DEPOSITION ON: ELECTRONIC VOTING AND THE INDIAN EVM

20 April 2020

To,

Citizens' Commission on Elections, India

Dear Chair Justice (Retd.) Lokur, Vice-Chair Habibullah and Other Members of the Commission,

We are election integrity, computer security and computer science researchers with hundreds of years of collective experience. We provide this deposition on:

(a) Compliance of electronic voting with the principles of democracy and

(b) EVM/VVPATs before and during polling, storage, counting and declaration of results.

The content of the deposition is summarized as follows.

ELECTRONIC VOTING AND THE PRINCIPLES OF DEMOCRACY

An accurate and incorruptible voting process provides legitimacy to elected representatives and is hence essential for a healthy democracy. Transparency is a key factor in achieving these goals; aspects of an election that may be observed and independently-verified by the public will naturally be viewed as accurate and incorruptible.

Electronic counting mechanisms—whether implemented in computer hardware and firmware as in Indian EVMs, or software as in western electronic voting systems—are not transparent to the voter, who does not know whether the vote was correctly recorded or counted. Internet access is not the only way to manipulate electronic voting machines; they provide a long time window—over the cycle of design, implementation, manufacture, testing, maintenance, storage and deployment—for insiders or criminals to attempt other means of access. The EVM is a computerized system and its internal logic can be changed by someone with physical access to the machine.

While one may publicly test an electronic voting system for some known problems before use, there are at least three challenges with testing. First, it is not possible to know every vulnerability. Second, and relatedly, it is not possible to determine how a computer software or hardware module will perform in all circumstances. Hence, even for each known vulnerability, it is not possible to fully test that an electronic voting system will function as desired in each possible scenario. Third, computerized systems, such as the EVM, can be programmed to determine when they are being tested and to behave as expected during the test. Thus, while one should test as extensively as possible, testing can only reveal some

problems. The absence of problems during testing does not mean that problems do not exist.

For the above reasons, no electronic voting machine, including the Indian EVM, can be assumed tamper-proof. Many countries—and even individual hackers—have the technical expertise to manipulate voting systems. The EVM is no exception. The vulnerabilities of electronic counting motivated France and The Netherlands to use paper ballots and hand count their recent elections. There are reports that Russia tried to change the 2014 election totals in Ukraine and to access voter databases in the 2016 US election.

Knowing that testing is not sufficient, what additional precautions can we take? While voters cannot observe the internal counting mechanism of an electronic system, the principles of public observation can and should be applied to elections that rely on electronic technology. Best practices require that the use of an electronic voting system be accompanied by the generation and secure curation of a voter-verified paper audit trail (VVPAT). After the election, in addition to public audits of all election processes, the paper record must be publicly audited to verify the election outcome. These public audits provide the counterweight to the vulnerabilities of electronic counting mechanisms.

In summary, elections relying on electronic voting machines should be conducted assuming the machines can be tampered with. Assurances from any official entity that the process or technology is tamper-proof are not sufficient. Voters and losing candidates should not have to trust an opaque machine and its counting mechanism, or an insider design, manufacture, testing and maintenance process. Every part of the election process and the technology should be open to examination and analysis by the candidates and the public. Transparency in design, implementation and use; an openness to the incorporation of ideas from the latest results in computer security; independent security testing of the design and implementation by experts and its feedback into the design cycle; education of the public on these aspects; full observation of the election process and manual audits of the VVPAT slips are all essential for high integrity elections that rely on electronic voting machines.

THE INDIAN EVM, VVPATS AND ELECTION PROCEDURES

The Indian EVM is interesting because its design is far simpler than that of other electronic voting machines. In India, it has greatly increased the efficiency of vote counting and facilitated enfranchising voters in remote areas. It has also made ballot box stuffing much harder. Pre-election procedures are, by and large, designed to be transparent and fair. **However, this is not sufficient to ensure high integrity elections.**

We are not aware of any evidence that any elections using Indian EVMs were rigged. However, the vulnerability of a fully-electronic vote counting mechanism is significant. Attackers can be sophisticated enough to avoid detection, and the absence of evidence does not imply that election integrity can be assumed. It is not sufficient to rule out some

specific attacks, because other attacks could be discovered by those who wish to meddle with elections. The Election Commission's excessive reliance on secrecy of design and the obviously false claim that the machines are tamper-proof greatly diminish the trustworthiness of the electoral process. The following changes can improve trustworthiness by increasing transparency:

1. EVM design and implementation, as well as the results of both software and hardware verification, should be **public and open to full independent review**. Reports from independent experts should be made available to the public, and the important vulnerabilities discovered should be addressed as part of a regular public process with comments from the public as well as experts not involved in the review.
2. A Voter Verifiable Paper Audit Trail (VVPAT) should be generated for **every EVM in every election**. The printed VVPAT slips should be stored securely and separately from the EVMs. The storage boxes should be sealed in the same manner that EVMs are sealed, with signatures from observers representing all candidates.
3. **Voters should be allowed to verify the printed VVPAT slip before the vote is cast**. The use of a paper trail can greatly enhance the integrity of an electronic voting system. VVPAT slips are, however, weaker than paper ballots because paper ballots exactly represent the intended vote, but the VVPAT slip does so only if it is verified by the voter. **The Indian VVPAT system does not allow the voter to verify the slip before the vote is cast.**

   The correct VVPAT protocol is to allow a voter to approve the VVPAT slip before the vote is cast, to cancel her vote if there is a discrepancy, and have the opportunity to vote from another machine. Such a protocol should be implemented with Indian EVMs and VVPATs.

   Additionally, it is virtually impossible to determine whether a voter reporting a discrepancy is lying, because the EVM can behave differently when being observed. Stringent punishment for voters unable to prove a reported discrepancy between the VVPAT slip and the vote is counterproductive in this scenario.
4. It is heartening that the recent Indian general election was carried out with full VVPAT capability and that VVPAT audits were carried out. However, the results of the audit were confusing and not easily available to the public. Additionally, auditing a fixed number of EVMs per constituency is not sufficient to verify elections with narrow margins. A robust, well-designed audit can provide considerable confidence in the outcome, and statistical principles would dictate when a full hand count would be required. Subtle differences among audits can result in a significant difference in the ability to detect problems. For this reason, **best practices in the design of robust election audits should be followed, and expert advice on their design sought**.
5. **Legislation** will be needed on what to do when the audit reveals an outcome different from that declared by the EVMs. Legislation on how/when/whether a candidate may

request a full manual count independent/instead of the audit would need to be developed, or existing legislation modified.

6. The use of risk-limiting audits using current EVMs, and end-to-end-independently-verifiable (E2E-V) techniques for future EVMs, may be explored.

If recommendations 1-5 above are followed, it may not be necessary to go back to paper ballots. If the VVPAT is not strengthened through improved voter-verification, secure storage, robust audit and supporting legislation, however, the vulnerabilities of the EVM will continue to pose a serious problem to election integrity and paper ballots could be preferred.

Please find, on subsequent pages, details on the above comments and short biographies of the signatories. Should you have additional questions, we would be happy to answer them. Please send them to Prof. Poorvi L. Vora, poorvi@gwu.edu.

Signatories

Note that affiliations below are included for identification purposes only and do not reflect the view of the signatories' employers or collaborators.

Poorvi L. Vora, (poorvi@gwu.edu), George Washington University, Washington, DC, USA

Alok Choudhary, Northwestern University, Evanston, Illinois, USA

J. Alex Halderman, University of Michigan, Ann Arbor, Michigan, USA

Douglas W. Jones, University of Iowa, Iowa City, Iowa, USA

Nasir Memon, New York University (Brooklyn), New York, New York, USA

Bhagirath Narahari, George Washington University, Washington, DC, USA

R. Ramanujam, Institute of Mathematical Sciences, Chennai, India

Ronald L. Rivest, Massachusetts Institute of Technology, Cambridge, Massachusetts

Philip B. Stark, University of California, Berkeley

K. V. Subrahmanyam, Chennai Mathematical Institute, Chennai, India

Vanessa Teague, Thinking Cybersecurity, Australia

DETAILED DEPOSITION

1. **Uniqueness of the Indian EVM:** The Indian EVM has an interesting design because it relies largely on hardware and firmware, unlike other electronic voting machines which are software-intensive. Additionally, it is a single-purpose machine; this implies that its design could be very simple, allowing for more thorough security analysis. Its prescribed use does not involve connections beyond its sole wired connection to the control unit, and it is not fitted for internet or other network access, including wireless access. The procedures used immediately pre-election are remarkably public. These features could serve to strengthen the integrity of elections run using Indian EVMs.
2. **Vulnerabilities in computerized counting:** Yet, no computerized vote counting device can be guaranteed to be tamper-proof. The Indian EVM relies on the implementation of computer logic in computer chips and circuitry rather than on hundreds of thousands of lines of computer software code. The chips were intended to be read-only—once manufactured to perform a certain computational task, the chips cannot be reprogrammed to perform another. They can, however, be replaced by other chips at any time in the long cycle of use of the EVMS. Further, the machines can contain undetected errors or intentional changes to the circuit designs at the time of manufacture.
3. **Two plausible attacks:**
    - Wolchok *et al* (2010)[1] describe and demonstrate the placement and use of a dishonest display board with a built-in wireless receiver controlled through wireless signalling. In the absence of wireless instructions, it will behave honestly, displaying the correct vote totals.
    - In response to an earlier announcement by the Election Commission (EC) inviting the public to demonstrate that EVMs can be hacked, Amaldev[2] describes the use of a small specially-designed device at one end of the cable connecting ballot and control units. While the Wolchok *et al* attack would need to be carried out before the device is sealed, the Amaldev attack can be carried out even after the device is sealed.

---

[1] Scott Wolchok, Eric Wustrow J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp "Security Analysis of India's Electronic Voting Machines" (video) *Proc. 17th ACM Conference on Computer and Communications Security CCS '10*, Chicago, October 2010. The display board, which contains the circuitry required to display the vote counts provided to it by the electronic counter, can be replaced by a dishonest display board at any time before the machine is first sealed for a particular election. It can then also be used in future elections. The dishonest display board contains circuitry to receive wireless instructions from the attacker, and to calculate new vote totals so as to provide the attacker's favorite candidate a win while arousing minimum suspicion.

[2] V. Amaldev, "How to Hack Indian EVMs", 30 April 2017.

4. **It is not about specific vulnerabilities**: Every so often one hears about a "new" vulnerability. For example, an RTI filing revealed in 2019 that the micro-controller chip used in EVMs is not one-time programmable[3] as claimed by the EC. The public does not know how to evaluate this risk to election security. On the one hand, there is little information in the public domain on the design of the Indian EVM[4], and it is not possible to independently verify the reassurances of the EC. On the other hand, the EC's case about the credibility of the EVM has been based on "trust us"[5], yet this is an example of an EC claim that has been proven to be false.

   The issue of EVM security has been made into a patchwork of known problems and whether these are being protected against. Every time a new problem comes to public view, especially when it is counter to an EC claim, public trust is diminished. Such a situation is particularly volatile and not conducive to trustworthy elections. A more stable scenario arises if election protection depends on public designs, processes and audits.

5. **Voting machine designs should be public**: It is not uncommon for computer security experts to miss vulnerabilities in their own designs[6]. For this reason, it is recommended that the design and implementation of any computerized voting system be widely observed and examined on a planned schedule. This makes it more likely that vulnerabilities are detected in the public domain, by experts, rather than left for detection by those wishing to do harm[7]. Once discovered, the vulneabilities can be addressed in a planned manner as well.

6. **Little transparency in EVM design:** The EC is relying on the secrecy of the design to

---

[3] Venkatesh Nayak, "What the EC Is Hesitant to Tell the Public About EVMs and VVPATs", The Wire, 22 May 2019

[4] The only information on the detailed design available is from statements from the EC, for example, press notes on 16 March 2017 and 8 August 2009 and the paper by Wolchok et al. Information on procedures is available through explanatory videos, such as, for example, EVM Training Film dated 10 March, 2014 and additional detailed documents.

[5] See, for example, (b), (d) and (f), section 7 of the EC's press note dated 16 March 2017, "Credibility of Electronic Voting Machines, Regarding". In the same press note, the EC says: "The Election Commission would like to underline that it always had a firm conviction and complete satisfaction that EVMs could not be tampered with. Its faith on the machine has never wavered through the conduct of elections in the last many years".

[6] For example, the original Needham-Schroeder public key protocol (1978) is vulnerable to a man in the middle attack; one of the simplest attacks on the Indian EVM described by Wolchok et al is a man in the middle attack.

[7] As an example of transparency improving the design of security technology, the National Institute of Standards and Technology (NIST) held public competitions for the Advanced Encryption Standard (AES) block cipher and the Secure Hash Algorithm (SHA-3) in 1997 and 2007 respectively. AES and SHA-3 are cryptographic standards underpinning secure electronic commerce, internet banking and all online international financial transactions. Designs were solicited in a public competition; experts from all over the world submitted entries which were published online; experts then attempted to demonstrate security vulnerabilities in the entries; the vulnerabilities thus detected were published online; the final winning designs were chosen based on their security and efficiency.

provide security[8]. Security best practices, however, require the assumption that the design is known by the enemy[9], whether it is public or not.

7. **Independent Review Necessary**: Best practices in election integrity include the engagement of an independent team of experts to perform a security analysis, the results of which are made public. (Note that independent EVM testing as currently performed does not include security testing/analysis.)

   For example, in 2007, the Secretary of State, California, USA, ordered the Top-To-Bottom-Review, by noted academic and other experts, of all of the voting machine models certified for use in the state. The resulting detailed report on system vulnerabilities was made public, and action was taken against systems that were found to be insecure.

   Every time the EC has invited examination of Indian EVMs, however, the examination has been severely limited[10], preventing true security analysis and missing the opportunity to educate the public on the strengths and vulnerabilities of its voting technology.

8. **Technical checks and balances can be circumvented:** The EC points to technical reasons why the published attacks are not possible, and to procedures in place that would detect the attacks. These are useful and serve the purpose of providing some deterrence. They are not, however, sufficient by themselves—in part because they are lacking, and in part because it is not possible to detect all possible attacks.

   - **Functionality Tests and Mock Polls:** There are a number of tests in place to check the performance of the hardware at various stages in the manufacturing and maintenance cycle[11] and later, during First Level Checking (FLC)[12]. Candidate representatives participate in a number of mock polls[13]. However, a competent attacker would manipulate the hardware to detect when it is being tested[14]. Hardware manipulated at time of manufacture or afterward could provide testers

---

[8] See, for example, (b), (d) and (f), section 7 of the EC's press note dated 16 March 2017, "Credibility of Electronic Voting Machines, Regarding".

[9] For example, Kerckhoffs' second principle states that the security of a system cannot depend on the design being secret; all security arguments must assume that those wishing to break system security would be able to determine the design, even if it is not public. See: Auguste Kerckhoffs, "La cryptographie militaire" *Journal des sciences militaires*, vol. IX, pp. 5–83, January 1883, pp. 161–191, February 1883. Peticolas, Fabien, *electronic version and English translation of "La cryptographie militaire"*.

[10] See, for example, the invitation of 20 May 2017.

[11] See, for example, (c), (e), (g) and (i) in section 7 of the EC's press note dated 16 March 2017, "Credibility of Electronic Voting Machines, Regarding".

[12] See section 9 (a-c) *ibid*.

[13] See section 9 (c, e, g, h)

[14] For example, Volkswagen pled guilty to the development and use of software to detect emissions control testing in its 2L Diesel cars, which used improved emission controls during testing as compared to normal use.

with the results they expected to see, yet perform differently when used in the election[15].

- **Randomization of EVMs:** EVMs are chosen at random for allocation to constituencies and polling booths, after they undergo the FLC and are sealed with special bands and signatures. The randomization procedure is performed in software; this is not a truly random process, but a pseudo-random process, which can be predicted by those who know the randomization algorithm and the parameters used. Additionally, the software generating the random numbers can be manipulated to produce a pre-determined set of numbers which will choose a pre-determined set of EVMs for a pre-determined location, and, even, booth. If the computer running the randomization software is on the internet, the randomization software can be manipulated easily. Even if it is not, however, the software can be manipulated without detection during manually-performed upgrades as well as at other times.
- **Candidate Order:** Candidate order is not known till the candidate list is finalized, by which time EVMs are already sealed. This is often provided as an argument for why EVMs cannot be rigged, as an attacker would not know what button would correspond to a vote for his favourite candidate. This is not a problem if the attacker has a means of signalling after the EVMs are sealed, as described earlier. Additionally, even in the absence of signalling, it is not a problem for someone who wishes to simply ensure that the true winner will not win—the dishonest hardware can be designed so as to exchange votes among all the candidates, for example.
- **Cryptography:** Cryptography can be used by one hardware module to confirm that the other module is what it claims to be, to prevent an attacker from inserting a dishonest module. However, the security of cryptography depends on the secrecy of key stored on the module, and this can often be detected through the use of sophisticated equipment by a determined attacker. Also changes in the data before encryption/digital signature and after decryption/verification of the digital signature will not be detected.

9. **EC's procedures can be circumvented:** The precautions of the EC can be circumvented, including by insiders such as maintenance engineers. It is also possible that all processes are not always followed as described (for example, VVPAT checks routinely unearth instances of mock election votes being included in the tally). Many irregularities came to light in the 2019 general election: unused EVMs were transported without security[16];

[15] Instructions to the dishonest hardware could be provided through the use of wireless signalling as by Wolchok *et al*, with the wireless receiver being a part of the dishonest hardware.

[16] Arnab Ganguly, "Uproar as EVMs moved in pvt vehicles; EC says they're unused", Mumbai Mirror, 22 May, 2019.

there was at least one complaint[17] of an EVM serial number not matching at counting time; an RTI filing revealed that 20 lakh EVMs[18] claimed to be delivered by the manufacturers are not in the possession of the EC. These belie the EC's claims of a tamper-proof process.

10. **EVMs cannot be assumed to be tamper-proof**: This is not because of a weakness in the EVM design per se (we do not know the design beyond that reflected in public information), but because no electronic system can be assumed to be tamper-proof. Additionally, the administrative procedures do not prevent all tampering as we have described above.
11. **Best practices require that voting systems be software/hardware-independent[19,20] and elections be evidence-based[21]:** The election process should be designed so that an undetected change in the voting system hardware or software cannot cause an undetected change in election outcome. This can be done through the generation of voter-verified evidence—in the form of paper records of the votes—and evidence that all the procedures were correctly performed[22].
12. **Regular generation and secure storage of VVPAT**: A complete VVPAT (each vote printed on paper) should be generated for each EVM in each election; the records should be stored securely, separate[23] from EVMs. As with secure EVM storage, the storage containers with VVPAT slips should be sealed and signed by representatives of all candidates. The use of paper VVPAT slips is not anywhere near as burdensome as the use of paper ballots, because each VVPAT slip lists a single candidate.
13. **Voter Verification**: Currently, VVPAT printers in India print the vote on a paper slip and display it to the voter for a few seconds, after which the slip falls into a storage container[24]. The voter is required to file an official complaint if the VVPAT slip is incorrect, with stringent punishment for false complaints. However, note that a dishonest EVM can avoid detection after the fact, and can, for example, behave honestly in demo mode. Stringent punishment to the voter in such a situation is

---

[17] Rajesh Kurup, "Urmila Matondkar files complaint over EVM discrepancies at Magathane polling station", Business Line, The Hindu, 23 May, 2019.

[18] Venkitesh Ramakrishnan, "'Missing' EVMs", Frontline, 24 May, 2019.

[19] Ronald L. Rivest and John P. Wack. "On the notion of `'software independence' in voting systems." (2006),

[20] 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.

[21] P.B. Stark and D.A. Wagner, "Evidence Based Elections", *IEEE Security and Privacy*, special issue on electronic voting, 2012.

[22] Many countries use paper in some form for their elections: 70% of the votes in the 2016 US election had a paper record. Neither Britain nor Germany use electronic voting for general elections. France and The Netherlands both hand-counted their most recent elections.

[23] See, for example, section 7.8.2 "Basic Characteristics of IV Systems", of the Voluntary Voting Systems Guidelines, Version 1 (2005), Volume 1.

[24] See, for example, Voter Verifiable Paper Audit Trail, training video.

counterproductive because it discourages voters from filing genuine complaints (as how can they be proven to be correct?). The correct protocol for generating the VVPAT is, however, as follows[25]: the vote is cast only after the voter has verified the printed slip. If the printed slip is incorrect, the voter cancels the vote and reports the problem, after which she is allowed to vote from another machine if she wishes. **This discrepancy with the correct protocol needs to be rectified if the VVPAT is to be of use in improving election integrity.**

14. **The VVPAT should be regularly audited**: It is not sufficient to generate VVPAT slips that are verified by voters, as the EVM may still record or count the vote incorrectly. The VVPAT slips need to be audited, or cross-checked. Audits involve the public, manual examination of a randomly-chosen sample of the slips to ensure that the announced outcome is correct, and pose a workload far smaller than that of a full hand count. A full hand count is performed if the audit reveals that there is a problem. **The design of a robust statistical audit also requires adherence to best practices, and audits should be designed by experts. Risk-limiting audits are strongly recommended**.

    Audits were performed in the general election of 2020 by cross-checking hand counts of the VVPAT slips with EVM counts. We consider how many EVMs should be cross-checked using India's current approach. Another approach is described by Mohanty et al[26].

    Abhay Bhatt Report: At the request of the Election Commission, Abhay Bhatt of Indian Statistical Institute, Delhi, and others provided a report describing how many EVMs should be cross-checked and why. The report recommends the cross-checking of only 479 EVMs across the country, independent of how many total EVMs there are. It says that, if a fraction of 2% or more of the EVMs *across the country* are faulty, cross-checking 479 chosen at random *across the country* will be sufficient to detect this fact with virtual certainty. This is a correct answer to the wrong question.

    The purpose of the cross-checking is to demonstrate that each constituency was correctly called. For this reason, the computation should be for each Lok Sabha constituency and not the entire country. We should ask how many EVMs need to be cross checked in a constituency to detect, for example, 2% faulty EVMs in that constituency. It is possible that only one constituency had faulty EVMs, but that there was a large enough number to change the outcome. A sample of 479 EVMs may not even include a single EVM from this constituency.

---

[25] "The voting system shall print and display a paper record of the voter ballot selections prior to the voter making his or her selections final by casting the ballot.", from section 7.9.1, page 137, Voluntary Voting Systems Guidelines, Version 1 (2005), Volume 1.

[26] Mohanty, V., N. Akinyokun, A. Conway, C. Culnane, P.B. Stark, and V. Teague, 2019. Auditing Indian Elections, Proceedings of E-Vote ID 2019. Lecture Notes in Computer Science, 11759, R. Krimmer, M. Volkamer, V. Cortier, B. Beckert, R. K¨usters, U. Serd¨ult and D. Duenas-Cid (Eds.) Springer Nature, Switzerland.

Cross-checking 5 EVMS per Assembly Constituency: The current approach of checking five EVMs per Assembly constituency[27] is sufficient to detect malfunctioning EVMs in wide margin contests but will not detect errors in narrow margin contests. For example, if about 1% of the EVMs in a Lok Sabha constituency are faulty, this fact will be detected only one-third of the time. Instead of auditing a fixed number of EVMs, the EC should audit as many EVMs as necessary to ensure that, if the outcome is incorrect, this fact is detected with a high pre-specified probability[28]. Additionally, if mismatches due to mock poll votes are detected, they need to be considered as errors in the cross check. At present, such mismatches are ignored; however, if these errors are made in all EVMs in a constituency, they could change an outcome with small margin and statistical estimates should take this into consideration.

15. **Legislation** will be required to deal with the case when the audit, and subsequent recount, reveal a different winner from the winner obtained from EVM counts. Legislation will also be required to regulate when, and if, a candidate can request a hand count. Best practices suggest that legislation be based on statistical principles, as opposed to the judgment of individual election officials, to the extent possible.
16. **E2E-V EVMs may be considered**: End-to-end-verifiable (E2E-V) voting systems[29] enable voters to independently verify the outcome of an election, without requiring them to trust election technology or election procedures, other than those performed in public on Election Day. It is possible that adding E2E-V capability—or some E2E-V techniques—to EVMs can improve their transparency, though this can only be definitively determined after a study of the constraints and use scenarios of Indian elections. E2E-V capability cannot, however, entirely replace the need for the VVPAT and its audit.
17. **Should paper ballots be used**: If recommendations 5, 7 and 11-15 above are implemented in their true spirit, it does not appear necessary to return to the use of paper ballots. The typical candidate list in Indian elections, as well as the number of voters, is large enough that paper ballots present inefficiencies and difficulty in election administration that can lead to disenfranchisement of voters in remote areas. The EVM, on the other hand, is far more efficient and portable and also helps prevent ballot stuffing. **However, if the VVPAT is not strengthened as described in recommendations 11-15, the vulnerability of EVMs will continue to pose a threat to election integrity and paper ballots may be preferred.**

---

[27] "VVPAT verification: Supreme Court orders counting of paper slips of five EVMs in every constituency", scroll.in, 8 April 2019.
[28] Poorvi L. Vora, "Can We Improve on the Integrity of our Elections?", https://www2.seas.gwu.edu/~poorvi/EVN/VVPAT-Cross-Checking.pdf 20 April 2020.
[29] Josh Benaloh, Ronald Rivest, Peter Y. A. Ryan, Philip Stark, Vanessa Teague, Poorvi Vora, 'End-to-end verifiability", arXiv:1504.03778, 15 April, 2015.

Biographies

Alok Choudhary is the Henry and Isabel Dever Professor of Electrical Engineering and Computer Science at Northwestern University. He also teaches at Kellogg School of Management, and is the founder, chairman and chief scientist of 4C Insights. He has received numerous prestigious awards including National Science Foundation's Presidential Young Investigator Award IEEE Engineering Foundation award, an IBM Faculty Development award, and an Intel Research Council award. He is a fellow of IEEE, ACM and American Academy of Sciences.

Choudhary has consulted for many companies including Publicis Group, Vivaki, Southwest, Intel, IBM, SPSS, Teradata, Microsoft, Sun Microsystems, Newsbank, Sony, Portland Group, Lucent, Oliver Weinmen, and Netezza. Alok Choudhary's work has appeared New York Times, Chicago Tribune, The Telegraph, The Investor Business Daily, ABC, PBS and many international media outlets all over the world.

Choudhary graduated with a PhD from University of Illinois, Urbana-Champaign in the field of Supercomputing. He has published more than 400 papers and graduated more than 35 PhDs. He gives talks in many international conferences. His research interests are in computer security, supercomputing, big-data science and algorithms their applications in marketing, medicine, physics, materials and climate understanding.

J. Alex Halderman is Professor of Computer Science and Engineering at the University of Michigan and Director of Michigan's Center for Computer Security and Society. His interests include computer and network security, Internet security measurement, censorship resistance, and electronic voting, as well as the interaction of technology with law and international affairs. Named one of Popular Science's "Brilliant 10" for 2015, his recent projects include ZMap, Let's Encrypt, and the TLS Logjam and DROWN vulnerabilities.

A noted expert on electronic voting security, Prof. Halderman helped demonstrate the first voting machine virus, participated in California's "top-to-bottom" electronic voting review, and demonstrated vulnerabilities in India's EVMs. When Washington DC invited the public to test its pilot Internet voting system, Halderman demonstrated security vulnerabilities that would allow malicious entities to add and replace votes. His analysis received national attention and resulted in DC's decision not to use the system. With Vanessa Teague, he demonstrated serious security vulnerabilities in the iVote Internet voting system used by New South Wales, Australia.

In 2015, Halderman received the Alfred P. Sloan Fellowship, which is awarded to "early career scientists and scholars of outstanding promise" "in recognition of distinguished performance and a unique potential to make substantial contributions to their field". He holds a Ph.D. from Princeton University.

Douglas W. Jones is a computer scientist at the University of Iowa. Together with Barbara Simons, he published "Broken Ballots: Will Your Vote Count?". His involvement with electronic voting research began in late 1994, when he was appointed to the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems. He chaired the board from 1999 to 2003, and has testified before the United States Commission on Civil Rights, the United States House Committee on Science and the Federal Election Commission on voting issues. In 2005 he participated as an election observer for the presidential election in Kazakhstan. Jones was the technical advisor for HBO's documentary on electronic voting machine issues, "Hacking Democracy", that was released in 2006. He was a member of the ACCURATE electronic voting project from 2005 to 2011. On Dec. 11, 2009, the Election Assistance Commission appointed Douglas Jones to the Technical Guidelines Development Committee, where he served until 2012. Jones received a B.S. in physics from Carnegie Mellon University in 1973, and a M.S. and Ph.D. in computer science from the University of Illinois at Urbana-Champaign in 1976 and 1980 respectively.

Nasir Memon is a professor in the Department of Computer Science and Engineering at NYU Polytechnic School of Engineering and director of the Information Systems and Internet Security laboratory. He is one of the founding members of the Center for Interdisciplinary Studies in Security and Privacy (CRISSP), a collaborative initiative of multiple schools within NYU including NYU-Steinhardt, NYU-Wagner, NYU-Stern and NYU-Courant. His research interests include digital forensics, biometrics, data compression, network security and security and human behavior. Memon earned a Bachelor of Engineering in Chemical Engineering and a Master of Science in Mathematics from Birla Institute of Technology and Science (BITS) in Pilani, India. He received a Master of Science in Computer Science and a PhD in Computer Science from the University of Nebraska.

Prof. Memon has published over 250 articles in journals and conference proceedings and holds a dozen patents in image compression and security. He has won several awards including the Jacobs Excellence in Education award and several best paper awards. He has been on the editorial boards of several journals and was the Editor-In-Chief of Transactions on Information Security and Forensics.

Memon is the co-founder of Digital Assembly and Vivic Networks, two early-stage start-ups in NYU-Poly's business incubators.

He is an IEEE fellow and a Distinguished Lecturer of the IEEE Signal Processing Society.

Bhagirath Narahari is the Associate Dean for Undergraduate Programs and Student Affairs and a Professor of Engineering and Applied Science in the Department of Computer Science in The School of Engineering and Applied Science at The George Washington University. Prof Narahari received his PhD in Computer Science from the University of Pennsylvania in 1987, and his Bachelors in Electrical Engineering from Birla Institute of Technology and Science, Pilani. Since 1987 he has been on the faculty in the School of Engineering and Applied Science at The George Washington University. From 1999 – 2002 he was the first Chair of

the Department of Computer Science, and he has been active in undergraduate education with over a dozen years' experience in undergraduate advising, curriculum development and has taught a number of undergraduate courses in Computer Science.

His research interests are in the areas of Software Security, Architecture support for trustworthy computing, Embedded Systems, Computer Architecture, Compiler optimization, Pervasive Computing, and Parallel Computing. Prof. Narahari has published several refereed articles in various areas of embedded systems, security, architecture, parallel processing and computer systems. His current research focuses on compiler, operating system and hardware support for software security, with projects funded by the National Science Foundation (NSF) and Air Force Office of Scientific Research (AFOSR). Prof. Narahari's prior research has been funded by the National Science Foundation, AFOSR, Rome Air Force Labs, NASA, NSA and America Online (AOL), and included research in power-aware computing, embedded systems, optimizing compilers, software systems and specification, and pervasive computing. His research projects have included both fundamental research and software deliverables including an open source research compiler infrastructure for the Intel Itanium processor.

Ronald L. Rivest is the Institute Professor of Computer Science in MIT's Dept. of Electrical Engineering and Computer Science. He is a member of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL), a member of the lab's Theory of Computation Group and is a leader of its Cryptography and Information Security Group. He is a founder of RSA Data Security and an inventor of the RSA public-key cryptosystem, and a co-founder of Verisign and of Peppercoin. Professor Rivest has research interests in cryptography, computer and network security, voting systems, and algorithms. He is a member of the National Academy of Engineering, the National Academy of Sciences, and is a Fellow of the Association for Computing Machinery, the International Association for Cryptographic Research, and the American Academy of Arts and Sciences. He is also on the EPIC Advisory Board.

Together with Adi Shamir and Len Adleman, Dr. Rivest was awarded the 2000 IEEE Koji Kobayashi Computers and Communications Award and the Secure Computing Lifetime Achievement Award. He also received, together with Shamir and Adleman, the 2002 ACM Turing Award and the 2009 NEC C&C Prize. He received an honorary degree from the University of Rome. He is a Fellow of the World Technology Network and a Finalist for the 2002 World Technology Award for Communications Technology. In 2005, he received the MITX Lifetime Achievement Award; in 2007, he received both the Computers, Freedom and Privacy Conference "Distinguished Innovator" award and the Marconi Prize. In 2008, he received an honorary doctorate from the Louvain School of Engineering at the Universite Catholique de Louvain (UCL). In 2010, he was awarded MIT's Kilian Faculty Achievement Award. He has extensive experience in cryptographic design and cryptanalysis, and served as a Director of the International Association for Cryptologic Research, the organizing body for the Eurocrypt and Crypto conferences, and as a Director of the Financial Cryptography Association.

Philip B. Stark is the Associate Dean, Division of Mathematical and Physical Science at the University of California, Berkeley. Prof Stark is on the Board of Advisors of the US Election Assistance Commission. He developed the notion of "risk-limiting audits", which are now required by the state of Colorado (C.R.S. 1-7-515) and this work has led to audit-related legislation in California: California AB2023, SB360, AB44. He served on California Secretary of State Bowen's Post Election Audit Standards Working Group. Dr. Stark has published more than one hundred articles and books, served on the editorial board of several scientific journals, and lectured at universities and professional societies in seventeen countries. He has consulted for the U.S. Department of Justice, the Federal Trade Commission, the U.S. Department of Agriculture, the U.S. Census Bureau, the U.S. Department of Housing and Urban Development, the U.S. Department of Veterans Affairs, the California Attorney General, the California Highway Patrol, and the Illinois State Attorney. He has testified to the U.S. House of Representatives Subcommittee on the Census; the State of California Senate Committee on Elections, Reapportionment and Constitutional Amendments; the State of California Assembly Committee on Elections and Redistricting; and the State of California Senate Committee on Natural Resources. In 2011, Dr. Stark received the University of California Chancellor's Award for Public Service for Research in the Public Interest.

K V Subrahmanyam is a Professor in the Computer Science group at the Chennai Mathematical Institute (CMI). He has been with CMI since its early days, and has played a pivotal role in establishing it as a premier centre for research and teaching in Mathematical Sciences in India.

His research focus has been on Computational complexity. Since 2004 he has worked at the crossroads of group representation theory, algebraic geometry and computer science, with a view towards understanding hard lower bound problems in computational complexity theory.

He is also interested in combinatorial and continuous optimization, machine learning and cryptography, having taught these courses many times in CMI's graduate and undergraduate programmes. Subrahmanyam did his PhD at the Tata Institute for Fundamental Research, Mumbai and has a PhD degree in Computer Science from Bombay University. He has a B. Tech. in Computer Science from IIT Bombay and an M. S. in Electrical Engineering from Vanderbilt University, USA.

Vanessa Teague is a cryptographer based in Melbourne, Australia. She is the CEO of Thinking Cybersecurity and Adjunct Associate Professor at the Australian National University. Her research focuses primarily on cryptographic methods for achieving security and privacy, particularly for issues of public interest such as election integrity and the protection of government data. She was part of the team (with Chris Culnane and Ben Rubinstein) who discovered the easy re-identification of doctors and patients in the Medicare/PBS open dataset released by the Australian Department of Health. She has co-

designed numerous protocols for improved election integrity in e-voting systems, and co-discovered serious weaknesses in the cryptography of deployed e-voting systems in NSW, Western Australia and Switzerland.

Poorvi L. Vora is Professor of Computer Science at The George Washington University. Her research focus has been on end-to-end independently verifiable (E2E) voting systems which enable voters and observers to audit election outcomes without requiring them to rely on the trustworthiness of election technology or unobserved election processes. She has recently also worked on risk-limiting election tabulation audits.

Vora was a member of the team that deployed polling-place, paper-ballot-based, E2E voting system Scantegrity II in the Takoma Park elections of 2009 and 2011, and of the team that developed remote voting E2E system Remotegrity and accessible voting variant Audiotegrity, used in 2011.

She has worked with the U.S. National Institute of Standards and Technology (NIST) on definitions of desired properties of E2E systems, and on information-theoretic models and measures of voting system security properties. She has been an Associate Editor for the IEEE Transactions on Information Forensics and Security.

Vora has Ph. D. and M.S. degrees in Electrical Engineering from North Carolina State University, an M.S. in Mathematics from Cornell University and a B. Tech. in Electrical and Electronics Engineering from IIT Bombay.