Citizens' Commission on Elections' Report on EVMs and VVPAT

Madan Lokur* Wajahat Habibullah† Hariparanthaman‡ Arun Kumar§
Subhashis Banerjee¶ Pamela Philipose‖ John Dayal** Sundar Burra††
M. G. Devasahayam‡‡

April 8, 2021

Abstract

The Citizens' Commission on Elections (CCE) was set up in March 2020 to critically analyse India's electoral processes in accordance with democracy principles. We present here an analysis of the Electronic Voting Machine (EVM) and the Voter Verified Paper Audit Trail (VVPAT) system, based on the first volume of the Commission's report [Lokur et al., 2021]. The main recommendations of the report are a) modify the current design of the VVPAT system to make it truly 'voter verified' and b) move away from certification of election equipment to end-to-end verifiability of the election outcome, which requires a well-defined audit process of manual counting of a statistically significant sample of the VVPAT slips.

1 Introduction

India's parliamentary election is the largest in the world, with 543 constituencies and well over 1 million voters per constituency on the average, and voting is conducted electronically since 2004. However, there is considerable doubt about the integrity of the Electronic Voting Machine (EVM) used by the Election Commission of India (ECI) and verifiability of compliance with democratic principles. This inevitably generated disquiet during the elections, especially during the 2019 parliamentary elections.

In what follows we present an analysis based on available literature and written depositions from concerned citizens and experts [Agarwal, 2020, Devasahayam, 2020, Nayak, 2020, Prasanna, 2020, Saraph, 2020, Sharma, 2020, Shukla, 2020, Sinha, 2020, Vora et al., 2020]. Depositions were also invited from the Election Commission of India and the members of its technical committee, however there was no response from them. The CCE also sent a questionnaire [The Citizens' Commission on Elections, 2020] to the ECI, members of its technical committee and some former Chief Election Commissioners; only one response [Gopalaswami, 2020] was received.

In Section 2 we examine the compliance of EVM based voting with democracy principles. In Section 3 we examine the issues related to the trustworthiness of the custody chain and post-election audits. In Section 4 we present our final recommendations.

2 Compliance of EVM based voting with democracy principles

In what follows in Section 2.1 we first briefly capture the current EVM design and the ECI's processes for conducting the elections, and then in Section 2.2 we examine and analyse the concerns with the EVM design.

2.1 The EVM design and ECI's processes

The deposition by Bappa Sinha [Sinha, 2020] summarises the ECI's EVM design and the associated processes.

*former Supreme Court Judge
†former Chief Information Commissioner
‡former Madras High Court Judge
§Malcolm S. Adiseshiah Chair Professor, Institute of Social Sciences
¶Professor of Computer Science and Engineering, IIT Delhi
‖Senior Journalist
**Writer and Activist
††former Secretary, Government of Maharashtra
‡‡IAS (retd)

2.1.1 EVM features

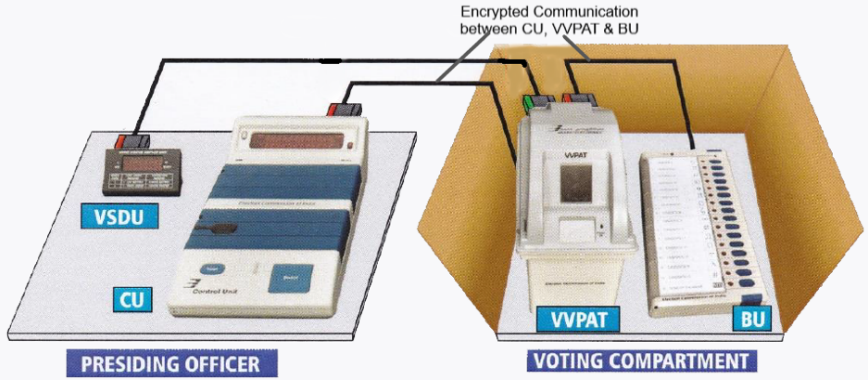

Figure 1: The schematic of ECI's EVM (original diagram from ECI's EVM & VVPAT manual [Election Commission of India, 2021]).

The main features of the EVM design are as follows. It is a Direct Recording Electronic (DRE) voting protocol. The EVM consists of a control unit (CU) which is placed on the presiding officer's desk. The CU is connected to the Voter Verifiable Paper Audit Trail (VVPAT) printer which is then connected to the ballot unit (BU). The VVPAT printer and the BU are kept in the voter booth. The VVPAT status display unit (VSDU) is kept with the presiding officer and displays the status of the VVPAT printer. The different components authenticate each other using digital certificates. The system is designed to stop functioning if paired with unauthorised components.

The communication between components is encrypted. It is a standalone system supposedly with no external communication channels, either wired or through radio. It only has designated interfaces for input and output of data according to specific protocols. As per ECI mandate it should be stand-alone (not computer-controlled) and "one-time programmable" (OTP).

2.1.2 The voting process

The following is the voting process using the EVM. A voter is allowed to proceed to the voting booth after eligibility and identity checks by polling officials. For a vote to be cast the presiding officer must first enable the BU by pressing a button on the CU. The voter casts the vote by pressing a button on the BU selecting a candidate. Once a button is pressed a light-emitting diode (LED) next to the button lights up and there is a long beep indicating that the vote has been recorded. The VVPAT simultaneously prints a small slip of paper that carries the symbol, name and serial number of the candidate selected by the voter. This slip is visible for seven seconds in the viewing window after which it drops off in to a secure box. Once a vote has been cast, the BU becomes inactive and does not respond to any more button presses, till the presiding officer schedules the next vote by again enabling the BU from the CU. There is a mandatory 12 second delay before the CU can enable the next vote to be cast. The casting of votes with key-presses are time stamped.

2.1.3 The design, engineering and manufacturing processes

The EVM software was developed by a select group of engineers from Bharat Electronic Limited (BEL) and Electronics Corporation of India Limited (ECIL) independent of each other, and the EVMs are sourced from both. Testing is done according to the software specification by multiple independent testing groups. The production group carries out production testing in the factory according to a Quality Assurance (QA) plan. Samples from production batches are tested by independent QA groups. BEL and ECIL are responsible for packaging and shipping the EVM systems to the states as directed by the ECI. Container trucks or sealed trucks with proper locking arrangements are used for transporting EVMs and VVPATs. Paper seals are put on the containers. All movement of EVMs are scheduled and monitored using an EVM Tracking Software (ETS), external to the machines, based on Global Positioning System (GPS). On receipt of the EVMs, the district election officers (DEOs) are supposed to video-graph the process of receipt of EVMs and then store them in strong rooms at the district headquarters.

2.1.4 The administrative processes

EVM Preparation: ECI allocates EVMs to States 200 days prior to polling. The EVMs are dispatched 180 days prior to polling and are tracked using the GPS based ETS software. There is a first level checking of the EVMs 3-6 months prior to polling where the internal parts are checked and the CU is sealed. The EVMs are assigned to constituencies using a first-stage randomization software 3 weeks prior to polling. In a second stage randomization the EVMs are assigned to polling booths two weeks before polling. Finally, after the last date for candidate withdrawal, the ballot paper is fixed on the BU, the candidate names are entered in an alphabetical order, a mock poll is conducted and the BU is sealed.

Polling day processes: The serial numbers of the EVM components are shared with the candidates and the polling agents so that they can inspect before commencement of the mock poll. A mock poll of at least 50 votes is conducted in each polling station and the EVM and VVPAT tallies are compared in presence of the polling agents. After the mock polling is over all buttons of the CU other than those used for polling are covered with paper seals. These paper seals are signed by the polling agents.

After polling is over the presiding officer presses the close button, after which no votes can be cast. The complete EVM unit is sealed and signed. Polling agents are allowed to put their own seals. The representatives of the candidates are allowed to travel behind the vehicle that carries the EVMs to the counting storage rooms. The counting storage rooms are sealed and guarded by the Central Reserve Police Force (CRPF). Candidates are allowed to put their own seals on the strongroom.

Counting day processes: First the EVM serial numbers, seals, the start and end times as recorded are verified by both election officials and polling agents. The CUs that do not display the result because they were not closed properly, or in case the total number of votes reported by the CU does not match that reported by the presiding officer, are kept aside for scrutiny. After announcement of results, candidates or counting agents can apply for VVPAT counts to the returning officer who has to take a decision on the matter.

Because of the above systems and processes the ECI and several other commentators [Sinha, 2020] believe that electronic voting using ECI's EVM is safe. In particular, they believe that though there can be no formal guarantees against hacking, hacking is practically impossible because of the tight processes and the secure custody chain of control. Further, they believe that since an EVM is not connected to network it cannot be hacked remotely.

2.2 Concerns with the EVM and our analysis

While banning electronic voting the German Constitutional Court made the following observation [NDI, 2009]:

> "The use of voting machines which electronically record the voters' votes and electronically ascertain the election result only meets the constitutional requirements if the essential steps of the voting and of the ascertainment of the result can be examined reliably and without any specialist knowledge of the subject . . .
>
> The legislature is not prevented from using electronic voting machines in elections if the possibility of a reliable examination of correctness, which is constitutionally prescribed, is safeguarded. A complementary examination by the voter, by the electoral bodies or the general public is possible for example with electronic voting machines in which the votes are recorded in another way beside electronic storage."

Several depositions [Devasahayam, 2020, Shukla, 2020, Vora et al., 2020, Sharma, 2020, Saraph, 2020, Prasanna, 2020, Nayak, 2020] have raised concerns that the EVM based voting may not measure up to the standards laid down by the German Constitutional court. Specifically, the democratic principles that any voting process for public elections should adhere to are [Devasahayam, 2020]:

1. The voting process should be transparent in a manner that the general public can be satisfied that their vote is correctly recorded and counted.
2. The voting and counting process should be publicly auditable.
3. Ordinary citizens should be able to check the essential steps in the voting process. If special expert knowledge is required then all should be able to select their own experts.

4. There should be verifiability in the counting of votes and ascertainment of the results reliably without any special knowledge.

5. An election process should not only be free and fair, but also be seen to be free and fair.

6. Election Commission should be in full control of the entire voting process, and the public at large should be able to verify.

7. Electronic processes, if they are to be used for voting, should be in sync with changing technologies and technological practices, and be subject to public scrutiny/examinability.

The compliance of the ECI's EVM+VVPAT based voting system to the above principles hinges crucially on the verifiability of the EVM and the voting and counting process. Much of the elaborate and complex processes of Sections 2.1.3 and 2.1.4 are required precisely because public verifiability of the election process is doubtful and the public has to inevitably trust various authorities.

Verifiability cannot be established by inviting people to hack the hardware system, as the ECI has done. ECI's challenge for demonstrating hacks is not meaningful, not only because sufficient time and access to tools were denied, but also because something has not yet been hacked provides no guarantee whatsoever that it cannot be hacked [Shukla, 2020]. Indeed, there are numerous examples of EVM hacking all over the world, including an earlier version of the Indian EVM [Shukla, 2020, Halderman, 2011]. Besides, the onus should be on the ECI and their experts to convince people - beyond doubt - that their design is secure, rather than illogically claiming it to be secure because the system has not yet been hacked [Vora et al., 2020, Vora, 2020]. That is not how computer security is conventionally defined.

It is well known that testing is never adequate to declare an electronic system as complicated as an EVM failsafe and verified [Vora et al., 2020, Sharma, 2020]. Testing can usually detect malfunctioning of an equipment but are known to be inadequate for detection of backdoor Trojan attacks, simply because the possibilities are too many. An EVM system composed of its various components can exist in one of a very large number of internal states, which, almost surely, is an exponential function of the configuration parameters. Examination of such large systems is an intractable problem, which often compels the examiners to rely on weaker forms of verification such as quality assurance (QA) methods - for instance, testing. However, well documented studies have shown that such weaker notions of verification can only detect a fraction of software errors (from this follows a common maxim that tests do not constitute a proof). In particular, it may be impossible to determine with reasonable amount of computation or testing whether such systems can ever reach a compromised state, perhaps due to hacking, where the democratic principles are violated [Sharma, 2020]. Also pre-determined and preset test patterns are known to be inadequate for verification of the integrity of a hardware-software codesign of a system as complex as an EVM [Vora et al., 2020].

The due diligence in the EVM design also appear to be lacking in several aspects. It appears that possibilities of side-channel attacks [Greenberg, 2020] have not even been considered [Devasahayam, 2020, Shukla, 2020]. There are numerous examples from all over the world of hacking electronic devices through electromagnetic and other channels [Greenberg, 2020], including of the *Software Guard Extensions* of sophisticated Intel^{TM} processors [Oleksenko et al., 2018]. In view of such possibilities the claims that the EVM has no external communication channels appear to be naive, especially considering that so much is at stake. The OTP (one-time programmable) aspect of the EVM is also doubtful [Sinha, 2020, Devasahayam, 2020, Shukla, 2020], because, in a response to a RTI query, it was revealed that the latest EVM uses the MK61FX512VMD12 microcontroller (from an US based multinational) which has a *programmable* flash memory. However, Sandeep Shukla [Shukla, 2020] points out that it cannot be written to if the JTAG pins are fused and memory lock bit is set. Unfortunately, this is impossible to verify since the details are not publicly available [Nayak, 2020] and the EVM design and prototype has not been made available for public audit.

Experts declaring it safe does not make the EVM+VVPAT verifiable. Besides, none of ECI's experts have credentials in computer security; in fact the majority of them are not even computer scientists [Shukla, 2020]. In addition to experts, ECI seems to be reposing trust in many other entities and organisations - including hardware manufacturers, software developers and testers, system assemblers and unmodelled custody chains - and is thus not entirely in control [Devasahayam, 2020, Vora et al., 2020, Saraph, 2020].

Many claims of the ECI and its experts do not stand up to scrutiny. Some examples are 'EVM is unhackable' [Shukla, 2020, 2018, Vora et al., 2020, Sharma, 2020], 'functionality tests and mock polls are sufficient' [Sharma, 2020, Vora et al., 2020], 'randomization of EVM allocations makes the process safe' [Vora et al., 2020], 'safe because candidate order is not known when EVM is sealed' [Vora et al., 2020], 'mutual authentication of EVM components makes it safe' [Vora et al., 2020], 'ECI's procedures cannot be circumvented' [Devasahayam, 2020, Vora et al., 2020, Saraph, 2020], 'ECI's VVPAT protocol makes

the voting process verifiable' [Vora et al., 2020, Sharma, 2020, Saraph, 2020]; all these claims have been convincingly challenged in the cited depositions received by the CCE.

Thus elections must be conducted assuming that the electronic voting machines may possibly be tampered with [Vora et al., 2020, Sharma, 2020]. After all, with modern data analytics it may require targeting the EVMs in just a few polling stations to swing the election results for a constituency [Shukla, 2020, 2018, Vora et al., 2020]. The long time window - over the cycle of design, implementation, manufacture, testing, maintenance, storage and deployment - may provide ample opportunity for insiders or criminals to attempt other means of access [Vora et al., 2020]. There is an overwhelming requirement of trust on such custody chains; such (often implicit) assumptions of trust in various mechanisms make the election process unverifiable [Vora et al., 2020, Sharma, 2020, Saraph, 2020].

2.3 Concerns with the VVPAT system

ECI's VVPAT system is not voter-verified in the true sense [Vora et al., 2020, Sharma, 2020, Saraph, 2020]. The correct VVPAT protocol should be to allow a voter to approve the VVPAT slip before the vote is cast, and provide an option to cancel her vote if she thinks there is a discrepancy [Vora et al., 2020]. There is no clear protocol for dispute resolution if a voter complains that a VVPAT printout is incorrect, as there is no non-repudiation of a cast vote [Sharma, 2020].

Also, there is no guarantee that every VVPAT slip that is finally counted has been verified by a legitimate voter (i.e., there has been no vote stuffing), or that every voter-verified slip is finally counted (i.e., there have been no deletion of votes). The VVPAT audit can at best ensure that the electronic and VVPAT tallies match, but that by itself - without *compliance audit* [Stark and Wagner, 2012] based protection against spurious vote addition or deletion in a manner verifiable by all candidates - provides no real guarantee [Sharma, 2020, Vora et al., 2020, Vora, 2020, Saraph, 2020].

Finally, since the VVPAT slips are not demonstratably in one-to-one correspondence with the electronic records, it needs to be clearly defined which of the two is the legal definition of a vote. Basic logic demands that it should be the VVPAT slip, but ECI seems to suggest that it is the electronic record.

The overall lack of transparency and public auditability, which are crucial for democratic principles of public elections, are worrisome [Sinha, 2020, Devasahayam, 2020, Shukla, 2020, Vora et al., 2020, Sharma, 2020, Saraph, 2020, Prasanna, 2020]. The non-verifiability of the EVM and VVPAT based voting protocol makes it impossible to rule out unpredictable manipulations by unpredictable entities, including by foreign players. It is essential that all aspects of an election may be observed, audited and independently-verified by the public to engender trust [Vora et al., 2020, Nayak, 2020, Shukla, 2020].

3 Aspects of EVM/VVPATs before and during polling, storage, counting and declaration of results

3.1 Trustworthiness of the custody chain of EVMs

Several depositions raised concerns regarding the efficacy of the processes described in Sections 2.1.3 and 2.1.4 for maintaining the integrity of the polling process. Specifically, the following anomalies were noticed in the Lok Sabha Elections 2019.

The ECI and the manufacturers-cum-suppliers of EVMs – ECIL and BEL – appear to have been evasive in response to RTI queries [Nayak, 2020]. In addition, the information on the audits conducted by STQC (Standardisation Testing and Quality Certification Directorate, Ministry of Electronics and Information Technology) and CFSL (Central Forensic Science Laboratory) have also been sketchy and evasive [Nayak, 2020]. The reluctance by the authorities to share information publicly – despite the Central Information Commission's (CIC) recommendation made in 2018 that information relating to the software used in EVMs be made public in the larger public interest – is surprising and worrisome [Nayak, 2020].

There were discrepancies in the voter turnout/votes polled data on the Electronic Voting Machines (EVMs) and the votes counted data on EVMs in over 373 constituencies [Agarwal, 2020, Devasahayam, 2020]. The four highest discrepancies were of 18,331, 17,871, 14,512 and 9,906 votes where the votes in the EVMs were in surplus. These numbers are clearly too large to be explained by inadvertently counted remnant mock polling data. Not only have there been no explanations forthcoming from the ECI regarding the discrepancies, but the ECI also pulled down the data from their website after an explanation was sought [Agarwal, 2020]. About 2 million EVMs were stated to be missing from the election commission. The ECI had no explanation for this [Devasahayam, 2020, Vora et al., 2020]. After the final vote was cast there were video reports from at least 10 different places of new EVMs being moved into strong rooms. ECI said these were reserve EVMs, but provided no evidence for this, and no explanation for why they need to be

moved just before counting rather than at the time of voting, when there was, in some cases, weeks between voting and counting. They also provided no explanation as to why, as required by the EC rules, there were no security officers accompanying these vehicles, and why these vehicles were often un-numbered, unofficial vehicles. Doubts arise as to whether these are part of the 2 million missing EVMs. There have also been reports of irregularities in the counting process [Devasahayam, 2020].

3.2 VVPAT counting

3.2.1 The controversy

The issue of how many EVMs need to be checked by comparing the electronic tally with a manual VVPAT slip tally for audit of the machine counts has also been mired in controversy.

In its letter dated 13.02.2018 the ECI directed the State chief electoral officers to mandatorily verify VVPAT paper slips in only one randomly selected polling station in each assembly constituency. The statistical basis for this directive was however unclear [Devasahayam, 2020, Prasanna, 2020]. 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 (some reports mention that they considered a total of 10.35 Lakh EVMs). It says that, if a fraction of 2% or more of the EVMs are faulty, cross-checking 479 chosen at random across the country will be sufficient to detect this fact with near certainty (very high probability) [Devasahayam, 2020, Prasanna, 2020, Vora et al., 2020, Vora, 2020, Saraph, 2020]. This was also supported by Rajiv Karandikar of the Chennai Mathematical Institute [Devasahayam, 2020].

In response to petitions in the Supreme Court from representatives of the civil society and opposition parties that the then standard of cross-checking one EVM per assembly constituency was not sufficient, the EC used the Bhatt Report to claim that their approach resulted in checking 4,125 EVMs over the entire country and was hence more than sufficient. However, the Supreme Court ordered the Election Commission to increase the number of cross-checked EVMs to five per Assembly constituency in order to assuage the concerns of the petitioners (this corresponds to 20,625 EVMs across the country). The court later turned down another set of petitions filed by civil society groups and opposition parties to count 50% of EVMs per constituency, saying that this was not necessary. The ECI claimed that manual VVPAT counting in 50% of the constituencies will delay the announcement of results [Devasahayam, 2020, Prasanna, 2020, Vora, 2020, Vora et al., 2020]. The rationale behind the SC's directive for cross checking only 5 EVMs per assembly constituency against manual VVPAT counts was never explained. It does not seem to have any statistical basis [Devasahayam, 2020, Prasanna, 2020, Vora, 2020, Vora et al., 2020]. Not cross-checking sufficient number of EVMs even after widespread public suspicions, and 21 opposition parties as well as civil society asking for it, diminishes public faith in the process [Devasahayam, 2020]. The SC also failed to direct what 'decision rules' must be followed by the ECI in the event of discrepancies between manual counting and electronic counting. [Devasahayam, 2020, Prasanna, 2020].

3.3 Our analysis

In probability theory and statistics, the sufficiency of sampling is usually determined by the hypergeometric distribution. It is a discrete probability distribution that describes the probability of k successes (random draws for which the object drawn has a specified feature, *in this case a defective EVM*) in n draws, without replacement, from a finite population of size N that contains exactly K objects with that feature, wherein each draw is either a success or a failure. [This is very similar to the binomial distribution that describes the probability of k successes in n draws with replacements.]

In an analysis using the hypergeometric distribution, Shetty [Shetty, 2018] shows that if 1% of the EVMs are assumed to be defective (give a mismatch with the VVPAT count), then, for a 99% probability of detecting at least one defective EVM, the sample sizes required, for various population sizes are given as per Figure 2. Figure 3 defines population. Figure 4 shows how the sample size must vary with the proportion of faulty EVMs. Quoting Shetty [Shetty, 2018]

> "Studying Figures 2 and 3 together, it is obvious that if the EVMs used in an Assembly Constituency are defined as the population, the population size (N) will be very small; the sampling fraction (n/N) will be very big; and the sample size (n) will vary considerably across Assembly Constituencies. The same is true if the EVMs used in a Parliamentary Constituency are defined as the population.
>
> If the EVMs in a State as a whole are defined as the population, there is considerable variation in population size from the very small (Sikkim) to the very big (Uttar Pradesh). For the nine

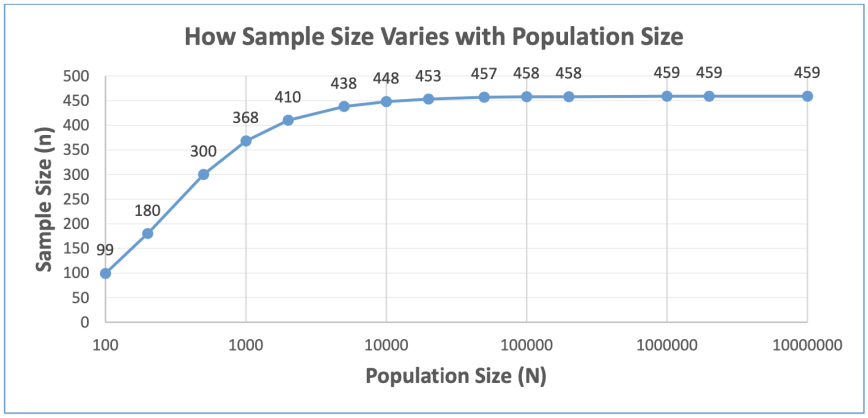

Figure 2: Sample size required as per hypergeometric distribution to detect at least one faulty EVM with 99% probability in a population with 1% faulty EVMs. In this particular example, it is seen that increase of population size beyond about 10,000 ($N/n > 20$) has little or no impact on the sample size. The figure has been taken from [Shetty, 2018]. This of course assumes the sampling to be homogeneous across the population.

Population Boundary	*Population Size (N) (Number of EVMs)*
Assembly Constituency	≈ 30 to 300
Parliamentary Constituency	≈ 300 to 1800
A State as a whole	Ranging from 589 (Sikkim) to 1,50,000 (U.P) For 9 States N < 10,000 For 20 States N > 10,000
India as a whole	≈ 10,00,000

≈ is the symbol for 'approximately equal'.

Figure 3: Defining population. The figure has been taken from [Shetty, 2018].

> smaller States with population size less than 10,000 EVMs, the sampling fraction (n/N) will be quite big and the sample size will vary considerably across the States. For the 20 bigger States with population size greater than 10,000 EVMs, the sample size will 'hit a plateau' in the 450s and further increase in population size will have little or no effect on it.
>
> If the EVMs used in India as a whole are defined as the population, due to the 'plateau effect', the sample size is just one more than that for U.P."

In view of the above, in most cases (almost all) ECI's prescribed sample size of "one EVM per assembly constituency" will fail to detect a faulty EVM with a very high probability. See [Shetty, 2018] for details. Using a similar analysis Vora et al. [Vora, 2020, Vora et al., 2020] show that with a 2% rate of faulty EVM, the SC's directive of checking 5 EVMs per assembly constituency will fail to detect a faulty EVM in roughly 50% of the cases.

The Bhatt report is clearly based on the profoundly mistaken premise of taking the whole country as one population. At a 2% fault rate the Bhatt approach is designed to detect only if roughly 20,000 EVMs are faulty. It completely misses the point that swinging a few tens of thousands of votes, with far fewer faulty EVMs, is sufficient to swing a single Lok Sabha seat [Devasahayam, 2020, Vora, 2020, Vora et al., 2020, Prasanna, 2020, Saraph, 2020, Shukla, 2020].

Note that, if the margin between the winner and the second highest vote getter is small, fewer EVMs need to be rigged, and, to detect this, more need to be checked. If the 'population' has to be defined at the level of an assembly constituency, the number of EVMs to be cross checked will depend on the margin, and, while it can be smaller than 30%, it can be larger than 50% as well. For example, in the extreme case of the margin being only one vote, a complete manual count will be necessary. In view of the above,

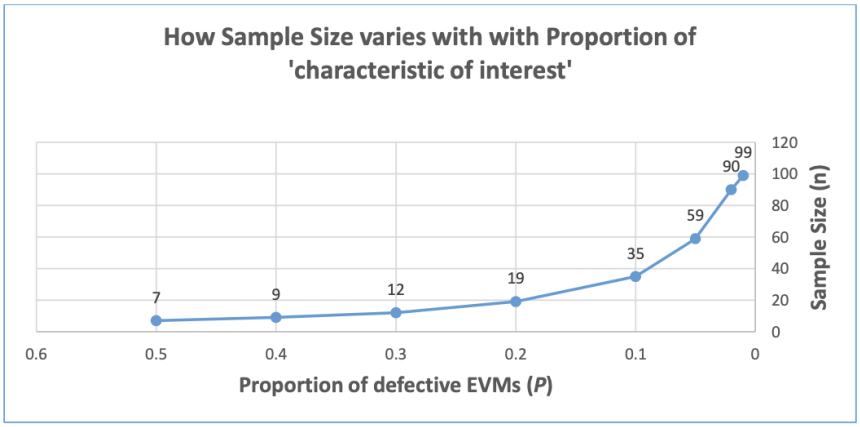

Figure 4: Variation of sample size with proportion of faulty EVMs fixing the population size to $N = 100$. The figure has been taken from [Shetty, 2018].

the civil society and opposition party concerns that 5 EVMs per constituency is not sufficient appear to be reasonable.

Thus, in practice, election outcomes may be changed by tampering significantly fewer EVMs than even what the civil society demands consider, and it is incorrect to assume that faulty (or hacked) EVMs are distributed homogeneously across the population. Moreover, the number of EVMs that need to be audited against manual VVPAT counts cannot be independent of the margins. However, with rigorous *risk-limiting audit procedures* that consider the margins [Lindeman et al., 2012, Bernhard et al., 2017, Vora, 2020, Vora et al., 2020, Stark and Wagner, 2012], it should be possible to audit election outcomes without necessarily manually counting all VVPAT slips. Complete manual counting should be the last resort.

4 Final recommendations

The analysis in the above two sections clearly demonstrates that the decision making processes within the ECI need to be much more logical, rigorous and principled compared to what it was during the 2019 parliamentary elections. Ad hoc systems and processes without adequate analysis of the properties and the guarantees should be avoided. Only then can elections using electronic means adhere to standard democratic principles, appear to be free and fair, and engender confidence in election outcomes.

Specifically, we make the following recommendations for the future:

Software and hardware independence: The electronic voting system should be re-designed to be software and hardware independent in order to be verifiable or auditable. EVMs cannot be assumed to be tamper-proof. As defined by Rivest [Rivest, 2008], *a voting system is software (hardware) independent if an undetected change in software (hardware) cannot lead to an undetectable change in the election outcome*. In other words, even if a voting machine is tampered to change the votes, it should be possible to detect so in an audit. This is not to say that a hardware based EVM cannot be used, but that the correctness of an election outcome should not depend on the assumption of correctness of the EVM. Any solution that relies crucially on the assumption of correctness of the EVMs is not software and hardware independent [Vora et al., 2020, Sharma, 2020].

To be compliant with democratic principles there is a definite need to move away from only certification of voting equipment and processes and instead demonstrate - end-to-end - that the outcome of an election is correct irrespective of machines and custody chains of EVMs. Two ways to do this are mentioned in the literature, namely, adopting rigorous and well established strategies for compliance and risk-limiting audits [Lindeman et al., 2012, Stark and Wagner, 2012, Bernhard et al., 2017] or by using a provably end-to-end verifiable cryptographic protocol, or both [Bernhard et al., 2017, Vora et al., 2020, Sharma, 2020].

End-to-end (E2E) cryptographic verifiability: One way to achieve software and hardware independence is to use E2E verifiable systems with provable guarantees of correctness [Vora et al., 2020, Sharma, 2020, Saraph, 2020, Bernhard et al., 2017]. The overall correctness of voting is established by the correctness of three steps: *cast-as-intended* indicating that the voting machine has registered

the vote correctly, *recorded-as-cast* indicating the cast vote is correctly included in the final tally, and *counted-as recorded* indicating that final tally is correctly computed. There must also be guarantees against *spurious vote injections* [Sharma, 2020]. These guarantees should be publicly verifiable.

ECI should explore the possibility of using an E2E verifiable system [Bernhard et al., 2017].

Re-design of the VVPAT system: The other way to achieve software independence is through risk limiting end-of-poll audits using VVPAT. For this, the VVPAT system should be re-designed to be fully voter-verified [Vora et al., 2020, Saraph, 2020, Sharma, 2020]. The voter should be able to approve the VVPAT printout before the vote is finally cast, and be able to cancel if there is an error.

Also, either the VVPAT slips must be in one-to-one correspondence with the electronic records (difficult, considering the secret ballot requirement), or it needs to be clearly defined which of the two is the legal definition of a vote. Simply declaring results based on the electronic counts violates democracy principles.

Moreover, in case a voter disputes that the vote has been incorrectly recorded, there must be a clear method of determination either in favour of the voter or in favour of the authorities [Sharma, 2020]. This may not be possible in a pure DRE based system like the ECI's EVM, because the machine may not make the same error when tested and because it is not possible to determine, without doubt, whether it did originally make the error. In this case, the voter cannot be penalized and a clear protocol for dispute resolution must be put in place.

End-of-poll audits: For proper end-of-poll audit using VVPAT, the ECI needs to change the currently prescribed policy with rigorous risk-limiting audit [Lindeman et al., 2012] based sampling strategies before the results are announced.

Also there must be a clear pre-announced protocol for deciding the outcome - including possible re-polling - if there is a mismatch between the VVPAT and the electronic tallies [Devasahayam, 2020].

Legislation: There has to be legislation to deal with the cases when the audit, and subsequent recount, reveal a problem. Legislation will also be required to regulate when, and if, a candidate can request a hand count. Best practices suggest that such legislation be based on established statistical principles, as opposed to the judgment of individual election officials, to the extent possible [Vora et al., 2020].

Independent review: The voting system design should be subjected to independent (of the government and ECI) review and the integrity of the election process should be subjected to independent audit. The findings should be made public.

Transparent processes: Finally, the election processes need to be completely transparent and should not have too many requirements of trust on authorities and experts, including on ECI [Devasahayam, 2020, Prasanna, 2020, Vora et al., 2020, Sharma, 2020, Saraph, 2020]. All design details should be publicly available. Also, there should be more public consultations, and public and civil society concerns should be transparently and fairly handled.

Finally, if we opt for electronic elections and bring computer science and statistics into public life, then we cannot leave their disciplinary rigour behind.

Acknowledgement

We thank all those who have deposed and Prof. Sanjiva Prasad (Computer Science and Engineering, IIT Delhi) who has mentored this study. We also thank all those who participated in the many discussions and provided input and insight.

References

Poonam Agarwal. Deposition by Poonam Agarwal. https://68df2dd4-cd8b-42a5-9d9d-6e0c5befdb3b.filesusr.com/ugd/528a17_2d2f40086c024b17921f310c8b0baed6.pdf, 2020.

Matthew Bernhard, Josh Benaloh, J. Alex Halderman, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa Teague, Poorvi L. Vora, and Dan S. Wallach. Public evidence from secret ballots. In *Electronic Voting - Second International Joint Conference, E-Vote-ID 2017, Bregenz, Austria, October 24-27, 2017, Proceedings*, pages 84–109, 2017. doi: 10.1007/978-3-319-68687-5_6. URL https://doi.org/10.1007/978-3-319-68687-5_6.

M. G. Devasahayam. Deposition by M G Devasahayam. https://68df2dd4-cd8b-42a5-9d9d-6e0c5befdb3b.filesusr.com/ugd/528a17_4753f5a2205c4c66867067465ae2671d.pdf, 2020.

Election Commission of India. Manual on Electronic Voting Machine and VVPAT. https://eci.gov.in/files/file/9230-manual-on-electronic-voting-machine-and-vvpat, 2021. [Accessed March 26, 2021].

Needamangalam Gopalaswami. Response to questionnaire. https://drive.google.com/file/d/1NqUvcLbt6dPyg5k-PmzQzpC40iLxxX0S/view, 2020.

Andy Greenberg. Hacker Lexicon: What Is a Side Channel Attack? https://www.wired.com/story/what-is-side-channel-attack/, 2020. [Online June 21, 2020].

Alex Halderman. Security Problems in India's Electronic Voting System. https://crcs.seas.harvard.edu/event/alex-halderman-security-problems-india%E2%80%99s-electronic-voting-system, 2011.

Mark Lindeman, Philip B. Stark, and Vincent S. Yates. BRAVO: Ballot-polling risk-limiting audits to verify outcomes. In *2012 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 12)*, Bellevue, WA, August 2012. USENIX Association. URL https://www.usenix.org/conference/evtwote12/workshop-program/presentation/lindeman.

Justice (Retd.) Madan Lokur, Wajahat Habibullah, Justice (Retd.) Hariparanthaman, Arun Kumar, Subhashis Banerjee, Pamela Philipose, Sundar Burra, and M. G. Devasahayam. An Inquiry into India's Election System: Report of the Citizens' Commission on Elections (Volume I). https://68df2dd4-cd8b-42a5-9d9d-6e0c5befdb3b.filesusr.com/ugd/528a17_cd1b5675fab34019b5f964c230d24f0b.pdf, 2021. [Online January 30, 2021].

Venkatesh Nayak. Deposition by Venkatesh Nayak. https://68df2dd4-cd8b-42a5-9d9d-6e0c5befdb3b.filesusr.com/ugd/528a17_b64a86e8f96440a2b70a99315993bba1.pdf, 2020.

NDI. The Constitutionality of Electronic Voting in Germany. https://www.ndi.org/e-voting-guide/examples/constitutionality-of-electronic-voting-germany, 2009. [Accessed June 8, 2020].

Oleksii Oleksenko, Bohdan Trach, Robert Krahn, Mark Silberstein, and Christof Fetzer. Varys: Protecting SGX enclaves from practical side-channel attacks. In *2018 USENIX Annual Technical Conference (USENIX ATC 18)*, pages 227–240, Boston, MA, July 2018. USENIX Association. ISBN ISBN 978-1-939133-01-4. URL https://www.usenix.org/conference/atc18/presentation/oleksenko.

S Prasanna. Deposition by Prasanna S. https://68df2dd4-cd8b-42a5-9d9d-6e0c5befdb3b.filesusr.com/ugd/528a17_07d226f15bb1445792ec586ac1cd93b0.pdf, 2020.

Ronald L. Rivest. On the notion of software independence in voting systems. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 366(1881):3759–3767, 2008. doi: 10.1098/rsta.2008.0149. URL https://royalsocietypublishing.org/doi/abs/10.1098/rsta.2008.0149.

Anupam Saraph. Deposition by Anupam Saraph. https://68df2dd4-cd8b-42a5-9d9d-6e0c5befdb3b.filesusr.com/ugd/528a17_35df51e14f884e9093c3eaa12403e37b.pdf, 2020.

Subodh Sharma. Deposition by Subodh Sharma. https://68df2dd4-cd8b-42a5-9d9d-6e0c5befdb3b.filesusr.com/ugd/528a17_e765d11eb2c7424787e37c10af691be3.pdf, 2020.

K. Ashok Vardhan Shetty. Winning Voter Confidence: Fixing India's Faulty VVPAT-based Audit of EVMs. https://www.thehinducentre.com/publications/policy-watch/article25607027.ece, 2018. [Online November 27, 2018].

Sandeep Shukla. Deposition by Sandeep Shukla. https://68df2dd4-cd8b-42a5-9d9d-6e0c5befdb3b.filesusr.com/ugd/528a17_ce2129018ee7404487b68808b721f01d.pdf, 2020.

Sandeep K. Shukla. Editorial: To use or not to? embedded systems for voting. *ACM Trans. Embed. Comput. Syst.*, 17(3):58:1–58:2, May 2018. ISSN 1539-9087. doi: 10.1145/3206342. URL http://doi.acm.org/10.1145/3206342.

Bappa Sinha. Deposition by Bappa Sinha. https://68df2dd4-cd8b-42a5-9d9d-6e0c5befdb3b.filesusr.com/ugd/528a17_a89ea35a3f754661be3aee94ca981c2e.pdf, 2020.

Philip B. Stark and David A. Wagner. Evidence-based elections. *IEEE Secur. Priv.*, 10(5):33–41, 2012. doi: 10.1109/MSP.2012.62. URL https://doi.org/10.1109/MSP.2012.62.

The Citizens' Commission on Elections. Some questions for the former Chief Election Commissioners, present CEC and Election Commissioners as well as the Members of the Technical Advisory Committee of ECI regarding the security and integrity of EVM voting and VVPAT counting. https://drive.google.com/file/d/1H7kEjZoas5lw7tyLwxh27MIDWNPAep0J/view, 2020.

Poorvi L. Vora. Deposition by Poorvi Vora. https://68df2dd4-cd8b-42a5-9d9d-6e0c5befdb3b.filesusr.com/ugd/528a17_8e7b98b93dbc4d1c85a346c6f4a0a59f.pdf, 2020.

Poorvi L. Vora, Alok Choudhary, J. Alex Halderman, Douglas W. Jones, Nasir Memon, Bhagirath Narahari, R. Ramanujam, Ronald L. Rivest, Philip B. Stark, K. V. Subrahmanyam, and Vanessa Teague. Deposition by Poorvi Vora et al. https://68df2dd4-cd8b-42a5-9d9d-6e0c5befdb3b.filesusr.com/ugd/528a17_2249d34f77c94e7da300aeeff4335a33.pdf, 2020.