Poorvi L. Vora

Department of Computer Science
The George Washington University
Washington D.C. 20052

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

Major Research Interests:

Electronic voting, cryptology, privacy, game theory, information theory, color imaging

Education

Ph.D., Electrical 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)

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)

Positions

Professor, AY 2015-current
Undergraduate Program Director, Jan 2021-June 2023
Department of Computer Science, The George Washington University

Board of Directors, 2021-current
Board of Advisers, 2015-2020
Verified Voting Foundation

Associate Professor, AY 2009-2015
Department of Computer Science, The George Washington University

Visiting Associate Professor, AY 2011-2012, on sabbatical
Department of Computer Science and Engineering, Indian Institute of Technology-Bombay

Assistant Professor, AY 2003-AY 2009
Department of Computer Science, The George Washington University

Faculty Computer Scientist – Intermittent Appointment, 2008-2011
Security Technology Group, National Institute of Standards and Technology

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
School of Biomedical Engineering, Indian Institute of Technology-Bombay

Lecturer, Summer 1994
Department of Electrical Engineering, Indian Institute of Technology-Delhi

Research Scientist, Nov. 1993 - May 1994
Ravi Database Consultants (RDC), Bombay, India

Awards

- Public Engagement Award, Election Verification Network, 2017
- School of Engineering and Applied Science Outstanding Teacher Award for Associate/Full Professors, 2015 "in recognition of her demonstrated ability to greatly improve student learning in difficult courses in her field, and her exceptional student advising and mentoring approach"
- ACM Teacher of the Year Award, 2009. Shared with Bhagirath Narahari "for having greatly impacted the life of the students of the Class of 2009"

Doctoral Students

1. Sarah Alzakari, 2021
   Dissertation Title: *Partly-Pseudo-Linear Cryptanalysis of Lightweight ARX Block Ciphers SPECK and SPARX*
   Now at Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia
2. Reham Almukhlifi, 2020
   Dissertation Title: *Linear Cryptanalysis of Reduced-Round Simon-like Ciphers Using Super Rounds*
   Now at Taibah University, Al Madinah, Saudi Arabia
3. Hua Wu, 2020
   Dissertation Title: *Apollo - End-to-end Verifiable Internet Voting with Recovery from Vote Manipulation*
   Now at Google
   Funded in part by NSF
4. Kerry A. McKay, 2011
   Dissertation Title: *Analysis Of ARX Round Functions In Secure Hash Functions*
   Now at NIST
   Funded in part by NSF
5. Benjamin Hosp (ARCS Scholar: 2005-06; 2006-07), 2011
   Dissertation Title: *The Privacy And Verifiability of Voting Systems: Measures and Limits*
   Now at Progeny
   Funded in part by NSF
6. Stefan Popoveniuc, 2009 (co-advised by David Chaum)
   Dissertation Title: *A Framework For Secure Electronic Voting*
   Now at Amazon
   Funded in part by NSF
7. Yu-An Sun, 2009
   Dissertation Title: *The Second Chance Offer: Optimal Strategies for Sellers and Bidders*
   Now at UAW Retiree Medical Benefits

Thesis Master's Students

1. Oliver Broadrick, *Risk-Limiting Audit PROVIDENCE and Round Size Considerations*. 2023.

2. Darakhshan Mir, *Related-key linear cryptanalysis of DES*. 2006.
   Ph.D., Rutgers University, 2013.
   Now tenured Associate Professor of Computer Science and John P and Mary Jane Swanson Professor in Engineering and the Sciences at Bucknell.

3. Rajat Bhatt, *Related-key attacks on pseudo-random number generators*. 2005.
   Now at Microstrategy.

Supervised Undergraduate Research I have supervised a large number of undergraduates doing research. Here I list only those who I have published with in peer-reviewed venues.

1. Oliver Broadrick (B.S., 2022, M.S., 2023, now in PhD Program at UCLA)
   Funded in part by NSF and SUPER. Co-author on one paper for undergrad. Thesis M.S. and one more paper, see above.

2. Grant McClearn (B.S., 2021, M.S., Stanford, 2023, now in pre-med program at Univ. Virginia)
   Funded in part by NSF and SUPER. Co-author on three papers. Honorable mention, SEAS R&D Showcase.

3. Sarah Morin (B.S., 2021, Clare Booth Luce Scholar, SEAS Distinguished Scholar)
   Funded in part by NSF and SUPER. Co-author on three papers. Honorable mention, SEAS R&D Showcase.

4. John Wittrock (B.S., 2013, SEAS Distinguished Scholar, now at Google)
   Funded in part by NSF. Co-author on one paper and one book chapter.

5. Tyler Kaczmarek (B.S., 2013, PhD, U.C. Irvine, 2018, now at MIT Lincoln Labs.)
   Funded in part by NSF and GW-SEAS Summer Undergraduate Program in Engineering Research (SUPER). Co-author on one paper.

6. Jan Rubio (B. S., 2011, Freudenthal Award, Pelton Award Second Prize, now co-founder, Upside)
   Funded in part by NSF. Co-author on two papers.

7. Alex Florescu (B.S., 2010, Arnold P. Meltzer Award for Best Computer Science Senior Design Project (2010), M. S., 2011, now at Google, UK)
   Funded in part by NSF. Co-author on two papers.

Post-Doctoral Researchers Supervised

1. Filip Zagórski, October 2010-November 2011
   now Assistant Professor, University of Wrocław, Wrocław, Poland
   Fully-funded by NSF

2. Mridul Nandi, December 2009-August 2010
   now Assistant Professor, Indian Statistical Institute
   Fully-funded by NSF

Visiting Faculty Hosted

Ronald L. Rivest, Andrew and Erna Viterbi Professor of Electrical Engineering and Computer Science, MIT, October 2009

Ricardo Custodio, Dept. of Computer Science, Universidade Federal de Santa Catarina (UFSC), Brazil, AY 2006-07

Research Sponsorship

1. Poorvi L. Vora (PI), "RAPID: Sequential Sampling in Stages for Statistical Election Audits".
National Science Foundation CNS-2015253. $199,662
February 1, 2020-January 31, 2021

2. Poorvi L. Vora (PI) and Michael R. Clarkson, "TWC: TTP Option: Small: Open-Audit Voting Systems—Protocol Models and Properties".
National Science Foundation CNS-1421373. $704,554
September 1, 2014-August 31, 2017

3. Poorvi L. Vora, "Reasoning about Protocols with Human Participants".
National Security Agency, Subaward on Prime Award to University of Maryland, College Park (UMCP)[1] .
Estimated total award: $305,642
February 7, 2014-February 6, 2017; currently granted for first two years, renewed annually

4. Poorvi Vora (PI), Gabriel Parmer. "RAPID: Secure Bulletin Boards and Absentee Voting in Real-World Independently-Verifiable Elections".
National Science Foundation CNS-0937267. $99,673.
July 1, 2011-June 30, 2013.

5. Poorvi Vora. "EAGER: Electronic End-to-End Independently Verifiable (E2E) Voting Systems".
National Science Foundation CNS-0937267. $239,767.
October 1, 2009-September 30, 2012.

6. Poorvi Vora. "Statistical cryptanalysis of block ciphers as channel communication".
National Science Foundation CCF-0830576. $141,643.
September 1, 2008-August 31, 2011.

7. Poorvi Vora. "CT-ISG: The Privacy and Verifiability of Practical Voting Systems".
National Science Foundation CNS-0831149. $180,478.
September 1, 2008-August 31, 2011.

8. Poorvi Vora (PI), Jonathan Stanton, Rahul Simha. "SGER: A Performance Ratings Framework for the Evaluation of Electronic Voting Systems".
National Science Foundation IIS-0505510. $85,582.
March 1, 2005-August 31, 2006.

9. Poorvi Vora.
Research Gift, Hewlett-Packard Co.. $30,000.
AY 2004-2005

10. Poorvi Vora (PI) and Sumit Joshi. "Randomized Auctions and the Economic Value of Privacy".
GW Dilthey Award. $12,129.
July-August 2004.

11. Poorvi Vora. Workshop Co-sponsorship: Threat Analyses for Voting System Categories: A Workshop on Rating Voting Methods (VSRW) 2006.
National Institute for Standards and Technology (NIST). Approximately $10,000.
Summer 2006.

[1] UMCP PI: Jonathan Katz.

Pedagogy

- **Classes Taught**

  At GW

  - *Special Topics: Game Theory in Computer Science*
  - *Cryptography*
  - *Advanced Cryptography*
  - *Computer Security*
  - *Discrete Structures II.*

  Guest Lectures:

  - CSCI 1010: Computer Science Orientation, multiple
  - Econ 8303, Microeconomics III: Fall 2013, four weeks
  - CSci 147, Team Project Development & Professional Ethics: Spring 2007, 2008
  - CSci 01, Computer Science Orientation: Fall 2006, 2007
  - CSci 178, Database Systems I: Fall 2003, 2004; Spring 2007
  - CSci 297, Electronic Voting: Fall 2004
  - CSci 41, Introduction to Computer Science: Fall 2004, 2005

  At IIT-Bombay

  Medical Signal and Image Processing, AY 1994-1995

  Partial Differential Equations, AY 1994-1995

  Computational Algebra and Number Theory, AY 2011-2012

  At Cornell University (While in graduate program — I had independent charge and was instructor for my section)

  Calculus I

  Calculus II

  Pre-freshman Mathematics

- **Curriculum Development**

  - Courses Proposed and Designed.
    - CSCI 3907/6907, Special Topics in Game Theory in Computer Science
    - CSCI 8331/381, Advanced Cryptography
    - CSCI 2312/124, Discrete Structures II (co-proposer: Abdou Youssef).
  - Courses Designed
    - CSCI 4331/6331/162, Cryptography
  - Director of CSIA graduate certificate program: Fall 2005-2011 (joint with former faculty member Jonathan Stanton until Fall 2008)

Selected Service

- Professional
  - Program Committees: *Voting*, 2016; *Vote-ID*, 2013, 2015; *WIFS*, 2012; *WOTE or EVT/WOTE*, 2006, 2007, 2011; *ICISS*, 2008, 2010; *CANS*, 2010; *NIST End-to-End Voting Workshop*, 2009; *RE-Vote*, 2009; *EVOTE*, 2008; *VoComp*, 2007; *ACM CCS*, 2006.
  - Invited Participation, Technical Team, End-to-End Verifiable Internet Voting Project of the Overseas Vote Foundation, 2014–2015
  - Associate Editor: *IEEE Transactions on Information Forensics and Security*, 2010-2013
  - Guest Editor: *IEEE Transactions on Information Forensics and Security*, special issue on electronic voting, December 2009.
    With: Ronald L. Rivest (Lead GE), David Chaum, Bart Preneel, Aviel D. Rubin, Donald G. Saari
  - Invited external expert, Selection Committee (faculty hiring and promotion), DAIICT, Gandhinagar, India: 2012, 2013
  - Invited Participant:
    - ∗ 2010 NSF Workshop on the Future of Trustworthy Computing, October 27-29, 2010, Arlington, VA
    - ∗ US-EU workshop on "International Co-operation in Trustworthy Systems: Security, Privacy and Trust in Large-Scale Global Networks & Services as Part of the Future Internet", Madrid, Spain, March 30-April 1, 2009, organized by the National Science Foundation and the European Union.
    - ∗ *DIMACS/Portia Working Group on Privacy in Data Mining*, 2004
  - Invited expert at meeting on New Currency Designs, Bureau of Engraving and Printing, Dept. of the Treasury, US Govt. Fall 2004
  - Reviewer for *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
  - Curriculum Committee Chair, 2021-2023
  - Undergraduate Adviser, AY 2013-2018; 2021-current
  - MS Adviser, AY 2003-2017
  - Faculty Mentor for Assistant Professor Claire Monteleoni, AY 2011-2017
  - Curriculum Committee: AY 2004; AY 2009-2011; AY 2014-2017;
  - Graduate Applications and Support Committee: AY 2003-2008; AY 2014-2015
  - Women in Computer Science (WiCS): AY 2003-2004 (introduced and managed); AY 2009 - 2011 (managed); AY 2012-2014
  - Director, graduate certificate program in Computer Security and Information Assurance: AY 2005-2011. (Co-director with Prof. Jonathan Stanton, 2005-2008)
  - Undergraduate Recruiting: several lectures at Chantilly Academy, part of the Fairfax County High School system.
- School of Engineering and Applied Science (SEAS)
  - Pelton Award (Best Senior Design Project) Judge: 2014, 2015
  - R&D Showcase – co-Chief Judge, 2015, 2016
  - Promotion & Tenure Subcommittee (elected for two year term: 2016-2018)

- Community
  - Written testimony to Maryland House Ways and Means Commitee, 2020, 2021, 2022.
  - *Board of Directors*, Verified Voting, 2021-current
  - Written deposition for Citizens Commission on Elections, India, 2020.
  - *Coordinating Committee*, Election Verification Network, 2018-2020.
  - Oral and written testimony to Maryland House Ways and Means Commitee, 2017, 2018.
  - Invited written and oral testimony, Maryland Legislature: House Ways and Means Committee Senate Education, Health and Environmental Affairs Committee Joint Hearing on Election Cybersecurity, 6 September 2017.
  - Oral and written testimony to State Board of Elections, MD, multiple times over 2016, 2017.
  - *Board of Advisers*, Verified Voting, 2015-2020
  - Member of the Scantegrity project, which deployed a voting system for Takoma Park city elections, 2009 and 2011
  - Guest Lectures on cryptography, Chantilly Academy, Fairfax County High Schools: Spring 2007, 2008, 2010
  - Chantilly Academy Award "in recognition and grateful appreciation of exceptional leadership support": 2007 and 2008.
  - Guest lecture on Pakistani poet Faiz Ahmed Faiz, Hunter College, NY. Course on *Partition Literatures.*

Publications

From 2004 onwards, I have attempted to list authors in alphabetical order in my publications. Those authors who are (intentionally) not listed alphabetically are marked with *.

Co-authors who were my students or post-docs at the time the work was done are marked with †.

Click on the paper title in the electronic copy of the CV to link to a copy of the paper.

Journal Papers Appeared (including Periodicals)

1. Reham Almukhlifi*† and Poorvi L. Vora. "Linear Cryptanalysis of Reduced-Round SIMECK Using Super Rounds" *Cryptography*, vol. 7, no. 1, 2023. Similar draft also available as IACR Cryptology ePrint Archive, vol. 2022, no. 1731, 9 February, 2023.

2. Sarah Alzakari*† and Poorvi L. Vora. "Partly-Pseudo-Linear Cryptanalysis of Reduced-Round Speck.". *Cryptography*, vol. 5, no. 1, 2021.

3. Reham Almukhlifi*† and Poorvi L. Vora. "Linear Cryptanalysis of Reduced-Round Simon Using Super Rounds.". *Cryptography*, vol. 4, no. 1, 2020. Similar draft also available as IACR Cryptology ePrint Archive, vol. 2020, no. 290, 7 March, 2020.

4. Sumit Joshi* and Poorvi L. Vora. "Weak and Strong Multimarket Bidding Rings". *Economic Theory*, vol. 53, no. 3, pp. 657-696, June 2012.

5. Sumit Joshi, Yu-An Sun† and Poorvi L. Vora. "Price Discrimination and Privacy: a Note". *International Journal of Game Theory*, vol. 13, no. 1, pp. 83-92, March 2011.

6. David Chaum* , Richard T. Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc†, Ronald L. Rivest, Peter Y. A. Ryan, Emily Shen, Alan T. Sherman, and Poorvi L. Vora. "Scantegrity II: End-to-End Verifiability by Voters of Optical Scan Elections Through Confirmation Codes". *IEEE Transactions on Information Forensics and Security*. Special issue on electronic voting. Vol. 4, No. 4, Part I, pp 611-627, December 2009.

7. Yu-An Sun† and Poorvi L. Vora. "Auctions and Differential Pricing: Optimal Seller and Bidder Strategies in Second-Chance Offers". *Computational Economics*, Vol. 34, No. 3, pp. 243-271, October 2009.

8. David Chaum, Ben Hosp†, Stefan Popoveniuc† and Poorvi L. Vora. "Accessible Voter Verifiability". *Cryptologia*, Vol. 33, No. 3, pp. 283-291, July 2009.

9. Stefan Popoveniuc† and Poorvi L. Vora. "A framework for secure electronic voting". *Cryptologia*, Vol. 34, No. 3, pp. 236-257, June 2010.

10. Rahul Simha and Poorvi L. Vora. "Vote Verification using Hard AI Problems". *Journal of Information Assurance and Security*, Vol. 3, No. 4, pp. 270-278, 2008.

11. Ben Hosp† and Poorvi L. Vora. "An information-theoretic model of voting systems". *Mathematical and Computer Modelling*, special issue on: Mathematical Modeling of Voting Systems and Elections: Theory and Applications. Vol. 48, Nos.9-10, pp. 1628-1645, November 2008.

12. David Chaum*, Aleks Essex*, Richard Carback, Jeremy Clark, Stefan Popoveniuc, Alan T. Sherman, Poorvi Vora. "Scantegrity: End-to-End Voter Verifiable Optical-Scan Voting". *IEEE Security and Privacy*, special issue on electronic voting, Vol 6., No. 3, pp. 40-46, May/June 2008.

13. Poorvi L. Vora. "An Information-Theoretic Approach to Inference Attacks on Random Data Perturbation and a Related Privacy Measure". *IEEE Transactions on Information Theory*, Vol. 53, No. 8, pp 2971-2977, August 2007.

14. 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, pp. 144, November 2004.

15. 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, October-December 2001.

16. Poorvi L. Vora. "Inner Products and Orthogonality in Color Recording Filter Design". *IEEE Transactions on Image Processing*, vol. 10, no. 4, pp. 632-642, April 2001.

17. Poorvi L. Vora, Joyce E. Farrell, Jerome D. Tietz, David H. Brainard. "Image Capture: Simulation of Sensor Responses from Hyperspectral Images". *IEEE Transactions on Image Processing*, vol. 10, no. 2, pp. 307-316, February 2001.

18. Poorvi L. Vora and H. Joel Trussell. "Mathematical Methods for the Analysis of Color Scanning Filters". *IEEE Transactions on Image Processing*, vol. 6, no. 2, pp. 321-327, February 1997.

19. Poorvi L. Vora and H. Joel Trussell. "Mathematical Methods for the Design of Color Scanning Filters". *IEEE Transactions on Image Processing*, vol. 6, no. 2, pp. 312-320, February 1997.

20. Poorvi L. Vora and H. Joel Trussell. "Measure of goodness of a set of color scanning filters". *Journal of the Optical Society of America-A*, vol. 10, no. 7, pp. 1499-1508, July 1993.

Guest Editor, Special Issue

1. Ronald L. Rivest*, David Chaum, Bart Preneel, Aviel D. Rubin, Donald G. Saari, Poorvi L. Vora. *IEEE Transactions on Information Forensics and Security*, vol 4, no. 4, Part I, December 2009. "Guest editorial".

Book Chapters

1. Richard T. Carback, David Chaum, Jeremy Clark, Aleksander Essex, Travis Mayberry, Stefan Popoveniuc, Ronald L. Rivest, Emily Shen, Alan T.Sherman, Poorvi L. Vora, John Wittrock, and Filip Zagórski, The Scantegrity Voting System and its Use in the Takoma Park Elections, Real-World Electronic Voting: Design, Analysis and Deployment, Feng Hao and Peter Ryan, CRC Press, Taylor & Francis Group, *in press*.

2. Ian Dickinson, Dave Reynolds, Dave Banks, Steve Cayzer, and Poorvi Vora. "User profiling with privacy: a framework for adaptive information agents". *Intelligent Information Agents: An AgentLink Perspective*, Chp. 4. Editors: Matthias Klusch, Sonia Bergamaschi, Pete Edwards, Paolo Petta. Springer Verlag, LNAI 2586, 2003.

Refereed Conference and Workshop Papers With Published Proceedings

Acceptance rates are mentioned where available.

1. Oliver Broadrick*†, Poorvi L. Vora and Filip Zagórski, "PROVIDENCE: a Flexible Round-by-Round Risk-Limiting Audit". USENIX Security, 2023. Acceptance Rate 422/1444 $\approx$ 0.292.
   Full version is at arXiv:2210.08717, first and only version, 17 October 2022.

2. Oliver Broadrick*†, Sarah Morin†, Grant McClearn†, Neal McBurnett, Poorvi L. Vora and Filip Zagórski, "Simulations of Ballot Polling Risk-Limiting Audits". Seventh Workshop on Advances in Secure Electronic Voting, in association with Financial Cryptography 2022.

3. Filip Zagórski*, Grant McClearn†, Sarah Morin†, Neal McBurnett and Poorvi L. Vora, "MINERVA–An Efficient Risk-Limiting Ballot Polling Audit", USENIX Security, 2021. Acceptance Rate 246/1316 $\approx$ 0.187.
   Full version with proofs is: Filip Zagórski*, Grant McClearn†, Sarah Morin†, Neal McBurnett and Poorvi L. Vora, "The Athena Class of Risk-Limiting Ballot Polling Audits", arXiv:2008.02315, first version 5 August 2020. Latest version 21 February, 2021.

4. Sarah A. Alzakari*†, Poorvi L. Vora. "Linear and Partly-Pseudo-Linear Cryptanalysis of Reduced-Round SPARX Cipher". *ATIS 2020*. Similar draft also available as IACR Cryptology ePrint Archive, vol. 2020, no. 290, 7 March, 2020.

5. Sarah Morin*†, Grant McClearn†, Neal McBurnett, Poorvi Vora and Filip Zagórski, "A Note on Risk-Limiting Bayesian Polling Audits for Two-Candidate Elections", Fifth Workshop on Advances in Secure Electronic Voting, workshop at Financial Crypto 2020. Full version with proofs is: Poorvi L. Vora. "Risk-Limiting Bayesian Polling Audits for Two Candidate Elections". CoRR abs/1902.00999, 2019.

6. Hua Wu*†, Poorvi Vora and Filip Zagórski. "Priv-Apollo - Secret Ballot E2E-V Internet Voting", *Voting '19*, workshop at Financial Cryptography, 2019.

7. Matthew Bernhard*, Josh Benaloh, J. Alex Halderman, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa Teague, Poorvi L. Vora, Dan S. Wallach: "Public Evidence from Secret Ballots", *E-Vote-ID*, 2017. Full version of the paper is at CoRR abs/1707.08619, 2017.

8. Dawid Gawel, Maciej Kosarzecki, Poorvi Vora, Hua Wu†, Filip Zagórski. "Apollo—End-to-end Verifiable Internet Voting with Recovery from Vote Manipulation", *E-Vote-ID*, 2016.

9. Tyler Kaczmarek*†, John Wittrock*†, Richard Carback, Alex Florescu†, Jan Rubio†, Noel Runyan, Poorvi L. Vora, Filip Zagórski†. "Dispute Resolution in Accessible Voting Systems: The Design and Use of Audiotegrity". *Vote-ID 2013*, Guildford, UK, 17-19 July, 2013. Springer LNCS vol. 7985, pp. 127-141. Acceptance Rate: 12/26 $\approx$ 0.46

10. Richard Carback, David Chaum, Jeremy Clark, Aleksander Essex, Poorvi L. Vora, Filip Zagórski†, "Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System". *ACNS 2013*, Banff, Canada, 25-28 June, 2013. Springer LNCS vol. 7954, pp. 441-457. Acceptance Rate: $33/150 \approx 0.22$

11. David Chaum, Alex Florescu†, Mridul Nandi†, Stefan Popoveniuc†, Jan Rubio†, Poorvi L. Vora, Filip Zagórski†. "Paperless Independently-Verifiable Voting". *VoteID 2011*, Tallinn, Estonia, 28-30 September 2011. Springer LNCS vol. 7187, pp 140-157. Acceptance Rate: $15/33 \approx 0.45$

12. Mridul Nandi†, Stefan Popoveniuc, Poorvi L. Vora. "Stamp-It: A Method for Enhancing the Universal Verifiability of E2E Voting Systems". *ICISS 2010*, Gandhinagar, India, 15-19 December 2010. Springer LNCS vol. Volume 6503, pp. 81-95. Acceptance Rate: $14/51 \approx 0.27$

13. Richard Carback*, David Chaum, Jeremy Clark, Aleksander Essex, Travis Mayberry, Stefan Popoveniuc†, Ronald L. Rivest, Emily Shen, Alan T. Sherman, Poorvi L. Vora. "Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy". *USENIX Security*, Washington, D.C., 11-13 August, 2010. Acceptance Rate: $30/202 \approx 0.15$

14. Stefan Popoveniuc, John Kelsey, Andrew Regenscheid, Poorvi Vora. "Performance Requirements for End-to-End Verifiable Elections". *EVT/WOTE 2010*, held in conjunction with USENIX Security, Washington, D.C., 9-10 August, 2010. Acceptance Rate: $15/38 \approx 0.39$

15. Alan T. Sherman*, Richard Carback*, David Chaum, Jeremy Clark, Aleksander Essex, Paul S. Herrnson, Travis Mayberry, Stefan Popoveniuc†, Ronald L. Rivest, Emily Shen, Bimal Sinha, Poorvi Vora. "Scantegrity Mock Election at Takoma Park". *EVOTE2010*, Bregenz, Austria, 21-24 July 2010. Acceptance Rate < 0.5

    - An abstract on this material was presented earlier with a slightly different author list, in a conference without published proceedings. This abstract is listed in a later section in this CV, and is mentioned here for completeness. Alan T. Sherman*, Richard Carback*, David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul S. Harrison, Travis Mayberry, Stefan Popoveniuc†, Ronald L. Rivest, Anne Sergeant, Emily Shen, Bimal Sinha, Poorvi Vora. "Scantegrity Mock Election at Takoma Park". *NIST End-to-End Voting Systems Workshop*, Washington DC, 13-14 October, 2009

16. Sumit Joshi, Yu-An Sun† and Poorvi L. Vora. "Privacy In A Multi-Stage Game – An Evolutionary Programming Approach". *Eproceedings of 10th Joint Conference on Information Sciences, 6th International Conference on Computational Intelligence in Economics & Finance*, Salt Lake City, Utah, 18-24 July 2007, pp 529-535.

17. Sumit Joshi, Yu-An Sun† and Poorvi Vora. "Randomization as a Strategy for Sellers During Price Discrimination, and Impact on Bidders' Privacy". Short paper, *5th ACM Workshop on Privacy in the Electronic Society (WPES)* held in association with *ACM CCS*, Alexandria, VA, 30 October, 2006, pp. 73-76. Acceptance Rate: $16/39 \approx 0.41$

18. Poorvi L. Vora* and Darakhshan J. Mir†. "Related-Key Linear Cryptanalysis". *IEEE International Symposium on Information Theory (ISIT)*, Seattle, WA, 9-14 July, 2006, pp. 1609-1613.

19. Sumit Joshi, Yu-An Sun†, Poorvi L. Vora. "The Privacy Cost of the Second-Chance Offer". *2005 ACM Workshop on Privacy in the Electronic Society (WPES)* held in association with *ACM CCS*, Alexandria, VA, 7 November, 2005, pp. 97-106. Acceptance Rate: $15/40 \approx 0.38$

20. Poorvi L. Vora. "Information Theory and the Security of Binary Data Perturbation". *INDOCRYPT 2004*, Chennai, India, 20-22 December, 2004. Springer LNCS 3348, pp. 136-147. Acceptance Rate: $30/147 \approx 0.20$

21. Cormac Herley*, Poorvi Vora and Shawn Yang. "Detection and Deterrence of Counterfeiting of Valuable Documents". *IEEE International Conference on Image Processing (ICIP)*, Singapore, 24-27 Oct. 2004, vol. 4, pp. 2423-2426.

22. Nasir D. Memon, Poorvi L. Vora, Boon-Lock Yeo, and Minerva M. Yeung. "Distortion-bounded authentication techniques". *SPIE Conference on Security and Watermarking of Multimedia Contents II*, San Jose, CA, 24-26 January 2000, vol. 3971, pp. 164-74.

23. K. Gopalakrishnan, Nasir D. Memon and Poorvi Vora. "Protocols for Watermark Verification". *Multimedia and Security Workshop of ACM International Multimedia Conference*, Orlando, Florida, GMD Report No. 85, Oct. 1999, pp. 91-94. (This paper was invited to a special issue of IEEE Multimedia, see section on journals and periodicals).

24. Poorvi L. Vora. "Robust Watermarking Using Argument Modulation". *PICS (Image Processing, Image Quality, Image Capture Systems)*, Savannah, Georgia, April 1999, p. 290-294.

25. Richard L. Baer, William D. Holland, Jack M. Holm, and Poorvi L. Vora. "A Comparison of Primary and Complementary Color Filters for CCD-based Digital Photography". *IS&T/SPIE Conference on Sensors, Cameras, and Applications for Digital Photography*, San Jose, CA, 27 January 1999, vol. 3650, pp. 16-25.

26. Nasir D. Memon and Poorvi L. Vora. "Authentication Techniques for Multimedia Content". *SPIE Conference on Multimedia Systems and Applications, Photonics East*, Boston, MA, 2 November 1998, vol. 3528, pp. 412-422.

27. Poorvi Vora and Cormac Herley. "Trade-offs Between Color Saturation and Noise Sensitivity in Image Sensors". *IEEE International Conference on Image Processing (ICIP)*, Chicago, IL, 4-7 October 1998, vol. 1, pp. 196-200.

28. Poorvi L. Vora, Joyce E. Farrell, Jerome D. Tietz and David H. Brainard. "Linear Models for Digital Cameras". *IS&T's 50th Annual Conference*, Cambridge, MA, 18-23 May 1997, pp. 377-382.

29. Poorvi L. Vora, Michael L. Harville, Joyce E. Farrell, Jerome D. Tietz, and David H. Brainard. "Image capture: synthesis of sensor responses from multispectral images". *SPIE/IS&T Conference on Color Imaging: Device Independent Color, Color Hard Copy, and Graphic Arts II*, 10 February 1997, San Jose, CA, vol. 3018, pp. 2-11.

30. Bhaskar Bhumkar[†], Poorvi L. Vora, B. Chandna and K. Shankar. "A set-theoretic approach to image reconstruction from projections". *IEEE International Conference on Image Processing (ICIP)*, Lausanne, Switzerland, 16-19 September 1996, vol. 2, pp. 737-740.

31. Poorvi L. Vora, H. Joel Trussell and Lawrence S. Iwan. "Design Results for a Set of Thin Film Color Scanning Filters". *IS&T/SPIE Symposium on Electronic Imaging, Science and Technology*, San Jose, CA, 6-10 February 1995, vol. 2414, pp. 70-75.

32. Poorvi L. Vora, H. Joel Trussell, and Lawrence S. Iwan. "Mathematical method for designing a set of color scanning filters". *SPIE and IS&T Conference on Color Hard Copy and Graphic Arts II*, San Jose, CA, 31 January-5 February 1993, vol. 1912, pp. 322-329. 1993.

33. H. J. Trussell and P. L. Vora. "On the Accuracy of Scanning Color Images". *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, San Francisco, CA, 23-26 March 1992,vol. 3, pp. 161-164.

34. Poorvi L. Vora and H. Joel Trussell. "Measures of Goodness of a Set of Color Scanning Filters". *SPIE and IS&T Conference on Color Hard Copy and Graphic Arts*, San Jose, CA, 11-14 February 1992, vol. 1670, pp. 344-352.

35. H. Joel Trussell and Poorvi L. Vora. "Bounds on restoration quality using a priori information". *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, New York, NY, 11-14 April 1988, vol. 3, pp. 1758-1761.

Refereed/Lightly-Refereed Conference and Workshop Papers Without Formal Proceedings

Many of these conferences allow the resubmission of these papers to other venues; further, many of these conferences also allow the submission of work published elsewhere.

1. Kerry A. McKay†, Poorvi L. Vora. "Pseudo-Linear Approximations for ARX Ciphers With an Application to Threefish-256". Second SHA-3 Candidate Conference, Santa Barbara, CA, 23-24 August 2010. Also available as IACR ePrint, see below.
2. David Chaum, Stefan Popoveniuc†, Poorvi L. Vora. "eTegrity and ePunchScan". *NIST End-to-End Voting Systems Workshop*, Washington DC, 13-14 October, 2009.
3. Stefan Popoveniuc† and Poorvi L. Vora. Similar or identical versions presented at:
   - Presented as "Remote ballot casting with Captchas". *3rd Benelux Workshop on Information and System Security (WISSEC)*, Eindhoven, The Netherlands, 13-14 November, 2008.
   - Presented as "Secure voting using infected computers". 8th Annual Security Conference, Las Vegas, Nevada, April 2009.
4. Stefan Popoveniuc† and Poorvi L. Vora. "A framework for secure electronic voting". *WOTE 2008*, held in conjunction with *8th Privacy Enhancing Technologies Symposium (PET)*, Leuven, Belgium, July 22-23, 2008.
5. Rahul Simha and Poorvi L. Vora. "Vote Verification using CAPTCHA-like Primitives". *WOTE 2007*, held in conjunction with *7th Workshop on Privacy Enhancing Technologies (PET)*, Ottawa, Canada, June 20-June 21, 2007. (Extended Abstract)
6. Ben Hosp† and Poorvi L. Vora. "An Information-Theoretic Model of Voting Systems". Similar or identical versions presented at:
   - *IAVoSS Workshop on Trustworthy Elections (WOTE)*, held in conjunction with *6th Workshop on Privacy Enhancing Technologies (PET)*, Cambridge, UK, June 29-June 30, 2006.
   - *Threat Analyses for Voting System Categories. A Workshop on Rating Voting Methods (VSRW)*, Washington, DC, 8-9 June 2006.
   - *Frontiers of Electronic Voting*, Dagstuhl Seminar Series, 2008. (This venue was unrefereed).

Abstracts

1. Alan T. Sherman*, Richard Carback*, David Chaum, Jeremy Clark, John Conway, Aleksander Essex, Paul S. Herrnson, Travis Mayberry, Stefan Popoveniuc†, Ronald L. Rivest, Anne Sergeant, Emily Shen, Bimal Sinha, Poorvi Vora. "Scantegrity Mock Election at Takoma Park". *NIST End-to-End Voting Systems Workshop*, Washington DC, October 13-14, 2009
2. Poorvi Vora. "The channel coding theorem and the security of binary randomization". *IEEE International Symposium on Information Theory (ISIT)*, Yokohama, Japan, 29 June-4 July 2003, pp. 306. (With Proceedings)

Invited Paper

1. Yu-An Sun and Poorvi L. Vora. "From eBay's Second Chance Offer to B2B Service Pricing: Similarity and Challenges". *Invited Paper*, 2009 IEEE International Conference on Service Operations, Logistics and Informatics. Chicago, July 2009.

Patent Applications Granted

1. Poorvi L. Vora and Verna E. Knapp. “Anonymous transactions based on distributed processing”. US 7187772. Issued 6 March 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, Poorvi L. Vora and Cormac Herley. “Multi-level detection and deterrence of counterfeiting of documents with reduced false detection”. US 6516078. Issued February 4, 2003.
4. Poorvi L. Vora, Verna E. Knapp and Umesh V. Vazirani. “Probabilistic Privacy Protection”. US 6470299. Issued October 22, 2002.
5. Poorvi L. Vora. “Robust watermarking for digital objects”. US 6463162. Issued October 8, 2002.
6. Cormac Herley and Poorvi Vora. “Detection and deterrence of counterfeiting of two-sided documents”. US6335794. Issued January 1, 2002. (The US government has shown interest in using this to prevent counterfeit)

Presentations by my Research Undergraduate Students at Undergraduate Student Conferences

1. Alex Florescu†, Stefan Popoveniuc†, Poorvi L. Vora. “Accessible Voting Interface Using an Interactive Voice System Model”, *20th Annual Argonne Symposium for Undergraduates in Science, Engineering and Mathematics*, Argonne National Laboratory, 13 November 2009.
2. Jan Michael Rubio†, Ben Hosp†, Poorvi L. Vora. “Comparing Privacy Properties of Mixnet Audits used by End-to-End Voting Systems”, *20th Annual Argonne Symposium for Undergraduates in Science, Engineering and Mathematics*, Argonne National Laboratory, 13 November 2009.

Selected Media Coverage

- Erin Cox, “Maryland’s Web-delivered ballots — more than 110,000 have been requested — must be hand-copied by poll workers to be counted”, Washington Post, 25 September, 2020.
- Divya Trivedi, “In EVM Do We Trust”, Frontline, 5 July 2019.
- Poorvi L. Vora, “How the World’s Largest Democracy Casts its Ballots”, The Conversation, 30 April, 2019 (invited). French translation, 7 May, 2019. Picked up by many media outlets including the San Francisco Chronicle and multiple Indian outlets.
- Maryland Legislators Consider Limiting Electronic Absentee Ballots, NBC4, 27 February 2019. Includes a TV clip of my testimony.
- Maryland Legislators Consider Limiting Electronic Absentee Ballots, NBC4. 18 October 2018. TV Appearance.
- Sam Biddle, “Are We Making Elections Less Secure Just to Save Time?”, The Intercept, 4 September 2018
- Emily Dreyfuss, “Smartphone Voting Is Happening, but No One Knows if It’s Safe”, Wired, 9 August 2018
- Rachel Chason, “Here’s why cybersecurity experts say Maryland’s ballot delivery system is a target for hackers”, The Washington Post, 1 April 2018
- Michael Dresser, “Maryland officials look to shore up election defenses after Russian tampering”, The Baltimore Sun, 23 February 2018

- Devesh Pandey, "EVMs cannot be perfectly secure, says expert", The Hindu (online), 14 May 2017. Shorter version in print

- Gaurav Vivek Bhatnagar, "Give Us Full Access to EVMs, Experts Tell Election Commission", The Wire, 25 April 2017

- Poorvi L. Vora, "Hacking EVMs: The EC has issued a challenge. It must first accept the challenge it faces", scroll.in 22 April, 2017

- Poorvi L. Vora, "The great EVM debate: Convincing the losers that they lost", scroll.in 17 March, 2017

- Jon Swaine, "Security experts join Jill Stein's 'election changing' recount campaign", The Guardian, 29 November 2016.

- T. J. Raphael. "So, what does it mean for there to be an election recount?", The Takeaway, Public Radio International, 29 November 2016. Includes 4-minute audio clip.

- Philip B. Stark and Poorvi L. Vora, "Maryland voting audit falls short", Baltimore Sun, Saturday, 28 October, 2016. Other contributors to this op-ed: Harvie Branscomb, Joe Kiniry, Mark Lindeman, Neal McBurnett, Ronald L. Rivest, John Sebes, Pamela Smith, Paul Stokes, Howard Stanislevic, Luther Weeks.

- *Wired*. March 21, 2016. Issie Lapowsky. "Utah's Online Caucus Gives Security Experts Heart Attacks".

- *Washington Post* April 6, 2015. "Can you vote for the next president on your smartphone? Not just yet" By Amrita Jayakumar.

- *Electionline Weekly* June 16, 2011. "Takoma Park, Md. tests online absentee voting". By Kristi Tousignant.

- *FairVote Blog* June 9, 2011. "Internet Voting 2.0 and Other Advances in Election Technology in Takoma Park". By Melanie Kiser.

- *WAMU News* (WAMU Radio is the DC NPR Affiliate). 4 November 2009. "Takoma Park Voters Use New System". By Matt Bush.

- *WAMU News* 3 November 2009. "New Voting Technology Makes Debut In Takoma Park". By Matt Bush.

- *WAMU News*. 21 October 2008. "George Washington University Helps Devise New Voting System". By Matt Bush.

- *NPR Morning Edition*. March 7, 2008. "Shift Back to Paper Ballots Sparks Disagreement". By Pam Fessler.

- *IEEE Spectrum*. January 2007. "Making Every E-Vote Count". By Steven Cherry

- *C-SPAN* November 1, 2004. "George Washington Univ. Panel on Electronic Voting Machines".

- *CNET News.com*. June 08, 2004. "High hopes for unscrambling the vote". By Declan McCullagh.

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

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