A secure approach to election scheme based on Naccache Stern Knapsack Cryptosystem

P.V.Lakshmi
Department of IT
GITAM University
Visakhapatnam
India

R. Suneetha
Department of CSE
GITAM University
Visakhapatnam
India

ABSTRACT

Election is a fundamental mechanism of democracy for people to elect a Government of their choice. Electronic voting is an emerging technology that guarantees privacy, security, correctness, verifiability and robustness. Recently, many researchers have proposed the improvements of efficient schemes on the electronic voting to ensure the security and privacy of voters. However, there is no scheme to solve the security and privacy problem of the electronic voting machine completely. We propose a new voting machine that utilizes Naccache Stern Knapsack Cryptosystem to enhance more security. Development of a secure electronic voting system based on our proposed software, enhanced the security and privacy for the voters.

Keywords

Electronic Voting System, Naccache Stern Knapsack Cryptosystem, Privacy, Security.

1. INTRODUCTION

Recently, electronic voting has gained more prominence and a variety of schemes have been proposed. Important requirements of electronic voting are protecting voter's privacy, ensuring robustness in election, guaranteeing universal verifiability of the correctness of the election tally, receipt-freeness and uncoercibility i.e., no voter should be able to prove to others how he voted and no party should be able to force another party to vote in a certain way or abstain from voting [1,2,3,4]. Due to advancement in technology, computer voting machine is not that difficult to use for the normal users. But, there is need to educate the people who are illiterate of using computers. The native approach is to issue a unique identification number to each voter which may disclose privacy of the voters. We have investigated many technologies that are necessary for security and privacy. Many cryptographic protocols have been proposed to overcome this difficulty [5, 6, 7]**).** In this paper we propose a secure and practical voting scheme for real world with following properties: - Eligibility**:** Only eligible voters are allowed to vote and every voter can cast only one vote. Privacy: All votes must be secret. A ballot cannot be linked back to the voter who casted it. Fairness: No participant can get extra information of the tally before the counting phase. Individual Verifiability: Each eligible voter can verify that his vote was correctly counted. Universal Verifiability: Any party and observer can check that the election is completely correct. The published final tally is consistent with the votes casted in all ballots. And the total number of ballots must be equal to the total number of the eligible voter's registrations. Receipt-freeness: Voter cannot get any information which can be used to prove what he voted to the coercer or the vote buyer. To provide security and privacy for the election Naccache Stern Knapsack Cryptosystem is proposed.

2. MATERIALS AND METHODS

Three main approaches in the electronic voting scheme are 1.Blind Signatures: The involved parties in these schemes are the voters, the administrator, the counter and the bulletin board. In cryptography, a blind signature is a form of digital signature in which the content of a message is disguised before it is signed. The resulting blind signature can be publicly verified against the original unblinded message in the manner of a regular digital signature. Blind signatures are typically employees in privacy-related protocols where the signer and message author are different parties. Examples include cryptographic election systems and digital cash schemes [5, 7, 8, 9]. 2. Homomorphic encryption: It is a form of encryption where one can perform a specific algebraic operation on the plaintext by performing an algebraic operation on the cipher text. The Homomorphic property of various cryptosystems can be used to create secure voting systems, collision-resistant hash functions and private information retrieval schemes. There are several efficient Homomorphic cryptosystems, RSA cryptosystem, ElGamal cryptosystem, Gold Wasser-Micali cryptosystem, Benaloh cryptosystem, Okamoto-Uchiyama cryptosystem, Paillier cryptosystem, Naccache-stern cryptosystem, Damgard-Jurik cryptosystem, Boneh-Goh- Nissim cryptosystem [10-14]. 3. Schemes using mix-nets also known as Digital mixes: Digital mixes make hard to trace communication by using a chain of proxy servers. Each message is encrypted to each proxy using public key cryptography [15, 16].

Proposed System We propose a new Electronic Voting machine which is secure, easy and ensures correctness. Although there is some security mechanisms used in Electronic Voting machine, they are not reachable up to the mark. One of the limitations with this is, candidate can know how many people from a polling place voted for him. In order to overcome this, we design a Computer based Voting System with highly secured properties.

Description of modules

Admin Login: Admin initializes the voting process by entering his id and password for the security purpose. He creates the database for the participants and competitors. If new voter, Checks for the eligibility details and creates the voter id. While registering, he generates private key with voter's id. Exiting User can directly attend this section by registering with his/her voter id. Requirements: 1. Admin login id and password 2. Voter eligibility details**.** *Registration:* Voter registers to the Registrar with voter id and proof by identification through fingerprint or signature authentication system. Registrar generates the credential (private key and voter id) for the verified voter by selecting an available credential number from prepared credential tags with in credential table. Registrar encrypts credential and sends to voter, who is voting at booth. Requirements:
1. Voter-Citizen id or signature authentication system.
2. Admin-Registrar id. 3. Credential number (c_no)
4. Credential *C*vi = (register_ID || c_no || sign (c_no))
5. Naccache Stern Knapsack Cryptosystem

Voting Phase: With the received credential, voter casts the vote by selecting his choice among the competitors and by submitting his work. He can't get any extra information regarding the voting details, even by paper work or electronic usage like USB devices. He can't modify his vote, once work is done; that is the final submission. Thus frauds and cheating can be eliminated. Also, he can't vote for multiple times. Since, there is a condition that number of votes cast is equal to number of voters registered and only one vote can cast per head. Requirements: Voter's credential, Admin, Decryption algorithm. *Tallying/Counting and Displaying:* After the voting, CA main office collects all the valid ballots from ballot boxes. Summation of votes could be formed without decrypting the ballots. In order to read the summation, CA office of at least *Aj* authorities are needed to verify their own shared private key to the CA main office. Private key s need not to be reconstructed from the set of valid CA's private keys. But only a subset of keys can be used to open ballot and as a result the summation of votes can be formed. And then final tally can be derived by threshold Elgamal Cryptosystem. As to ensure the correctness of electronic voting, any party or observer verifies that if the number of created credential is equal to the number of cast ballots. And number of cast ballot is also equal to the number of registered voters. Finally, check that the final tally counted from every bulletin board, CA ballot boxes and printed ballot boxes are the same.

Threshold ElGamal Cryptosystem

The objective of a threshold public-key encryption scheme is to share a private key among the receivers such that message can only be decrypted when a set of minimum number of receivers cooperate together. A threshold system consists of a key generation protocol to generate the distributed private key for receivers and a decryption protocol to decrypt cipher text without reconstructing the main private key. Each authority A_j will share a x_j € Zq of a secret x. The authorities publish the value $y_j = g^{xJ}$. The share key x_j can be reconstructed from any subset Λ of *t* shares by using appropriate Lagrange coefficients,

$$X = \sum_{j \in \Lambda} X_j \lambda_{j,\Lambda}$$

where $\lambda_{j,\Lambda} = \prod_{l \in \Lambda / \{j\}} l / 1\text{-}j$ (1)

Encryption of m with public key
$y = g^x$ is $(a, b) = (y^k m, g^k)$. In order to decrypt a cipher text without reconstructing the secret X, the authorities execute the following protocol. Each authority Aj broadcasts

$$w_j = p^{xj}$$

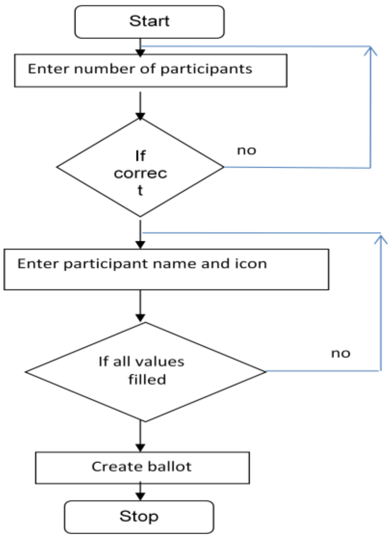
and proof in zero knowledge that his distributed private key is correct by verify that

$$\log_g h_j = \log_p w_j \qquad (2)$$

In equation (1), let Λ denote any subset of t authorities who passed the proof of zero knowledge. The plaintext can be recovered as

$$m = y / \prod_{j \in \Lambda} w^{\lambda j,\Lambda}{}_j$$

Admin:



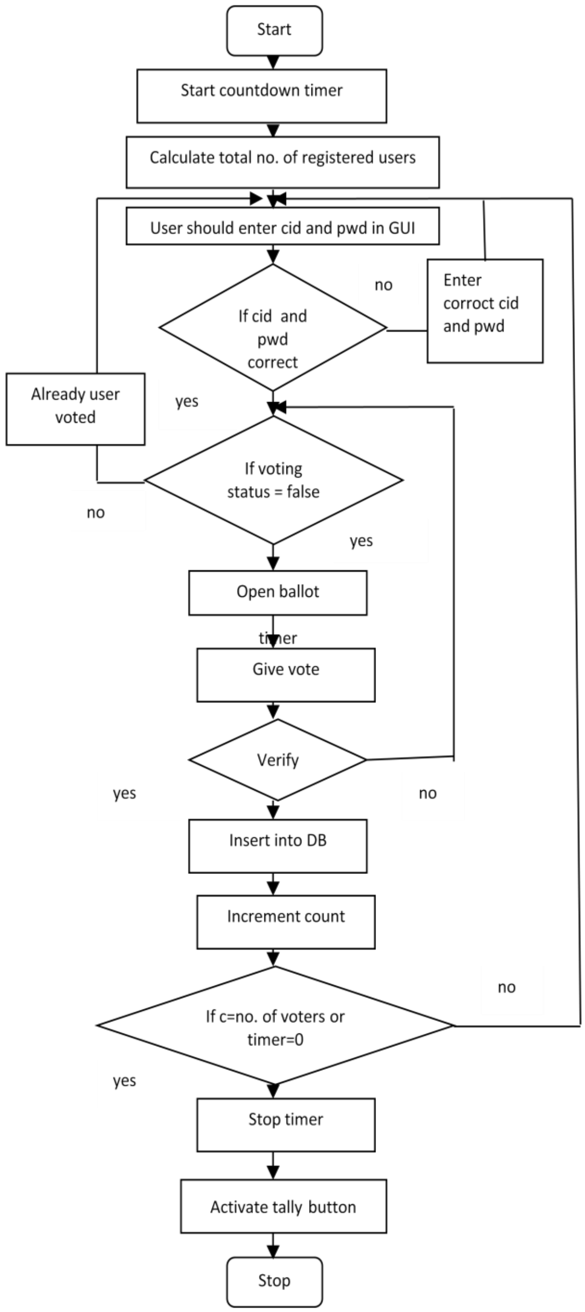
Naccache Stern Knapsack Cryptosystem

In Naccache Stern Knapsack (NSK) cryptosystem the cipher text is obtained by multiplying the public key indexed by the message bits and the clear text is recovered by factoring the cipher text raised to the secret power. Encryption requires four multiplication/bytes and decryption is equivalent to RSA decryption and it involves three stages namely, Key generation, Encryption, Decryption.

i. Key generation

Select an integer (n)
Generates prime number (p)
Select secret key (s) such that $s < p\text{-}1$ and gcd(p-1, s) = 1
Generates ṇ +1 public keys using $V_i = {}^{s}\sqrt{p_i}$ mod P

Voter:



i*i Encryption*

In the proposed algorithm the plaintext is converted to ciphertext using the following steps:

Plaintext is given by:

$$m = \sum_{i=0}^{n-1} 2^i m_i$$

Formula used to encrypt the given plaintext is as follows:

$$c = \prod_{i=0}^{n-1} v_i^{\,mi} \bmod p$$

iii. Decryption:

The decrypted message is again converted to the original plaintext as shown below:

Cipher text is given by: $C^s \bmod p$

Plaintext is given by

$$m = \sum_{i=0}^{n-1} \frac{2^i}{p_i - 1} \left\{ gcd\,(p_i, c^s \bmod p) - 1 \right\}$$

3. CONCLUSION

By using homomorphic scheme, the election scheme allows us to produce a summation of votes without decrypting them. Furthermore, the system uses threshold ElGamal cryptosystem to prevent a single malicious authority or a small number of authorities to open or tally. The final tally is kept a secret until a group of trustable vote counter authorities cooperate together to use their share key to open the final tally. Our system is also receipt-fairness as it does not allow each voter to specify the random number himself, voter cannot get any information for his vote buyer to link to his cast ballot. Vote counting is done in the system by decrypting votes with CA's share key, thus it could be used to confirm with the tally from various copies of that system in various places. In the analysis phase, our designed electronic voting system covers overall requirements of electronic (computer) voting system and with some simple concepts, the system may encourage people to believe more in electronic system services. As now-a-days everyone is using computer as general equipment, this process is more appropriate.

4. REFERENCES

[1] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2):84–88, 1981.

[2] Richard DeMillo, Nancy Lynch, and Michael J. Merritt. Cryptographic protocols. In Proceedings of the 14th Annual Symposium on the Theory of Computing, pages 383–400, 1982.

[3] Josh C. Benaloh. Verifiable secret-ballot elections. PhD Thesis, Yale University, Department of Computer Science, 1987. Number 561.

[4] Josh Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections. In STOC '94, pages544–553, 1994.

[5] 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.

[6] K.R.Iversen" A cryptography scheme for computerized general elections" Advances in cryptology .Proc of Crypt91, LNCS 576, Springer –verlag,pp 405-419, 1991.

[7] 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.

[8] Kazue Sako. Electronic voting schemes allowing open objection to the tally. In Transactions of

IEICE, vol. E77-A No.1, Jan. 1994.

[9] 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.

[10] 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.

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

[12] 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.

[13] 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.

[14] 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.

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

[16] Masayuki Abe. Mix-networks on permutation networks In Advances in Cryptology | ASIACRYPT '99, vol. 1716 of LNCS, pp. 25-273. Springer-Verlag, 1999.