Secure EVS by using blind signature and cryptography for voter's privacy & authentication

Patil V.M.
Department of Computer Science, Shri Shivaji College, Akola-444001, MS, India, vinmpatil2@yahoo.co.in

Abstract- *In the era of networking and internet we can easily replace the traditional election process with the electronic voting system (EVS). To form the democratic government faith on the election system play a major role and it is also essential. During implementation of EVS we must satisfy all security requirements. Every voter and contesting candidates as well as political party to believe on this system individual and universal verification are also essential. In the proposed protocol we can use the blind signature, pseudo code, dynamic changing vote (dynaVote) etc. to solve the above problem.*

Key Words: Blind signature sceme, Pseudo code, DynaVote, Discrete Logarithm

1. INTRODUCTION:

In democracy, election is a fundamental Instrument to express the public opinion to form a democratic government. The traditional process of election is quite tedious, time consuming, cumbersome because voter's come in person and vote at pre-assigned voting booth. But in era of networking and internet, we can overcome this problem by using the electronic voting system (EVS). EVS is expected to make our modern social life more convenient, efficient , inexpensive and. without disturbing the daily routine life. It is possible by voter to vote to its desire candidate in the National Election Day from his home or at working place. While using EVS it must satisfy the some security requirements such as Authentication, Voter privacy, confidentiality, Integrity, Verifiability etc. because electronic voting system is more vulnerable than traditional voting process. Digital processing of data can easily manipulate, updated, and copied. Hence may result in widespread fraud and corruption during the election period. In this paper, we try to design, a new protocol that help, the traditional voting process and guarantee those requirements for EVS and reduce human interface, error and easy-to-use by voter.

2. SECURITY REQUIREMENTS:

Implementation of EVS over of network for large scale elections that satisfied all security requirements, it is not an easy task. Design of secure e-voting protocol over a network is much more difficult to achieve without these security requirement there is an opportunities for widespread fraud and corruption. In order to overcome there difficulties we should find out the following requirements [1, 2, 3, 4, 5].

a) Eligibility
b) Authentication
c) Voter's privacy
d) Confidentiality
e) Integrity
f) Individual & universal verifiability
g) Receipt freeness
h) Robustness
i) Fairness

2.1 Eligibility: only eligible voter can vote in the elections.

2.2 Authentication: EVS must provide a mechanism to check the validity of voter. During the registration authentic officer must verity the eligibility of voter and preserve the notion of one person-one-vote.

2.3 Confidentiality: Voter's opinion should be kept confidential; a voting protocol must not allow to prove that whose vote for whom. This is required to avoid the opportunity of vote buying and extortion.

2.4 Integrity: In EVS, there are numbers of physical ballot. The ballots are a digital nature & protocol must ensure that only valid voter are counted in the final tally and no one can change anyone else's vote.

2.5 Individual and Universal variability:

Voters should have the choice to verity his vote that actually counted in a final tally. And also universally verify any vote counted and are valid vote & absent vote.

2.6 Receipt freeness: The proof of a particular candidate selected or in front of candidate or representative of the candidate. Voting should

be done in such way that there is no chance of vote buying or sale.

2.7 Robustness: The Voting system should not disturb by any individual or group. The system should be able to withstand multiple technical failures.

2.8 Fairness: During the voting stage, the intermediate result should not be obtained by any authority / system that influence the entire result.

3. Related Work

The security of electronic voting system based on two assumptions. Firstly voter's privacy and confidentiality and secondly the untraceable communication channel, exist between voting centre and vote collection centre. Many EVS protocols have been design and proposed during the last 20 years [6]. But nobody can give a complete solution, to the best of our knowledge for large scale elections over a network. The first e-voting protocol for large scale elections was proposed by Chaum [7]. The voter's privacy & fairness is proposed for large scale election by Fujioka et al.[8] . However, accuracy can be violated due to the malicious authority can add votes, if any voter abstains during the voting. The security of the boyd's scheme [8] based on difficulty of discrete logarithm problem. Fairness property is not satisfied in the boyd's scheme. Barani-Dastjerdi et al [9] proposed threshold scheme for EVS to reduce the cheating by voters, candidate and administrators. Pseudonyms are generated by centre and distributed to all registered voter via secure communication channels between the center and all voter is not suitable for the large scale election. Horster et al [10] proposed a voting scheme with multiple administrator by using multisignature scheme and threshold encryption technique to distribute role of the voting authorization center to the several administrator. If atleast one of the administrator is honest then the fairness property of the voting scheme is satisfied. However that can increase the no. of communication steps between voter and administrators. The ring signature scheme [11] was developed by R. Rivest al in 2001. It was a special group signature scheme, but that did not require the creation of a group, a signature only require randomly chose a portion of a public keys and members and then creating a ring signature through his private key. The threshold signature scheme [12] was first introduced by Y. Desmedt and Y. Frank in 1991. A threshold signature enables a group to share signing power with other members. It is commonly used in a group security by employing cipher elements. In 2002, Bresson, stern and szydlo firstly constructed a threshold ring signature scheme[13] based on ring signature scheme by Rivest et al[12].

4.1 Security mechanism of EVS:

In this system, main question arise for voter's authentication and voter's privacy. Voter's privacy is achieved by using blind signature scheme for its confidentiality and digital signature used for voter's authentication. Ballot registration also required for Duplication & coping also secure communication channels need to carry the ballot & data.

4.2 The proposed scheme:

The Proposed scheme requires four stages.

4.2 (a) Preparation stage:
- **i) Voter's registration & Identification**
- **ii)Contesting candidate registration stage.**

4.2 (b) Voting stage
- **i) Voter's identification**
- **ii)Preparation Voter's ballot and registration of ballot**
- **iii) Casting of Vote**
- **iv) Individual verification**

4.2 (c) Counting stage
- **i) Individual & Universal verification**
- **ii) Counting of ballot**
- **iii) Declaration of results**

4.2 (a) Preparation stage:

Requires the following two stages:

i) Voter's registration& identification:

Firstly identity the voter, by its previous record or its photo identity or by residence proof. (A appointed authority of govt.) by the trusted officer of election commissioner. After voters verification as a citizen of country in that particular region. The registration authority go to voter's registration for voting purpose. The voting centre generate large prime number **p** generates **q** of private key **X** and public key **Y** as follows [15,16].

$$Y \equiv g^{X} \pmod{p} \quad \text{---------} \quad (1)$$

The voting center publish prime no. **p**, generates **q** and public key **Y** on the ballot board. We assume that voting center registered their public key & send it the central database [CDB] & also store in a local database [LDB].

In this paper, we use the following notification.

Xi - Private key of voter Vi

Yi - Public key of voter Vi

CDB - a central Database

LDB - a local Database

PV - Pseudonyms of the voters

C - Set of candidates

Ci - Candidate i , Ci Є C

PCi - Pseudonym of the candidate i

Bi - Ballot of voter Vi, Vi Є V

B' - Voter's blinded Ballot

Br - Ballot sign by voting centre (Register Ballot)

V - Voter list

At the registration stage, voter gets a private key Xi & public key Yi, voter apply for his pseudonym PVi, identity based on this registration. PVi Є PV – is a list of pseudonym identity which are unlinkable to the voter's registration identity [6]. Voter's real registration identity is hidden to the voting authorities. Thus, voter becomes anonymous while he is using the PVi in his communications with the voting authorities. The election authority can easily check validity of any PVi by applying the public Key Yi of voter Vi identity card. This process is carried out voter's authentication and authorization stage. PVi is a blindly signed identity. In this scheme voter perform blind signature with PV authority in order to obtain PV-list.

Thus voter can get its **(Xi, Yi, PVi)**

Where Xi Є X, Yi Є Y & PVi Є PV

ii) **Contesting candidate registration stage:**

The election authorization centres prepare a list of contesting candidate as per the procedure of applying candidates for contesting the election. The voting authority chooses a large prime no. **pi** & publishes it on a Bulletin Board. It is known that, discrete logarithmic problem is computationally infeasible in the field of integer modulo **p** [15, 16]. It generate **g**, of secrete key **Si,** public key **Pi** as follows

$$pi = g^{si} \text{ (Mod P)}$$

The election authority also publish the table of contesting candidates [17] list on a Public bulletin Board as follows

Table 1- Contesting candidate list

S.No.	Candidate Name	Candidate Pseudonym
c1	n1 ----------	Pc1
c2	n2 ----------	Pc2
c3	n3 ----------	Pc3

Pseudonym is a unique random no. generated for each candidate.

4.2 (b) Voting stage:

In voting stage, eligible voter go to the polling both or at the Home or office (If he already obtain a permission from election authority to vote in its own computer device that has the facility of high speed internet) in the National Election Day and verify its identity about the eligibility & still not voted.

i) Voter's identification:

Step1: Voter should arrivers at the poll station/polling booth with her any identity (I-card / multi propose identity card /active RFID tags).

Step 2: The polling officer, verities that voter is already register with photo identity.

Step 3: Election authority should provide pseudonym of the voter Vi by using his real registration identity and private key Xi and public key Yi. PVi is nothing between lists of approved anonymous pseudo identities which are linkable to voter's registration identity.

Step 4: After completing this stage, voter Vi can use PVi at any time in the election day during the election period. Voter's real registration identity is hidden to the voting authorities and voter also anonymous during his communication with election authority about the pseudo no. PVi.

Step 5: But central election authority can easily cheek the identity and eligibility of any voter Vi by using its public key Yi

Step 6: PVi Є PV is a list of blindly signed identities before the election period by center election authority and store in a central database system CDB. The PVi is a unique identification throughout the Nation that can help to Prevent Double / Registration of voters.

Step 7: Bio-matrix identity we can also use to prevent the double registration or re-registration & store the data in a central database CDB.

ii) Preparation Voter's ballot and registration of ballot:

Step 1: In voting stage, it voter enter in a polling station, poll officer cheek that it is eligible for voting & he / She has not yet voted. ie the voter is eligible for casting a vote.

Step 2: After completing the verification of voter, election officer, prepare a Ballot –**B** for a voter Vi Є V, The preparation of ballot for voter as follows.

Ballot Generating and signing [17]

$B \equiv (PVi)^{PCi} \pmod p$

Step 3: The voter blind the ballots as follows.

bf : blinding factor
bf : unblinking factor
bf.bf ≡ 1(mod p -1)
B' blinded ballot of the voter
$B' = B^{bf} \pmod p$

Step 4: The voter sign the blinded ballot (B'). in this case, undeniable signature scheme [63, (12)] is applied blinded ballot (B')

$R \equiv B'^{K} \pmod p$ k Є Zp_{-1}

$K.(B' + S) = x.r \pmod{p-1}$

Step 5: Voter send (**PVi, s, r, B'**) to the voting authorization center.

iii) Registration of the voter's ballot

Step 1: The election authority center cheek the voter's Xi & Yi to verify the voter previously applied for registration. If the voter has applied the registration more than once then stop the registration of stage. This also verity by using the Bio-matrix information available on ID cards/ in the central database system.

Step 2: The election authority center sign the ballot generate by voter for registration of Ballot B'

Step 3: the voting authorization center verify the voter's signature (s, r) using signature conformation protocol [15]. If the signature is invalid then stop the registration stage otherwise the election authority stores the identity ID to prevent the multiple registration of voter.

Step 4: The election authority center generate the signature (s, r) of the blinded ballot.

K Є Zp_{-1}

$R \equiv B'^{K} \pmod p$

$K = (B' + S) \equiv X.R \pmod{P-1}$

Step 5: The election authority center sends the undeniable signature (S, R) to the voter

(Ballot obtains)

Extraction of the Registered Ballot

Signed by the voting Authorization center

Step 1: The voter receives (S, R) from the voting authorization center

Step 2: The voter extracts the registered Ballot Br as follows.

$Br \equiv R^{(B' + S).bf\ -1.R-1 \pmod p}$

$\equiv B'^{K(B' + S).bf\ -1.R-1 \pmod p}$

$\equiv B'^{X.R\ bf\ -1.R-1 \pmod p}$

$\equiv B'^{X.\ bf.\ bf\ -1\ \pmod p}$

$\equiv B^{X \pmod p}$

(since $bf.bf^{-1} \equiv 1 \pmod{p-1}$,

$R.R^{-1} \equiv 1 \pmod{p-1}$)

iii) Casting of Vote (Ballot obtaining phase & casting of a vote)

Step 1: After obtaining a registered ballot Br this registered ballot is a dynamic ballot [55] In dynamic ballots the ordering of contesting candidates are dynamically created and changes for each voter. Therefore the proposed protocol is called as "Dyna Vote"

Step 2: Voter selects his candidate and creates his candidate selection PCi Є PC, using dynamic Ballot.

Bc : voters vote casted ballot

$Bc \equiv (PCi.PVi)^{PVi} \pmod p$

Step 3: Voter send a massage M to the election authority, which contain election date, time & Bc.

M ≡ (Bc, date , time)

Step 4: Election authority received a massage from voter, and conformed that it is received from registered voter by applying a key.

Step 5: Authority apply a public key Yi & PVi of concern voter & also register ballot Br and store in a central database CDB to publish in a Bulletin Board.

iv) Individual verification

Step 1: The registered ballot Br contain the pseudonym of the voter PVi and his candidate selection PCi

Step 2: For individual verification of the voter, voter can enter his pseudonym PVi and candidate PCi obtain in registered ballot & See that massage from LDB.

Response value Rv

Rv = PCi.PVi

That is prove that his vote enter in a total of required candidate PCi Є PC, since PCi & PVi is a unique in a LDB & CDB with date & time after casting a vote.

Step 3: This valid only for short period after casting of a vote before to close a transaction process of casting of vote after that it will be immediately closed since it is a possibility of vote buying & sale and to prove that his vote for a particular candidate in presence of candidate or any person nominated by candidate on his party representative.

Step 4: After completion of casting & Verification of vote. The data will be immediately transferred to centered database CDB for conformation of Ballot & to avoid double voting. It will be total impossible to reassess the data & concern ballot.

4.2 (c) Counting stage: In a counting **,** phase the following stages are involved. Before going to counting and declaration of result ,we must conform the any doubt and fraud and finally ,verify the ballot.

i) Individual & Universal verification:
We have given public key Yi, private Key Xi, pseudo key PVi Є PV of every individual voter. That also note down date, time and selected candidate pseudo key PCi Є PC & every ballot B is also verified with ballot numbers.

$Bni \equiv B^{Yi} (\text{mod } p)$

In public Bulletin, we should publish a ballot registration number with pseudo key PVi of individual voter Vi Є V. In this way, any voter Vi can cheek that his vote is counted properly in a final fully with his registered ballot no. and pseudo key PVi. In this time no any pseudo contesting candidate no PCi Є PC will be display during individual verification. In case of universal verification, as per the display of BB registered Ballot no & its pseudo PVi. We can cheek that all the voter list in a BB are counted in a final tally with verification of no. of voter are casting their vote and no. of voter are absent during the voting period & total no. of registered voter PV in a central database system.

ii) Counting of ballot:
Counting will be performed after complete of election period & after complete individual & universal verification on per the declaration in a public Bulletin Board.

Before counting we can decrypt the candidate choice of voter as follows [13]:

$Bc \equiv (PCi.PVi)^{PVi(\text{mod } p)}$

$Bc \equiv {}_{PCi}(PCi.PVi)^{PVi(\text{mod } p)}$

$(\text{mod } p)PCi \equiv Bc / PVi^{PC(\text{mod } p)}$

iii) Declaration of results:
After decrypting the encrypted candidate & counting the each candidate vote separately as per given in the above figure: we must declare a result.

Total vote = number of absent vote(A)

+ Number of vote of candidate PC1

+ Number of vote of candidate PC2

+ ……..

+ Number of vote of candidate PCn.

I.e. Total vote = A + M1 + M2 + ...+ Mn.

Security Analysis:

EVS is noting but the digital database any one change, modify, copy, the data very easily. Therefore it will need to satisfy the e-requirement of voting system[14,15,16].

[1] Voter's privacy can easily be satisfied due to the issue of PVi to registered vote by providing the blind signature of election authority & there is no any link between PVi & registered ID.

[2] Voter had already been registered & provided a private key Xi & public Yi uniquely with bio-matrix information to avoid multiple or duplicate registration of voter by linking with central database CDB. Hence this can prove the voter's eligibility & identity and also the uniqueness of the voter.

[3] Voter and any political party can cheek the each any every vote with individual & in a universally. Therefore it can satisfy the accuracy of EVS.

[4] There is no any chance of vote buying / selling. Since privacy of votes are possible and only last casting of vote will be counted in a final tally and voting is possible in a election booth and prior permission of election authority in case of impossible to after the election booth.

[5] Any fraud or modification of single vote or tapping of information can be deleted. Hence system is Robustness & verifiable at any intermediate time.

Conclusion

The above protocol is fully secure for large scale election system. The bio-matrix authentication system provides the uniqueness. i.e., only one person one registration & one person one vote in a election period possible that need a extra H/w & S/w. There is no any link between pseudo key & registration of voter hence it fallow the voter privacy & confidentially & universal & individual verifiability of voter is main objective of the protocol.

References

[1] Subariah Ibrahim, Maznah Kamat, Mazleena Sullab, and shah Rizan Abdul Aziz (2003) *4the National conference on Telecommunication Technology proceedings, Malaysia*, 2003 IEEE, 193-197.

[2] Cramer R., Gnnaro R. and Schocnmakers B. and Yong M. (1996) *Eurocrypt 9c LNCS* 1070, 72-83.

[3] Coranor L.R. and Cytron R.K. (1996) *Design and implementation of a practical security conscious Electronic Pollind system, Washington university: Computer science Technical report.*

[4] Xiangdong Li, Michael Carliale, Andis C.Kwan, Linlamg Amara Enemuo and Michael Anshel, (2007) *An Elementary Electronic voting Protocol using RFID" IEEE*.

[5] Sung–Hyon YUN and Sung-Jin LEE . *The network Based Electronic voting scheme suitable for large scale election,* 218-222.

[6] Orhan Cetinkaya, Ali (2007) *International Conference on Availability ,Reliability and security (ARES'07).*

[7] Chaum D. (1981) *Communication of ACM*, 24, 84-88.

[8] Fujioka A. Okamoto T. and Ohta K. (1992) *AUSCRYPT' 92, Australiya*, 244-251.

[9] Colin Boyd (1990) *In advance in cryptology, proceedings of EUROCRYPT89, LNCS* 434, 617-625.

[10] Ahmad Baraani –Destjerdi, Josef Pieprzyk & Reihaneh Satavi-Naini (1995) *Proceedings of COMPAC'* 95, 143-148.

[11] Patrick Horster, Markus Michels and Holer Pctousen, (1995) *Proceedings of COMPSAC,95*, 149-155.

[12] Rivest R., Shamir A. and Tayman Y. (2001) *Proceedings of Asiacrypt 2001; Lnecs 2248 Springer Verlag,* 552-565.

[13] Desmedt Y. and Frankel Y. (1992) *Proceedings, LNCS 576 , Springer-Verlag*, 457-469.

[14] Bresson E., Etern J. and Szydlo M. (2002) *Crypto 02 LNCS 2442 Springer Veriag,* 465-480.

[15] Whitfield Diffie, Martin E Hellman (1976) *IEEE Transactions on Information Theory* 22(6), 644-654.

[16] Taher Elgamal (1985) *IEEE Transactions on Information Theory* 31(4), 469-472.

[17] Sung – Hyon YUM, Sung – Jun LEE (2003) *An electronic voting scheme based on undeniable Blind signature scheme 2003, IEEE,* 163-167.

[18] Ziangdongli, Michael Carlisle, Andis C. Kwan, Lin Le Ung (2007) *IEEE*, 234-238.

[19] Alsushi Fajioka, Tatsuaki Okamob. *Proceedings & AUSCR YPT 192.*

[20] Znen Yu Wu, Fuh Gwo Jeag, Tzer Sh young chen (2006) *IEEE*, 1351-1353.

[21] Sung Hyun YUN and Sung Jin LEE. *The Network Based Electronic Voting Scheme suitable for large scale Election*, 218-222.

[22] Hirt M. and Sako K. (2000) *EUROCRYPTOO Bruges, Belgium*, 539-556.

[23] Juels A., Calalano D. and Jakobsson M. (2005) *ACM Workshop on privacy in the Electronic Society, VA*, 61-70.

[24] Sung-Hyun YUN, Sung, Jin LEE (2003) *IEEE.*

[25] Iyappan P., Arivnd K. S., Getha N., Vanitha S. (2009) *Emerging Trends in Engineering and Technology ICETET – 09* , 808-812.

[26] Subariah Ibrahim, Mazmah Kamal, Mazleena Salleb and Shah Rizan Abdul Aziz. 4th National Conference an Telecommunication Technology proceedings, Shah Alam, Malaysia.