SECURED ELECTRONIC VOTING PROTOCOL USING HYBRID CRYPTOSYSTEM

[1]KALAICHELVI V & [2]CHANDRASEKARAN R.M
[1]Asst. Professor (Ph. D Scholar), SRC- Sastra University, Kumbakonam, India
[2]Professor, Annamalai University, Annamalai Nagar, India
E-mail: kalaichelvi2k@yahoo.com

Abstract:

Electronic Voting play a really vital role in the democracy of our life. In this paper, we propose an electronic voting protocol. Our scheme does not require a special voting channel and communication can occur entirely over the current Internet. This method integrates the Internet convenience and cryptology. In the existing protocol the Tallier has to wait until the decryption key is received from the voter. So it will consume lot of time. But, the proposed protocol is based on the hybrid cryptosystem. In this, the ballot is encrypted using faster secret key algorithm and the digital envelope is encrypted using Tallier's public key. So, the Tallier will decrypt the digital envelope using his own private key to get the secret key and then the encrypted ballot is decrypted using that secret key. So, comparatively the proposed protocol consumes less time. This paper also analyzes the various security issues involved in an electronic voting like security, privacy, authentication, anonymous, uniqueness, accuracy, fairness, efficiency and uncoercibility.

Keywords: E-voting, Cryptosystem, Privacy and anonymous.

1.0 Introduction:

Conventional Voting consists of the following four phases: i) **Authentication –** Alice walks into a voting precinct and authenticates herself by showing her voting credentials; this step is public and verified by the officials present in the room. At the end of the authentication process, Alice is given a paper ballot on which to write her vote. ii) **Vote –** The vote takes place in a protected booth where she cannot be seen by anyone. Alice casts her vote by writing it with a pencil on the paper ballot; she then folds the paper ballot and puts it in the ballot box where all the votes are mixed. Since no one can see what Alice writes and there are no marks on the paper ballots, Alice's vote is anonymous. iii) **Count votes –** At the end of the voting time, the officials open the box containing the paper ballots and publicly count the votes; the results are then announced. iv) **Verification –** Various types of verification are used or possible; most procedures are indeed public and overseen by representatives of competing parties. The opposite interests of the parties warrant the first level of protection against fraud. A recount is also possible if there is a presumption of fraud or error.

1.1 Issues in Conventional Voting

Conventional voting (such as voting by paper or signature voting) has many problems.i) Printing of ballot paper is expensive. ii) Voting consumes lot of time. iii) Counting is prone to errors. iv) Maintaining convenient poll booths is very difficult. iv) There is no good relationship between the government and popular, popular cannot trust the government and depend on it, voter here is like a blind person that must rely on the other person to vote for him. v) Sometimes, government coerced and carries on the voters to vote for a particular candidate, and eliminate them from voting freely. vi) Some candidates trying to win by buy the votes from the voters. vii) Government can cheat by substitute the original ballot by derivative ones.

According to all what is mentioned above, the whole world is moving on towards the trend of evoting. Electronic voting systems are expected to be the solution for the weakness in traditional voting systems.

The rest of the paper is organized as follows: Section 2 describes the existing voting protocol. Section 3 presents the problem definition of the proposed protocol, module description and features of the proposed protocol. Section 4 discusses the analysis of the proposed protocol and results. Section 5 presents the conclusion.

2.0 Related Work

In the last few years a numerous number of researches propose different e-voting systems, and some countries and states around the world implement their e-voting system. However, this numerous number of e-voting schemes can be categorized into three main categories. The categories based on the cryptography mechanism used to build the system. The first category is e-voting system based on blind signature technique [1-3] the second category is e-voting system based on Mix-Nets [5-6]. The third and the last category is e-voting

system based on homomorphic signature Properties [4-11]. Chaum was the first one to introduce blind signature and mixed nets. In general this different proposed system agree that the system should not be verifiable voting system (which mean the voter has no way to prove their voting activity) as a prevent technique against vote buying problem. However, some other e-voting system allows voter to prove their voting activities. Since the voting buying and the privacy of the voter is a critical problem in the Jordanian voting system we design our scheme as anonymous and unverifiable e-voting system, which categorize under the first category "blind signature-based e-voting system".

3.0 PROPOSED VOTING PROTOCOL

This protocol consists of five phases and three parties are involved such as Voter, Validator and Tallier.

3.1Setup

During this stage, voting parameters are initialized. They include candidates, voters and authorities' eligibility criteria, voting procedures, ballot validity rules and counting rules. Eligible candidates register themselves, and the registration and tally authorities are selected in this stage. Afterward, the voting parameters, candidates and authorities are made public such that they can be publicly known and verified.

3.2Registration

The process of voter registration is always done by the electoral officials before few days of the election. In this phase, each eligible voter will be identified by the electoral officials and issue the smart token (smart card) to the eligible voter. The smart card contains Unique ID (UID), Iris Pattern, name, age, sex, and address details. The Unique ID is a 14 digit number (IND/TN/99/0000078) and it will be generated automatically for each registered user. In this IND specifies the Country, TN specifies the State; next two digit specifies (for example. 99) District and then the last 7 digit is the ID for the corresponding person**.**

In addition, the key informations such as Tallier's public key (KU_T) will be stored in the smartcard. It will be generated and issued by the electoral officials. Once all the above details are stored in the smart token, it will be verified and issued by the electoral officials. This step has to be started and completed before the process of election.

3.3 Authentication

The voter authentication step is the first step in the process of voting. In this case, to increase the security biometric authentication protocol is used. First, the voter should insert the smart token into the Smart card Reader. Once the smart token is inserted, the voting software retrieves the 14-digit Unique ID information and checks whether he is already voted or not by checking the status bit. This status bit is used for achieving **uniqueness** by enabling this bit only when the voter cast his vote. If the status bit is set, the voter will be denied from accessing. If it is not, again the voting software retrieves the iris pattern information from the smart token and it will be compared with the live iris pattern. If it is matched, the voting software will provide the candidate details to cast the vote. Otherwise, the voter is denied. For Iris Comparison, this thesis exploits VeriEye SDK software**.**

3.4 Voting

This step will be started only after successful authentication. The Tallier will provide the corresponding candidate details to the Voter. Once the candidate is selected by the voter, it will be transferred in an encrypted form to the Tallier (Equation 3.1-3.2).

[Encrypted Ballot || Digital Envelope || Unique ID]→ Tallier (3.1)

ie.,

$$[(E_{Ks}(\text{Ballot})] \,||\, E_{KUT}[(K_s) \,||\, \text{Unique ID}] \rightarrow \text{Tallier} \quad (3.2)$$

Where

$\mathbf{KU_T}$ - Tallier's Public Key $\mathbf{KR_T}$ - Tallier's Private Key

$\mathbf{K_S}$ - Symmetric Secret key

Once the Tallier receives the above information, the Tallier only can decrypt the Digital envelope using his private key (KR_T) to get Ks. Others cannot. Once he retrieves the key information Ks, using Ks the ballot will be decrypted [Shown in Fig.3.1 – Fig.3.2].

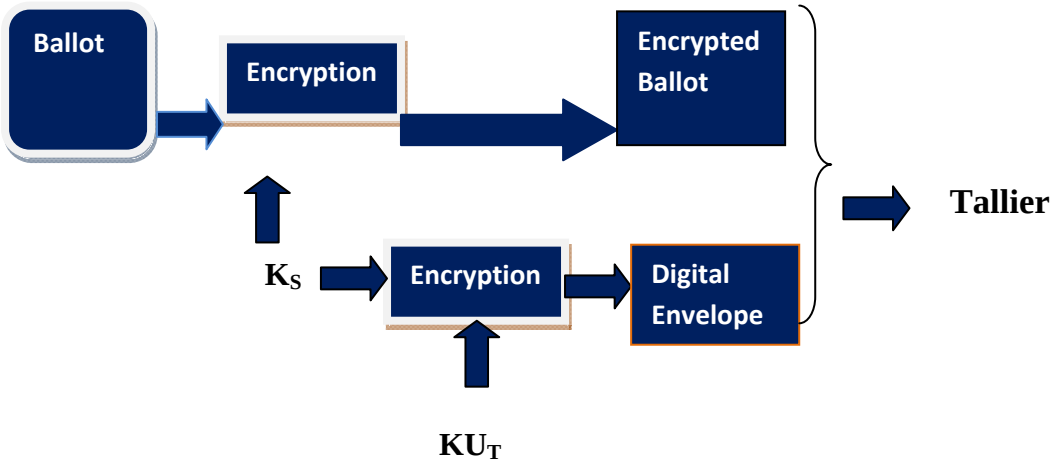


Fig.3.1 Voter Send's encrypted ballot to Tallier

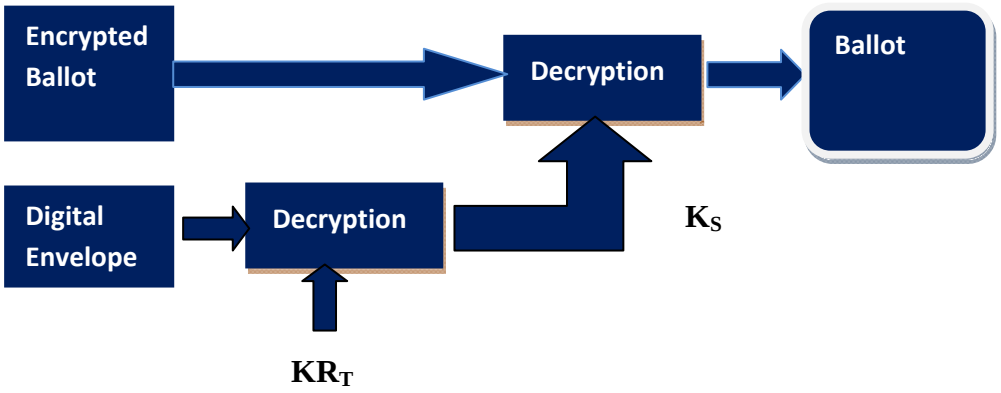


Fig.3.2 Tallier Verifies the Ballot

Once it is done, the Tallier will send just the confirmation message nothing other than that to the voter. At the same time, the Tallier will send confirmation to the authenticator to set the status bit. The voting count will be incremented for the corresponding candidate in the DB.

In the existing voting protocol, once the vote is casted, the tallier has to wait until the decryption key is received from the voter. The existing voting protocol is very complex and it will be very difficult for the average user to follow it and it is time consuming process.

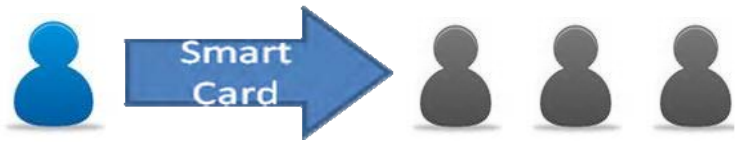
But, the proposed protocol uses Hybrid cryptosystem for achieving confidentiality and Authentication and integrity. ie., To encrypt the ballot it uses symmetric key cryptosystem using one-time symmetric key (Ks) and to encrypt the One-time symmetric key it uses public key cryptosystem using Tallier's public key(KU_T).

3.5 Counting and Result Announcement

Once the election time is over, the Result will be announced by the Electoral officials.

The following steps illustrate the Proposed Voting Protocol as shown in Fig.3.3.

Step 1:



Validator distributes Secret ID Tag (smart token) to the Voter

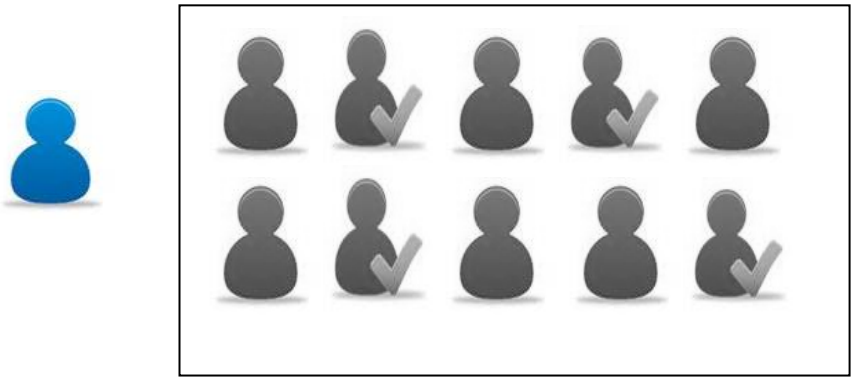
Validator **Voters**

Step 2:

Voter provides the Smart token

Voters **Validator**

Step 3:



Validator checks voters off from the list of registered voters

Validator **Voters**

Step 4:

Validator sends the authenticated message to the Tallier

Validator **Tallier**

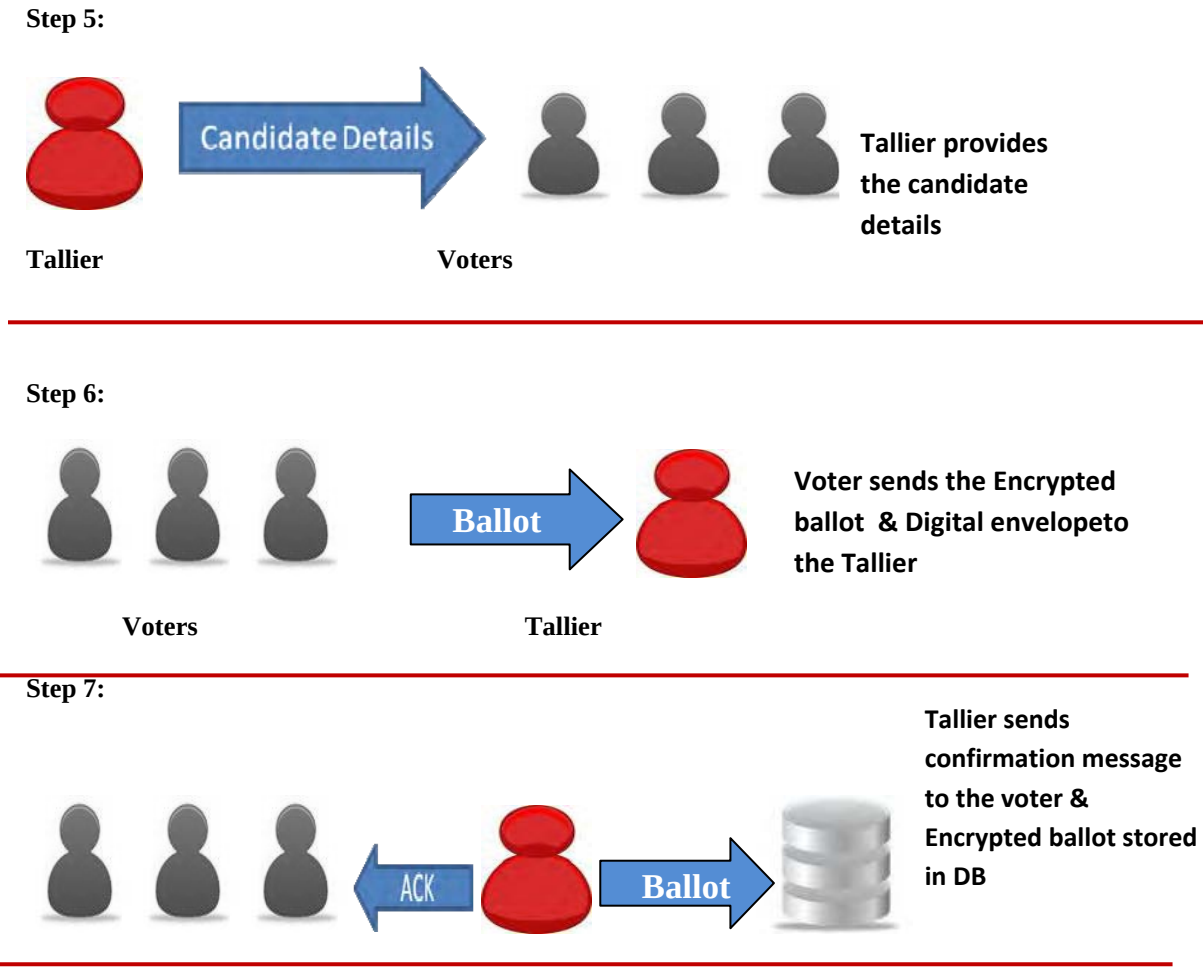


Fig.3.3 Steps involved in the Proposed Protocol

4.0 ANALYSIS AND DISCUSSIONS

4.1 Analysis of the Properties of the Proposed Protocol

This section discusses about how the proposed protocol satisfies all the voting requirements such as accuracy, uniqueness, efficiency, security, privacy, authentication, eligibility, fairness, Verifiability, anonymity and uncoercibility.

Eligibility Issues: No one can vote without going through the correct procedure for registration to get the smart card from the electoral officer. Only the smart card holder can eligible to vote, others cannot.

Security Issues: It is very difficult for the hacker to find out the symmetric key (secret key) to decrypt the encrypted vote during the time of transferring the vote from the voter to tallier. The digital envelope can be decrypted only by the Tallier because he is only having the corresponding private key (KR_T). Others cannot open that message.

To get the secret key value, the digital envelope should be opened first. This can be done only by tallier, others cannot. Then only the ballot can be decrypted using that secret key.

Single Transaction/ Efficiency: The Transactions in the existing protocol are multiple, as the tallier has to send the receipt to the voter to get the decryption key to decrypt the encrypted votes. In the proposed protocol these functions are carried out in a single transaction, as the tallier does not have to wait for the decryption key from the voter. The advantages of the proposed single transaction voting protocol over the existing protocols are less complexity in implementation and consumption of very less time in the voting process.

Moreover, this proposed protocol is based on the hybrid cryptosystem. That is, it uses the new high speed symmetric key cryptosystem to encrypt the ballot and it also uses asymmetric key cryptosystem only for sharing the secret key value.

But, the existing protocols are based on the asymmetric key cryptosystem. These protocols are very complex and slower in speed. It will be very difficult for the average people to follow it.

Fairness Issues: In our scheme, no one can acquire any information about the tally result before the voting deadline. Because the counting DB will be maintained only by the Tallier. Therefore no one can learn or predict the outcome of each vote before the tally announcement.

Uniqueness Issues: No voter is able to vote more than once, by maintaining the status bit information; it prevents the double voting. Whenever vote is casted by the voter, the status bit will be updated for the corresponding person.

Privacy and Fairness This scheme achieves **privacy** and **fairness** issues because no one can acquire any information about the tally result before the voting deadline. Because the tally DB will be maintained securely by tallier (electoral officials). Therefore no one can learn or predict the outcome of each vote before the tally announcement.

Anonymity Issues: In the existing protocol, to guarantee verifiability, the voter's encrypted vote will be sent to the voter with the key value to decrypt that vote. By decrypting that vote, the voter can verify that the voter's vote has been counted correctly. If it is verified by the voter, it violates the anonymity and Uncoercibility property.

So, this protocol advocate those voters not be allowed to verify their votes by themselves. It is not necessary to allow voter to verify (or Show to bribers) their votes in the announcement phase.

Uncoercibility Issues: No voter will be coerced to casting for particular candidate. Because there is no receipt, no one can know which candidate voter vote to, so there is no coerce.

Since the voter is at a remote location, we cannot be sure that the voter is who she avows to be, unless we use a biometric authentication protocol. Even with the use of biometrics to authenticate, both eligible person and Eve (political person) sit in front of the same system (reserved for election) doing the authentication and Eve voting or monitoring the votes, as he wants. If voter wants to sell her vote, and Eve is not present, she can take a picture of his voting and give it to Eve as proof. In any case, the remoteness of the voter makes the abolition of the sale of votes impossible to fulfill for online voting. Because of this reason, this proposed protocol partially achieves uncoercibility property.

Receipt-freeness: Ensures that the voter can be convinced that his/her ballot is counted without getting a receipt. That is, it just sends the confirmation message to the voter nothing other than that during the voting phase. This electronic method minimizes the possibility of bribes and is environmentally friendly by making a paperless process. Because of this reason, the proposed protocol partially achieves verifiability property.

4.2 COMPARISON

The Table 4.1 presents the comparison of the various protocols and Fig.4.1 presents the performance comparison of various protocols.

. Table 4.1 Comparison of the Various Protocols

Property	**Simple Protocol**	**Two Agency Protocol**	**Blind Signature Protocol**	**Sensus Protocol**	**Proposed Protocol**
Eligibility	Yes	Yes	Yes	Yes	Yes
Accuracy	No	Medium	Yes	Yes	Yes
Fairness	No	No	Yes	Yes	Yes
Efficiency	No	No	Medium	Yes	High
Privacy	No	No	Yes	Yes	Yes
Security	No	Yes	Yes	Yes	Yes
Uniqueness	No	No	Yes	Yes	Yes
Authentication	No	Medium	Yes	Yes	Yes
Verifiability	No	Yes	Yes	Yes	Medium
Anonymity	No	No	No	No	Yes
Uncoercibility	No	No	No	No	Low

The existing voting Protocols were compared with the proposed protocol. From the results, it is easy to understand that the proposed protocol achieves better performance.

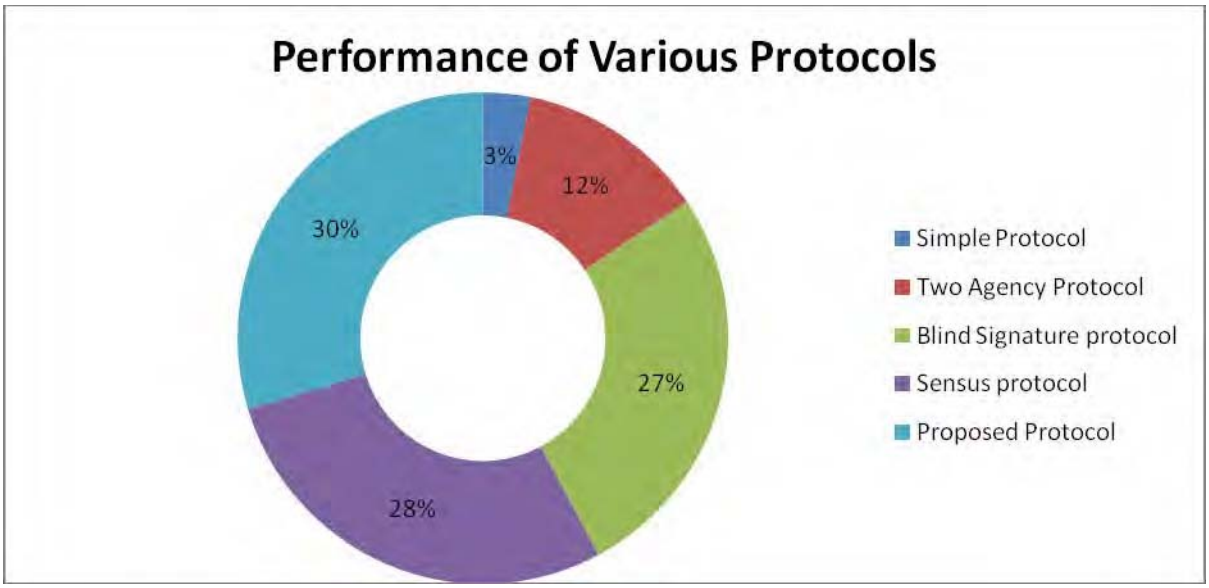


Fig.4.1 Comparison of the various Protocols

5.0 Conclusion:

Electronic voting play a vital role in the democracy of our life. This proposed protocol is compared with the various existing protocols. In the existing protocol the Tallier has to wait until the decryption key is received

from the voter. So it will consume lot of time. But, the proposed protocol is based on the hybrid cryptosystem. In this, the ballot is encrypted using faster secret key algorithm and the digital envelope is encrypted using Tallier's public key. So, the Tallier will decrypt the digital envelope using his own private key to get the secret key and then the encrypted ballot is decrypted using that secret key. So, comparatively the proposed protocol consumes less time.

References:

[1] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. "A practical secret voting scheme for large scale elections". In Advances in Cryptology |AUSCRYPT '92, pp. 244-251, 1992.

[2] W. Juang and C. Lei, "A secure and practical electronic voting scheme for real world environment," IEICE Trans. On Fundamentals, E80-A(1), January 1997.

[3] Kazue Sako. Electronic voting schemes allowing open objection to the tally. In Transactions of IEICE, vol. E77-A No.1, Jan.1994.

[4] Tatsuaki Okamoto. Receipt-free electronic voting schemes for large scale elections. In Proc. Of Workshop on Security Protocols '97, vol. 1361 of LNCS, pp. 25-35.Springer-Verlag, 1997.

[5] Markus Jakobsson. A Practical Mix. In Advances in Cryptology | EU-ROCRYPT '98, vol. 1403 of LNCS,pp. 448-461, Springer-Verlag, 1998.

[6] Masayuki Abe. Mix-networks on permutation networks In Advances in Cryptology

[7] |ASIACRYPT '99, vol. 1716 of LNCS, pp. 25-273. Springer-Verlag, 1999. Josh Cohen Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections (extended abstract). In Proc. 26th ACM Symposium on the Theory of Computing (STOC), pp. 544-553.ACM, 1994.

[8] Ronald Cramer, Matthew K. Franklin, Berry Schoenmakers, and Moti Yung. Multi-authority Secret-ballot elections with linear work. In Advances in Cryptology | EUROCRYPT '96, v ol. 1070 of LNCS, pp.72-83.Springer-Verlag, May 1996.

[9] Ronald Cramer, Rosario Gennaro, and Berry S choenmakers. A secure and optimally efficient multi-authority election scheme. European Transactions on Telecommunications, 8:481-489, 1997. Preliminary version in Advances in Cryptology | EUROCRYPT '97.

[10] Kazue Sako and Joe Kilian. Secure voting using partially compatible homomorphisms. In Advances in Cryptology | CRYPTO '94, vol. 839 of LNCS, pp.411-424. Springer-Verlag, 1994.

[11] Kazue Sako and Joe Kilian. Receipt-free mixtype voting scheme A practical solution to the implementation of a voting booth. In Advances in Cryptology | EUROCRYPT '95, vol. 921 of LNCS, pp. 393- 403. Springer-Verlag, 1995.