

Poorvi L. Vora

Dept. of Computer Science
George Washington University
Washington D.C. 20052

202 994 1864
poorvi@gwu.edu
<http://www.seas.gwu.edu/~poorvi>

Major Research Interests:

Privacy, cryptology, electronic voting, game theory, information theory and coding

Education

Ph.D., Computer Engineering. North Carolina State University (1993)

Dissertation Title: Optimization Criteria and Numerical Analysis in the Design of Colour Scanning Filters

Dissertation Adviser: H. Joel Trussell

M.S., Mathematics. Cornell University (1990)

Informal focus: Commutative Algebra

M.S., Electrical Engineering. North Carolina State University (1988)

Thesis Topic: Bounds on the Improvement of Restoration Using Spatial a priori Information

Thesis Adviser: H. Joel Trussell

B. Tech., Electrical Engineering. Indian Institute of Technology, Bombay (1986)

Experience

Assistant Professor, Fall 2003-current

Dept. of Computer Science, George Washington University

At Hewlett-Packard Co. (Oct. 1995-July 2003)

– *Security Architect*, Office of the CTO, Imaging and Printing, Oct. 2002-Aug. 2003

– *Senior Technical Contributor*, Hewlett-Packard Labs., Jan. 2001-Oct. 2002

– *Project Manager*, Mar. 2000-Jan. 2001

– *Member Tech. Staff and Project Scientist*, Hewlett-Packard Labs., Oct. 1995-Mar. 2000

Assistant Professor, Fall 1994-Fall 1995

Biomedical Engineering, Indian Institute of Technology, Bombay

Research Scientist, Nov. 1993-May 1994

Ravi Database Consultants (RDC), Bombay, India

Current Doctoral Students

Yu-An Sun, Benjamin Hosp (ARCS Scholar: 2005-06, 2006-07), Ricardo Martin

Graduated Thesis Master's Students

Rajat Bhatt, (2005), Darakhshan Mir (2006).

Research Grants

1. Poorvi Vora, Jonathan Stanton, Rahul Simha. SGER: A Performance Ratings Framework for the Evaluation of Electronic Voting Systems. National Science Foundation. \$85,582. March 1, 2005-February 28, 2006.
2. Poorvi Vora. Stream Ciphers, Fast Encryption and Digital Rights Management in the Home. Research gift from Hewlett-Packard, \$30,000.
3. Poorvi Vora and Sumit Joshi. Randomized Auctions and the Economic Value of Privacy. Dilthey Award. \$12,130. July-August 2004.

Classes Taught

At *GW*: Discrete Structures II (undergraduate); Computer Security Systems I (undergraduate and graduate); Cryptography (undergraduate and graduate); Advanced Cryptography.

At *IIT-Bombay*: Medical Signal and Image Processing; Partial Differential Equations; Medical Physics (jointly with A. Mahajan)

At *Cornell*: Calculus; Pre-freshman Mathematics

Curriculum Development

- Designed and proposed Advanced Cryptography.
- Co-proposer on changes in doctoral program.
With: Bhagirath Narahari, Rahul Simha, Xiuzhen Cheng, Jonathan Stanton and Shmuel Rotenstreich.
- Co-proposer on changes in undergraduate security option and graduate security certificate.
With Jonathan Stanton.
- Co-designer and co-proposer, Discrete Structures II.
With Abdou Youssef.

Service

External

- Co-chair, Technical Committee, and Organizer, *Voting Systems Ratings Workshop*, 2006.
- Program Committee: *VoComp*, 2007; *ACM CCS*, 2006; *WOTE*, 2006 and 2007.
- Session Chair: *ACM CCS*, 2006; *SKM*, 2006
- Invited expert at meeting on New Currency Designs
Bureau of Engraving and Printing, Dept. of the Treasury, US Govt, 2004
- Founding Member of *Voting System Performance Ratings (VSPR)*
- Chair, Working Group on Privacy Measurement Criteria, *VSPR*
- Participant, *DIMACS/Portia Working Group on Privacy in Data Mining*, 2004
- Reviewer: *IEEE Trans. Info. Security and Forensics*, *IEEE Trans. Computers*, *IEEE Trans. Image Proc.*, *IEEE Trans. Signal Processing*, *IEEE Trans. Knowledge and Data Engineering*, *IEEE Security and Privacy*, *Electronic Imaging*, *Journal Optical Society of America - A*.

Departmental

- Co-Director, graduate certificate program in Computer Security and Information Assurance.
With Jonathan Stanton. Fall 2005 - current.
- Outreach Committee, Fall 2003 - current.
- Graduate Admissions and Support Committee: Fall 2003 - current.
- Curriculum Committee: AY 2004-2005

– Prelim Exam Committee: AY 2003-2004.

Publications

Journal Papers

1. Poorvi Vora. An Information-Theoretic Approach to Inference Attacks on Random Data Perturbation and a Related Privacy Measure. *In review*
2. P.L. Vora, B. Adida, R. Bucholz, D. Chaum, D.L. Dill, D. Jefferson, D.W. Jones, W. Lattin, A.D. Rubin, M.I. Shamos, and M. Yung. Evaluation of Voting Systems. *Inside Risks Column. Communications of the ACM*, vol. 47, no. 11, pg. 144, November 2004.
3. K. Gopalakrishnan, Nasir D. Memon and Poorvi Vora. Protocols for Watermark Verification. *IEEE MultiMedia*, special issue on Multimedia and Security, vol. 8, no. 4, pp. 66-70, Oct.-Dec. 2001. Also in *Proceedings of the Multimedia and Security Workshop*, Oct. 1999.
4. Poorvi L. Vora. Inner products and orthogonality in colour recording filter design. *IEEE Trans. Image Proc.*, vol. 10, no. 4, pp. 632-642, Apr. 2001. Available in pre-reviewed form as Hewlett-Packard Technical Report, HPL-98-189, November 1998.
5. Poorvi L. Vora, Joyce E. Farrell, Jerome D. Tietz, David H. Brainard. Image capture: modelling and calibration of sensor responses and their synthesis from multispectral images. *IEEE Trans. Image Proc.*, vol. 10, no. 2, pp. 307-316, Feb. 2001. Available in pre-reviewed form as Hewlett-Packard Technical Report, HPL-98-187, November 1998.
6. Poorvi L. Vora and H. Joel Trussell. Mathematical Methods for the Analysis of Color Scanning Filters. *IEEE Trans. Image Process.*, vol. 6, no. 2, pp. 321-327, Feb. 1997.
7. Poorvi L. Vora and H. Joel Trussell. Mathematical Methods for the Design of Color Scanning Filters. *IEEE Trans. Image Process.*, vol. 6, no. 2, pp. 312-320, Feb. 1997.
8. P. L. Vora and H. J. Trussell. Measures of goodness of a set of color scanning filters. *Journal of the Optical Society of America-A*, vol. 10, no. 7, pp. 1499-1508, 1993.

Conference Papers

1. Sumit Joshi, Yu-An Sun, Poorvi Vora. Randomization as a Seller Strategy during Price Discrimination, and its Impact on Bidder Privacy. *ACM Workshop on Privacy in the Electronic Society*, October 2006.
2. Poorvi L. Vora, Darakhshan Mir. Related-Key Linear Cryptanalysis. *Int. Symp. Info. Theory*, July 2006.
3. Sumit Joshi, Yu-An Sun, Poorvi Vora. The Privacy Cost of the Second-Chance Offer. *ACM Workshop on Privacy in the Electronic Society*, October 2005.
4. Lillie Coney, Joseph L. Hall, David Wagner, Poorvi L. Vora. Towards a Privacy Measurement Criterion for Voting Systems. Poster Paper, *National Conference on Digital Government Research*, Atlanta, May 2005.
5. Poorvi Vora. Information Theory and the Security of Binary Data Perturbation. *Progress in Cryptology - INDOCRYPT 2004: 5th International Conference on Cryptology in India*, Chennai, India. pp 136-147. LNCS 3348. December 2004.
6. Cormac Herley, Poorvi Vora and Xuguang Yang. Detection and Deterrence of Counterfeit of Valuable Documents. *Proceedings, Int. Conf. Image Proc.*, 2004.
7. Poorvi Vora. The channel coding theorem and the security of binary randomization. *Proc., 2003 IEEE Int. Symposium of Information Theory*, Yokohama, Japan, June 30 - July 4, pp. 306, 2003.
8. Nasir Memon, Boon-Lock Yeo, Minerva Yeung and Poorvi Vora. Distortion bounded authentication techniques. *Proceedings of the SPIE, Security and Watermarking of Multimedia Contents II*, vol.3971, pp. 164-74, 24-26 Jan. 2000.

9. Poorvi Vora. Robust Watermarking Using Argument Modulation. *PICS (Image Processing, Image Quality, Image Capture Systems)*, 1999.
10. R. L. Baer, W. D. Holland, J. Holm and P. L. Vora. A Comparison of Primary and Complementary Color Filters for CCD-based Digital Photography. *SPIE/IS&T*, 1999.
11. Nasir Memon and Poorvi Vora. Authentication Techniques for Multimedia Content. *Photonics East*, Boston, MA, Oct. 1998.
12. C. Herley and Poorvi Vora. Trade-offs between noise sensitivity and color saturation in image sensors. *Proceedings, Int. Conf. on Image Proc.*, 1998.
13. P. L. Vora, J. E. Farrell, J. D. Tietz, D. H. Brainard. Linear Models for Digital Cameras. *Proceedings, IS&T's 50th Annual Conf.*, 1997.
14. P. L. Vora, J. E. Farrell, J. D. Tietz, M. Harville, D. H. Brainard. Image capture: synthesis of sensor responses from multispectral images. *SPIE and IS&T Conf. on Color Imaging: Device-Independent Color, Color Hard Copy, and Graphic Arts II*, 1997
15. B. Bhumkar, B. Chandna, K. Shankar and P. L. Vora. A Set Theoretic Approach to Image Reconstruction from Projections. *Int. Conf. On Image Proc.*, 1996.
16. P. L. Vora, H. J. Trussell and L. Iwan. Design Results for a Set of Thin Film Color Scanning Filters. *IS&T/SPIE Symposium on Electronic Imaging, Science and Technology*, 1995.
17. A Mathematical Method for the Design of Color Scanning Filters. *IS&T/SPIE Symposium on Electronic Imaging, Science and Technology*, 1993.
18. H. J. Trussell and P. L. Vora. On the Accuracy of Scanning Color Images. *International Conf. on Acoustics, Speech and Signal Processing*, 1992.
19. P. L. Vora and H. J. Trussell. Measures of Goodness of a Set of Color Scanning Filters. *SPIE and IS&T Conf. on Color Hard Copy and Graphic Arts*, 1992.
20. H. J. Trussell and P. L. Vora. Bounds on Restoration Quality Using Spatial a priori Information. *International Conf. on Acoustics, Speech and Signal Processing*, 1988.

Book Chapters

1. I. Dickinson, D. Reynolds, D. Banks, S. Cayzer, P. L. Vora. User profiling with privacy: a foundation for adaptive information agents. *Intelligent Information Agents: An AgentLink Perspective*, Chp. 4. Editors: Matthias Klusch, Sonia Bergamaschi, Pete Edwards, Paolo Petta. Springer Verlag, LNCS State of the Art Surveys, 2003.

Technical Reports not Listed Above

1. Poorvi L. Vora. David Chaum's Voter Verification using Encrypted Paper Receipts. IACR eprint archive, no. 2005/050. February 2005. <http://eprint.iacr.org/2005/050.pdf>
2. Cormac Herley, Xuguang Yang, Poorvi Vora. HP-Confidential report on counterfeit deterrence, 1999
3. Renato Kresch, Xuguang Yang, Poorvi Vora. HP-Confidential report on counterfeit deterrence, 2001
4. P. L. Vora, J. E. Farrell, J. D. Tietz, D. H. Brainard. Digital Color Cameras - 2 - Spectral Response. Hewlett Packard Technical Report, HPL-97-54, March 1997. <http://www.hpl.hp.com/techreports/97/HPL-97-54.html>
5. P. L. Vora, J. E. Farrell, J. D. Tietz, D. H. Brainard. Digital Color Cameras - 1 - Response Models. Hewlett Packard Technical Report, HPL-97-53, March 1997. <http://www.hpl.hp.com/techreports/97/HPL-97-53.html>

Standards Position Papers

1. P. L. Vora, D. Reynolds, I. Dickinson, J. Erickson, D. Banks. Privacy and Digital Rights Management. A position paper for the W3C workshop on Digital Rights Management, January 2001, Antibes, France.
2. J. Erickson, M. Williamson, D. Reynolds, P. L. Vora and P. Rodgers. Principles for Standardization and Interoperability in Web-based Digital Rights Management. A position paper for the W3C workshop on Digital Rights Management, January 2001, Antibes, France.

Patent Applications Granted

1. Poorvi Vora and Verna Knapp. Anonymous transactions based on distributed processing. US 7,187,772. Issued March 6, 2007.
2. Cormac Herley, Xuguang Yang, Poorvi Vora. Detection and deterrence of counterfeiting of documents having a characteristic color. US 6748100. Issued June 8, 2004.
3. Xuguang Yang, Cormac Herley and Poorvi Vora. Multi-level detection and deterrence of counterfeiting of documents with reduced false detection. US 6516078. Issued February 4, 2003.
4. Poorvi Vora, Umesh Vazirani, Verna Knapp. Probabilistic Privacy Protection. US 6470299. Issued October 22, 2002.
5. Poorvi Vora. Robust watermarking for digital objects. US 6463162. Filed September 30, 1998. Issued October 8, 2002.
6. Cormac Herley and Poorvi Vora. Detection and deterrence of counterfeiting of two-sided documents. US6335794. Issued January 1, 2002.

Open-Source Release in Preparation

Ben Hosp, Rahul Simha, Jonathan Stanton, Poorvi Vora. Citizen Verified Voting. Open-source release of cryptographic core of electronic voting software.

Selected Recent Invited Presentations and Participation

1. Cryptanalysis
 - Indian Institute of Sciences, Bangalore, India, December 2006
 - Information Theory Seminar, University of Maryland, College Park, April 2006
 - Hewlett-Packard Laboratories, Princeton, February 2006
 - IBM Research, Hawthorne, February, 2006
2. Privacy.
 - TAMI/PORTIA Workshop, MIT, June 2006
 - Hewlett-Packard Laboratories, Palo Alto, August 2005.
 - DIMACS/Portia Workshop on Privacy in Data Mining, Rutgers University, March 2004
 - IBM Research, Hawthorne, April, 2003
 - Workshop on Privacy in Data, Carnegie Mellon University, March, 2003
 - Stanford Security Seminar, 2002
 - Georgia Tech Security Seminar, 2002
 - Microsoft Research, Redmond, 2002
 - Microsoft Research, Silicon Valley, 2002

3. Electronic Voting

- NSF Washington Area Trustworthy Systems Hour (WATSH) October 2004
- IEEE Student Chapter, Rochester University, September 2004
- REU Student Group, Brooklyn Polytechnic University, July 2004
- DIMACS Workshop on Electronic Voting, Rutgers University, May 2004

Media coverage

New York Times March 2, 2004. Science Edition. Did your vote count? New coded ballots may prove it did. By Sara Robinson.

SIAM News Volume 37, Number 3, April 2004. Works in progress: trustworthy cryptographic voting systems. By Sara Robinson.

CNET News.com. June 08, 2004. Electronic voting: Moving beyond the ballot box. Declan McCullagh.

Non-technical Publications and Presentations

1. Translations from The Urdu of Faiz Ahmed Faiz:

- On my return from Dacca. (*Dacca se wapasi par*), *To Topos Poetry International, PACIFICA: PEACE & the SEA*, Vol. 5, pg. 50, 2003.
- Shackles on your feet. (*Aaj Bazaar Mein*), *To Topos Poetry International, PACIFICA: PEACE & the SEA*, Vol. 5, pg. 49, 2003.
- August '52" (*Agast '52*), *To Topos Poetry International, PACIFICA: PEACE & the SEA*, Vol. 5, pg. 48, 2003.
- Poorvi Vora and Susan Chacko. The Ocean of Your Eyes. (*Teri Samandar Ankhon Mein*), 1995. <http://www.indolink.com/Poetry/oceanEye.html>.

2. Guest lecture on Faiz Ahmed Faiz, Hunter College, NY. Course on *Partition Literatures*.

Personal: U. S. citizen

Interests: road cycling, jazz dance, translating Urdu Poetry into English.