A Powerful Protocol for Electronic - Voting using a HYBRID Crypto Realm

[1]K. N. Sandhya Sarma, [2]S. Umamaheswari
[1,2]Dept. of IT and Science, Dr. G. R. Damodaran College of Science Coimbatore, TamilNadu, India

Abstract
This paper reinvigorates a powerful e-voting protocol which solves debated security issues. This scheme assures voter's privacy & anonymity. We have reformed a protocol that integrates blind signature scheme, secret sharing technique and homomorphic encryption which ensures fair voting and eliminate criminal deception in voting. The initialization of this proposed protocol begins with identification of voters followed by authentication. With the inclusion of public proxy server we have successfully simulated our protocol which solves anonymity of the voters. The cryptographic approach securely transmits the vote of each voter in a high security lane. In the final phase of our protocol that begins with collection of votes; and by using homomorphic encryption we have secretly processed all the ballots in an encrypted form only. Due to this approach only the final computed result is revealed in encrypted form which is intelligible by using Secret sharing scheme.

Keywords
Blind Signature, Secret Sharing, Public Proxy, Encryption, E-Voting

I. Introduction

Democracy is framed on the principles of elections. An 'election' is a process to obtain an accurate result representing a set of participant's answers to a posed question. A 'vote' is what physically represents a participant's answer to a particular question [1]. It is a fact that many of the eligible voters may not participate in election. The reason behind this is the inconvenience caused to reach the polling stations. The enormous evolution of internet technologies changes way of communication. Internet voting is an alternative solution to increase the polling stations. Internet voting provides an easy way and it allows the voters to participate in the election from any location. Voters can cast their vote while at work or from home or anywhere else in the globe via Internet.

The main aspect of e-voting is that its design should be simple and similar to the traditional voting. It should also provide high degree of trust and security as compared to the manual voting system. The ideas of voting through internet have been proposed by many researchers from both theoretical and practical perspective.

In order to be widely acceptable and in a way to be implemented, every voting system should have certain requirements. The main attributes that an "ideal" internet voting system should possess are presented in [2, 3]. They are stated as follows:

A. Accuracy

A voting system is considered to be accurate when 1) No one can alter a vote. 2) A valid vote cannot be tampered, deleted or miscounted from the final tally. 3) An invalid vote cannot be counted in the tally.

B. Democracy/Uniqueness

Democratic schemes ensures:

1. Only legitimate voters can cast the vote
2. Every eligible voter has voted only once.

C. Privacy/Anonymity

1. No one can link a vote to the voter
2. None of the voters can find out how a particular voter has voted.

D. Fairness

Any intermediate outcome cannot be revealed before the finalization of tally center.

E. Verifiability

All the voters can also verify their vote that has been counted during the tally.

F. Robustness

A dishonest voter cannot disrupt the voting.

G. Convenience

Voters do not need any special skill and can complete the voting quickly and easily.

H. Mobility

Voters can vote from anywhere irrespective of the location.

Our work can easily be explained in following manner which initiates from the next section that describes more about the different cryptographic techniques useful for e-voting schemes. The section following that is a short survey on few internet voting protocols. In section4 we introduce our proposed e-voting scheme. In section 5 we analyze our scheme and the last section presents our conclusions.

II. Cryptographic Preliminaries

A. Blind Signature

Blind Signature is a method in cryptography introduced by David Chaum [4]. It is a form of digital signature in which the content of a message is blinded before it is signed. The resulting blind signature is verified against the original and the unblinded message just like a digital signature. A blind decryption can be applied employing the RSA public key. In order to achieve this goal, the data to be signed is disguised before it is given to the signer using a blinding function. This function usually involves the public key 'e'of the signer and a random number 'k'.

$$m' = blind_e(m,k).$$

The signer signs the blinded message as

$$m' = sign_d(m').$$

After the signer has signed the blinded data m', using the private key d, the resulting blinded signature s' can be transformed to ordinary digital signature. The unblinding function used for this is

$$m = unblind(m',r).$$

B. Homomorphic Encryption

It is a special type of cryptography in which the sum of two encrypted values is equal to the encrypted sum of values. The encryption algorithm E () is homomorphic if given E(x) and

E(y), one can obtain E(x ¬ y) without decrypting x; y for some operation ¬.

Homomorphism is an algebraic property useful in electronic voting schemes because it allows finding of the sum of the ballots without decrypting them. RSA [5], El-Gamal [6], Pailler [7] encryption schemes are homomorphic and are used in electronic voting schemes. RSA is a multiplicative homomorphic algorithm

$c_i = E(m_i) = m_i^e \bmod N$

Public key is modulus N and exponent e

$c_1 \cdot c_2 = m_1^e \cdot m_2^e \bmod N = (m_1 \cdot m_2)^e \bmod N$ $E(m_1) \cdot E(m_2) = E(m_1 \cdot m_2)$

El-Gamal [8] is an additive homomorphic algorithm. Given two plaintexts m1 and m2 and two corresponding cipher texts

$c_1 = \text{Encrypt}(m_1) = (x_1, y_1)$

$c_2 = \text{Encrypt}(m_1) = (x_2, y_2)$

We can compute

$(x_1 .x_2 , y_1 .y_2) = (\alpha^{k1} . \alpha^{k2} \bmod p, \alpha^{m1} .\beta^{k1} .\alpha^{m2} .\beta^{k2} \bmod p)$

$= (\alpha^{k1+k2} \bmod p, \alpha^{m1+m2} .\beta^{k1+k2} \bmod p)$

$= \text{Encrypt}(m_1 + m_2)$

C. Secret Sharing

Secret sharing refers to method for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use on their own. Shamir [10] and Blakely's [11] Secret Sharing is important in information security and network security and have broad applications in the real world. Threshold (t,n) secret sharing scheme allows a dealer to distribute a secret value S to 'n' players; such that atleast (t<n) players are required to reconstruct the secret. Shamir's Secret Sharing scheme is based on polynomial interpolation over a finite field while Blakely's secret sharing has a different approach based on hyper plane geometry.

III. Related Work

Our proposed work is based on Fujiako.et.al [3] voting protocol, Sensus protocol [2] and Yu-Yi Chen.et.al [13] protocol. Fujiako. et.al [3] proposed a secret voting scheme suitable for large scale elections. The computation and communication overhead is small even if number of voters is large. The drawback of this work is the voter cannot complete voting session until the tallying. The voter cannot submit the decryption key until after the voting phase of the election is over. As a result votes cannot be cast in a single session. The Sensus protocol [2] by Cranor.et.al [2] is based on the ideas of Fujioka.et.al [3] and solved this issue of voter waiting till the end of the voting phase. They proposed a scheme where the voter may submit the decryption key immediately after receiving a receipt from the tallier and thus can complete the entire voting process in one single session. In both the protocols the voter privacy and security is concerned more. Voters are relied on to check whether their vote is counted correctly or not. Then again voter has to revisit the polling site after the announcement of the results to verify their votes. Another drawback of both these protocols is anonymity.

Yu-Yi.et.al [13] proposed another secure anonymous scheme which overcomes the drawbacks of the above said protocols. The anonymity is achieved by using public proxy servers. Secret sharing mechanism is employed to ensure that all votes are counted correctly. But it is not practical to apply secret sharing on each vote. The proposed scheme makes use of homomorphic encryption to easy the tallying process and secret sharing mechanism to reveal the result.

IV. The Proposed Protocol

We have proposed some important schemes in our work which will enlighten our protocol more powerful by following phases:

A. Initialization Phase

The voter is authenticated using an identification procedure which is very difficult than traditional paper voting. There are three approaches to identify the user of an e-voting system: Through something the user knows, the user is & the user has [14].

Knowledge of username and its corresponding password is the most widely used identification process ("something the user knows"). It is simple but can lead to vote coercibility and vote selling very easily. The second approach is using Public Key Infrastructure (PKI). In this case every voter will have a secret key pair ("something the user has") authenticated by the electoral authority. Here the voter's private key requires high protection and using of smart cards or user held cryptographic token can be used as they are tamper proof in most of the practical situations. The third approach is biometric identification ("something the voter is"). The fingerprints of the vote is taken as biometric measurement and sent. It is then matched with previously stored pattern.

A combination of these three identification approaches can be taken for authenticating the user. Once the user is authenticated by the verifying center, ballot is issued to the voter which contains a unique identification code large enough to avoid duplicates with other voters. The verifying center also maintains the list of voters who were given the valid ballot to vote.

B. Vote Casting Phase

Each voter generates 'n' set of messages, where 'n' represents the number of candidates. Each set contains either a"yes" or "no". The voter blinds each message and sends them with blinding factor to the authenticator.

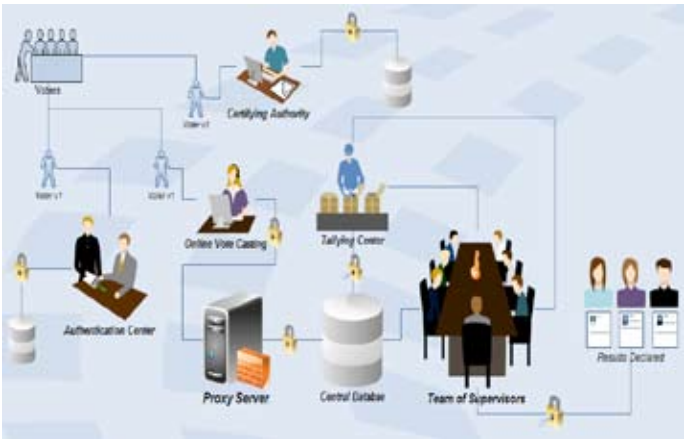

Fig. 1: Proposed Scheme

C. Authentication Phase

Authenticator checks its database to make sure that the voter has not submitted his blinded votes for signature previously. It then individually signs each message and sends them back to the voter, storing the voter identification code in its database. The vote is hidden from the authenticator. The voter unblinds the messages and is left with a set of votes signed by the authenticator. (The votes are signed but not encrypted, so the voter can easily check which vote is "yes" and which is "no").

D. Voting Phase

The voter encrypts each message using homomorphic encryption and sends the set of messages to the proxy server. Homomorphic

encryption is where the voter encrypts his or her vote and computes a proof that demonstrates the correct construction of the vote. The proof does not reveal any information about the vote. The proposed scheme uses El-Gamal [6] encryption which is additively homomorphic. The proxy sends the encrypted vote and the proof to the tallying center, hiding the IP address of the voter.

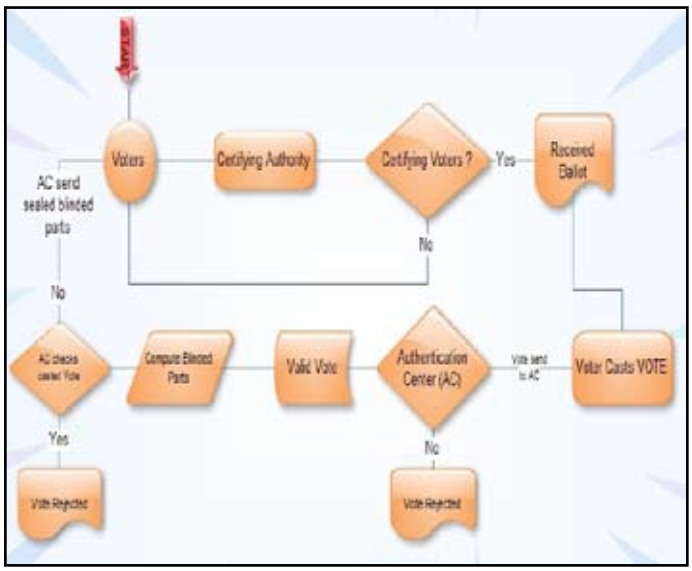

Fig. 2: Flowchart 1: Authentication Phase

E. Counting Phase

All the encrypted votes are multiplied together and the decryption of the final result gives the sum that would have been obtained by adding the votes. The key used to decrypt the result is shared among several supervisors who must co-operate in the decryption process to obtain the final result. Secret Sharing scheme is used to determine the secret key. The number of votes received and the number of votes recorded by the authenticator and the proxy server can be used to verify the tally.

The following notations are used to explain the scheme:

V_i = Voter i.

ID_i= ID of voter i.

n = number of voters

m = number of candidates

(ad, ae, an) = Key pair of Authentication Center [AC]

(id, ie) = voter's key pair

α_1, α_2, k is large random numbers used for encryption & decryption

(HK_{pub}, HK_{pr}) Homomorphic encryption key pair.

HK_{pub} = (p, β, α_2) HK_{pr}= a

The implementation steps include:

1. Authentication Phase

1. {V_i→[CA]}.Voter sends his identification to the certifying authority.
2. {[CA] → V_i}. CA certifies the voter and sends the ballot Bi to voter.
3. {B_i→ B_i/m={v_{i1}, v_{i2}, v_{i3}, vim}}.The Ballot contains 'm' parts where 'm' represents the number of candidates.
4. {B_i=Σv_{ij}}.vij is the jth part of voter i. The voter casts the vote.
5. {b_{ij} = $\alpha 1^{ae}$ * v_{ij} (mod n)}. The voter blinds each part using the public key pair (ae, an) of the [AC].
6. {V_i→ [AC]}.Voter sends { b_{ij}, ID_i , b_{ij}^{id} } to AC.
7. AC opens the seal using ad and verifies $(b_{ij}^{id})^{ie}$ = b^{ij}.
8. Checks the list, whether the voter has previously casted any vote.
9. AC signs each blinded part of the ballot by computing L_{ij}= b_{ij}^{ad} (mod an).
10. AC sends L_{ij} sealed with ie back to the voter.

2. Casting Phase

11. Voter opens L_{ij} with id. S_{ij}= $\alpha_1^{-1}L_{ij}$ (mod an). Voter unblinds the vote and finds the signature.
12. Voter verifies L_{ij} by using the equation v_{ij} = (L_{ij})ae mod an. S_{ij} is the signature of the AC for b_{ij}.
13. Each v_{ij} has to be encrypted. E (v_{ij}) = (cx_{ij}, cy_{ij}) where cx_{ij}= α_2^k mod p and cy_{ij} = ((α_2)$_{vij}$. β^k) mod p.

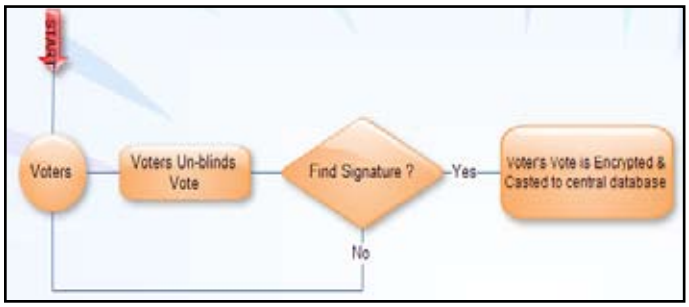

Fig. 3: Flowchart 2: Casting Phase

3. Voting Phase

14. {(cx_{ij},cy_{ij}), S_{ij} } → [TC] the cipher of each part along with the signature is sent to the Tallying Center through The cipher parts of each vote are multiplied in such a way that the sum of the votes received by each candidate is obtained in the decrypted form.

$$\prod_{j=1}^{m} CX_i = (cx_{i1} * cx_{i2} * cx_{i3} * ..... * cx_{im}) = x_{ij}$$

And

$$\prod_{j=1}^{m}$$

$$CY_i = (cy_{i1} * cy_{i2} * cy_{i3} * .... * cy_{im}) = y_{ij}$$

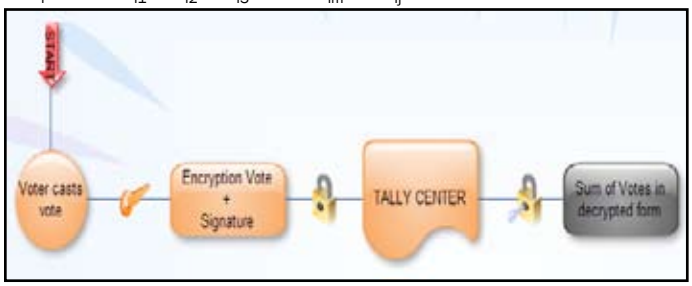

Fig. 3: Flowchart 3: Voting Phase

4. Counting phase

15. There will be 'm' tuples of (CX, CY) representing the encrypted results of 'm' candidates.
16. Each (CX_i, CY_i) has to be decrypted using the secret homomorphic key HK_{pr} = a.
17. The secret key 'a' is obtained to the tallying center by computing a Lagrange interpolation polynomial. Shamir's threshold scheme is adopted which states given't' points, a secret can be recovered.
18. Given't' points (a_i,b_i) 1<=i<=t. Lagrange Interpolation formula gives

$$f(x) = \sum_{i=1}^{t} y_i * \prod_{i<=j<=t, j>i} (x-x_j) / (x_i-x_j)$$

f (0) =a=secret key. The secret key can be recovered only if a threshold't' number of supervisors co-operate and give their share.

19. Each (CX_j, CY_j) is decrypted yielding the result R_j of each candidate by computing $\alpha_2^{Rj} = (CX_j)^{-a} * CY_j \pmod p$

20. R_1, R_2, R_3, R_m will correspond to the total votes gained by each candidate.

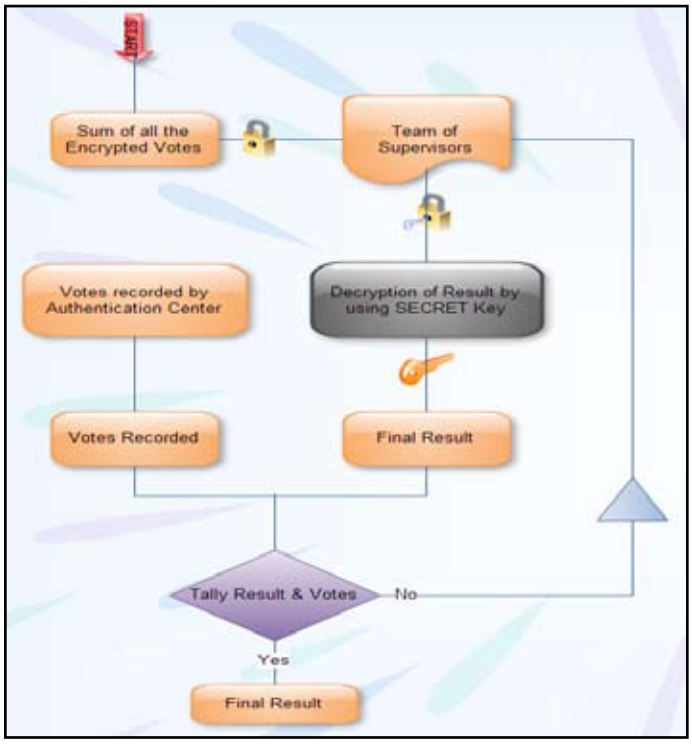

Fig. 4: Flowchart 4: Counting Phase

V. Analysis of Our Reinvigorated Protocol

A. Fairness

Counting accomplished with homomorphic encryption secret sharing scheme is the extreme phase of our scheme. As each part of the vote is encrypted, no one can predict or learn the outcome of each vote before the tally. In our scheme, intruders will not have any idea about the intermediate results before the announcement of the result because the result is also in encrypted form and can be decrypted only by the delegate power of authorities. Any change by the authorities is not possible as the number of votes casted and number of authenticated voters, are recorded and compared.

B. Eligibility

In our scheme, only legal voters are permitted to vote. Assume that no one can break the ordinary digital signature scheme. In case a dishonest voter tries to vote, the authenticator checks the list and the person has to create a valid pair of the ballot and the signature by himself.

C. Anonymity

The relation between the voter's identity and the ballot is hidden by blind signature scheme. The link between the voter's identity and the ballot is cut at the proxy server before it is being sent to the tallying center. Moreover to ensure that it is impossible to trace a ballot to a voter, the network address of the packet is replaced by the proxy address. In this scheme each vote is encrypted and it is difficult to trace the identity of the voter.

D. Unreusability

To vote twice, voter should get more than a pair of valid ballot and the signature. As the verification is done by one center and the authentication is done by another center, it is difficult for a voter to get the pair of a valid ballot and the signature.

E. Accuracy

All the valid votes will be counted. It cannot be altered either by the administrator, proxies, and supervisors or even by the voter himself.

F. Uncoercibility

There are occasions when the voter is forced to change his vote. This can happen when the voter is asked to verify his vote after the casting. In the proposed scheme, the voter is not allowed to change or verify his vote, once it is casted. The tally center also cannot change a vote because it is in the encrypted form. The supervisors are allowed to access only the result using secret sharing scheme, so there is no question of tampering the vote by them.

VI. Conclusion

We have successfully reformed an improved e-voting scheme which anonymizes the voter's identity from the vote and permits the voter to enroll their vote safely and securely. The scheme also hides voter's secrecy. All the requirements for an ideal electronic voting system cited above as anonymity, accuracy, privacy, eligibility, uniqueness and fairness are satisfied by our scheme. Each candidate has a bank of votes in an unintelligible form. After the termination of tally process, the result is in encrypted form. All the encrypted votes need not be decrypted here in our scheme; instead of that we are calculating the sum of the encrypted votes. The result is then flashed by using secret sharing scheme.

References

[1] Julie Ann Staub,"An analysis of Chaum's voter-verifiable election scheme", Thesis, University of Maryland;2005

[2] Cranor L.F, Crtron RK,"Sensus: A security-conscious electronic polling system for the internet, system science", Proceedings of the 30th Hawaii International Conference on system Science: 1997, Vol. 3, pp. 561-70.

[3] Fijioka A, Okamoto T, Ohta K,"A practical secret voting scheme for large scale elections", Advances in Cryptology-AUCRYPT'92 Proceedings. Springer-Verlag; 1993. pp. 6.15-6.19.

[4] David Chaum, R.Rivest, A.Sherman,"Blind signatures for untraceable payments", In blind signatures for Untraceable Payments (New York, 1982), Plenium Press, pp. 199-203.

[5] Ronald L.Rivest, Adi Shamir, Leonard Adleman, "A method for obtaining Digital Signatures and Public-key Cryptosystems", Number MIT/LCS/TM-82. 1977

[6] Taher El-Gamal,"A public-key cryptosystem and a signature scheme based on discrete logarithms", pp. 10–18, 1985.

[7] Pascal Paillier, David Pointcheval,"Efficient public-key cryptosystems provably secure against active adversaries", In ASIACRYPT '99: Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security, pages 165–179, London, UK, 1999. Springer-Verlag.

[8] Mohammed Al-Fayoumi, Sttar Aboud,"Blind Decryption and Privacy Protection", American Journal of Applied Sciences 2 (4), pp. 873-876, 2005.

[9] Rebecca Meissen"A Mathematical Approach to Fully Homomorphic Encryption".
[10] Adi Shamir,"How to Share a Secret", Communications of the ACM, Vol. 22, No. 11, pp. 612-613, Nov. 1979
[11] G. R. Blakley,"Safeguarding cryptographic keys", American Federation of Information Processing Societies Proceedings, New York. June 04-June 07.48, pp. 313–317, 1979.
[12] Karro J, Wang J.,"Towards a practical, secure, and very large scale online election", Computer Security Applications Conference, (ACSAC'99) Proceedings. 15th Annual; 1999. pp. 161e9.
[13] Chen Y-Y, Jan J-K, Chen C-L.,"The design of a secure anonymous Internet voting system", Journal: Computers & Security, 2004, Vol. 23.
[14] Bruce Schneier,"Applied Cryptography Second Edition: protocols", algorithms and source code in C,1996.

Ms. Sandhya Sarma. K. N. received her B. Sc degree in Computer Science from Mahatma Gandhi University, Kerala, India, the MCA degree from Indira Gandhi National Open University, Delhi, India, and is currently pursuing her M. Phil - Computer Science at Dr G R Damodaran College of Science, Coimbatore, India. Her specialization is Information Security and core research interests include Cryptography, Network Security and Secret Sharing.

Ms. S Umamaheswari received her MCA degree from Bharathidasan University, Trichy, India and M. Phil degree from Bharathiar University, Coimbatore, India. She is currently pursuing her Ph.D. in Computer Science and working as Assistant Professor for the past 12 years in School of Information Technology and Science, Dr G R Damodaran College of Science, Coimbatore, India. Her current research interests include Web Programming, Cloud Computing, Mobile Databases and Mobile Ad Hoc Networks.