Rebecca N. Wright

Department of Computer Science
Barnard College
3009 Broadway
New York, NY 10027 USA

Phone: +1 (212) 853–0219
E-mail: rwright@barnard.edu
Web: www.cs.columbia.edu/∼rwright

Education

Yale University New Haven, CT

Ph.D. in Computer Science, December 1994. Advisor: Professor Michael J. Fischer.
Dissertation: *Achieving Perfect Secrecy Using Correlated Random Variables.*
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

Barnard College, Columbia University New York, NY

Druckenmiller Professor of Computer Science	July 2019 – present
Chair, Computer Science Department	July 2024 – present
Faculty Director, Vagelos Computational Science Center	January 2019 – present
Member, Data Science Institute (Columbia)	July 2019 – present
Affiliate, Computer Science (Columbia)	November 2019 – present
Co-Chair, Center for Cybersecurity, Data Science Institute (Columbia)	January 2023 – present
Director, Computer Science Program	July 2019 – June 2024
Chair, Center for Cybersecurity, Data Science Institute (Columbia)	July 2020 – December 2022
Visiting Professor, Computer Science	January 2019 – June 2019

Led the creation of Barnard's Computer Science department. Directing the Diana T. and P. Roy Vagelos Computational Science Center. Engaged in research in security, privacy, and computing education. Founded Computing Fellows program.

Rutgers University Piscataway, NJ

Visiting Professor, Computer Science	July 2019 – June 2021
Professor, Computer Science	July 2010 – June 2019
Graduate Faculty, Electrical & Computer Engineering	February 2012 – June 2019
Director, DIMACS	September 2011 – November 2018
Deputy Director, DIMACS	September 2007 – August 2011
Associate Professor, Computer Science	September 2007 – June 2010

As Director of DIMACS (the Center for Discrete Mathematics and Theoretical Computer Science), set direction, ran programs, and obtained funding. Co-founder of the Douglass-DIMACS Computer Science Living-Learning Community. Carried out research in security, privacy, and accountability.

Stevens Institute of Technology Hoboken, NJ
Professor, Computer Science September 2006 – July 2007
Associate Professor, Computer Science 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.

Rutgers University Piscataway, NJ
Visiting Research Associate, DIMACS 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 and Holmdel, 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

Barnard College New York, NY
2019 – present

Courses taught:
COMS BC3420 Privacy in a Networked World — Fall 2024,
Fall 2023, Fall 2022, Spring 2022, Spring 2021, Spring 2020, Fall 2019
FYSB BC1736 Tech & Society: Good, Bad, & Other — Fall 2021, Fall 2020
COMS BC3997 New Directions in Computing: Guest Lecture Series — Spring 2022,
Fall 2021, Spring 2020

Undergraduate independent study advising:

Lilly Enekes, Spring 2025
Anissa Arakal, Spring 2024
Erica Chen, Spring 2024
Rissa Chua, Spring 2024, Fall 2023
Renee Saw, Spring 2024
Sam Kim (Columbia), Spring 2024
Catarina Coelho, Fall 2023
Ruitong Liu, Fall 2023
Melissa Marie Wang, Fall 2023
Vicky Zhou, Fall 2023
Esme Li, Spring 2023
Dipashreya Sur, Spring 2023, Fall 2022
Serra Goker, Fall 2022
Sanya Mehta, Fall 2022
Wendy Sung, Fall 2022
Elvina Wibisono Fall 2022
Jacquie Zhang, Fall 2022
Luiza Leschziner, Spring 2021
Esmé Ablaza, Spring 2020
Minghan Zhu (Columbia), Spring 2020

Rutgers University Piscataway, NJ
2007 – 2018

Courses taught:

01:198:294 Great Ideas and Applications in CS — Spring 2018, Spring 2017
16:198:500 Light Seminar on Secure Computation — Fall 2013
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

Douglass-SAS-DIMACS Computer Science Living-Learning Community:

Co-founder (in 2016) and faculty advisor (2016–2018) for the Douglass-SAS-DIMACS Computer Science Living-Learning Community (CS LLC) for first-year women at Rutgers. LLC participants live in a common residence hall and are provided with an educational, leadership development, and community-building program that supports their progress as Rutgers students and as computer science majors.

Douglass-DIMACS Computing Corps:

Co-founder (in 2012) and faculty advisor (2012–2018). The Douglass-DIMACS Computing Corps is a group of women undergraduate students at Rutgers that meet biweekly through the academic year. Throughout the year, undergraduate students work with CS faculty and graduate students to design and carry out fun, educational, and interactive group activities for middle school girls to excite them about computing.

Ph.D. student thesis advising:

Cong Zhang, Ph.D., 2020.
Dissertation: *Order-Revealing Encryption: New Constructions and Barriers*

Neil Lutz. Ph.D., 2017.
Dissertation: *Algorithmic Information, Fractal Geometry, and Distributed Dynamics*

Jason Perry. Ph.D., 2015.
Dissertation: *Putting Secure Computation to Work*

Darakhshan Mir, Ph.D., 2013.
Dissertation: *Differential Privacy: An Exploration of the Privacy-Utility Landscape*

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

Additional Ph.D. student independent study advising:

Daniel Bittner, Fall 2018, Spring 2018, Fall 2017, Spring 2017
Joseph Wegehaupt, Spring 2013, Fall 2012
Sai Lu, Spring 2012, Fall 2011
Syeda Arzoo Zehra, Fall 2009, Spring 2009
Aleksander Nikolov, Fall 2009
Imdadullah Khan, Winter 2008

Additional doctoral committees:

Fatma Betül Durak, Rutgers University, 2017
Erick Chastain, Rutgers University, 2016
Aaron Segal, Yale University, 2016
Debayan Gupta, Yale University, 2016
Liina Kamm, University of Tartu, 2016 (as "opponent")
Brian Thompson, Rutgers University, 2013
Saman Zarandioon, Rutgers University, 2012
Tin Lam, Rutgers University, 2011
Gayathri Chandrasekaran, Rutgers University, 2011
Andre Madeira, Rutgers University, 2009
Justin Brickell, University of Texas at Austin, 2009
Antonio Nicolosi, New York University, 2007

Additional qualifying exam committees:

Fatma Betül Durak, Rutgers University, 2016
Priya Govindan, Rutgers University, 2015
Zhe Wang, Rutgers University, 2013
Ana Paula Centeno, Rutgers University, 2012
Chris Mansley, Rutgers University, 2010
Chih-Cheng Chang, Rutgers University, 2009
Brian Thompson, Rutgers University, 2009
Andre Madeira, Rutgers University, 2008

Undergraduate research students advised:

Gianna Schwarz, DIMACS REU program, Summer 2017
Uttara Aggarwal, Fall 2010

Leilani Gilpin (UC San Diego), DIMACS REU program, Summer 2010
Swara Kopparty (Harvard), DIMACS REU program, Summer 2010

Stevens Institute of Technology Hoboken, NJ
2002 – 2007

Courses taught:
CS465 Privacy in a Networked World — Spring 2005
CS601 Algorithmic Complexity — Spring 2007, Fall 2005, Spring 2004, Spring 2003
CS625 Foundations of Distributed Computing — Spring 2006, Fall 2002
CS668 Foundations of Cryptography — Fall 2004, Fall 2003
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 Wetzel, February 2005 – June 2007)
Vijay Ramachandran (February 2006 – July 2007)

University of California at Berkeley Berkeley, CA
July 2006

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.

Rutgers University Piscataway, NJ
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.*

Rutgers University Piscataway, NJ
Summer 2002

Mentor for student Ursula Whitcher (Swarthmore) in the DIMACS *Research Experience for Undergraduates* program.

AT&T Florham Park, Murray Hill, and Holmdel, NJ
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 Princeton, NJ
Summer 2000

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.

Rutgers University Piscataway, NJ
Summer 1995

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

Polytechnic University Brooklyn, NY
Adjunct Faculty Spring 1996

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

Awards and Honors

Barnard College, *Linda A. Bell Award for Collaborative Creativity and Excellence in Teaching*, 2026

Association of Computing Machinery, *Fellow*, Citation: for contributions to security and privacy, and for leadership in computing research and education, 2025

Association for Computing Machinery, Special Interest Group on Algorithms and Computation Theory, *SIGACT Distinguished Service Award*, 2019

Institute of Electrical and Electronic Engineers, *Fellow*, Citation: for contributions to applied cryptography and privacy, 2018

Association of Computing Machinery, *Distinguished Member*, for Scientific Contributions to Computing, 2017

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 (Awarded by NSF but declined by Wright)

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

Barnard College, *Senior Certificate of Distinction*, 1988

Columbia College, *Dean's List*, four semesters

Grants and Gifts

Columbia University (with gift funds from Google Cyber NYC Institutional Research Program), *Cyber NYC Cross-Institutional Research Experiences for Undergraduates Program*, March 2024–June 2027, Principal Investigator, $298,282

Columbia University, (with gift funds from Google Cyber NYC Institutional Research Program), *Visual Explanations of Privacy-Accuracy Tradeoffs in Differential Privacy Systems*, July 2023–December 2024, Co-Principal Investigator, $80,000

National Science Foundation, *Computing Fellows Program: Increasing Meaningful Computing Engagement Across Disciplines*, NSF DUE-2142628, February 2022–January 2026, Principal Investigator, $299,953

Craig Newmark Philanthropies, *Building a Program in Computer Science at Barnard College*, restricted gift, March 2020, $250,000

Northeastern University, Center for Inclusive Computing, *Advancing Women in Computing at Columbia and Barnard*, restricted gift, February 2020, $170,075

National Science Foundation, *2019 Secure and Trustworthy Cyberspace PI Meeting*, August 2019–July 2020, Principal Investigator, $99,088

National Science Foundation, *Big Ten Academic Alliance Summit on Advancing Undergraduate Women in STEM*, July 2019–June 2020, Co-Principal Investigator, $49,999

National Science Foundation, *RCN: DIMACS/Simons Collaboration on Lower Bounds in Complexity Theory*, October 2018–September 2021, Principal Investigator, $499,490. (Became Former Principal Investigator in March 2020)

National Science Foundation, *RCN: DIMACS/Simons Collaboration in Bridging Continuous and Discrete Optimization*, NSF CCF-1740425, September 2017–August 2020, Principal Investigator, $500,000. (Became Former Principal Investigator in March 2020.)

European Commission, *Accelerating EU-US DialoGue for Research and Innovation in Cyber-Security and Privacy (AEGIS)*, EC 740647, May 2017–April 2019, Partner, €500,000, Rutgers portion €22,300

National Science Foundation, *EAGER: Collaborative: Algorithmic Framework for Anomaly Detection in Interdependent Networks*, NSF CNS-1646856, September 2016–August 2019, Principal Investigator, $200,057. (This is a collaborative project with another NSF grant awarded simultaneously to the University of Tennessee, for a total, including Rutgers, of $299,995.)

National Science Foundation, *BD Spokes: PLANNING: NORTHEAST: Collaborative: Planning for Privacy and Security in Big Data*, NSF IIS-1636764, September 2016–March 2019, Principal Investigator, $89,963. (This is a collaborative project with another NSF grant awarded simultaneously to Pennsylvania State University (later transferred to Boston University), for a total, including Rutgers, of $99,963.)

National Science Foundation, *REU Site: DIMACS REU in Computing Theory and Applications Impacting Society*, NSF CCF-1559855, April 2016–March 2019, Principal Investigator, $383,771

Verisign, *Differential Privacy, Multi-target Search, and Anomaly Detection*, unrestricted gift from Verisign Labs through their University Gift/Collaboration program, November 2015, $25,000

Galois, Inc., *Jana: Ensuring Secure, Private and Flexible Data Access*, subcontract on grant from **DARPA**, September 2015–March 2020, Principal Investigator, $1,013,723. (Partially subcontracted to Barnard in July 2019.)

National Science Foundation, *Computer Science Living-Learning Community for Women at Rutgers*, NSF DUE-1504775, July 2015–June 2019, Principal Investigator, $249,999

National Science Foundation, *RCN: DIMACS/Simons Collaboration in Cryptography*, NSF CCF-1523467, May 2015–April 2019, Principal Investigator, $500,000

National Science Foundation, *CIRCLE: Catalyzing and Integrating Research, Collaboration, and Learning in Computing, Mathematics, and their Applications*, NSF CCF-1445755, August 2014–July 2022, Principal Investigator, $1,199,934. (Became Co-Principal Investigator and Former Principal Investigator in March 2020.)

National Science Foundation, *2014 NSF/DIMACS Workshop for Aspiring PIs in Secure and*

Trustworthy Cyberspace, NSF CNS-1441026, May 2014–April 2015, Principal Investigator, $99,987

National Science Foundation, *REU Site: DIMACS REU in Computing Theory and Multidisciplinary Applications*, NSF CCF-1263082, April 2013–March 2017, Principal Investigator, $360,699

Yale, *Systematization of Secure Computation*, subcontract on grant from **DARPA**, January 2013–February 2015, Principal Investigator, $311,784

National Science Foundation, *BIGDATA: Mid-Scale: ESCE: Collaborative Research: Discovery and Social Analytics for Large-Scale Scientific Literature*, NSF IIS-1247696, January 2013–December 2018, Principal Investigator, $1,004,784. (This is a collaborative project with two other NSF grants awarded simultaneously to Princeton (later transferred to Columbia) and Cornell, for a total, including Rutgers, of $2,998,873. Dr. Paul Kantor was the Rutgers PI until his retirement.)

National Science Foundation, *Enhancing the Capacity for Information Assurance Education Through Interdisciplinary Collaboration*, NSF DGE-1241315, November 2012–October 2015, Co-Principal Investigator, $292,670

National Science Foundation, *Workshop for Aspiring PIs in Secure and Trustworthy Cyberspace*, NSF CNS-1265542, October 2012–September 2013, Principal Investigator, $99,992

Applied Communication Sciences, *SPADE: Secure and Private Database Execution*, subcontract on grant from **IARPA**, October 2011–March 2013, Principal Investigator, $203,857

Applied Communication Sciences, *EPP-SCOT: Encrypted Private Publish-Subscribe using Conditional Oblivious Transfer*, subcontract on grant from **IARPA**, October 2011–March 2013, Principal Investigator, $64,814

National Science Foundation, *Three New DIMACS Special Focus Programs*, NSF CCF-1144502, September 2011–August 2017, Principal Investigator, $698,995

National Science Foundation, *Distributed Computing with Adaptive Heuristics*, NSF CCF-1101690, September 2011–August 2015, Principal Investigator, $398,267

University of California – San Diego, *US and China Workshop Series to Build a Collaborative Framework for Developing Shared Software Infrastructure*, subcontract on grant from **National Science Foundation**, September 2011–August 2012, Principal Investigator, $21,623

National Science Foundation, *Efficient Privacy Methods using Linear Programming*, NSF CCF-1018445, September 2010–August 2014, 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, Principal Investigator, $800,000

National Science Foundation, *Accountability and Identifiability*, NSF CNS-1018557, August 2010–July 2014, 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 2015, Co-Principal Investigator, $2,105,009

National Science Foundation, *Second INCO-TRUST Workshop*, NSF CNS-1040356, July 2010–June 2013, Principal Investigator, $90,907

National Science Foundation, *REU Site: DIMACS/DIMATIA U.S./Czech International REU Program*, NSF CNS-1004956, March 2010–February 2014, Principal Investigator, $621,583

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 2012, 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 2013, 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.)

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

Boards and Advisory Committees:

- **Advisory Board**, *Northeast Big Data Innovation Hub*, 2019–present
- **Privacy and Technology Advisory Board**, *Electronic Registration Information Center* (ERIC), 2014–present
- **Board**, *Committee on Widening Participation in Computing Research (formerly Committee on the Status of Women in Computing Research), Computing Research Association* (CRA-WP), 2012–present
- **Committee of Visitors**, *National Science Foundation, Computer and Information Science and Engineering Directorate, Computing and Communication Foundations Division*, 2023
- **Advisory Board**, *CISPA-Stanford Center for Cybersecurity*, 2017–2022
- **Advisory Committee**, *Computing Research Association Center for Evaluating the Research Pipeline (CERP)*, 2012–2022
- **Mathematics and Physical Sciences Scientific Advisory Board**, *Simons Foundation*, 2018–2021
- **Committee on State Voter Registration Databases**, *The National Academies*, 2007–2010
- **Advisory Board**, Columbia University Computer Science Department, 2008–2010
- **Board of Directors**, *International Association for Cryptologic Research* (IACR), 2001–2005. (2001–2002, appointed position. 2002–2005, elected position.)

Editorial Boards:

- **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**, *PeerJ Computer Science*, 2015–2026
- **Editorial and Advisory Board**, *International Journal of Information and Computer Security*, 2004–2017
- **Editorial Board**, *Journal of Computer Security*, 2001-2011
- **Editorial Board**, *The Handbook of Information Security*, Wiley, Hossein Bidgoli, editor, 2005

Conference and Workshop Organizational Leadership:

- **Steering Committee**, *ACM Conference on Computer and Communications Security*, 2018–present
- **Technical Program Chair**, *2019 National Science Foundation Secure and Trustworthy Cyberspace Principal Investigators' Meeting*, Alexandria, VA, October 27–29, 2019
- **Local Arrangements Co-Chair**, *57th Annual IEEE Symposium on Foundations of Computer Science*, October 9–11, 2016
- **Local Arrangements Co-Chair**, *55th Annual IEEE Symposium on Foundations of Computer Science*, October 19–21, 2014
- **Chair**, *2014 NSF/DIMACS Workshop for Aspiring PIs in Secure and Trustworthy Cyberspace*, August 17, 2014
- **Co-Chair**, *DIMACS/BIC/A4Cloud/CSA International Workshop on Trustworthiness, Accountability and Forensics in the Cloud*, June 6–7, 2013
- **Local Arrangements Co-Chair**, *53rd Annual IEEE Symposium on Foundations of Computer Science*, October 20–23, 2012
- **Chair**, *NSF/DIMACS Workshop for Aspiring PIs in Secure and Trustworthy Cyberspace*, October 15, 2012
- **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.

- **DIMACS Executive Committee**, *Stevens Institute of Technology representative*, 2005–2007
- **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
- **DIMACS Projects Committee**, 1996–2002

Conference and Workshop Program Committees:

- *26th ACM Conference on Computer and Communications Security*, London, UK, November 11–15, 2019
- *3rd International Symposium on Cyber Security, Cryptography, and Machine Learning*, Be'er Sheva, Israel, June 27–28, 2019
- *2nd International Symposium on Cyber Security, Cryptography, and Machine Learning*, Be'er Sheva, Israel, June 21–22, 2018
- *Symposium and Bootcamp on the Science of Security*, Raleigh, NC, April 10–11, 2018
- *Grace Hopper Celebration of Women in Computing, Security/Privacy track*, Houston, TX, October 19–21, 2016
- *32nd International Conference on Data Engineering*, Helsinki, Finland, May 16–20, 2016
- *Symposium and Bootcamp on the Science of Security*, Urbana-Champaign, IL, April 21–22, 2015
- *ACM Symposium on Principles of Distributed Computing*, Paris, France, July 15–19, 2014
- *Symposium and Bootcamp on the Science of Security*, Raleigh, NC, April 8–9, 2014
- *Fourth International Conference on Web Science*, Evanston, IL, June 22–24, 2012
- *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
- *1st ACM Workshop on Security and Artificial Intelligence*, Alexandria, VA, October 27, 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 and Special Focus Organizing Committees:

- *CRA-WP Grad Cohort*, Seattle, WA, March 5–7, 2026
- *CRA-WP Grad Cohort for Women*, Denver, CO, April 3–5, 2025
- *CRA-WP Grad Cohort for Women*, Minneapolis, MN, April 11–13, 2024
- *DIMACS/MACS Workshop on Usable, Efficient, and Formally Verified Secure Computation*, Boston University, Boston, MA, March 13–14, 2019
- *AEGIS EU-US Roundtable on the Interplay of Technology and Policy in Data Privacy*, Vienna, Austria, December 5, 2018
- *DIMACS / Northeast Big Data Hub Workshop on Overcoming Barriers to Data Sharing including Privacy and Fairness*, Rutgers University, Piscataway, NJ, October 23–24, 2017
- *DIMACS / Northeast Big Data Hub Workshop on Privacy and Security for Big Data*, Rutgers University, Piscataway, NJ, April 24–25, 2017
- *DIMACS Big Data Initiative on Privacy and Security*, 2016–2018
- *DIMACS Special Focus on Cryptography*, 2015–2019
- *DIMACS/RUCIA Workshop on Information Assurance in the Era of Big Data*, Rutgers University, Piscataway, NJ, February 6, 2014
- *CCICADA/DIMACS Brainstorming Workshop on Cybersecurity Education*, Rutgers University, Piscataway, NJ, October 7, 2013
- *Dagstuhl Seminar on Privacy-Oriented Cryptography*, Schloss Dagstuhl – Leibniz Center for Informatics, Germany, September 16–21, 2012
- *DIMACS Special Focus on Cybersecurity*, 2011–2017
- *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

- *DIMACS Special Focus on Algorithmic Foundations of the Internet*, 2007-2014
- *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

Award Selection Committees:

- **Scholar Selection Director**, *SWSIS Scholarships for Women Studying Information Security*, a joint project of the Committee on Widening Participation in Computing Research (CRA-WP) and Applied Computer Security Associates (ACSA), 2014–2023
- **Selection Committee**, *SIGACT Distinguished Service Award*, 2020–2022
- **Career Development Grant Selection Panel**, *American Association of University Women*, 2019
- **Selection Committee**, *GREPSEC: Underrepresented Groups in Security Research Workshop*, 2019
- **Selection Committee**, *IEEE Symposium on Security and Privacy Test of Time Award*, 2019
- **Fellows Committee**, *IEEE Computer Society*, 2018
- **Computing Innovations Fellows Selection Committee**, *a project of the Computing Community Consortium and the Computing Research Association*, 2009

Grant Proposal Review:

- *National Science Foundation*, 21 grant proposal review panels, two site visits, and several ad hoc reviews, 2002–present.
- *Natural Sciences and Engineering Research Council of Canada*, 2014
- *Canada Foundation for Innovation*, 2012, 2004
- *Lawrence Livermore National Labs*, Strategic Initiative review, 2008
- *Austrian Science Fund*, 2007
- *American Mathematical Society* for *National Security Agency*, Mathematical Sciences Program, 2008, 2006

- *Israel Science Foundation*, 2006
- *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.*

Founder, *Cyber NYC Research Experience for Undergraduates (REU).* **Director**, 2024 and 2025.

Founder, *ProfessHers mailing list.* **Moderator**, 2008–2016. Sponsored by the Committee on the Status of Women in Computing Research of the Computing Research Association (CRA-W).

Barnard Committees:

- *College-wide Committees*

  President's Council, Spring 2025
  Faculty Budget and Planning Committee (elected), 2022-2025
  Advisory Committee on Appointments, Tenure, and Promotions (elected), 2021–2024
  Provost Search Committee, 2023–2024

- *Other committees*

  Faculty Advisory Committee, Center for Engaged Pedagogy, 2020–present
  Faculty Advisory Committee, Athena Center, 2021–present
  Artificial Intelligence Curricular Task Force, 2023
  Workday Ambassador Network, 2021

Rutgers Committees:

- *Computer Science Department committees*

  Executive Committee (elected), 2009–2013, 2015–2017
  Faculty Search Committee, 2010–2011 (Co-chair)
  Publicity Committee, 2008–2009
  Peer Evaluation Committee (elected), 2007–2008
  Teaching Effectiveness Committee, 2007–2008

- *Other Rutgers committees*

  School of Graduate Studies Executive Council (elected), 2018–2019
  Computing Coordination Council, 2009–2019
  School of Arts and Sciences Rules of Procedure Committee (elected), 2015–2016
  School of Engineering Dean Evaluation Committee, 2013–2014
  Strategic Planning Committee on Envisioning Tomorrow's University, 2013
  School of Arts and Sciences Committee on Faculty Development, 2011
  School of Engineering, Dean Search Committee, 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

- *Other Institute committees*

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

Selected Invited Talks

NYC Privacy Day, *Understanding Differential Privacy Adoption Challenges for Technical Implementers*, NYU Tandon, May 1, 2026

UR2PhD Undergraduate Mentoring Workshop & Research Showcase, *A Computing Research Career: What is it and how do I prepare for it?*, **Keynote Speaker**, New Orleans, LA, April 24, 2026

Center for Learning, Computing, and Imagination Research Talk, *Undergraduate Computing Engagement with Computing Fellows Across Disciplines*, University of Washington, Seattle, WA, March 10, 2026

Distinguished Lecture in Computer Science, *Differential Privacy in Practice*, New Jersey Institute of Technology, Jersey City, NJ, September 24, 2025

Dagstuhl Seminar on Building Privacy-Preserving Technologies of Societal Impact, *Understanding Differential Privacy Adoption Challenges for Technical Implementers*, Schloss Dagstuhl – Leibniz Center for Informatics, Germany, July 27 – August 1, 2025

Data Science Day 2025, *Accountability in Computing*, Columbia University, New York, NY, April 2, 2025

Illinois Computer Science Summer Teaching Workshop, *Undergraduate Computing Engagement with Computing Fellows Across Disciplines*, online, June 2-3, 2025

DivHacks Diversity Hackathon, *Privacy in a Networked World*, **Keynote Speaker**, Columbia University, New York, NY, October 6, 2024

25th European Symposium on Research in Computer Security (ESORICS), *Accountability in Computing*, **Keynote Speaker**, online, September 14–18, 2020

Three Decades of DIMACS: The Journey Continues, *Increasing Women's Participation in Computing*, New Brunswick, NJ, November 21–22, 2019

Symposium and Bootcamp on the Science of Security (HotSoS), *Accountability in Com-*

puting, **Keynote Speaker**, Nashville, TN, April 1–3, 2019

Hasso Plattner Institute Cybersecurity Symposium on Big Data and Artificial Intelligence: Driving the Future of Cybersecurity, *Protecting Your Digital Identities*, **Keynote Speaker**, New York, NY, September 25–26, 2018

CRA-W Distinguished Lecture Series, *Privacy in Today's World*, New Jersey Women in Computing Celebration, Kean College, Union, NJ, April 4, 2018

Muhlenberg College Lectures & Forum and Math/CS Colloquium, *Privacy in Today's World*, February 9, 2018

2017 ACM CCS Workshop on Women in Cyber Security, *Privacy in Today's World*, **Keynote Speaker**, Dallas, TX, October 30, 2017

Federal Privacy Research and Development Interagency Working Group, *Differentially Private Anomaly Detection*, **Invited Briefing**, August 1, 2017

CRA-W Virtual Undergraduate Town Hall Series, *Privacy in Today's World & Getting Involved in CS Extra-curricular Activities*, online presentation hosted by Computing Research Association – Women, April 18, 2017

The 15th International Information Security for South Africa Conference, *Differential Privacy in Practice*, **Keynote Speaker**, Johannesburg, South Africa, August 17–18, 2016

Celebration of Ada Lovelace Day, *How Safe is Your Information Online?*, Hofstra University, Hempstead, NY, October 14, 2014

The New Jersey Governor's School of Engineering and Technology, *Privacy in a Data-Rich World*, **Keynote Speaker**, Rutgers School of Engineering, Piscataway, NJ, July 16, 2014

Privacy in a Big Data World – A Symposium of the National Academies Board on Research Data and Information, *Changing Landscapes in Privacy in a Big Data World*, Washington, DC, September 23, 2013

Center for Interdisciplinary Studies in Security and Privacy INSPIRE(d) Seminar, *Differentially Private Modeling of Human Mobility at Metropolitan Scales*, NYU Polytechnic University, Brooklyn, NY, May 8, 2013

Security and Privacy Day, *Differentially Private Modeling of Human Mobility at Metropolitan Scales*, Stevens Institute of Technology, Hoboken, NJ, May 17, 2013

The 5th International Workshop on Privacy and Anonymity in the Information Society, *Privacy and Accountability in the Information Society*, **Keynote Speaker**, Berlin, Germany, March 30, 2012

Women in Theory, *Privacy and Accountability in the Information Society*, Princeton University, Princeton, NJ, June 23–27, 2012

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 Seminar 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 – Leibniz Center for Informatics, 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

Michael J. Fischer's 60th Birthday Celebration, *Fischer's Cryptographic Protocols*, held as part of ACM Symposium on the Principles of Distributed Computing, Needham, MA, July 13, 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

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

Dagstuhl Seminar on Cryptography, *Tight Bounds for Shared Memory Systems Accessed by Byzantine Processes*, Schloss Dagstuhl – Leibniz Center for Informatics, 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

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 Seminar on Cryptography, *Secure Communications over Echo Lines*, Schloss Dagstuhl – Leibniz Center for Informatics, 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

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

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

DIMACS Workshop on 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

DAX Data Science and AI Exchange, *Thematic Session on Privacy & Security*, New York, NY, April 14, 2026. Panelist.

Computing Research Association Conference, *The Security Risks of Generative AI: From Identification and Mitigation to Responsible Use*, Snowbird, UT, July 23–25, 2024. Panelist.

Barnard Computer Science, the Hasso Plattner Institute, and the German Center for Research and Innovation, *Building Individual, Societal and Digital Resilience: An Interdisciplinary Panel Discussion*, New York, NY, March 8, 2023. Panelist and co-organizer.

Vagelos Computational Science Center and Barnard Neuroscience, *Computing in Neuroscience*, New York, NY, February 7, 2023. Co-organizer and moderator.

Barnard Computer Science and Barnard Science and Public Policy programs, *Bias in AI: Why It's a Problem and What Should Be Done About It*, online, May 12, 2021. Co-organizer and moderator.

Barnard Computer Science and Columbia Data Science Institute, *The Social Dilemma: Shaping the Future of Social Media*, online, October 21, 2020. Co-organizer.

CUE.NEXT: Envisioning the Future of Computing in Undergraduate Education, *Selected Institutions Share Past and Current Initiatives*, Washington, DC, December 5–6, 2019. Panelist.

Three Decades of DIMACS: The Journey Continues, *The Future of Centers*, Washington, DC, November 21–22, 2019. Panel moderator.

AAAS 2019 Annual Meeting, *Scientific Session on Socio-Technical Cybersecurity: It's All About People*, Washington, DC, February 14–17, 2019. Panelist.

Invited Briefing to the U.S. Senate's Diversity in Tech Caucus, Washington, DC, June 22, 2016. Representing CRA-W.

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*, Massachussetts 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.

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.

Sixth International Financial Cryptography Conference, *Privacy Tradeoffs: Myth or Reality?*, South Hampton, Bermuda, March 11–14, 2002. 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.

Patents

Off-line generation of limited-use credit card numbers, A. Rubin and R. Wright, US patent US2002-0073045 A1, issued 6/13/2002

Publications: Journal papers

[1] "Understanding Privacy-Utility Tradeoffs in Differentially Private Online Active Learning," D. Bittner*, A. Brito, M. Ghassemi*, S. Rane, A. Sarwate, and R. Wright, *Journal of Privacy and Confidentiality*, Vol. 10, No. 2, 2020, doi: 10.29012/jpc.720

[2] "From Keys to Databases – Real-World Applications of Secure Multi-Party Computation," D. Archer, D. Bogdanov, Y. Lindell, L. Kamm, K. Nielsen, J. Pagter, N. Smart, and R. Wright, *The Computer Journal*, Vol. 61, No. 12, 2018, pp. 1749–1771

[3] "Privacy-preserving Machine Learning as a Service," E. Hesamifard*, H. Takabi, M. Ghasemi§, and R. Wright, *Proceedings on Privacy Enhancing Technologies*, Vol. 2018, No. 3, 2018, pp. 123-142

[4] "Dynamics at the Boundary of Game Theory and Distributed Computing," A. Jaggard, N. Lutz*, M. Schapira, and R. Wright, *ACM Transactions on Economics and Computation (TEAC)*, Vol. 5, No. 3, 2017, Article 15

[5] "A Practical Differentially Private Random Decision Tree Classifier," G. Jagannathan*§, K. Pillaipakkamnatt, and R. Wright, *Transactions on Data Privacy*, Vol. 5, No. 1, 2012, pp. 273–295

[6] "Communication-Efficient Privacy-Preserving Clustering," G. Jagannathan*, K. Pillaipakkamnatt, R. Wright, and D. Umano†, *Transactions on Data Privacy*, Vol. 3, No. 1, 2010, pp. 1–25

[7] "Private Multiparty Sampling and Approximation of Vector Combinations," Y. Ishai, T. Malkin, M. Strauss, and R. Wright, *Theoretical Computer Science*, Vol. 410, No. 18, 2009, pp. 1730–1745

[8] "Privacy-Preserving Imputation of Missing Data," G. Jagannathan*and R. Wright, *Data & Knowledge Engineering*, Vol. 65, No. 1, 2008, pp. 40–56

[9] "Secure Multiparty Computation of Approximations," J. Feigenbaum, Y. Ishai, T. Malkin, K. Nissim, M. Strauss, and R. Wright, *ACM Transactions on Algorithms*, Vol. 2, No. 3, 2006, pp. 435–472

[10] "Privacy-Preserving Computation of Bayesian Networks on Vertically Partitioned Data," Z. Yang* and R. Wright, *IEEE Transactions on Knowledge and Data Engineering*, Vol. 18, No. 9, 2006, pp. 1253–1264

[11] "Statewide Databases of Registered Voters," P. Hawthorn, B. Simons, C. Clifton, D. Wagner, S. Bellovin, R. Wright, A. Rosenthal, R. Spencer Poore, L. Coney, R. Gellman, and H. Hochheiser, *Communications of the ACM*, Vol. 49, No. 4, 2006, pp. 26–28

*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

[12] "Experimental Analysis of a Privacy-Preserving Scalar Product Protocol," Z. Yang* R. Wright, and H. Subramaniam†, *International Journal of Computer Systems Science and Engineering*, Vol. 21, No. 1, 2006, pp. 47–52

[13] "Tight Bounds for Shared Memory Systems Accessed by Byzantine Processes," N. Alon, M. Merritt, O. Reingold, G. Taubenfeld, and R. Wright, *Distributed Computing*, Vol. 18, No. 2, 2005, pp. 99–109

[14] "PORTIA: Privacy, Obligations, and Rights in Technologies of Information Assessment," D. Boneh, J. Feigenbaum, A. Silberschatz, and R. Wright, *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering*, Vol. 27, No. 1, 2004, pp. 10–18

[15] "An Authentication Logic with Formal Semantics Supporting Synchronization, Revocation, and Recency," S. Stubblebine and R. Wright, *IEEE Transactions on Software Engineering*, Vol. 28, No. 3, 2002, pp. 256–285

[16] "Experimental Performance of Shared RSA Modulus Generation," R. Wright and S. Spalding‡, *Algorithmica*, Vol. 33, No. 1, 2002, pp. 89–103

[17] "Depender Graphs: A Method of Efficient Fault-Tolerant Certificate Distribution," R. Wright, P. Lincoln, and J. Millen, *Journal of Computer Security*, Vol. 9, No. 4, 2001, pp. 323–338

[18] "Probabilistic Quorum Systems," D. Malkhi, M. Reiter, A. Wool, and R. Wright, *Information and Computation*, Vol. 170, No. 2, 2001, pp. 184–206

[19] "Secure Communication in Minimal Connectivity Models," M. Franklin and R. Wright, *Journal of Cryptology*, Vol. 13, No. 1, 2000, pp. 9–30

[20] "The Ω Key Management Service," M. Reiter, M. Franklin, J. Lacy, and R. Wright, *Journal of Computer Security*, Vol. 4, No. 4, 1996, pp. 267–287

[21] "Bounds on Secret Key Exchange Using a Random Deal of Cards," M. Fischer and R. Wright*, *Journal of Cryptology*, Vol. 9, No. 2, 1996, pp. 71–99

Publications: Books and book chapters

[22] *Accountability in Computing: Concepts and Mechanisms*, J. Feigenbaum, A. Jaggard and R. Wright, Foundations and Trends in Privacy and Security, Vol. 2, No. 4, (2020), pp. 247–399, doi.org: 10.1561/3300000002

[23] "Privacy in a Networked World," R. Wright, *Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2007 Symposium*, The National Academies Press, (2008), pp. 5–12

[24] "Cryptography," R. Wright, *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

[25] "Finite-State Approximation of Phrase-Structure Grammars," F. Pereira and R. Wright*, *Finite-State Language Processing*, (1997), MIT Press, Cambridge, MA, Emmanuel Roche and Yves Schabes, editors, pp. 149–173

[26] "An Application of Game-Theoretic Techniques to Cryptography," M. Fischer and R. Wright*, *Advances in Computational Complexity Theory*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Vol. 13, American Mathematical Society, (1993), Jin-Yi Cai, editor, pp. 99–118

[27] "Cryptographic Protection of Databases and Software," J. Feigenbaum, M. Liberman, and R. Wright, *Distributed Computing and Cryptography*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Vol. 2, American Mathematical Society, (1991), Joan Feigenbaum and Michael Merritt, eds, pp. 161–172

Publications: Books and journal special issues edited

[28] *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

[29] *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

[30] *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

[31] *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

[32] *Proceedings of Financial Cryptography '03*, Lecture Notes in Computer Science, Vol. 2742, Springer-Verlag, (2003), Rebecca N. Wright, editor

[33] *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

[34] "Improving Undergraduate Computing Engagement with Computing Fellows Across Disciplines," E. Melville*, M. Wright, J. Rosales, S. Akhtar, and R. Wright, *Proceedings of the 56th ACM Technical Symposium on Computer Science Education (SIGCSE)*, 2025, pp. 763–769

[35] "The Experience of Near-Peer Computing Mentors: Strengthening and Expanding Women's Computing Identities in Undergraduate Interdisciplinary Contexts," J. Rosales, E. Melville*,

*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

M. Wright, S. Akhtar, and R. Wright, *Proceedings of the 55th ACM Technical Symposium on Computer Science Education (SIGCSE)*, 2024, pp. 1154–1160

[36] "Computing Fellows across Disciplines: Preliminary Results," J. Rosales, E. Melville*, M. Wright, S. Akhtar, Z. Webb-Mack, and R. Wright, *Proceedings of the 54th ACM Technical Symposium on Computer Science Education (SIGCSE)*, 2023, pp. 1310–1310

[37] "Living-Learning Community for Women in Computer Science at Rutgers," R. Wright, S. Nadler, T. Nyugen, C. Sanchez Gomez, and H. Wright, *Proceedings of the 50th ACM Technical Symposium on Computer Science Education (SIGCSE)*, 2019, pp. 286–292

[38] "Using Noisy Binary Search for Differentially Private Anomaly Detection," D. Bittner*, A. Sarwate, and R. Wright, *Cyber Security Cryptography and Machine Learning — Proceedings of the 2nd International Symposium on Cyber Security Cryptography and Machine Learning (CSCML)*, Lecture Notes in Computer Science, Vol. 10879, Springer, 2018, pp. 20–37

[39] "Computer Science Living-Learning Community for Women at Rutgers: Initial Experiences and Outcomes (Abstract Only)," R. Wright, J. Stout, G. Cochran, T. Nyugen, and C. Sanchez Gomez, *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE)*, 2018, p. 1075

[40] "Differentially Private Noisy Search with Applications to Anomaly Detection (Abstract)," D. Bittner*, A. Sarwate, and R. Wright, *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security (AISec)*, 2017, p. 53. ([38] is an extended version of this paper.)

[41] "Differentially Private Online Active Learning with Applications to Anomaly Detection," M. Ghassemi*, A. Sarwate, and R. Wright, *Proceedings of the 9th ACM Workshop on Artificial Intelligence and Security (AISec)*, 2016, pp. 117–128

[42] "Self-stabilizing Uncoupled Dynamics," A. Jaggard, N. Lutz*, M. Schapira, and R. Wright, *Algorithmic Game Theory — Proceedings of the 7th International Symposium on Algorithmic Game Theory (SAGT)*, Lecture Notes in Computer Science, Vol. 8768, Springer, 2014, pp. 74–85

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

[44] "Uncovering Facebook Side Channels and User Attitudes," S. Lu*, J. Lindqvist, and R. Wright, *Proceedings of the Workshop on Web 2.0 Security and Privacy*, 2014. (Online proceedings only)

[45] "Open vs. Closed Systems for Accountability," J. Feigenbaum, A. Jaggard, and R. Wright, *Proceedings of Symposium and Bootcamp on the Science of Security (HotSoS)*, 2014

*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

[46] "Strange Bedfellows: How and When to Work with Your Enemy," A. Jaggard and R. Wright, *Proceedings of the 22nd International Workshop on Security Protocols*, Lecture Notes in Computer Science, Vol. 8809, Springer, 2014, pp. 263–267

[47] "Practical and Privacy-Preserving Policy Compliance on Outsourced Data," G. Di Crescenzo, J. Feigenbaum, D. Gupta*, E. Panagos, J. Perry*, and R. Wright, *Proceedings of 2nd Workshop on Applied Homomorphic Cryptography and Encrypted Computing*, Lecture Notes in Computer Science, Vol. 8438, Springer, 2014, pp. 181–194

[48] "DP-WHERE: Differentially Private Modeling of Human Mobility," D. Mir*, S. Isaacman, R. Cáceres, M. Martonosi, and R. Wright, *Proceedings of IEEE International Conference on Big Data*, 2013, pp. 580–588

[49] "Privacy-Preserving Publish/Subscribe: Efficient Protocols in a Distributed Model," G. Di Crescenzo, B. Coan, J. Schultz, S. Tsang, and R. Wright, *Proceedings of the 8th International Workshop on Data Privacy Management (DPM)*, 2013, pp. 114–132

[50] "The Design Space of Probing Algorithms for Network-Performance Measurement," A. Jaggard, S. Kopparty‡, V. Ramachandran, and R. Wright, *Proceedings of ACM SIGMETRICS*, 2013, pp. 105–116

[51] "Efficient and Private Three-Party Publish/Subscribe," G. Di Crescenzo, J. Burns, B. Coan, J. Schultz, J. Stanton, S. Tsang, and R. Wright, *Proceedings of the 7th International Conference on Network and System Security (NSS)*, 2013, pp. 278–292

[52] "A Differentially Private Estimator for the Stochastic Kronecker Graph Model," D. Mir* and R. Wright, *Proceedings of the 2012 Workshop on Privacy and Anonymity in the Information Society*, 2012, pp. 167–176

[53] "Towards a Formal Model of Accountability," J. Feigenbaum, A. Jaggard, and R. Wright, *Proceedings of the 2011 New Security Paradigms Workshop (NSPW)*, 2011, pp. 45–56

[54] "Accountability and Deterrence in Online Life," J. Feigenbaum, J. Hendler, A. Jaggard, D. Weitzner, and R. Wright, *Proceedings of the Third International Conference on Web Science (WebSci)*, 2011, pp. 7:1–7:7

[55] "Brief Announcement: Distributed Computing with Rules of Thumb," A. Jaggard, M. Schapira§, and R. Wright, *Proceedings of the 30th Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC)*, 2011, pp. 333-334

[56] "Pan-private Algorithms via Statistics on Sketches," D. Mir*, S. Muthukrishnan, A. Nikolov*, and R. Wright, *Proceedings of the 30th ACM Symposium on Principles of Database Systems (PODS)*, 2011, pp. 37–48

[57] "Distributed Computing with Adaptive Heuristics," A. Jaggard, M. Schapira§, and R. Wright,

*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

Proceedings of Innovations in Computer Science, 2011, pp. 417–443. ([4] is an extended version of this paper.)

[58] "A Practical Differentially Private Random Decision Tree Classifier," G. Jagannathan*, K. Pillaipakkamnatt, and R. Wright, *Proceedings of the Ninth IEEE International Conference on Data Mining – Workshops*, 2009, pp. 114–121. ([5] is an extended version of this paper.)

[59] "A Differentially Private Graph Estimator," D. Mir* and R. Wright, *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.]*

[60] "Privacy-Preserving Evaluation of Generalization Error and Its Application to Model and Attribute Selection," J. Sakuma and R. Wright, *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

[61] "Interstate Voter Registration Database Matching: The Oregon-Washington 2008 Pilot Project," R. M. Alvarez, J. Jonas, W. Winkler, and R. Wright, *Proceedings of the 2009 Electronic Voting Workshop / Workshop on Trustworthy Elections*, 2009. (Electronic proceedings only)

[62] "The Impact of Communication Models on Routing-Algorithm Convergence," A. Jaggard, V. Ramachandran, and R. Wright, *Proceedings of the 29th International Conference on Distributed Computing Systems (ICDCS)*, 2009, pp. 58–67

[63] "Rationality and Traffic Attraction: Incentives for Honest Path Announcements in BGP," S. Goldberg*, S. Halevi, A. Jaggard, V. Ramachandran, and R. Wright, *Proceedings of the ACM SIGCOMM 2008 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM)*, 2008, pp. 267–278

[64] "Privacy-Preserving Reinforcement Learning," J. Sakuma, S. Kobayashi, and R. Wright, *Proceedings of the 25th International Conference on Machine Learning (ICML)*, 2008, pp. 864–871

[65] "On the Lindell-Pinkas Secure Computation of Logarithms: From Theory to Practice," R. Ryger* O. Kardes*, and R. Wright, *Proceedings of the International Workshop on Practical Privacy-Preserving Data Mining*, 2008. (Electronic proceedings only)

[66] "Private Inference Control for Aggregate Queries," G. Jagannathan* and R. Wright, *Proceedings of the Seventh IEEE International Conference on Data Mining – Workshops*, 2007, pp. 711–716

[67] "Towards Privacy-Preserving Model Selection," Z. Yang*, S. Zhong, and R. Wright, *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

*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

[68] "Private Multiparty Sampling and Approximation of Vector Combinations," Y. Ishai, T. Malkin, M. Strauss, and R. Wright, *Proceedings of the 34th International Colloquium on Automata, Languages and Programming (ICALP)*, 2007, pp. 243–254. ([7] is an extended version of this paper.)

[69] "Privacy-Preserving Data Imputation," G. Jagannathan* and R. Wright, *Proceedings of the Sixth IEEE International Conference on Data Mining – Workshops*, 2006, pp. 535–540. ([8] is an extended version of this paper.)

[70] "Secure Set Membership Using 3SAT," M. de Mare* and R. Wright, *Proceedings of the Eighth International Conference on Information and Communications Security (ICICS)*, 2006, pp. 452–468

[71] "Privacy-Preserving Queries on Encrypted Data," Z. Yang*, S. Zhong§, and R. Wright, *Proceedings of the 11th European Symposium on Research In Computer Security (Esorics)*, 2006, pp. 479–494

[72] "A New Privacy-Preserving Distributed k-Clustering Algorithm," G. Jagannathan*, K. Pillaipakkamnatt, and R. Wright, *Proceedings of the 2006 SIAM International Conference on Data Mining (SDM)*, 2006, pp. 492–496. ([6] is an extended version of this paper.)

[73] "Implementing Privacy-Preserving Bayesian-Net Discovery for Vertically Partitioned Data," O. Kardes*, R. Ryger*, R. Wright, and J. Feigenbaum, *Proceedings of the ICDM Workshop on Privacy and Security Aspects of Data Mining*, 2005, pp. 26–34

[74] "Distributed Data Mining Protocols for Privacy: A Review of Some Recent Results," R. Wright, 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

[75] "Anonymity-Preserving Data Collection," Z. Yang*, S. Zhong§, and R. Wright, *Proceedings of the 11th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, (KDD)*, 2005, pp. 139–147

[76] "Privacy-Preserving Distributed k-Means Clustering over Arbitrarily Partitioned Data," G. Jagannathan*and R. Wright, *Proceedings of the 11th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, 2005, pp. 593–599

[77] "Privacy-Enhancing k-Anonymization of Customer Data," S. Zhong§, Z. Yang*, and R. Wright, *Proceedings of the 24th ACM Symposium on Principles of Database Systems (PODS)*, 2005, pp. 139–147

[78] "Privacy-Preserving Classification of Customer Data without Loss of Accuracy," Z. Yang*, S. Zhong§, and R. Wright, *Proceedings of the 2005 SIAM International Conference on Data Mining (SDM)*, 2005, pp. 92–102

*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

[79] "Improved Privacy-Preserving Bayesian Network Parameter Learning on Vertically Partitioned Data," Z. Yang* and R. Wright, *Proceedings of the ICDE International Workshop on Privacy Data Management*, 2005, pp. 43–52. ([10] is a combined and extended version of this paper and [81].)

[80] "Experimental Analysis of Privacy-Preserving Statistics Computation," H. Subramaniam†, R. Wright, and Z. Yang*, *Proceedings of the VLBD Workshop on Secure Data Management*, Lecture Notes in Computer Science, Vol. 3178, Springer, 2004, pp. 55–66. ([12] is an extended version of this paper.)

[81] "Privacy-Preserving Bayesian Network Structure Computation on Distributed Heterogeneous Data," R. Wright and Z. Yang*, *Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, 2004, pp. 713–718. ([10] is a combined and extended version of this paper and [79].)

[82] "Accountable Privacy," M. Burmester, Y. Desmedt, R. Wright, and A. Yasinsac, *Proceedings of the Twelfth International Workshop on Security Protocols*, Lecture Notes in Computer Science, Vol. 3957, Springer, 2004, pp. 83–96

[83] "Fischer's Cryptographic Protocols," R. Wright, *Proceedings of Twenty-Second Annual ACM Symposium on Principles of Distributed Computing (PODC)*, 2003, pp. 20–22. Invited paper.

[84] "Privacy Tradeoffs: Myth or Reality? (Panel Summary)," R. Wright, L. 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

[85] "Tight Bounds for Shared Memory Systems Accessed by Byzantine Processes," M. Merritt, O. Reingold, G. Taubenfeld, and R. Wright, *Proceedings of 16th International Symposium on Distributed Computing (DISC)*, Lecture Notes in Computer Science, Vol. 2508, Springer-Verlag, 2002, pp. 222–236. ([13] is an extended version of this paper.)

[86] "Off-Line Generation of Limited-Use Credit Card Numbers," A. Rubin and R. Wright, *Proceedings of Financial Cryptography 2001 (FC)*, Lecture Notes in Computer Science, Vol. 2339, Springer-Verlag, 2002, pp. 196–209

[87] "Selective Private Function Evaluation with Application to Private Statistics," R. Canetti, Y. Ishai§, R. Kumar, M. Reiter, R. Rubinfeld, and R. Wright, *Proceedings of Twentieth Annual ACM Symposium on Principles of Distributed Computing (PODC)*, 2001, pp. 293–304

[88] "Secure Multiparty Computation of Approximations," J. Feigenbaum, Y. Ishai§, T. Malkin, K. Nissim*, M. Strauss, and R. Wright, *Proceedings of 28th International Colloquium on Automata, Languages and Programming (ICALP)*, Lecture Notes in Computer Science, Vol. 2076, Springer-Verlag, 2001, pp. 927–938. ([9] is an extended version of this paper.)

[89] "Efficient Fault-Tolerant Certificate Revocation," P. Lincoln, J. Millen, and R. Wright, *Pro-*

*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

ceedings of the Seventh ACM Conference on Computer and Communications Security (CCS), 2000, pp. 19–24. ([17] is an extended version of this paper.)

[90] "Reasoning about Trust and Insurance in a Public Key Infrastructure" J. Millen and R. Wright, *Proceedings of 13th IEEE Computer Security Foundations Workshop (CSFW)*, IEEE Computer Society, 2000, pp. 16–22

[91] "Dynamic Byzantine Quorum Systems" L. Alvisi, D. Malkhi, E. Pierce*, M. Reiter, and R. Wright, *Proceedings of the International Conference on Dependable Systems and Networks (DSN)*, 2000, pp. 283–292

[92] "Obstacles to Freedom and Privacy by Design," *Proceedings of the 10th Conference on Computers, Freedom and Privacy (CFP)*, R. Wright, Workshop on Freedom and Privacy by Design, 2000, pp. 97–100

[93] "Influencing Software Usage," L. Cranor and R. Wright, *Proceedings of the 10th Conference on Computers, Freedom and Privacy (CFP)*, Workshop on Freedom and Privacy by Design, 2000, pp. 45–55

[94] "Certificate Revocation the Responsible Way," J. Millen and R. Wright, *Proceedings of Computer Security, Dependability, and Assurance: From Needs to Solutions*, IEEE Computer Society, 1999, pp. 196–203. Invited paper

[95] "Experimental Performance of Shared RSA Modulus Generation," S. Spalding‡ and R. Wright, *Proceedings of the Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, January 1999, pp. 983–984. ([16] is an extended version of this paper.)

[96] "Probabilistic Byzantine Quorum Systems," D. Malkhi, M. Reiter, A. Wool, and R. Wright, *Proceedings of Seventeenth Annual ACM Symposium on Principles of Distributed Computing (PODC)*, 1998, p. 321. ([18] is a combined and extended version of this paper and [99].)

[97] "SubScribe: Secure and Efficient Data Delivery/Access Services in a Push-Based Environment," A. Datta, A. Celik*, A. Biliris, and R. Wright, *Proceedings of the First International Conference on Telecommunications and Electronic Commerce (ICTEC)*, 1998, (page numbers unknown, 30 pages)

[98] "Secure Communication in Minimal Connectivity Models," M. Franklin and R. Wright, *Advances in Cryptology – Proceedings of Eurocrypt '98*, Lecture Notes in Computer Science, Vol. 1403, Springer-Verlag, 1998, pp. 346–360. ([19] is an extended version of this paper.)

[99] "Probabilistic Quorum Systems," D. Malkhi, M. Reiter, and R. Wright, *Proceedings of Sixteenth Annual ACM Symposium on Principles of Distributed Computing (PODC)*, 1997, pp. 267–273. ([18] is a combined and extended version of this paper and [96].)

*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

[100] "The Ω Key Management Service," M. Reiter, M. Franklin, J. Lacy, and R. Wright, *Proceedings of the Third ACM Conference on Computer and Communications Security (CCS)*, 1996, pp. 38–47. ([20] is an extended version of this paper.)

[101] "An Authentication Logic Supporting Synchronization, Revocation, and Recency," S. Stubblebine and R. Wright, *Proceedings of the Third ACM Conference on Computer and Communications Security (CCS)*, 1996, pp. 95–105. ([15] is an extended version of this paper.)

[102] "An Efficient Protocol for Unconditionally Secure Secret Key Exchange," M. Fischer and R. Wright*, *Proceedings of the 4th Annual Symposium on Discrete Algorithms (SODA)*, 1993, pp. 475–483

[103] "Multiparty Secret Key Exchange Using a Random Deal of Cards," M. Fischer and R. Wright*, *Advances in Cryptology – Proceedings of Crypto '91*, Springer-Verlag, Lecture Notes in Computer Science, Vol. 576, 1992, pp. 141–155. ([21] and [26] are extended versions of parts of this paper.)

[104] "Finite-State Approximation of Phrase-Structure Grammars," F. Pereira and R. Wright*, *Proceedings of the 29th Annual Conference of the Association for Computational Linguistics (ACL)*, 1991, pp. 246–255. ([25] is an extended version of this paper.)

Other publications

[105] "Public Interest Technology (PIT) Roundtable Discussions PIT Benefits, Barriers, and Recommendations for the Computing Research Community," A. Soley, D. Mulligan, J. Kurose, and E. Gonzalez, Computing Research Association, 2025, contributor

[106] "AI and Human Rights: Building a Tech Future Aligned With the Public Interest," All Tech Is Human, 2022

[107] "Keynote: Privacy in Today's World," R. Wright, *Proceedings of the 2017 Workshop on Women in Cyber Security (CyberW)*, 2017, pp. 7–10

[108] "Schooling excellence," R. Wright and M. Cozzens, International Innovation, North America edition, Research Media, 2013, pp. 17–19

[109] "Your Data and Your Privacy: Do you know what 'they' can tell about you?," P. Kehle and R. Wright, A curricular module in the DIMACS Value of Computational Thinking project, for use in high-school classrooms, 2013

[110] "Accountability as an interface between cybersecurity and social science," J. Feigenbaum, A. Jaggard, and R. Wright, in Lance J. Hoffman, editor, Social Science, Computer Science, and Cybersecurity Workshop Summary Report, 2013. George Washington University CSPRI report GW-CSPRI-2013-02

*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

[111] "Improving State Voter Registration Databases: Final Report," Committee on State Voter Registration Databases, National Research Council, The National Academies Press, 2010

[112] "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

[113] "Statewide Databases of Registered Voters: Study Of Accuracy, Privacy, Usability, Security, and Reliability Issues," P. Hawthorn, B. Simons, S. M. Bellovin, C. Clifton, L. Coney, R. Gellman, H. Hochheiser, A. Rosenthal, R. Poore, D. Wagner, and R. Wright, commissioned by the U.S. Public Policy Council of the Association for Computing Machinery (USACM), 2006

[114] "Achieving Perfect Secrecy Using Correlated Random Variables," R. Wright*, Ph.D. Thesis, Department of Computer Science, Yale University, YALEU/CSD/RR #1058, January 1995

[115] "Can You Keep a Secret? An Introduction to Cryptography," R. Wright*, *Omnibus*, Yale University Computing & Information Systems Supplement to the Yale Weekly Bulletin and Calendar, Vol. 6, No. 3, November 1993

[116] "DataMesh research project, phase 1," J. Wilkes, C. Chao, R. English, D. Jacobson, S. Lo*, C. Ruemmler†, B. Sears, A. Stepanov, and R. Wright*, *Proc. USENIX Workshop on File Systems*, 1992, pp. 63–69

[117] "A Library for Multithread Synthetic Trace Generation," R. Wright*, Hewlett-Packard Laboratories Technical Report HPL–92–108, 1992

*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