CRYPTOGRAPHY IN ELECTRONIC VOTING SYSTEMS

Dr Orhan Çetinkaya
(PhD) Institute of Applied Mathematics, METU, Ankara, Turkey
2272VP 23, Voorburg, Netherlands
E-mail: corhan@ceng.metu.edu.tr

─Abstract ─

Electronic democracy is a necessity in this era of computers and information technology. Electronic voting (eVoting) is one of the pillars of the e-democracy, which refers to the use of computers or computerised voting equipments to cast and to tabulate ballots in an election in a trustable manner. Due to the nature of electronic systems the security and reliability of the system should be handled properly in order to make the eVoting system as an applicable alternative to the paper based voting system for the governmental elections.

The use of cryptography helps to achieve the trustworthiness of the system. Cryptography can be used at certain points in the voting process in order to persuade the citizens that a fully secure system has been developed and the whole election process is fulfilled properly and securely. Based on this fact, eVoting systems have shown an increasing trend towards the use of cryptography to increase public confidence in the eVoting process.

This paper discusses the use of cryptography in the eVoting systems. It firstly describes the eVoting process with the associated actors. It also gives an eVoting classification. Then, it explains the challenging eVoting security requirements and shows how cryptography, i.e. key cryptographic primitives, cryptographic building blocks, can be used to overcome these challenges.

Key Words: *Electronic voting, cryptography, eVoting*
JEL Classification: O3 - Technological Change; Research and Development

1. INTRODUCTION

Voting is regarded as one of the most effective methods for individuals to express their opinions on a given topic. The main goal of any voting system is to assure the votes were recorded as cast and tabulated as recorded without revealing the identities of the voters. Electronic voting (eVoting) refers to the use of computers or computerised voting equipment to cast ballots in an election. Due to the rapid growth of computer technologies and advances in cryptographic techniques, electronic voting is now an applicable alternative for small scale non-critical elections. However; in many cases, voting needs to be performed in a large scale such as in governmental elections; thus, security requirements become even more critical. Electronic voting is a challenging topic in advanced cryptography. The challenge arises primarily from the need to achieve security and democracy requirements such as privacy, accuracy, receipt-freeness and verifiability. Therefore, electronic voting has been intensively studied in the last decades.

When paper based voting system is applied, voter can be convinced that his vote is counted in the final tally since observers participate to the whole voting process. In the paper based voting system; the voter, after being authenticated by the authority, receives a blank ballot, makes his choice on the ballot in a polling-booth and casts it into the ballot box in front of the authority. After the voting period has been completed, the ballot box is opened and the ballots are counted by the authorities in front of the observers and public. The counting result is announced. After all counting results are combined, election result is publicised. In the paper based voting system, the voter casts his vote by himself without any influence and nobody can see voter’s vote except himself. Voter cannot cast more than one vote. Vote collecting, counting and tabulating are done in front of observers publicly. Meanwhile, representatives of political parties, observers of independent non-governmental organizations and international organizations are welcome to be present and can observe the election process.

When voting takes place in an electronic environment, possibility of fraud is unavoidable since ensuring the trust is not as simple as the paper based voting system. At any step in the eVoting process, eVoting results can be manipulated if there are lack of security and cryptography. Majority of people may accept and use eVoting, but people have some doubts about the privacy, security and accuracy of the system. They cannot easily trust the eVoting system unless security of the system is achieved. If cryptography is applied on eVoting systems, then the trustworthiness will be increased and more voter participation can easily be achieved.

Many controversies have been raised and many inconsistencies have been reported with the experienced real world electronic elections. These experiences showed that the electronic voting protocols certainly need to use advanced cryptography to make electronic voting secure and applicable. In order to persuade the citizens that a fully secure system has been developed and the whole election process is fulfilled securely without any corruption, cryptography has been used at certain points in the voting process. In recent years eVoting systems have shown a special interest to the use of cryptography so as to increase public confidence in the eVoting process such as symmetric-key cryptography, public-key cryptography, digital signature, blind signatures, cryptographic hash function, pseudo random number generation, homomorphic encryption, zero-knowledge proof, mix-nets and bulletin board.

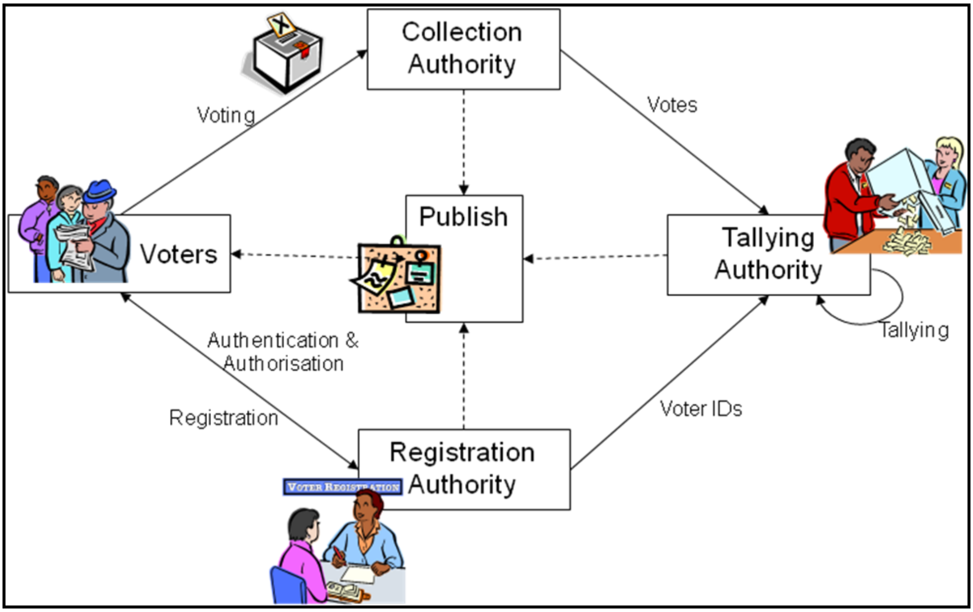
This paper briefly explains the electronic voting process, classification and security requirements. It also explains how cryptography can be used in eVoting systems; in other words, which cryptographic primitives, cryptosystems, cryptographic algorithms and building blocks can be used in the eVoting systems.

2. E-VOTING: PROCESS, CLASSIFICATION AND REQUIREMENTS

2.1. A Typical Voting Process

The main process of any electronic election is almost standard although a wide variety of electronic voting systems and protocols exist. A general electronic voting process and the actors involved can be summarised as in Figure 1. In any voting system, the following actors take place in the election.

Figure 1: A Typical Voting Process



- *Voter*: Voter has the right for voting, and he votes in the election.
- *Registration Authority:* Registration authority (or authorities) registers eligible voters prior to the election day. These authorities ensure that only

the registered voters can vote, and they vote only once on the election day. Registration authorities can be the registrar, authenticator, authoriser, ballot distributor, validator and/or key generator.

- *Collection Authority*: The collection authority (or authorities) collects all cast votes. Collection authorities can be collector and/or ballot box authority.
- *Tallying Authority:* The tallying authority (or authorities) tallies the results of the election and tabulate them. Tallying authorities can be counter, tabulator and/or tallier.

The following four stages describe the voting process in any voting system.

- *Registration*: Voters register to vote, and the registration authority compiles the list of eligible voters before the election day.
- *Authentication and Authorisation*: On the election day registered voters request ballots or voting privilege from the registration authority. Registration authority checks the credentials of the voters attempting to vote and only allows those who are eligible and have registered before, and have not already voted to proceed.
- *Voting*: Voter casts his vote.
- *Tallying*: The tallying authority counts the votes and announces the election results.

2.2. eVoting Classification

Based on the voting equipment and voting location, electronic voting can be classified in five different types. Table 1 summarises all of these including paper based voting. Being a stand-alone or network (controlled/uncontrolled) enabled is the main driving factors in the classification.

DRE voting: Direct Recording Electronic (DRE) machine is physically hardened electronic equipment with running special purpose voting software. It lacks a tamper-proof audit-trail. Satisfying accuracy and verifiability is almost impossible at DRE voting since any fraud during the voting process is unrecoverable and undetectable. This is similar to the current paper-based voting systems. The votes are cast inside a voting booth at a polling site; however, cast votes are recorded in electronic ballot boxes.

Poll-site voting: In poll-site voting, the votes are cast by using public computers at a polling site. Voting booths are not used, but a public polling-site is provided. The computers at the site are connected over a closed and controlled network. Cast votes are recorded by a counting authority server instead of electronic ballot boxes. Voters can be authenticated and authorised at the site before allowed to access to the voting machines, or they can have some voting credentials prior to the voting period.

Poll-site kiosk voting: In poll-site kiosk voting, the votes are cast inside a voting booth at a polling site as in DRE voting. Typically, voting booths at the site contain electronic voting terminals, and they are connected with a closed and controlled network. Cast votes are recorded by a counting authority server instead of electronic ballot boxes. Voters are authenticated and authorised at the site before allowed to access to the voting booths. Votes are cast using the terminal inside the voting booths.

Poll-site Internet voting: In this type, the votes are cast by using public computers at a polling site over Internet. Voting booths are not used, but a public polling-site is provided. The computers at the site are online over an uncontrolled network. Cast votes are recorded by a counting authority server instead of electronic ballot boxes. Voters can be authenticated and authorised at the site before allowed to access to the voting machines, or they can have some voting credentials prior to the voting period.

Remote Internet voting: Voters cast their votes over Internet. For authentication, the credentials of voters are verified prior to the voting period through the use of a password or some type of authentication token.

Table 1: Voting Types

	Stand-alone Voting	***Networked Voting***	
		Controlled Network	**Uncontrolled Network**
Paper Voting	Paper Based Voting	N/A	N/A
Electronic Voting	DRE Voting	Poll-site kiosk voting	Poll-site Internet voting
		Poll-site voting	Remote Internet voting

2.3. eVoting Security Requirements

Based on the in-depth literature review, it is expected from any voting system to satisfy the following security requirements.

Voter Privacy: A particular voter and his cast vote should be unlinkable. No one except the voter should be able to determine the value of the vote cast by the voter. Voter privacy must be preserved during the election as well as after the election (Cranor, 1997).

Eligibility: Only eligible and authorized voters can vote (Fujioka, 1992), (Burmester, 2003).

Uniqueness: Only one vote for each voter should counted (Forsgren, 2001).

Fairness: No participant can gain any knowledge, except his vote, about the (partial) tally before the counting stage (Aditya, 2004). Even the counter authority should not be able to have any idea about the results.

Uncoercibility: Any coercer, including the authorities, should not be able to extract the value of the vote (Burmester, 2003) and should not be able to coerce a voter to cast his vote in a particular way.

Receipt-freeness: Voter must neither be able to obtain, nor construct a receipt which can prove the content of their vote (Benaloh, 1994) both during the election and after the election ends.

Accuracy: The published tally should be correctly computed from correctly cast votes (Burmester, 2003). So, any vote cannot be added, altered, deleted, invalidated or copied in the final tally without being detected.

Universal Verifiability: Any participant or passive observer can convince himself of the validity of individual votes and of the final tally of the election.

Individual Verifiability: Each eligible voter can verify that his vote is counted correctly.

In addition to eVoting security requirements, there are also system level requirements such as efficiency, convenience, transparency, scalability, mobility and flexibility.

3. CRYPTOGRAPHY IN ELECTRONIC VOTING

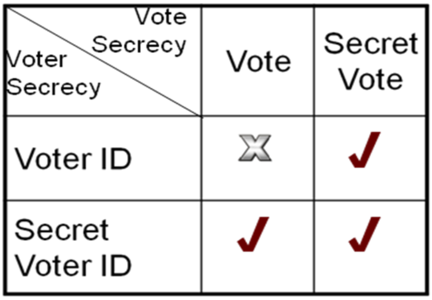
Based on how voters submit votes to the tallying authority, the following broad classification for voting protocols can be stated. This classification has four possibilities for the secrecy of the voter-vote relationship as shown in the Table 2.

- *No secrecy*: Secrecy is not applied anywhere, it is not useful as it offers no privacy.
- *Secret Vote*: Secrecy is applied to the vote. The voters anonymously submit votes.

- *Secret Voter*: Secrecy is applied to the voter ID. The voters openly submit encrypted votes.
- *Secret Voter & Vote*: Secrecy is applied for both voter ID and vote. The voters anonymously submit encrypted votes.

As the first one does not provide any privacy, it is not preferred to use. The last one is more complex and not practical. Therefore, almost all eVoting studies have been focused on the second and third options since they are enough to achieve the privacy requirements.

Table 2: Voter-Vote Relationship

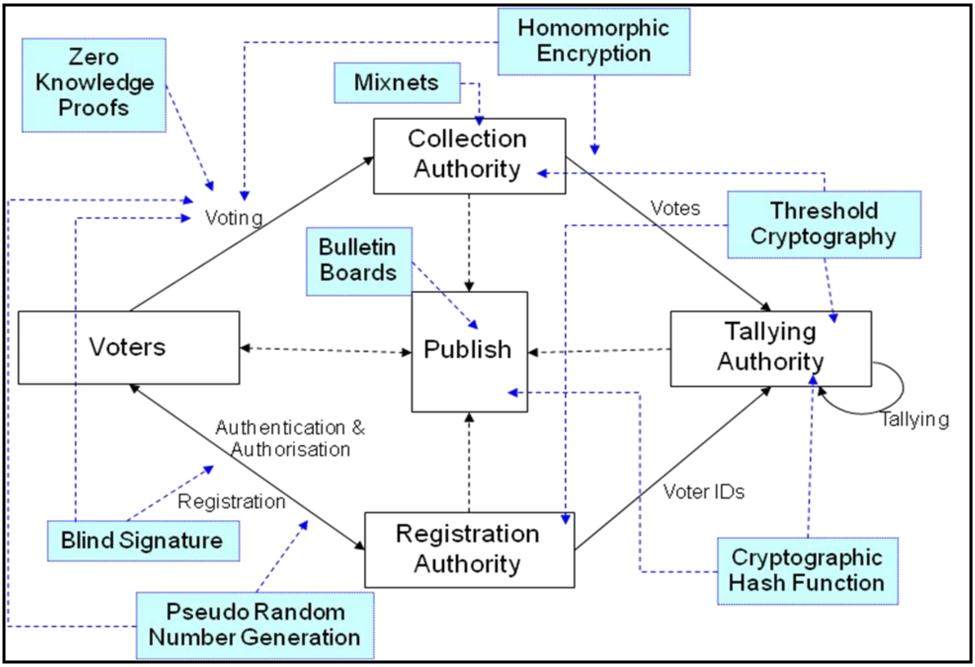


Vote Secrecy Voter Secrecy	Vote	Secret Vote
Voter ID	✗	✓
Secret Voter ID	✓	✓

In order to satisfy the eVoting security requirements, cryptography plays a crucial role at the different stages of the voting process. Figure 2 gives an overview about how cryptography supports to the eVoting.

Symmetric-key cryptography, public-key cryptography and digital signature are used as cryptographic primitives. The following building blocks and/or cryptosystems use these primitives.

Figure 2: The interaction between the eVoting and cryptography.



3.1. Blind Signature

A blind signature is a form of digital signature in which the content of a message is concealed (i.e. blinded) before it is signed (Chaum, 1982). Blind signatures are the equivalent of signing carbon paper lined envelopes. Writing a signature on the outside of such envelope leaves a carbon copy of the signature on a slip of paper within the envelope. When the envelope is opened, the slip will show the carbon image of the signature.

A distinguishing feature of blind signatures is their unlinkability: The signer cannot drive any association between the signing process and the signature, which is later made public. The resulting blind signature can be publicly verified against the original, unblinded message by means of a regular digital signature. RSA public key cryptosystem is used to implement the blind signatures.

Blind signature is used to provide privacy in eVoting systems (Cetinkaya, 2007). The voter submits the vote and his identity, registration authority signs the voter's identity and blindly signs the vote and returns them to the voter, voter removes the signed id and submits the signed vote. Registration authority uses blind signatures to authorise the votes to authorised voter, prevent double voting; voter register and obtain pseudonym.

3.2. Cryptographic Hash Function

A cryptographic hash function is a hash function *h* with certain additional security properties, which takes an arbitrary size input *x* and outputs a fixed length output *h(x)*. Although a cryptographic hash function is deterministic and efficiently computable, it should behave as much as possible like a random function. Hash functions are assumed to be public; therefore if *x* is given, anyone can compute *h(x)*.

Digital signatures and data integrity are the most common cryptographic uses of hash functions. With digital signatures, a long message is usually hashed (using a publicly available hash function), and only the hash-value is signed. The party receiving the message then hashes the received message and verifies that received signature is correct for this hash-value. This saves both time and space compared to signing the message directly. MD5, SHA-1, SHA-256 are well known hash algorithms. SHA-256 is the preferred cryptographic hash function in practice.

Hash functions are used to log the voter interactions and the voting authorities' activities in the eVoting protocols so that the message logs are cryptographically protected, and the auditing can be done easily. The intermediate hash values can be periodically time-stamped by the central agency in order to allow detecting the message log tampering attempts. Some of the hash values can be shared with the public on the bulletin boards. In electronic voting systems, the verifiability requirement is one of the key requirements to give confidence to the voters. Hash functions provide key features to enable verifiability of the system, and increase the accuracy of the system.

3.3. Pseudo Random Number Generation

Pseudo random number generator (PRNG) is a deterministic algorithm to generate a sequence of numbers with little or no discernible pattern in the numbers. The sequence is not truly random since it is determined solely by a relatively small set of initial values. Although sequences that are closer to truly random ones can be generated using hardware random number generators, most pseudo random generator algorithms produce sequences which are uniformly distributed.

Many classes of PRNGs exist, but the goal of a PRNG in cryptography is the production of pseudo random data that are computationally indistinguishable from statistically ideal random data. A PRNG is cryptographically secure, on condition that it is computationally infeasible to predict the next output even if all the previous outputs and the complete algorithm are given.

Some eVoting systems need to produce random numbers in a secure way at certain point of the voting process such session identity numbers, ballot numbers, candidate numbers. If the eVoting protocol uses blind signatures for the eligibility and voter privacy requirements, PRNG helps to produce proper random numbers.

3.4. Homomorphic Encryption

Another commonly proposed way of achieving privacy in voting protocols is to use homomorphic encryption. A cryptosystem is homomorphic when $E(s1) \circ E(s2) = E(s1 \Diamond s2)$, where E is a public encryption function, s is a secret message, and $\circ$ and $\Diamond$ are some binary operators. Note that the binary operators may be equal. Thus, it is possible to compute the combination of the individual messages without having to retrieve the individual messages themselves. Thereby, the individual messages can remain confidential. Two popular examples of homomorphic cryptosystems are ElGamal (ElGamal, 1985) and Paillier (Paillier, 1999) cryptosystems.

In voting protocols based on homomorphic encryption, as the encrypted votes gather, it results in the accumulation of votes. The voting result is then obtained from the accumulation of votes while no individual ballot is opened and the corresponding individual vote remains secret.

In homomorphic encryption based protocols (Benaloh, 1994), (Cramer, 1997), (Hirt, 2000), voting results are obtained easily so ballot tabulations are conducted more efficiently when the number of candidates or choices is small. A great advantage of this approach is that voters may openly authenticate themselves to the voting servers; there is no need for anonymous channels to ensure voter privacy.

Electronic voting protocols based on homomorphic encryption have more security properties than other protocols, but their communication complexity is quite high. They are most suitable for yes-no or 1-out-of-L voting. A known implementation of this approach can be found in a European Union project; the CyberVote project, funded by the European Commission, has developed a prototype system.

In the homomorphic encryption, the results of different form of operations on the plain and encrypted text are the same. Therefore, the encrypted votes can be summed up, and then the encrypted total votes can be decrypted as bulk sum. However, zero knowledge proof is needed to ensure correct vote is totalled to prevent inaccurate result; proofing that the vote is correct without revealing the vote itself. Threshold cryptography is also needed to distribute the power to decrypt, and to prevent cheating counter authorities to disclose individual vote.

3.5. Zero-Knowledge Proof

In cryptographic protocols it is often needed to prove some statement to someone without revealing any extra information. This is accomplished by zero-knowledge proofs. Zero-knowledge proofs are used mostly by authentication systems where one party wants to prove its identity to a second party via some secret information but does not want the second party to learn anything about this secret. Zero knowledge proof protocols are two-party protocols between a prover and a verifier. They allow the prover to convince the verifier that he knows a secret, but without giving any information about the secret. After the execution of the protocol the verifier has gained zero knowledge concerning the secret.

The zero-knowledge protocol overcomes major concerns with widely used password based authentication. In a simple password based authentication, the verifier authenticates the prover based on a password. The verifier has some, if not complete, knowledge of the prover's password. The verifier can thus impersonate the prover to a third party with whom the prover may share the same password.

Zero-knowledge proof is used between the voter and the voting authorities or within the voting authorities. It is especially useful for voter authentication. The voter does not have to send his password credentials to the authorities.

As the voting authorities (verifier) does not learn anything about voter's (prover) secret (no knowledge transferred between two parties), he cannot impersonate the voter to a third party. Also the voter cannot cheat the voting authority with several iterations of the protocol. Eligibility and accuracy of the eVoting system is assured by using zero-knowledge proof.

3.6. Threshold Cryptosystem

A (t, n) threshold cryptosystem is a system to distribute secret keys or operations of a cryptosystem between n parties in order to remove single point of failure. The required trust in the cryptographic service is distributed among the group of authorities. The goal is to allow any subset of more than t parties to jointly reconstruct a secret and perform the computation while preserving security even in the presence of an active adversary which can corrupt up to t (a threshold) parties. A minority of compromised authorities can be tolerated.

Threshold schemes based on the discrete log problem are relatively easy to build. On the other hand, there are some technical difficulties in RSA, in particular, key generation which requires that the product of two primes be obtained without any single party knowing these two primes.

When the (t, n) threshold cryptosystem is used in any eVoting protocol, the private key is secretly shared among the authorities/participants, while one public key is published. Any group of at least *t* authorities can jointly decrypt votes encrypted under this public key using a distributed decryption protocol. An adversary thus needs to compromise at least *t* of the voting authorities/participants to decrypt the messages.

Threshold cryptography can also be used to distribute signature operations among several participants. In order to sign the voter's message *m*, more than *t* participants execute an interactive signature generation protocol by using their secret shared keys and obtain the signature of *m* that can be verified by anybody using the public key.

Threshold cryptography is mostly used to provide the fairness since it requires more than one authority (*t* authorities) to make the decryption/signing operations. In order to start the tallying process *t* out of *n* authorities should make a consensus. The value of *t* can be any number between 1 and *n*. The secret key can be shared among the different authorities such as non-profit organisations, non-governmental bodies, different party representatives etc. By using threshold cryptography, the counting stage could not start during the election period.

3.7. Mix-nets

Mix-networks (mix-nets) are the most common approach to achieve anonymity. The general concept of mix nets is based on permuting and shuffling the messages in order to hide the relationship between the message and its sender. However, the details, as to the implementation of mixing protocols, change depending on configurations and arrangements of mix-nets.

A mix-net typically consists of a set of mix servers which are responsible for mixing the incoming inputs and producing a shuffled output. In mix-nets, there are n mix-servers $M_1, ..., M_n$; each with its own public key $_{Ei}$ and private key D_i. Each server processes the input messages. The process can be either re-encryption or decryption depending on the mix-net types. Then, each server permutes the processed messages and forwards them to the next mix server.

The first mix-nets are decryption mix-nets (Chaum, 1981), (Jakobsson, 2001) where messages are wrapped in several layers of encryption and then are routed through mix servers, each of which peels off a layer of encryption and then forwards them in random order to the next one. In decryption mix-nets, decryption in each mix server is repeated until all layers are removed. Later re-encryption mix-nets were introduced (Sako, 1995), (Golle, 2004) where the incoming messages are not decrypted, but re-encrypted in each mix server. In re-encryption mix-nets, decryption occurs after shuffling is completed.

The major drawback of the decryption and re-encryption mix-nets is that one server may compromise and cheat by removing or replacing any number of items. Therefore, they are extended to be verifiable. In verifiable mix-nets, a mix server additionally has to prove in zero knowledge that it decrypts/re-encrypts and shuffles the inputs correctly. There are several approaches to obtaining verifiable mix-nets; the main difficulty in these approaches is inefficiency of proof techniques. The call for proving that the mixing is correct causes an excessive computational cost for mix servers, so their implementation is not practical.

Using mix-nets in voting protocols is generally called as mix voting. As a general approach, a voter casts his vote over a mix-net, and it is assumed that a vote cannot be linked to a particular voter. In mix-net based voting protocols, voters prepare their ballots stating for whom they wish to vote and encrypt their ballots. Then, they send their cast ballots to the mix-network. Firstly, mix server takes the list of the encrypted votes and mixes them in a random order. Later, it re-encrypts/decrypts the votes and forwards all votes to the next mix server. The next mix server takes the votes and shuffles them in the same way as the first server. Successively, each mix server takes the votes sent by the previous server, shuffles them and sends the produced list to the next mix server. The list produced by the last mix server is called the final votes list. The list is counted after the final decryption/encryption and published.

3.8. Bulletin Board

A bulletin board (Chaum, 1981) is a public broadcast channel with universally accessible memory where a party may write information via secure communication in the designated areas. The information can be read by any party. Bulletin boards are commonly used in electronic voting protocols. All communications with the bulletin boards are public and therefore can be monitored. Generally, data already written into a bulletin board cannot be altered or deleted in any way, but it can be read or appended.

In traditional paper-based voting systems, people cannot make individual verifiability directly. However, the voter casts his vote into the ballot box by himself. Since the security of the ballot box is guaranteed, individual verifiability is, in a way, assured. Although this requirement is not directly satisfied in paper based voting, it should explicitly be fulfilled in electronic voting protocols due to the nature of computer systems and electronic equipment. Besides the voter's individual verification, the voting process, steps and published tally would be verified by third party observers. Thus bulletin board gives full support to fulfil the verification and accuracy requirements of the eVoting systems.

5. CONCLUSION

The main goal of any voting system is to assure the votes were recorded as cast and tabulated as recorded without any corruption. The greatest challenge in eVoting is to develop a fully secure system that provides security and democracy in a fully verifiable manner, and preserves the anonymity of the voter and the vote relationship. Cryptography plays a crucial role to overcome the challenges.

Employing cryptography in electronic voting systems would improve the integrity of the system and increase public confidence in the process of voting. As a result eVoting systems in recent years have shown an increasing trend towards the use of the science of cryptography.

BIBLIOGRAPHY

Aditya, R., B. Lee, C. Boyd and E. Dawson (2004), "Implementation issues in secure e-voting schemes", *The 5th Asia-Pacific Industrial Engineering and Management Systems Conference,* Goldcoast, Australia.

Benaloh, J. and D. Tuinstra (1994), "Receipt-free secret-ballot elections", *In Proceedings of the 26th ACM Symposium on the Theory of Computing,* pp. 544-553, 1994.

Burmester, M. and E. Magkos (2003), "Towards secure and practical e-elections in the new era", *Chapter in Information Security - Secure Electronic Voting,* Kluwer Academic Publishers, pp. 63-76.

Cetinkaya, O. and A. Doganaksoy (2007), "A Practical Verifiable E-Voting Protocol for Large Scale Elections over a Network", *In Proceedings of the 2nd International Conference on Availability, Reliability and Security (ARES'07),* Vienna, Austria, pp. 432-442.

Chaum, D. (1981), "Untraceable electronic mail, return addresses, and digital pseudonyms", Communications of ACM, vol. 24, pp. 84-88.

Chaum, D. (1982), "Blind signatures for untraceable payments", *CRYPTO'82,* pp. 199-203.

Cramer, R., R. Gennaro, and B. Schoenmakers (1997), "A secure and optimally efficient multi-authority election scheme", *EUROCRYPT'97,* Germany.

Cranor, L. and R. Cytron (1997), "Sensus: A security-conscious electronic polling system for the Internet", *Hawaii International Conference on System Sciences, Hawaii*.

ElGamal, T. (1985), "A public key cryptosystem and a signature scheme based on discrete logarithms*", In Advances in Cryptology* - *CRYPTO'84*, pp. 10-18. Springer-Verlag.

Forsgren, O., U. Tucholke, S. Levy and S. Brunessaux (2001), "Report on electronic democracy projects, legal issues of Internet voting and users (i.e. voters and authorities representatives) Requirements Analysis", *European Commission CYBERVOTE Project*, D4 vol. 3.

Fujioka, A., T. Okamoto and K. Ohta (1992), "A practical secret voting scheme for large scale elections", *AUSCRYPT'92*, Australia, pp. 244-251.

Golle, P., M. Jakobsson, A. Juels and P. Syverson (2004), "Universal re-encryption for mixnets", *In Proceedings of CT-RSA'04*, pp. 163-178.

Hirt, M. and K. Sako (2000), "Efficient receipt-free voting based on homomorphic encryption", *EUROCRYPT'00*, Bruges, Belgium, pp. 539-556.

Jakobsson, M. and A. Juels (2001), "An optimally robust hybrid mix network", *In Proceedings of the 20th Annual ACM Symposium on Principles of Distributed Computing (PODC 01)*, ACM Press, pp. 284-292.

Paillier, P. , "Public-key cryptosystems based on composite degree residuosity classes", EUROCRYPT'99, pp. 223-238, 1999.

Sako, K. and J. Kilian (1995), "Receipt-free mix-type voting scheme: a practical solution to the implementation of a voting booth", *EUROCRYPT'95*, Malo, France, pp. 393-403.