th International Conference, CANS 2010*, Lecture Notes in Computer Science, Vol. 6467, Springer, (2010), Swee-Huay Heng, Rebecca N. Wright, Bok-Min Goi, editors.
- [23] *Special Issue on Computer and Communications Security*, ACM Transactions on Information and System Security, Vol. 12, No. 2, (2008), Rebecca N. Wright and Sabrina De Capitani di Vimercati, editors.
- [24] *Special Issue on Privacy and Security Aspects of Data Mining*, International Journal of Information and Computer Security, Vol. 2, No. 1, Inderscience Publishers (2008), Stan Matwin, LiWu Chang, Rebecca N. Wright, and Justin Zhan, editors.
- [25] *Proceedings of the 13th ACM Conference on Computer and Communications Security*, ACM Press, (2006), Rebecca N. Wright, Sabrina De Capitani di Vimercati, and Vitaly Shmatikov, editors.
- [26] *Proceedings of Financial Cryptography '03*, Lecture Notes in Computer Science, Vol. 2742, Springer-Verlag, (2003), Rebecca N. Wright, editor.
- [27] *Network Threats*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Volume 38, American Mathematical Society, (1998), Rebecca N. Wright and Peter G. Neumann, editors.

Publications: Refereed conferences and workshops

- [28] “Towards a Formal Model of Accountability,” (with J. Feigenbaum and A. Jaggard), *Proceedings of the 2011 New Security Paradigms Workshop (NSPW)*, 2011, to appear.

*Ph.D. student at the time work was performed.

†M.S. student at the time work was performed.

‡Undergraduate student at the time work was performed.

§Postdoctoral researcher at the time work was performed.

- [29] “Accountability and Deterrence in Online Life,” (with J. Feigenbaum, J. Hendler, A. Jaggard, and D. Weitzner), *Proceedings of the Third International Conference on Web Science (WebSci)*, 2011.
- [30] “Brief Announcement: Distributed Computing with Rules of Thumb,” (with A. Jaggard and M. Schapira[§]), *Proceedings of the 30th Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC)*, 2011.
- [31] “Pan-private Algorithms via Statistics on Sketches,” (with D. Mir*, A. Nikolov*, and S. Muthukrishnan), *Proceedings of the 30th ACM Symposium on Principles of Database Systems (PODS)*, 2011.
- [32] “Distributed Computing with Adaptive Heuristics,” (with A. Jaggard and M. Schapira[§]), *Proceedings of Innovations in Computer Science*, 2011, pp. 417–443.
- [33] “A Practical Differentially Private Random Decision Tree Classifier,” (with G. Jagannathan* and K. Pillaipakkamatt), *Proceedings of the Ninth IEEE International Conference on Data Mining – Workshops*, 2009, pp. 114–121. ([1] is an extended version of this paper.)
- [34] “A Differentially Private Graph Estimator,” (with D. Mir*), *Proceedings of the Ninth IEEE International Conference on Data Mining – Workshops*, 2009, pp. 122–129. [Note: Some of the results in this paper are incorrect.]
- [35] “Privacy-Preserving Evaluation of Generalization Error and Its Application to Model and Attribute Selection,” (with J. Sakuma), *Advances in Machine Learning – Proceedings of the First Asian Conference on Machine Learning (ACML)*, Lecture Notes in Computer Science, Vol. 5828, Springer, 2009, pp. 338–353.
- [36] “Interstate Voter Registration Database Matching: The Oregon-Washington 2008 Pilot Project,” (with R. M. Alvarez, J. Jonas, and W. Winkler), *Proceedings of the 2009 Electronic Voting Workshop / Workshop on Trustworthy Elections*, 2009. (Electronic proceedings only.)
- [37] “The Impact of Communication Models on Routing-Algorithm Convergence,” (with A. Jaggard and V. Ramachandran), *Proceedings of the 29th International Conference on Distributed Computing Systems (ICDCS)*, 2009, pp. 58–67.
- [38] “Rationality and Traffic Attraction: Incentives for Honest Path Announcements in BGP,” (with S. Goldberg*, S. Halevi, A. Jaggard, and V. Ramachandran), *Proceedings of the ACM SIGCOMM 2008 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM)*, 2008, pp. 267–278.
- [39] “Privacy-Preserving Reinforcement Learning,” (with J. Sakuma and S. Kobayashi), *Proceedings of the 25th International Conference on Machine Learning (ICML)*, 2008, pp. 864–871.
- [40] “On the Lindell-Pinkas Secure Computation of Logarithms: From Theory to Practice,” (with

*Ph.D. student at the time work was performed.

†M.S. student at the time work was performed.

‡Undergraduate student at the time work was performed.

§Postdoctoral researcher at the time work was performed.

- R. Ryger* and O. Kardes*), *Proceedings of the International Workshop on Practical Privacy-Preserving Data Mining*, 2008. (Electronic proceedings only.)
- [41] “Private Inference Control for Aggregate Queries,” (with G. Jagannathan*), *Proceedings of the Seventh IEEE International Conference on Data Mining – Workshops*, 2007, pp. 711–716.
- [42] “Towards Privacy-Preserving Model Selection,” (with Z. Yang* and S. Zhong), *Proceedings of the First ACM SIGKDD International Workshop on Privacy, Security, and Trust in KDD (PinKDD’07)*, Lecture Notes in Computer Science, Volume 4890, Springer, 2008, pp. 138–152. (Post-proceedings.)
- [43] “Private Multiparty Sampling and Approximation of Vector Combinations,” (with Y. Ishai, T. Malkin, and M. Strauss), *Proceedings of the 34th International Colloquium on Automata, Languages and Programming (ICALP)*, 2007, pp. 243–254. ([3] is an extended version of this paper.)
- [44] “Privacy-Preserving Data Imputation,” (with G. Jagannathan*), *Proceedings of the Sixth IEEE International Conference on Data Mining – Workshops*, 2006, pp. 535–540. ([4] is an extended version of this paper.)
- [45] “Secure Set Membership Using 3SAT,” (with M. de Mare*), *Proceedings of the Eighth International Conference on Information and Communications Security (ICICS)*, 2006, pp. 452–468.
- [46] “Privacy-Preserving Queries on Encrypted Data,” (with Z. Yang* and S. Zhong[§]), *Proceedings of the 11th European Symposium on Research In Computer Security (Esorics)*, 2006, pp. 479–494.
- [47] “A New Privacy-Preserving Distributed k -Clustering Algorithm,” (with G. Jagannathan* and K. Pillaipakkamatt), *Proceedings of the 2006 SIAM International Conference on Data Mining (SDM)*, 2006, pp. 492–496. ([2] is an extended version of this paper.)
- [48] “Implementing Privacy-Preserving Bayesian-Net Discovery for Vertically Partitioned Data,” (with O. Kardes*, R. Ryger*, and J. Feigenbaum), *Proceedings of the ICDM Workshop on Privacy and Security Aspects of Data Mining*, 2005, pp. 26–34.
- [49] “Distributed Data Mining Protocols for Privacy: A Review of Some Recent Results,” (with Z. Yang* and S. Zhong[§]), *Proceedings of the Secure Mobile Ad-hoc Networks and Sensors Workshop (MADNES’05)*, Lecture Notes in Computer Science, Vol. 4074, Springer, 2005, pp. 67–79. Invited paper.
- [50] “Anonymity-Preserving Data Collection,” (with Z. Yang* and S. Zhong[§]), *Proceedings of the 11th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, (KDD)*, 2005, pp. 139–147.
- [51] “Privacy-Preserving Distributed k -Means Clustering over Arbitrarily Partitioned Data,” (with

*Ph.D. student at the time work was performed.

†M.S. student at the time work was performed.

‡Undergraduate student at the time work was performed.

§Postdoctoral researcher at the time work was performed.

- G. Jagannathan*), *Proceedings of the 11th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, 2005, pp. 593–599.
- [52] “Privacy-Enhancing k -Anonymization of Customer Data,” (with S. Zhong[§] and Z. Yang*), *Proceedings of the 24th ACM Symposium on Principles of Database Systems (PODS)*, 2005, pp. 139–147.
- [53] “Privacy-Preserving Classification of Customer Data without Loss of Accuracy,” (with Z. Yang* and S. Zhong[§]), *Proceedings of the 2005 SIAM International Conference on Data Mining (SDM)*, 2005, pp. 92–102.
- [54] “Improved Privacy-Preserving Bayesian Network Parameter Learning on Vertically Partitioned Data,” (with Z. Yang*), *Proceedings of the ICDE International Workshop on Privacy Data Management*, 2005, pp. 43–52. ([6] is a combined and extended version of this paper and [56].)
- [55] “Experimental Analysis of Privacy-Preserving Statistics Computation,” (with H. Subramaniam[†] and Z. Yang*), *Proceedings of the VLBD Workshop on Secure Data Management*, Lecture Notes in Computer Science, Vol. 3178, Springer, 2004, pp. 55–66. ([7] is an extended version of this paper.)
- [56] “Privacy-Preserving Bayesian Network Structure Computation on Distributed Heterogeneous Data,” (with Z. Yang*), *Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, 2004, pp. 713–718. ([6] is a combined and extended version of this paper and [54].)
- [57] “Accountable Privacy,” (with M. Burmester, Y. Desmedt, and A. Yasinsac), *Proceedings of the Twelfth International Workshop on Security Protocols*, Lecture Notes in Computer Science, Vol. 3957, Springer, 2004, pp. 83–96.
- [58] “Fischer’s Cryptographic Protocols,” *Proceedings of Twenty-Second Annual ACM Symposium on Principles of Distributed Computing (PODC)*, 2003, pp. 20–22. Invited paper.
- [59] “Privacy Tradeoffs: Myth or Reality? (Panel Summary),” (with L. J. Camp, I. Goldberg, R. Rivest, and G. Wood), *Proceedings of Financial Cryptography 2002 (FC)*, Lecture Notes in Computer Science, Vol. 2357, Springer-Verlag, 2003, pp. 147–151. Invited paper.
- [60] “Tight Bounds for Shared Memory Systems Accessed by Byzantine Processes,” (with M. Merritt, O. Reingold, and G. Taubenfeld), *Proceedings of 16th International Symposium on Distributed Computing (DISC)*, Lecture Notes in Computer Science, Vol. 2508, Springer-Verlag, 2002, pp. 222–236. ([8] is an extended version of this paper.)
- [61] “Off-Line Generation of Limited-Use Credit Card Numbers,” (with A. Rubin), *Proceedings of Financial Cryptography 2001 (FC)*, Lecture Notes in Computer Science, Vol. 2339, Springer-Verlag, 2002, pp. 196–209.

*Ph.D. student at the time work was performed.

†M.S. student at the time work was performed.

‡Undergraduate student at the time work was performed.

§Postdoctoral researcher at the time work was performed.

- [62] “Selective Private Function Evaluation with Application to Private Statistics,” (with R. Canetti, Y. Ishai[§], R. Kumar, M. Reiter, and R. Rubinfeld), *Proceedings of Twentieth Annual ACM Symposium on Principles of Distributed Computing (PODC)*, 2001, pp. 293–304.
- [63] “Secure Multiparty Computation of Approximations,” (with J. Feigenbaum, Y. Ishai[§], T. Malkin, K. Nissim*, and M. Strauss), *Proceedings of 28th International Colloquium on Automata, Languages and Programming (ICALP)*, Lecture Notes in Computer Science, Vol. 2076, Springer-Verlag, 2001, pp. 927–938. ([5] is an extended version of this paper.)
- [64] “Efficient Fault-Tolerant Certificate Revocation,” (with P. Lincoln and J. Millen), *Proceedings of the Seventh ACM Conference on Computer and Communications Security (CCS)*, 2000, pp. 19–24. ([12] is an extended version of this paper.)
- [65] “Reasoning about Trust and Insurance in a Public Key Infrastructure” (with J. Millen), *Proceedings of 13th IEEE Computer Security Foundations Workshop (CSFW)*, IEEE Computer Society, 2000, pp. 16–22.
- [66] “Dynamic Byzantine Quorum Systems” (with L. Alvisi, D. Malkhi, E. Pierce*, and M. Reiter), *Proceedings of the International Conference on Dependable Systems and Networks (DSN)*, 2000, pp. 283–292.
- [67] “Obstacles to Freedom and Privacy by Design,” *Proceedings of the 10th Conference on Computers, Freedom and Privacy (CFP)*, Workshop on Freedom and Privacy by Design, 2000, pp. 97–100.
- [68] “Influencing Software Usage,” (with L. Cranor), *Proceedings of the 10th Conference on Computers, Freedom and Privacy (CFP)*, Workshop on Freedom and Privacy by Design, 2000, pp. 45–55.
- [69] “Certificate Revocation the Responsible Way,” (with J. Millen), *Proceedings of Computer Security, Dependability, and Assurance: From Needs to Solutions*, IEEE Computer Society, 1999, pp. 196–203. Invited paper.
- [70] “Experimental Performance of Shared RSA Modulus Generation,” (with S. Spalding[‡]), *Proceedings of the Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, January 1999, pp. 983–984. ([11] is an extended version of this paper.)
- [71] “Probabilistic Byzantine Quorum Systems,” (with D. Malkhi, M. Reiter, and A. Wool), *Proceedings of Seventeenth Annual ACM Symposium on Principles of Distributed Computing (PODC)*, 1998, p. 321. ([13] is a combined and extended version of this paper and [74].)
- [72] “SubScribe: Secure and Efficient Data Delivery/Access Services in a Push-Based Environment,” (with A. Datta, A. Celik*, and A. Biliris), *Proceedings of the First International Conference on Telecommunications and Electronic Commerce (ICTEC)*, 1998, (page numbers unknown, 30 pages).

*Ph.D. student at the time work was performed.

†M.S. student at the time work was performed.

‡Undergraduate student at the time work was performed.

§Postdoctoral researcher at the time work was performed.

- [73] “Secure Communication in Minimal Connectivity Models,” (with M. Franklin), *Advances in Cryptology – Proceedings of Eurocrypt ’98*, Lecture Notes in Computer Science, Vol. 1403, Springer-Verlag, 1998, pp. 346–360. ([14] is an extended version of this paper.)
- [74] “Probabilistic Quorum Systems,” (with D. Malkhi and M. Reiter), *Proceedings of Sixteenth Annual ACM Symposium on Principles of Distributed Computing (PODC)*, 1997, pp. 267–273. ([13] is a combined and extended version of this paper and [71].)
- [75] “The Ω Key Management Service,” (with M. Reiter, M. Franklin, and J. Lacy), *Proceedings of the Third ACM Conference on Computer and Communications Security (CCS)*, 1996, pp. 38–47. ([15] is an extended version of this paper.)
- [76] “An Authentication Logic Supporting Synchronization, Revocation, and Recency,” (with S. Stubblebine), *Proceedings of the Third ACM Conference on Computer and Communications Security (CCS)*, 1996, pp. 95–105. ([10] is an extended version of this paper.)
- [77] “An Efficient Protocol for Unconditionally Secure Secret Key Exchange,” (with M. Fischer), *Proceedings of the 4th Annual Symposium on Discrete Algorithms (SODA)*, 1993, pp. 475–483.
- [78] “Multiparty Secret Key Exchange Using a Random Deal of Cards,” (with M. Fischer), *Advances in Cryptology – Proceedings of Crypto ’91*, Springer-Verlag, Lecture Notes in Computer Science, Vol. 576, 1992, pp. 141–155. ([16] and [20] are extended versions of parts of this paper.)
- [79] “Finite-State Approximation of Phrase-Structure Grammars,” (with F. Pereira), *Proceedings of the 29th Annual Conference of the Association for Computational Linguistics (ACL)*, 1991, pp. 246–255. ([19] is an extended version of this paper.)

Other publications

- [80] “Improving State Voter Registration Databases: Final Report,” Committee on State Voter Registration Databases, National Research Council, The National Academies Press, 2010.
- [81] “State Voter Registration Databases: Immediate Actions and Future Improvements, Interim Report,” Committee on State Voter Registration Databases, National Research Council, The National Academies Press, 2008.
- [82] “Statewide Databases of Registered Voters: Study Of Accuracy, Privacy, Usability, Security, and Reliability Issues,” (with P. Hawthorn, B. Simons, S. M. Bellovin, C. Clifton, L. Coney, R. Gellman, H. Hochheiser, A. Rosenthal, R. Spencer Poore, and D. Wagner), commissioned by the U.S. Public Policy Council of the Association for Computing Machinery (USACM), 2006.
- [83] “Achieving Perfect Secrecy Using Correlated Random Variables,” Ph.D. Thesis, Department of Computer Science, Yale University, YALEU/CSD/RR #1058, January 1995.

*Ph.D. student at the time work was performed.

†M.S. student at the time work was performed.

‡Undergraduate student at the time work was performed.

§Postdoctoral researcher at the time work was performed.

- [84] “Can You Keep a Secret? An Introduction to Cryptography,” *Omnibus*, Yale University Computing & Information Systems Supplement to the Yale Weekly Bulletin and Calendar, Vol. 6, No. 3, November 1993.
- [85] “A Library for Multithread Synthetic Trace Generation,” Hewlett-Packard Laboratories Technical Report HPL-92-108, 1992.

Patents

Off-line generation of limited-use credit card numbers, (with A. Rubin), US patent application, serial number 682830, application date 10/23/2001, patent pending.

*Ph.D. student at the time work was performed.

†M.S. student at the time work was performed.

‡Undergraduate student at the time work was performed.

§Postdoctoral researcher at the time work was performed.