AFFIDAVIT OF POORVI L. VORA

POORVI L. VORA, being duly sworn, deposes and says the following under penalty of perjury:

1. My name is Poorvi L. Vora. I am a Professor of Computer Science at The George Washington University (GW) in Washington, DC. I submit this Affidavit in support of Jill Stein's Petition for a hand recount of all ballots in Wisconsin.
2. I have Ph. D. and Master's degrees in Electrical Engineering from North Carolina State University, Raleigh, NC, a Master's degree in Mathematics from Cornell University and a Bachelor's degree in Electrical and Electronics Engineering from the Indian Institute of Technology, Bombay, India. My CV is attached as Exhibit A.
3. My research in the last dozen or so years has focused on computer security and privacy, with a special focus on secure electronic voting systems.
4. I have published peer-reviewed research on the design of secure end-to-end-verifiable (E2E-V) voting systems which are software-independent voting systems that enable voters and observers to perform especially powerful election audits. I have also helped the National Institute of Standards and Technology develop definitions of E2E-V system properties.
5. With my students and collaborators, I contributed to the design and deployment of an E2E-V voting system called Scantegrity in the municipal elections of the City of Takoma Park in 2009 and 2011. 2009 marked the first time an E2E-V system was used in a government election. We also designed accessible and absentee voting variants of Scantegrity, which were used by Takoma Park in 2011.

6. I was an invited contributor to the Open Vote Foundation study: “The Future of Voting: End-to-End Verifiable Internet Voting - Specification and Feasibility Study” which concluded that secure internet voting is not possible at this time.

7. I have recently been providing public comment in person at meetings of the State Board of Elections in Maryland to urge Maryland to carry out an election audit using its voter-verified paper ballots.

8. I have been on program committees of several conferences and review panels for National Science Foundation research awards. I have been an Associate Editor for the IEEE Transactions on Information Forensics and Security, and Guest Editor, special issue on electronic voting, IEEE Transactions on Information Forensics and Security, December 2009.

9. I regularly teach a course on Cryptography (mathematical techniques that enhance computer security and are used in the design of secure voting systems and secure electronic commerce) for undergraduate and graduate students. I also often teach a more general course on Computer Security, and a course on Advanced Cryptography.

10. It is, of course, important for a voting system to produce the correct tallies. The system should also be designed to enable voters and observers to verify that it produced the correct tallies once the election is over.

11. When votes are cast on paper ballots which are hand counted, the verification is performed through public observation of the counting process. When counts are computed using inherently unobservable software-based systems, the verification of the tallies has not always been possible.

12. Software-based voting systems are very complex and may consist of hundreds of thousands of lines of code[1].

13. It is hence not possible to find all bugs in voting system software; nor is it possible to completely characterize its behavior in all possible scenarios. For the same reasons, it is not possible to determine with certainty the absence of malicious software hiding within what might appear to be many thousands of lines of legitimate software code. Additionally, it is not possible to confirm with certainty that the code running on the machines is the code that was examined.

14. One approach to dealing with this fundamental challenge of verifying the outcome of software-based voting systems is the notion of software-independence,[2][3] as described by Rivest and Wack. A software-independent voting system is one in which an undetected change in the voting system software will not cause an undetected change in election outcome. Note that a software-independent system is not one that does not use software. It is a system that has a means of verifying the election outcome, independent of the software that computed it (because that software could have bugs and malicious code that have not been detected).

15. One way of achieving software-independence is through the use of voter-verified paper records (VVPRs) securely stored and used to audit the election after it is completed.

[1] For example, the Everest study, ("EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing", Final report, December 2007, http://www.patrickmcdaniel.org/pubs/everest.pdf)states that the team was provided with "670,000 lines of code, encompassing twelve programming languages and five hardware platforms" for its study of the ES&S system, which includes a version of the Model 100 scanner used in some Wisconsin jurisdictions this year.

[2] Ronald L. Rivest and John P. Wack. "On the notion of ``software independence'' in voting systems." Prepared for the TGDC, and posted by NIST at the given url. (2006-07-28) https://people.csail.mit.edu/rivest/RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf

[3] Ronald L. Rivest. "On the notion of `software independence' in voting systems." *Philosophical Transactions of The Royal Society A* 366,1881 (2008) pp. 3759--3767.

VVPRs may consist of (a) printouts from Direct-Recording Electronic (DRE) machines, verifiable by voters as correctly representing their votes or (b) paper ballots completed by voters and fed into optical scanners that tabulate the votes.

16. As a general principle, both optical scanners and DREs are computers running software and hence vulnerable to the same problems—bugs, malware, intentional alterations, etc.—as all software.[4]

17. Hence the mere act of recording a vote on paper is not sufficient for software independence. The securely-stored paper records need to be examined to ensure that they are consistent with the election outcomes declared by the voting system software. If they are not examined, any unintentional software bugs, intentional alterations to the vote or to the tally, or procedural errors leading to an incorrect election outcome will not be detected.

18. A voter using a DRE enters her vote with guidance from the user interface. The DRE prints out a record of her choices. If she approves it, her vote is cast on the DRE, and the paper record is stored securely. Assuming the voter examined the system's representation of her vote carefully before approving it, the voter knows the system understood her vote for what it was intended to be.

19. A voter using an optical scanner marks a paper ballot and feeds it into the scanner. She does not know if it has read her votes correctly.

[4] From the Everest study: "… although they do not appear the same as your typical desktop or laptop computer, all the components of the ES&S system are fully programmable computers capable of running arbitrary software stored in easily modifiable memory. Therefore use of the term "firmware" to refer to the software controlling the hardware components of the ES&S system is somewhat misleading. The code running on the iVotronic [DRE] or Model 100 [optical scanner] is in no way less susceptible to bugs, tampering, or co-option than any other part of the Unity system."

20. The scanner uses light measurements to determine what ballot positions have marks on them, and may store the images thus generated as ballot scans. While the scans do originate through a physical process, they are not like photographs. They are computer data, stored as ones and zeroes and handled by computer software. As a general principle, though the specifics may vary with the specific op-scan system, they can be deleted, replaced or tampered with like any other computer data.

21. Once the scanner has obtained the scan data, it uses instructions regarding the order and position of the various contests and options to determine the votes on a ballot. These ballot programming instructions are delivered, shortly before every election, generally through a removable memory device.

22. A scanner may misinterpret a vote for various reasons: a voter may not have marked the oval as expected to—she may check the oval or circle the candidate's name; a voter may make very light marks on the ballot that are not detected; the voter may enter a write-in vote thinking she needs to both mark the oval next to her candidate and write-in the name; some optical scanners may not detect red ink[5]; ballot programming errors or intentional hacking can lead to votes being swapped among candidates. Newer scanners use more sophisticated techniques to deal with light marks and some identify problem ballots for humans to adjudicate. However, one cannot rely on scanners to do so without error. And scanners cannot detect programming errors or intentional attacks.

23. Logic and Accuracy testing (L&A testing) is intended to test for some of the above problems before the elections, but human error can result in the tests not being correctly completed and equipment malfunction can result in the equipment behaving differently

[5] In 2004, in Napa County, CA, a primary election lost 6,000 votes because the scanner was not calibrated to read all types of ink. See: Kim Zetter, "E-Vote Snafu in California County," Wired, 2004. http://archive.wired.com/politics/security/news/2004/03/62721.

on Election Day. Further, a competent attacker would have the system behave as expected when tested, and maliciously during the election[6].

24. Once the DRE or the optical scanner obtains the vote–whether after confirmation by the voter using a DRE or after the votes are read by an optical scanner–the votes are tabulated electronically by software.

25. In principle, at any point in the above process, software can alter the votes or the tallies The University of Connecticut Center for Voting Technology Research (VoTeR Center) evaluated the security of AV-OS tabulators, a model also used in Wisconsin, on the request of the Connecticut Secretary of the State (SOTS) Office, in 2011. They reported[7]: "the memory cards used with AV-OS can be tampered with, thus proving the seriousness of the Hursti Hack. VoTeR Center also discovered new security vulnerabilities of AV-OS. We note that if the memory cards or the AV-OS tabulators are left unattended — within or without the tabulator — they can be tampered with in a matter of minutes. The effects of tampering with the AV-OS and memory cards on the election outcome can be devastating: votes cast on ballots can be reassigned to arbitrary candidates, leading to invalid election results. Subsequent reports by VoTeR Center document additional integrity issues with AV-OS systems. In particular, we determined that even if the memory card is sealed and pre-election testing is performed, one can carry out a devastating array of attacks against an election using only off-the-shelf equipment and

[6] Volkswagen's 2L Diesel cars were found to use more emission controls when they were being tested than during normal use. On examination, it was found that their software was written to detect when a test was underway. See: https://en.wikipedia.org/wiki/Volkswagen_emissions_scandal In our case, software manipulated without vendor knowledge could also provide testers with the results they expected to see. Then the software could perform differently when used in the election.

[7] VoTeR Center: UConn Center for Voting Technology Research, "Technological Audits of Optical Scan Voting Systems: Summary for 2007 to 2010 Connecticut Elections", Kiayias et al, reference. October 19, 2011, Version 1.1. https://voter.engr.uconn.edu/voter/wp-content/.../VC-TechAudits-2007-2010c.pdf

without having ever to access the card physically or opening the AV-OS system enclosure. For example, the attacks can lead to the following: Neutralizing candidates: The votes cast for a candidate are not recorded; Swapping candidates: The votes cast for two candidates are swapped; Biased Reporting: The votes are counted correctly by the terminal, but they are reported incorrectly using conditionally-triggered biases." I am not aware if the systems have been modified to resist these specific attacks since they were discovered; regardless, they illustrate the general principle that op-scan systems of this kind are very vulnerable.

26. The method of delivery of the malicious code depends on the type of scanner used. In older op-scan systems, the removable memory used to store counts also stores a computer program to print the results that can be manipulated to print different results.[8][9] In newer op-scan systems such as the Model 100 also used in WI, the removable memory also delivers software updates, and can be used as a means of delivering malicious code[10].

27. Note that one cannot depend on detecting the above types of alteration without a manual review of the paper votes (or, potentially, a forensic audit) because the software process is unobservable and because it is possible for a competent attacker to erase their tracks.

28. In the event that an election outcome were incorrect, the only way to detect this with high certainty is to manually examine the paper votes cast. Rescanning and retabulation of the ballots, even if by another scanner, could lead to the same error or malware, delivered by the same source, having the same influence on the retabulated election outcome.

[8] The "Hursti Hack", https://en.wikipedia.org/wiki/Hursti_Hack

[9] See Doug Jones' comments on Andrew Appel's blog post at: https://freedom-to-tinker.com/2016/09/20/which-voting-machines-can-be-hacked-through-the-internet/

[10] Andrew Appel, "Which voting machines can be hacked through the internet?", blog post, Freedom to Tinker, September 20, 2016. https://freedom-to-tinker.com/2016/09/20/which-voting-machines-can-be-hacked-through-the-internet/

Moreover, where the same scanner is used, as I understand the Wisconsin recount procedures permit, the problem is exacerbated because any attack on the scanner's software (software that is often referred to as "firmware") would make the recount vulnerable as well. Manual examination of securely-stored paper ballots can greatly increase certainty in the outcome.

29. For the above reasons, it is important to make the election audit a standard part of the election process and, where there is no audit procedure, to perform a recount of paper ballots. When paper ballots are available, they provide very reliable independent evidence about voter intent.

30. Given the unhealthy interest demonstrated by foreign powers in influencing the 2016 presidential election, I believe we would send the incorrect signal if we were not to review the voter-verified paper records of the election. We would be making very clear to a potential future attacker how to go about attacking the system. In contrast, if we review the voter-verified paper records from this election, it will serve as an important deterrent to dissuade potential cyberattackers in future elections.

This affidavit was executed on the 28th day of November, 2016 in the District. of Columbia

Poorvi Vora

POORVI L. VORA

Sworn to before me this 28th day of November, 2016.

Stacey Lawrence

Notary Public

My Commission Expires: Oct. 31 2021

JENNIFER STACEY LAWRENCE
NOTARY
PUBLIC
My Comm. Exp.
Oct 31, 2021
DISTRICT OF COLUMBIA

Exhibit A

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 and Electronics Engineering. Indian Institute of Technology, Bombay (1986)

Positions

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

Board of Advisers, 2015-current
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

- 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 (current)
2. Hua Wu (current)
3. Reham Almukhlifi (current)
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.com
   Funded in part by NSF
7. Yu-An Sun, 2009
   Dissertation Title: *The Second Chance Offer: Optimal Strategies for Sellers and Bidders*
   Now at PARC

Thesis Master's Students

1. Darakhshan Mir, *Related-key linear cryptanalysis of DES*. 2006.
   Ph.D., Rutgers University, 2013.
   Now tenure-track Assistant Professor and Jane W. Griffith Faculty Fellow at Bucknell.
2. Rajat Bhatt, *Related-key attacks on pseudo-random number generators*. 2005.
   Now at Microstrategy.

Supervised Undergraduate Research

1. Katherine Walker, current.
   Funded in part by NSF.
2. Brannon McGraw (B.S., 2015, now at Visa)
   Funded in part by SUPER.

3. John Wittrock (B.S., 2013, SEAS Distinguished Scholar, now at AppNexus)
   Funded in part by NSF. Co-author on one paper.

4. Tyler Kaczmarek (B.S., 2013, now in doctoral program at U.C. Irvine)
   Funded in part by NSF and GW-SEAS Summer Undergraduate Program in Engineering Research (SUPER). Co-author on one paper.

5. Jan Rubio (B. S., 2011, Freudenthal Award, Pelton Award Second Prize, now at oPower)
   Funded in part by NSF. Co-author on two papers.

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

7. Jacob Alperin-Sheriff (B.S., 2010, Ph. D., Georgia Tech., 2015, now at NIST).
   Funded in part by NSF.

Post-Doctoral Researchers Supervised

1. Filip Zagórski, October 2010-November 2011
   now Assistant Professor, Wroclaw University of Technology, 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) and Michael R. Clarkson, "TWC: TTP Option: Small: Open-Audit Voting Systems—Protocol Models and Properties".
   National Science Foundation CNS-1421373. $688,554
   September 1, 2014-August 31, 2017

2. 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

3. 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.

4. 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.

[1] UMCP PI: Jonathan Katz.

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

6. 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.

7. 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.

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

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

10. 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.

Pedagogy

- **Classes Taught**

  At GW

  - *Computer Security*
  - *Cryptography*
  - *Advanced Cryptography*
  - *Discrete Structures II.*

  Guest Lectures:

  - 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**
  - Director of CSIA graduate certificate program: Fall 2005-2011 (joint with former faculty member Jonathan Stanton until Fall 2008)
  - Course Director
    - Computer Security (graduate—6531/283—and undergraduate—4531/172)
    - Cryptography (graduate—6331/284—and undergraduate—4331/162)
    - Advanced Cryptography (graduate: 8331/381)
  - Courses Proposed and Designed.
    - CSCI 8331/381, Advanced Cryptography
    - CSCI 2312/124, Discrete Structures II (co-proposer: Abdou Youssef).
  - Courses Designed
    - CSCI 4331/162, Cryptography

Selected Service

- Professional
  - 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
  - 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 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
  - Undergraduate Adviser, AY 2013-current
  - MS Adviser, AY 2003-current
  - Faculty Mentor for Assistant Professor Claire Monteleoni, AY 2011-current
  - Curriculum Committee: AY 2004; AY 2009-2011; AY 2014-current
  - 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
  - Testimony to State Board of Elections, MD, September 2016
  - 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. Sumit Joshi* and Poorvi L. Vora. "Weak and Strong Multimarket Bidding Rings". *Economic Theory*, vol. 53, no. 3, pp. 657-696, June 2012.

2. 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.

3. 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.

4. 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.

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

6. Stefan Popoveniuc[†] and Poorvi L. Vora. “A framework for secure electronic voting”. *Cryptologia*, Vol. 34, No. 3, pp. 236-257, June 2010.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

Journal Papers in Preparation

1. Filip Zagórski, Richard T. Carback, David Chaum, Jeremy Clark, Aleksander Essex, Jonathan Katz and Poorvi L. Vora, “The Remotegrity Protocol and its Properties”.

2. Kerry McKay[†] and Poorvi L. Vora. “Analysis of ARX Functions: Pseudo-linear Cryptanalysis and a Diffusion Metric”.

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, TravisMayberry, Stefan Popoveniuc, Ronald L. Rivest, Emily Shen, Alan T.Sherman, Poorvi L. Vora, John Wittrock, and Filip Zagrski, 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. 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.

2. 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

3. 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

4. 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

5. 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

6. 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

7. 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

8. 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

9. 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.

10. 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 ≈ 0.41

11. 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.

12. 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 ≈ 0.38

13. 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 ≈ 0.20

14. 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.

15. 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.

16. 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).

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

18. 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.

19. 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.

20. 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.

21. 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

Relevant Selected Recent Invited Presentations on Secure Electronic Voting

- Remote Voting Conference, CDAC under the aegis of Department of Electronics and Information Technology (DeitY), Govt. of India, June 2015
- DC Area Privacy and Security Seminar (DC-APS), April, 2013
- National Institute of Standards and Technology, Gaithersburg, MD, May 2011
- Indian Institute of Technology, Bombay, January 2011
- Indian Institute of Technology, Hyderabad, January 2011
- Information Systems Seminar, Princeton University, April 2010
- Hewlett-Packard Labs., Princeton, NJ, April 2010

Selected Media Coverage

- *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.