Receipt Issuing, Contendable Remote Poll-Site Voting

Prashanth P. Bungale and Swaroop Sridhar
Department of Computer Science
The Johns Hopkins University

Abstract

This paper presents the design of an electronic voting system in which a voter can vote not only from his home poll-site, but from *any* poll-site, in a manner that guarantees total voter anonymity. The core concentration of this work is the design of a mechanism in which a voter can be given a *receipt* to acknowledge his vote and at the same time prevent any occurrence of vote-selling or voter coercion. The voter shall be able to confirm his vote – from anywhere – after election results have been published. If deemed necessary, the voter shall be able to *anonymously* contend the election results from *any* election office. The details of the protocol have been sketched in the paper.

1. Introduction

People all over the world are starting to take a hard look at their voting equipment and procedures, and trying to figure out how to improve them. There is a strong inclination towards moving to Electronic Voting in order to enhance voter convenience, increase voter confidence and voter turnout. However, there are serious technological and social aspects that come into play while designing the voting system, which we have addressed in accordance to the previously identified requirements.

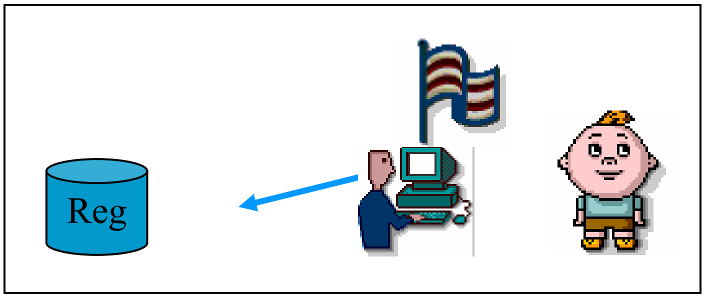
The main focus of this work is addressing the open question of providing a mechanism in which a voter can be given a *receipt* to acknowledge his vote (which facilitates vote confirmation and vote contention), and at the same time prevent any occurrence of vote-selling or voter coercion. Much of the present literature views receipt-freeness as the *necessity* for precluding vote-selling and voter coercion. There is a clear picture of a tradeoff between the "mutually exclusive" issues of receipt issuance and voter security. We intend to overcome this tradeoff and thus ensure the voter's confidence in that his vote has been counted as cast, without compromising voter security.

2. Design

In this section, we present the protocol flows and an analysis of the various components of our design. We do this by walking through the various phases of the election process.

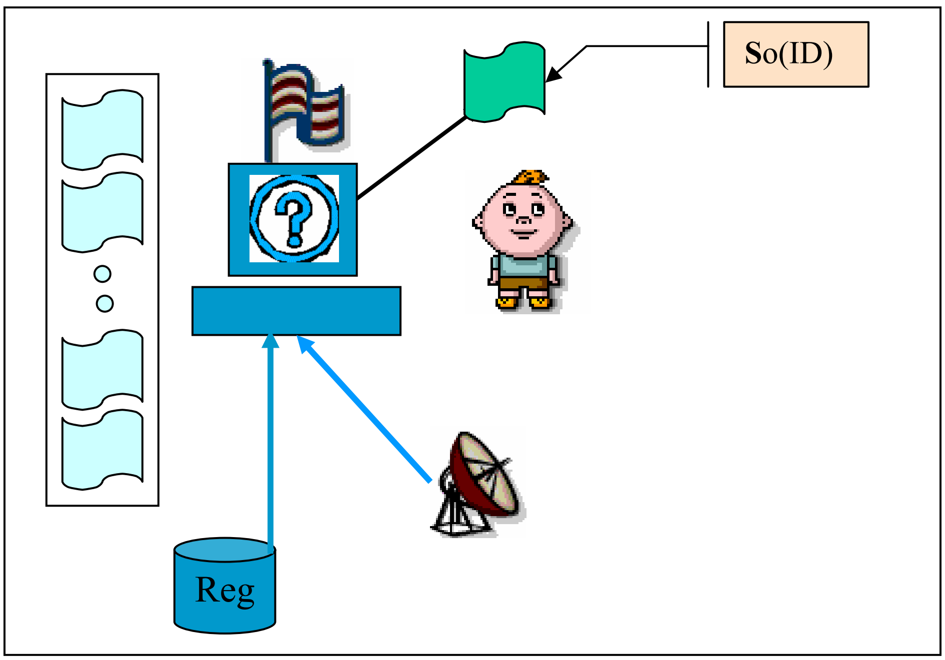
2.1. Voter Registration

Voter registration shall be done *in person* at the various offices before the Election Day. The officer shall register the person's identification (Signature, ID no., etc.) and the offices for which he is eligible to vote, in the database.



2.2. Voter Authentication and Vote Initialization

On the Election Day, the officer at the poll site authenticates the voter against the registration database using some kind of identification information presented to him. Once the voter is authenticated, the officer initializes a memory stick with the voter's identification information and information about the ballot to be used, then, signs it with his private key, and hands it over to the voter.



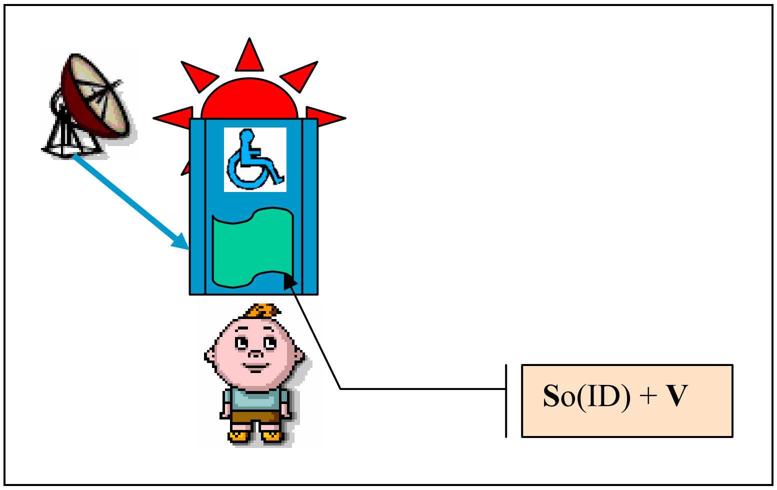
In the case of remote poll-site voting, the officer at the remote poll-site gets the voter's registration information from the remote database and uses this to authenticate the voter. He then requests and receives the identification information, signed by the officer at the voter's home poll-site, and initializes a memory stick with it (S_{o2}(ID)), which is finally handed over to the voter.

Analysis: Since the memory stick is signed by an election officer, the voter cannot forge votes, for example, by bringing lots of memory sticks with him to the poll-site. Moreover, the privacy and anonymity of the voter are totally uncompromised, as the memory stick is signed by the officer at his home poll-site, irrespective of where the voter actually casts his vote.

2.3. Vote Generation

In our design, the vote generation machine (which just records the voter's choices into the memory stick) and the vote casting machine (which is used to actually cast the vote, receive a receipt and form the audit trail) are *(physically)* isolated from each other, so that it is sufficient to subject the vote casting machine alone – which is kept as simple as possible – to thorough testing, verification and certification.

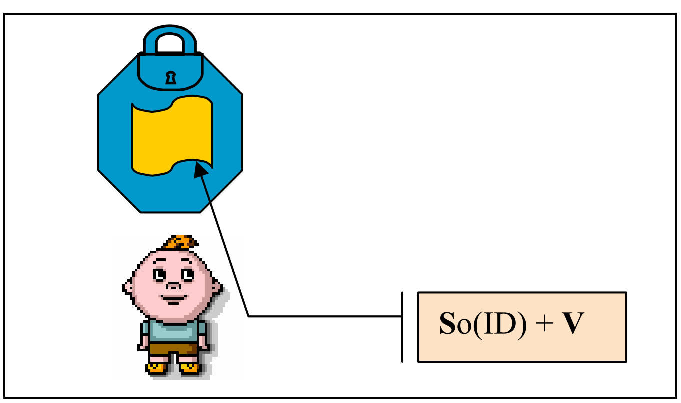
The voter takes the initialized memory stick and inserts it into a vote generation machine, placed such that his privacy is ensured. The machine presents the voter with the concerned ballot (downloading it, if necessary, from his home poll-site), and provides him with an easy-to-use and unambiguous interface to generate his vote. The interface provided also caters to the needs of multilingual voters and disabled (e.g., blind) voters.



Analysis: The vote generation machine can be proprietary, so that it can be independently designed and developed by multiple manufacturers. Since it caters to the needs of multilingual and disabled voters, it facilitates equality of access to all voters.

2.4. Vote Verification

The voter takes his generated vote and inserts it into the vote casting machine, which comprises a simple display that displays the information present on a memory stick. He then verifies the vote as displayed by the machine. If the voter is not satisfied with his current choices, he can revert back to the vote generation phase, correct his vote, and then re-verify his vote. This correction can be made as many number of times as he wishes.



Analysis: Since the vote casting machine is designed to be extremely simple, is completely open-source and is subject to thorough testing, verification and certification, the voter can be SURE that the vote choices recorded in his memory stick are exactly as displayed on the display unit of the machine. Also, since the voter is able to verify and correct his vote, we achieve the goal of reflecting the correct intention of the voter in the recorded vote.

2.5 Vote Casting, Issue of Receipts and Generation of Audit Trail

In addition to the simple display and memory stick reader units mentioned above, the vote casting machine has sufficient computation power to execute encryption and other necessary cryptographic algorithms. It also has ports connected to network hosts, which help communicate with other vote-casting machines. Lastly, it has output ports connected to the tallier(s).

2.5.1 Home poll-site voting

After the voter satisfactorily confirms his vote, he casts the vote, at which time the following actions are performed:

i) The vote, 'V', present on the memory stick, is signed by the officer's private key and by the private keys of many observers (possibly, mutually adversarial parties such as political parties) to get $S_{o, p, p, p, \ldots}(V)$*.

ii) A copy of this signed vote is recorded on another memory stick, which is stored internally to form a part of the (anonymous) permanent physical audit-trail.

iii) Another copy of the signed vote is sent to the vote tallier, which will then take this vote into account for tallying. In addition to the vote tallier machine kept by the election office, the copy of the signed vote can optionally be broadcast to multiple vote tallier machines belonging to various observers (again, mutually adversarial parties). Note that the voter's identification information is not stored either on the audit trail or on the copies sent to the vote talliers.

iv) Now, a (unique) random number 'N' is generated, and the signed vote, $S_{o, p, p, p, \ldots}(V)$, (prepared in step (i) above) on the voter's memory stick is encrypted using this as the symmetric key, to get $Ec_N (S_{o, p, p, p, \ldots}(V))$.

v) This is further encrypted using the officer's public key to get $E_o (Ec_N (S_{o, p, p, p, \ldots}(V)))$.

vi) This is then permanently sealed (possibly by blowing a fuse on the memory stick) before the memory stick is finally handed over to the voter.

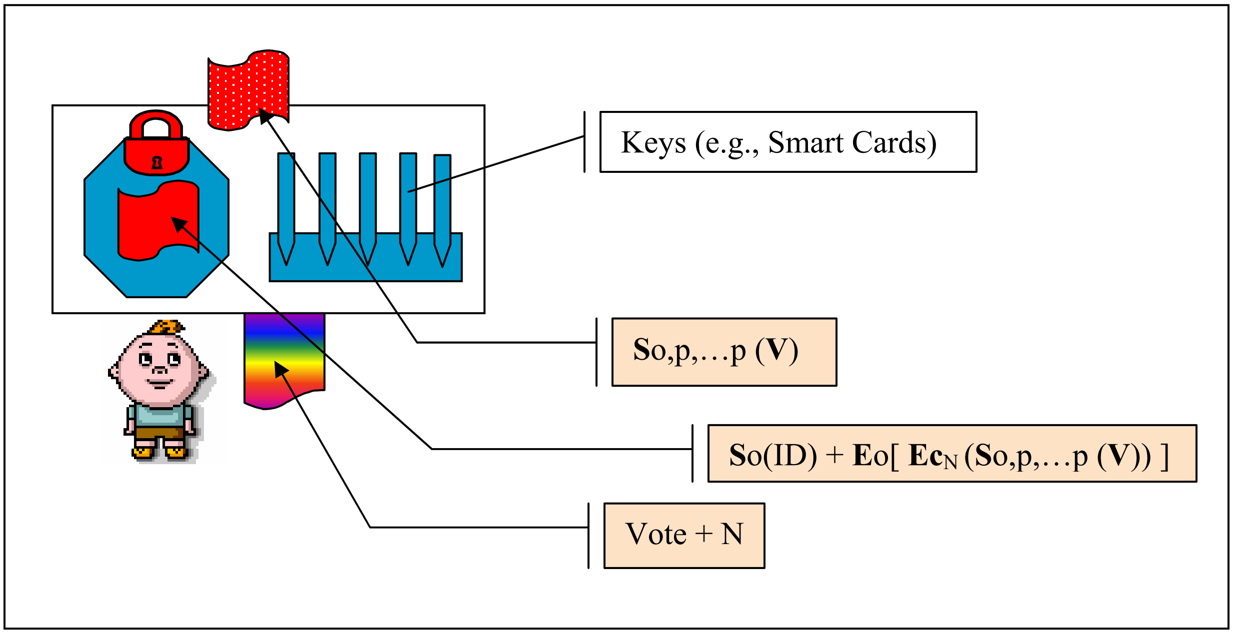
vii) A print-out of the number 'N' and the name of the candidate voted for, is issued to the voter. This, along with the memory stick handed over in step (vi) above, forms the receipt for his vote cast. The print-out facilitates vote-verification and memory stick facilitates vote-contention

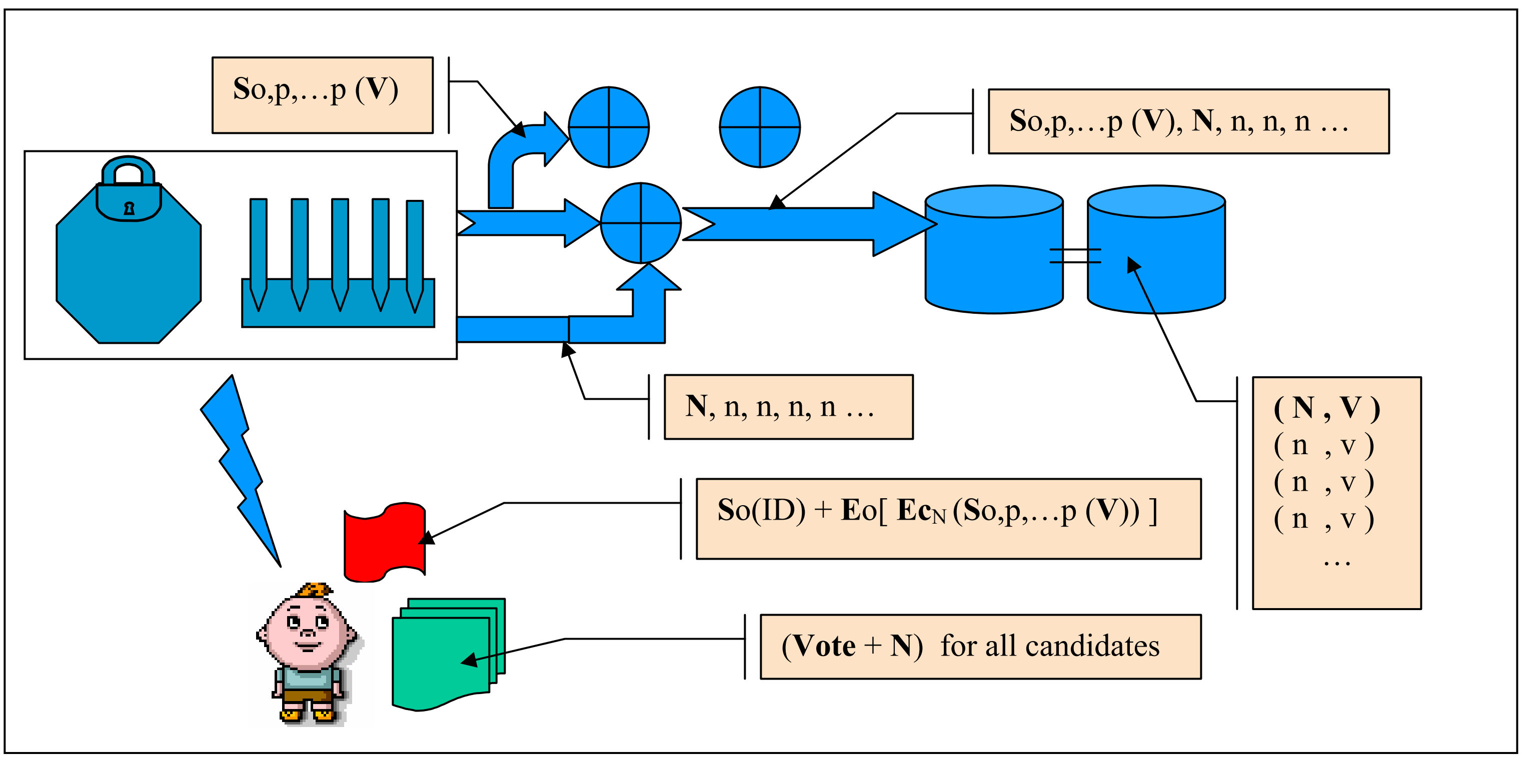
viii) In addition to the correct receipt, the machine also issues fake receipts – identical to the legitimate one – which are print-outs of some more (unique) random numbers (n, n, n, …) with the names of all the other candidates. This step is necessary to prevent voter coercion and vote selling.

---

* - 'E' stands for public-key encryption; 'Ec' stands for symmetric-key encryption; 'S' stands for signature

ix) Finally, the signed vote, $S_{o,\ p,\ p,\ p,\ \ldots}(V)$, and the random numbers, (N, n, n, n, …), generated above are transmitted to the database.





Analysis:

i) Since the vote is signed by many observers – in addition to the election officer – who have no reason to collude amongst themselves, vote forging / ballot stuffing is prevented.

ii) Since the voter's identification information is not tagged on to his vote anywhere else other than the memory stick that the voter takes away with him, the anonymity and privacy of the voter are ensured.

iii) Since there is a physical audit trail, accurate recounts in the case of contested elections are facilitated.

iv) Since there are redundant talliers, incorrect tallies can be detected.

v) Since the political parties' talliers do not receive the 'N' values corresponding to the votes, there is no possibility of timing attacks by them.

vi) Because:

   a. The vote is encrypted by the officer on the memory stick handed over to the voter
   b. Fake receipts (print-outs) identical to the legitimate one are issued

   There is no possibility that he can prove to somebody else that he has voted in some way. Thus, voter coercion and vote-selling are prevented.

vii) Since the memory stick is sealed, possibly by blowing a fuse or something similar to that, the vote can never be modified.

viii) At the time of vote contention (when the voter takes his memory stick to contend the way his vote was counted), since the vote on the memory stick is encrypted by the number 'N', known only to the user, it is not possible even for the election officer to view the vote.

ix) Since the database of (N,V) is maintained in a redundant fashion, reliability is ensured.

2.5.2 Remote poll-site voting

In the case of remote poll-site voting, after the voter satisfactorily confirms his vote, he casts the vote, at which time the following actions are performed:

i) The vote, 'V', present on the memory stick, is signed by the remote poll-site officer's private key (S_{o1}) and, along with the identification information, is encrypted with the home poll-site officer's public key (E_{o2}) to get E_{o2} [S_{o2}(ID) + S_{o1}(V)] and sent to the remote poll-site's vote casting machine through the network host (along a private network, with redundant connectivity).

ii) The home poll-site (local) officer decrypts the message using his private key and then the vote, 'V', present on the memory stick, is signed by the local officer's private key and by the private keys of many local observers (possibly, mutually adversarial parties such as political parties) to get $S_{o2, p, p, p, \ldots}$(V).

iii) A copy of this signed vote is locally recorded on a memory stick, which is stored internally to form a part of the (anonymous) permanent physical audit-trail at the home poll-site.

iv) Another copy of the signed vote is sent to the local vote tallier(s), which then take this vote into account for tallying.

v) Now, a (unique) random number 'N' is generated, and the signed vote, $S_{o2, p, p, p, \ldots}(V)$, on the voter's memory stick is encrypted using this as the symmetric key, to get Ec_N ($S_{o2, p, p, p, \ldots}(V)$). Also random numbers (n,n,n ..) for all other candidates are generated.

vi) This is further encrypted using the local officer's public key to get E_{o2} (Ec_N ($S_{o, p, p, p, \ldots}(V)$)). This is then encrypted along with the remote officer's public key (E_{o1}) along with the Identification Information and the (random number, vote) pairs to get E_{o1} [S_{o2} (ID) + E_{o2}[Ec_N ($S_{o2,p2,\ldots p2}$ (V))] + (N,V), (n,v), (n,v),…] and sent to the remote poll site's vote casting machine through the network host.

vii) This is then decrypted at the remote poll-site by using the officer's private key, and the S_{o2} (ID) + E_{o2}[Ec_N ($S_{o2,p2,\ldots p2}$ (V)), so obtained, is stored onto the voter's memory stick and permanently sealed before the memory stick is finally handed over to the voter.

viii) A receipt print-out corresponding to each of the (N,V) pairs (received in the message) is issued to the voter in that order. The first receipt, along with the memory stick handed over in step (vii) above, form the receipt for his vote cast.

Analysis:

i) Since all the phases of the voting process (from obtaining the ballot to vote casting, audit trail and vote tallying) are performed virtually as though the voter is voting from his home poll-site, the voter CANNOT vote at multiple remote poll-sites.

ii) Complete voter privacy and anonymity is ensured as the vote signing, random number generation, vote storage, audit trail formation, are all performed at his home poll-site and there is no way to tell where the voter actually 'cast' his vote.

iii) Since the messages across the network are encrypted in a manner proven to be cryptographically secure, voter confidentiality is maintained.

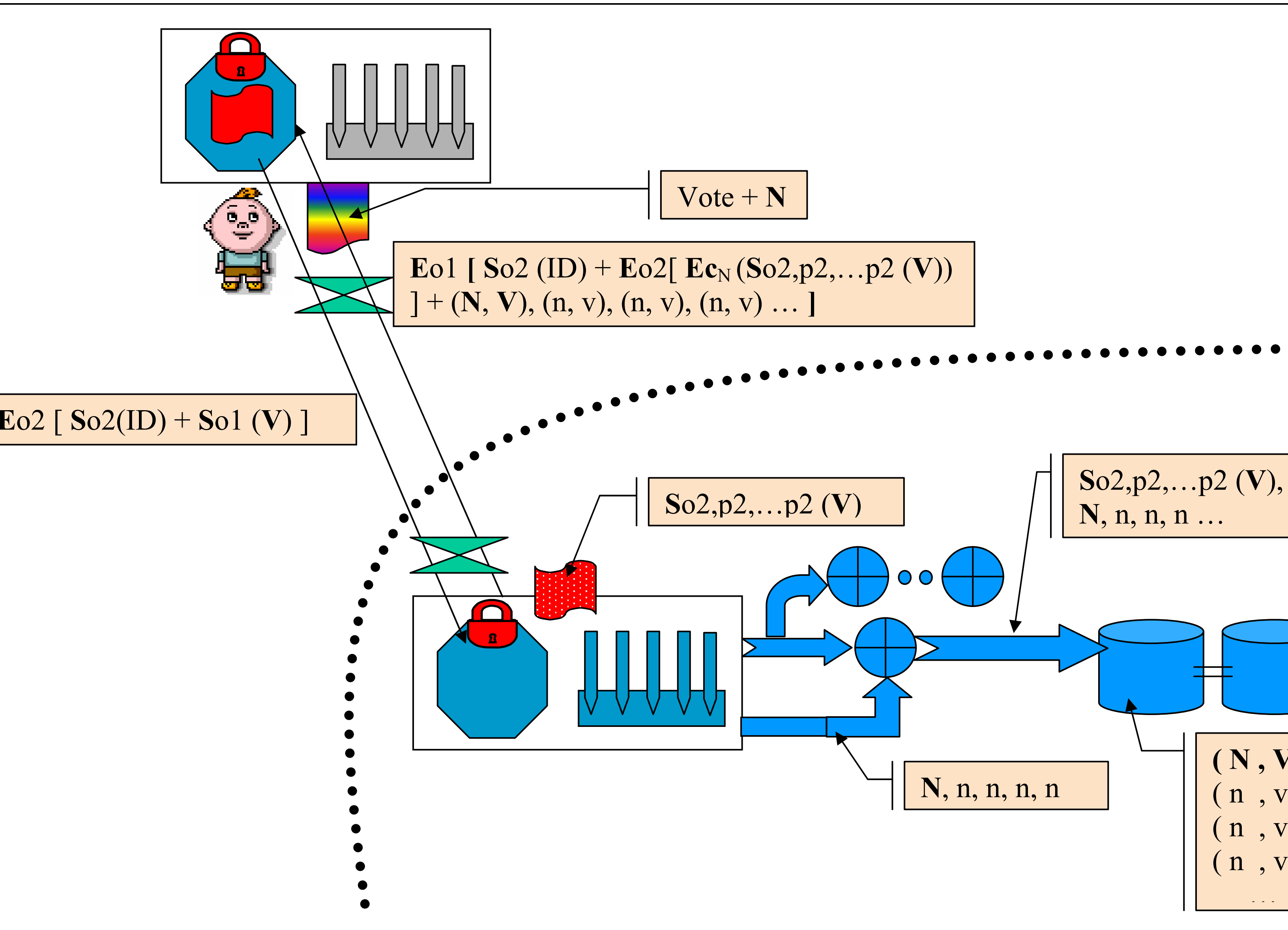
iv) Since messages are authenticated, bogus requests are not entertained.

v) Since ID is carried with each message, multiple requests for the same ID can be dishonored. This prevents replay attacks.

vi) Since the information is transmitted over a private network, possibilities of attack are limited.

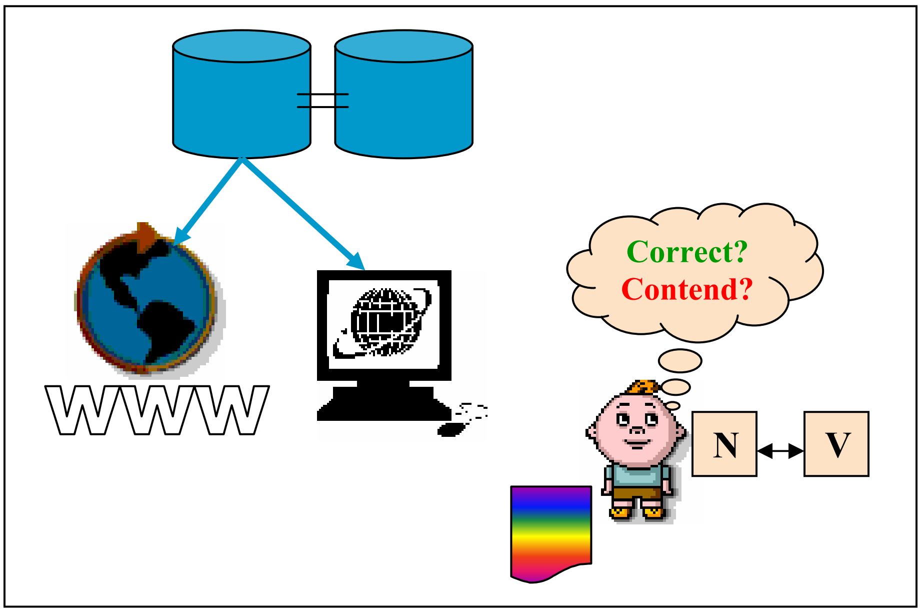
vii) Since redundant connectivity is maintained, availability is sustained.

viii) Since Network connectivity is provided by the network host, Vote casting machine, as such, can be kept simple.


Vote + N
Eo1 [So2 (ID) + Eo2[Ec$_N$ (So2,p2,…p2 (V))] + (N, V), (n, v), (n, v), (n, v) …]
Eo2 [So2(ID) + So1 (V)]
So2,p2,…p2 (V)
So2,p2,…p2 (V),
N, n, n, n …
N, n, n, n, n

2.6. Vote Tally Publishing

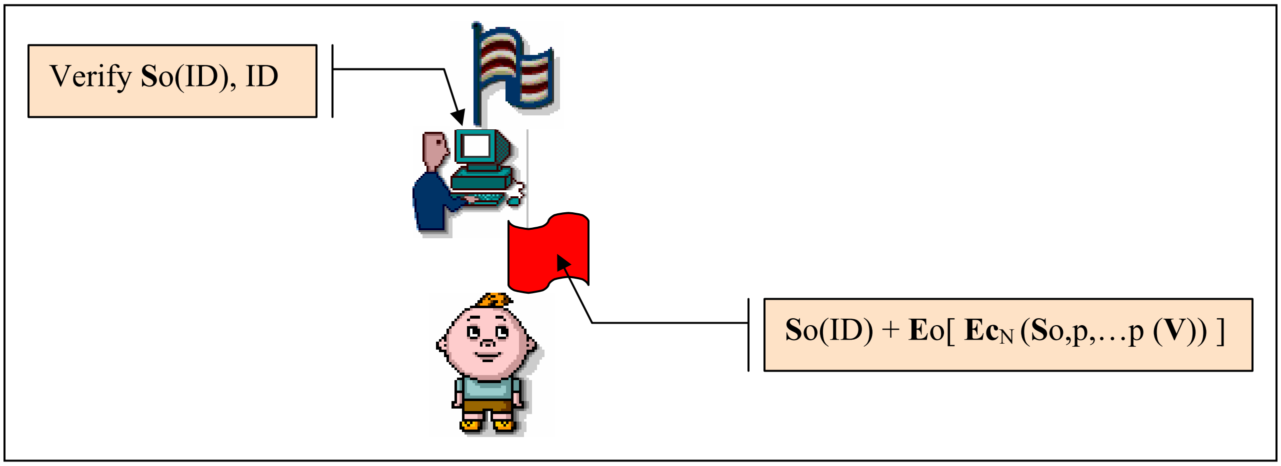
After the voting period ends, at some pre-announced point of time, the vote tallies are published on the Internet and at kiosks – placed at strategic locations such as public offices and shopping malls – maintained by the election office. The actual information published is nothing but the pairs of (number, name of candidate voted for). Here, the pair may correspond to a legitimate vote that was taken into account for tallying, or to a fake vote that is just present to prevent voter-coercion and vote-selling. The voter then checks the published tally to see if the vote corresponding to the number on the legitimate receipt issued to him is correct. If so, the voter is sure that his vote has been counted as he had cast it. If not, the voter can decide to contend his vote using the memory stick.



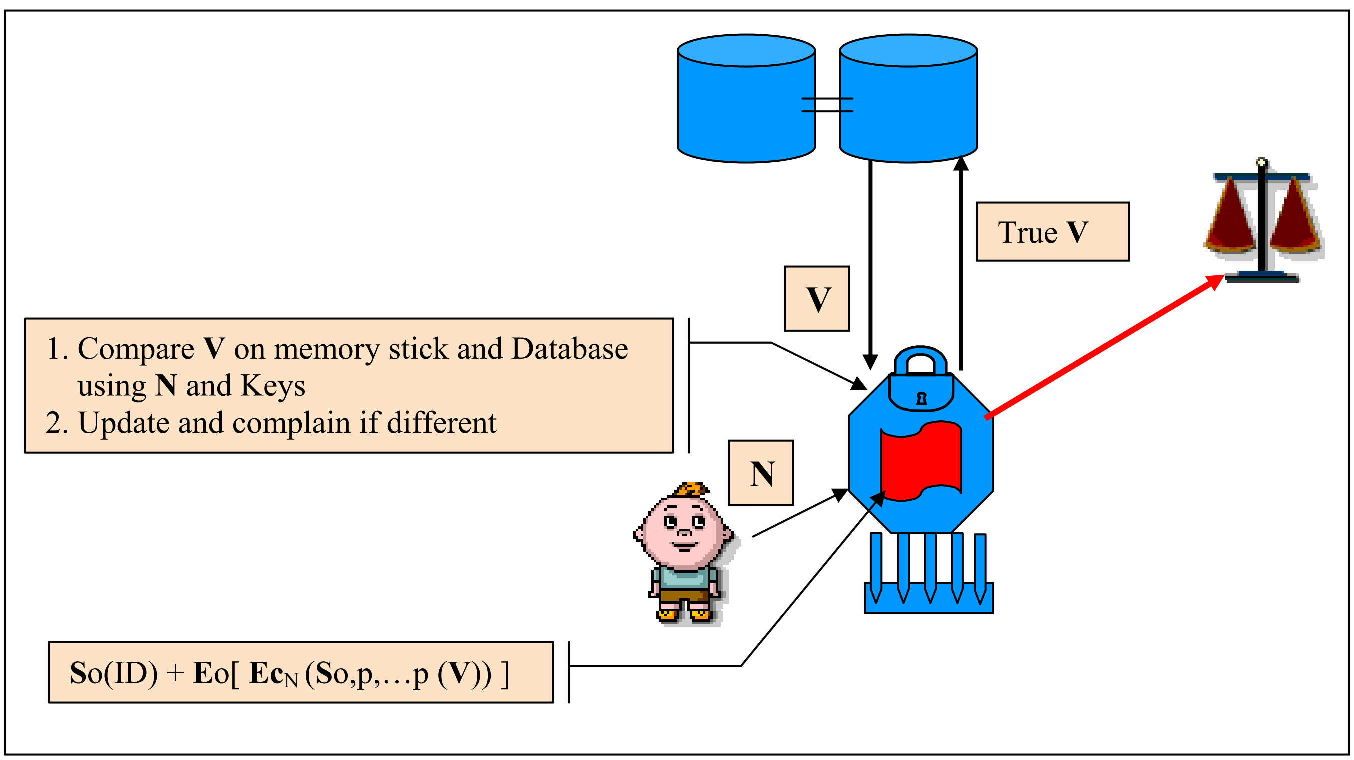
Analysis: Since the vote tally is being published both on the Internet and at strategically placed, election-office-controlled kiosks, equality of access to all voters is ensured (as the system does not assume Internet access to be available to all the voters). Also, since the fake vote pairs are also published, again, voter coercion and vote-selling are prevented. Finally, since the tally is published on multiple replicated servers, it alleviates the problem caused by denial of service (DOS) attacks.

2.7 Vote Contention

If the voter decides to contend his vote, he takes his memory stick and goes to the nearest election office to do so. Here, he is first authenticated with respect to the memory stick that he is carrying, by checking if the identification information is signed properly on the memory stick, and next verifying if that information is the same as the identification information presented by the voter to the officer.



Once authenticated, the voter then goes to the vote contending machine (which is again placed such that voter's privacy is ensured) and inserts his memory stick. The machine compares the vote on the memory stick (after decrypting it with the officer's private key and then decrypting this with the number 'N' entered by the user, and finally verifying the signatures) with the published vote. If different, the vote tally is corrected and the correct vote is published, and a complaint is lodged with the commissioner or some other higher authority that there was an inconsistency in the vote tally and thus, there may be a need to order a recount of the votes in order to get the correct, accurate picture of the election results.



In the case of remote poll-site voting, the authentication phase would be the same. However, during the actual contention phase, since the vote present on the memory stick can be decrypted only by using the home-poll-site election officer's key, the encrypted vote,

$E_o[\ Ec_N\ (S_{o,p,\ldots p}\ (V))\ ]$, along with the number 'N' entered by the voter, are sent to the voter's home-poll-site's machine, after being signed by this machine, and encrypted using the destination's public key. At the home-poll-site, the message is decrypted; the signature of the source is first verified; then it is decrypted using its private key, verified for the correct signatures and then compared with the vote tally. Finally, a message about the result of the contention is sent to the source machine, which then displays it to the voter.

Analysis: Since the vote contention is performed virtually as though he were doing it from his home-poll-site, he can contend at *any* poll-site. Also, since the comparison, correction and complaint are performed with respect to 'N', anonymous contention is ensured.

3. Implementation Considerations

For the implementation of our design, we have chosen the following options. They could be replaced with any other suitable option, if any, as and when deemed necessary, as our design should work irrespective of what choices are made for the various implementation considerations.

- Encryption:
    - Public key: RSA with 1024-bit keys
    - Symmetric key: AES with 256-bit key
- Signature:
    - RSA applied on hash
- Private keys stored on smart cards and Public keys stored and distributed on CD's.
- Network
    - Private Network (Direct dialup / cable, etc.)
    - Redundant Connectivity

4. Conclusion

In this paper, we have presented the design of an electronic remote poll-site voting system. The key issue addressed by our work has been the issue of receipt to the voter to acknowledge his vote, which facilitates vote confirmation and vote contention, and at the same time preventing any occurrence of vote-selling or voter coercion. Much of the present literature views receipt-freeness as the *necessity* for precluding vote-selling and voter coercion. There is a clear picture of a tradeoff between the "mutually exclusive" issues of receipt issuance and voter security. We have overcome this tradeoff and thus ensured the voter's confidence in that his vote has been counted as cast, without compromising voter security.

Also, our design successfully meets *all* the previously identified requirements of mobility, convenience, transparency, flexibility, support for disabled voters, accuracy, eligibility, uniqueness, auditability, voter-confirmation, issue of receipts, no over-voting, under-voting, documentation and assurance, cost-effectiveness, voter authenticity, voter anonymity, system integrity, data integrity, secrecy / privacy, non-coercibility and no vote-selling, reliability, availability, system disclosability, system accountability, and distribution of authority.