A Receipt-free Multi-Authority E-Voting System

Adewole A. Philip
Department of Computer Science
University of Agriculture
Abeokuta, Nigeria

Sodiya Adesina Simon
Department of Computer Science
University of Agriculture
Abeokuta, Nigeria

Arowolo Oluremi. A.
Department of Computer Science
Tai Solarin College of Education
Ijebu-Ode, Nigeria

ABSTRACT

The existing e-voting schemes satisfied requirements such as eligibility, completeness, 'no vote duplication', privacy but have not been able to solve the problems of universal verifiability, coercion, bribery and fairness in the overall election process. In this work, a receipt-free multi-authority e-voting system is proposed to solve the drawbacks of the existing e-voting systems is proposed. The proposed scheme employs ElGamal encryption for ensuring the security of votes because of its probabilistic nature. ElGamal which is homomorphic with multiplication is modified to be additive homomorphic in order to ensure voters' privacy and overall election efficiency. A trusted centre is involved in the scheme to distribute the shared secret key among the authorities and the Shamir(t, n) threshold scheme is used for key distribution. The authorities will then use this share secret to decrypt the encrypted ballot. 1-out-of-L re-encryption is used to guarantee receipt-freeness. The proposed scheme is divided into registration, validation, vote casting and tallying phases. The security analysis of the scheme was then carried out to show its effectiveness.

General Terms

Electronic voting security

Keywords

Coercion, EDSA, ElGamal, Homomorphic Encryption, Receipt-freeness, Shamir Secret Sharing, Threshold Cryptosystem.

1. INTRODUCTION

In many democracies over the years, there has been decrease in the number of voters coming for election because of the inconvenient voting system and electoral fraud. Due to the fast development of computer technology and web application, many electronic voting systems (and internet voting systems) have been developed to eliminate the inadequacies associated with the conventional voting system. Electronic voting is the collection and wide spread of citizens' opinions with the help of some electronic means involving vote casting, ballot transmission, vote counting and auditing. Electronic voting has many advantages over the traditional way of voting. Some of these advantages are lesser cost, faster tabulation of results, greater accuracy, and lower risk of human and mechanical errors, it offers improved accessibility for the people with disabilities, and it provides multiple-language support for the ballots. Electronic voting will increase voter convenience and voter confidence in the accuracy of election results [5].

A secured e-voting system should not only satisfy requirements of completeness, privacy, non-reusability, eligibility, fairness, verifiability, and robustness, but also receipt-freeness and non-coercion. The notions of receipt-freeness and coercion were introduced to deal with vote-selling and coercion in e-voting systems in [4]. In [19] two threats were mentioned to address in a fair and democratic election process: voter coercion and vote buying. Internet-based voting does not introduce these problems, but it does have the potential to exacerbate them by extending the reach and data collection abilities of an attacker. In a voting system with coercers, a voting scheme must ensure that the voter should not be able to prove to a third party that he has cast a particular vote. Hirt [20] stated that he must neither obtain nor be able to construct a receipt proving the content of his vote (receipt-freeness).

In a real large-scale general election, some voters may decide not to vote after the registration phase. In this case, if the issue of votes is controlled by a single authority, he/she may add extra ballots as he/she wishes, sacrificing privacy and fairness of a secure e-election. To overcome this problem, the issue of votes must be controlled by multiple authorities. Electronic voting can only be secured using cryptography. It should be noted that deterministic cryptosystem like RSA (though very strong and secure) cannot be used to secure ballots effectively because it produces one long cipher text that an attacker can be able to construct by carefully studying it. Instead, a probabilistic encryption (that can produce several cipher text for one vote) should be used. Examples are ElGamal and Pailler which can be proven to be homomorphic.

For an e-voting system to be secure, it has to function effectively in potentially insecure environments such as the internet. In [8], the following requirements were asserted that any e-voting scheme must accomplish:

- **Privacy**: A system is private if neither election authorities nor anyone else can link any ballot to the voter who cast it and no voter can prove that he or she voted in a particular way.
- **Universal Verifiability**: provides the facility that anyone in the voting system should be able to in-dependently verify that all valid votes have been counted correctly.

- **Robustness**: The system is robust, if it ensures that all the system can recover from the faulty behaviour of any (reasonably sized) location of parties; i.e. Failure resulting from partial authorities or voters can be detected or tolerated.
- **Efficiency**: The computational loads must be light and able to be performed within a reasonable amount of time.
- **Eligibility**: Only the eligible voters, who pass the authentication process, can be allowed to vote.
- **Completeness:** It is unable to fake a vote, that is unable to remove a valid vote from the final tally, and unable to add an invalid vote to the final tally.
- **Uncoercibility (sic)**: No voter can be forced to vote in a particular way. Voters should not be able to prove their vote and how they voted to the coercer.
- **Receipt-freeness**: ensures that the voter can be convinced that his ballot is counted without getting a receipt.

  In [14], the author corroborates the above listed statements while adding the following ones:
- **Unreusability (sic):** No voter can vote twice.
- **Fairness:** Nothing must affect the voting. i.e., no intermediate election results can be known to anyone.

In this paper, a multi-authority electronic voting that will prevent electoral fraud caused by centralised voting systems and ensure fairness is proposed. ElGamal cryptosystem is probabilistic in nature and must be additive homomorphic for it to be suitable for e-voting. Election based on homomorphic encryption are not receipt-free, a 1-out-of-L re-encryption process on ElGamal cryptosystem was used along with homomorphic encryption to satisfy non-coercion and receipt-freeness.

The rest of this paper is organised as follows. Section 2 discusses related works. The architecture of the Receipt-free Multi-authority E-voting Scheme is presented in Section 3. Procedure for implementing e-voting system is described in Section 4. The security analysis is carried out in Section 5. The work is concluded in Section 6.

2. RELATED WORKS

Chaum [7] proposed the first voting scheme and introduced the concepts of mix-nets in an anonymous channel. The re-encryption net also based on anonymous channel was proposed by Jakobsson [17]. The concept of blind signatures was introduces in [6] that involves digitally authenticating and signing a message hidden from the signer (i.e. blinded). It significant feature is its “unlinkability”.

Cramer [11] proposed multi-authority secret sharing scheme based on homomorphic encryption. This scheme satisfies universal verifiability. With homomorphic property, let $E(v_1)$ and $E(v_2)$ be encryptions of ballots v_1 and v_2. Then, $E(v_1) \otimes E(v_2) = E(v_1 \oplus v_2)$ of the “sum” of the votes.

Cohen and Fischer [10] proposed a robust and verifiable cryptographically secure election scheme based on a r-th residuosity assumption. Wang [33] proposed an electronic voting scheme based on blind signature that distributes the powers to more administrators, but, if the voting center is not trustful and IP trace between the voting center and voters is available, then, the proposed scheme will be easily forgeable.

The first scheme claimed to be receipt-free was proposed by Benaloh and Tuinstra [4], although it was later shown to be not [19]. Okamoto [27] proposed a scheme with receipt-freeness that makes use of blind signatures. It assumes the existence of an anonymous untappable channel and requires three times of voter and system interaction in the course of an election. That is, they require every voter to participate even in the tallying phase. Sako and Kilian [30] proposed an e-voting scheme with multi-authority using mix-net and homomorphic encryption, which is postulated to be receipt-free Even though its receipt-freeness cannot be guaranteed under the commonly used assumption that only one mix center is honest, it served as a basis for the later work of [19] and a more efficient approach in [2]

Juels [19] proposed a receipt-free voting scheme, which is one of the most efficient and practical schemes to date. It only requires one of the tallying authorities to be honest for providing receipt-freeness while the ballot secrecy depends on the anonymous channel and the honesty of at least one among the group of the registrars (entities responsible for registration) and tallying authorities. In addition, it can even provide a stronger form of receipt-freeness, called as coercion resistance, which defends against randomization, forced abstention and simulation attacks (details can be found in [19]). However, coercion-resistance does not allow the voters to verify whether their votes have been counted (i.e., no universal verifiability). An independent introduction of the idea appeared in [26].

Okamoto [27] proposed a voting scheme which he himself later showed to lack the postulated receipt-freeness. He later presented an improved version of the previous work using blind signatures. Sako and Kilian [30] proposed a multi-authority scheme employing a mix network to conceal candidate choices, and a homomorphic encryption scheme for production of the final tally. The modelling of their scheme was clarified and refined by Michels and Horster[23]. The Sako and Kilian scheme served as a conceptual basis for the later work of [20], the most efficient (and correct) receipt-free scheme voting to date. A recenly proposed scheme by [22] had the support of tamper-resistant hardware, but has been flawed.

Wei [35] recognized that Groth’s schemes do not satisfy receipt-freeness for a voter can exploit the randomness she chooses in encryptions or commitments to construct a receipt. In their paper, a receipt-free variant of the limited vote election protocol was constructed. A third party called “randomizer” is employed to re-encrypt the votes and to mask the commitments made by the voters while preserving the validity of the votes. The construction is generic and can be easily modified to introduce receipt-freeness into other types of Groth's e-voting schemes.

Magkos [22] proposed a receipt-free e-voting scheme based on the virtual voting booth that is implemented with a smart card. Receipt-freeness is achieved by distributing the voting procedure between the voter and the smart card. The voter and the smart card jointly contribute randomness for the encryption of the ballot. However, Magkos Burmester-Chrissikopoulos' e-voting scheme must assume that the briber or the coercer does not monitor the voter during the every moment of voting, which is clearly unreasonable, i.e., it cannot effectively prevent bribe and coercion in practical environments.

Juang et al. [18] proposed a robust and verifiable multi-authority secret voting scheme which meets the requirements of large-scale general elections. This scheme uses a uniquely blind threshold signature scheme to get blind threshold electronic votes such that any voter can abstain from voting after the registration phase. It also uses the threshold cryptosystem to guarantee fairness among the candidates' campaigns and to provide a mechanism for ensuring that any voter can make an open objection to the tally if his vote has not been published. In this scheme, the computations among voters are independent and voters only have to send an anonymous message to the counter after the registration phase. This scheme preserves the privacy of a voter from the counter, administrators, scrutineers and other voters. Completeness, robustness and verifiability of the voting process are ensured and hence no one can produce a false tally or corrupt or disrupt the election.

Wei-Chi et al. [35] described an e-voting scheme that can solve or at least lessen the problems of bribe and coercion, and can be realized with current techniques. By using smart cards to randomize part content of the ballot, the voter cannot construct a receipt. By using physical voting booths, bribers and coercers cannot monitor the voter while he votes. Unlike conventional voting systems, the voter of the proposed scheme can choose any voting booth that is convenient and safe to him. Michael [23] described Civitas as the first electronic voting system that is coercion-resistant, universally and voter verifiable, and suitable for remote voting. Their paper describes the design and implementation of Civitas. Assurance is established in the design through security proofs, and in the implementation through information-flow security analysis. Experimental results give a quantitative evaluation of the tradeoffs between time, cost, and security.

Orunsolu [28] presented an agent-based architecture for e-voting. They used elliptic curve and digital signature to increase integrity of communication of election details within the layers in the scheme. The architecture was based on the notion of completeness, privacy, non-coercion, verifiability and fairness. Chinniah [8] described a new multi authority electronic voting scheme based on elliptic curves is proposed. According to the proposed scheme, each voter casts the vote as a point on the elliptic curve and the final tally is computed with the assistance of multiple authorities. A trusted centre is involved in the scheme to distribute the shared secret key among the authorities and the Shamir (t, n) threshold scheme is used for key distribution. The proposed scheme also meets the essential requirements of e-voting system. Ultimately, the proposed voting scheme fortifies the security properties of the electronic voting procedure, since the secrecy of the particularized vote is preserved by ElGamal cryptosystem and Elliptic curve discrete logarithm problem.

The scheme [8] does not satisfy receipt-freeness despite the use of EC-ElGamal (very difficult to crack). In our paper, re-encryption of the ballot cipher text is used so that no one would be able to construct a receipt. Also, modified ElGamal (homomorphic) was used instead of the elliptic curves in [8].

3. THE PROPOSED E-VOTING SCHEME

3.1 Cryptographic Primitives

3.1.1 ElGamal Cryptosystem

The ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key agreement protocol. It was described by Taher Elgamal [12]. It has the advantage that same plaintext gives a different cipher text (with near certainty) each time it is encrypted. The probabilistic ElGamal public-key scheme is commonly used in electronic voting schemes.

Let G be a multiplicative group of prime order q with generator g. The private key x is chosen at random from Zq to compute $y = g^x mod\, p$ and the corresponding public key is (p, g, y). Given a message m ε G, the encryption of m is given by $(a, b) = (g^r, y^r m)$ in mod p for a randomly chosen r ε Zq. To decrypt the cipher text (a, b), compute the plaintext $m = \frac{b}{a^x} mod\, p$ using private key x because $\frac{\mathrm{b}}{\mathrm{a^x}} \text{ mod p} = \frac{\mathrm{y^k m}}{\mathrm{g^{kx}}} \text{ mod p} = \frac{\mathrm{g^{kx} m}}{\mathrm{g^{kx}}} \text{ mod p} = \text{m mod p}$

3.1.2 Homomorphic Encryption

Generally, e-voting schemes require a probabilistic cryptosystem that is homomorphic. Let operation ⊕ be defined on the message space and an operation ⊗ be defined on the cipher space, such that the "product" of the encryptions of any two votes v_1, v_2 is the encryption the "sum" of the votes i.e. E (v_1)⊗ E(v_2)=E (v_1 ⊕ v_2). Examples of homomorphic cryptosystems are the additive version of ElGamal and Paillier. ElGamal by nature is homomorphic with multiplication**:** For cipher texts $(a_1, b_1) = (g^{r1}, y^{r1}. m_1)$ and $(a_2, b_2) = (g^{r2}, y^{r2}. m_2)$ Then, is an encryption of $m_1.m_{2.}$ Since $E(m_1)E(m_2) = (a_1, b_1).(a_2, b_2) = (a_1. a_2, b_1. b_2)$

$$= (g^{r1}. g^{r2}, y^{r1}\, m1 . y^{r2}\, m2)$$

$$= (g^{r1+r2}, y^{r1+r2}.m_1 m_2 = E(m_1.m_2)$$

The encrypted votes are summed using the homomorphic property of the encryption function (without decrypting them). Finally, a set of trustees cooperate to decrypt the final tally (the secret key for the encryption scheme is divided between the trustees). The advantages of using homomorphic schemes are efficiency and verifiability: many operations can be carried out on the encrypted votes, in public, so they are both verifiable and can be performed during the voting process (without interaction between the voting authorities) [25].

3.1.3 Additive Homomorphic Encryption

As shown above, ElGamal is only homomorphic with multiplication, the cipher text needs to be modified slightly to make it additive homomorphic or practical groups can be obtained from elliptic curves over finite fields. The discrete logarithm problem for elliptic curves is considered to be harder. Consider the homomorphic property of EC-ElGamal,

Suppose $(C_1, C_2) = (r.e_p,\ m + r.(d.e_p))$ and $(C_1^1, C_2^1) = (r^1.e_p,\ m^1 + r^1.(d.e_p))$ are encryptions of messages m and m^1, then is an encryption of m+m^1 since

$$\begin{aligned}&(C_1, C_2) + (C_1^1, C_2^1) = (C_1 + C_1^1, C_2 + C_2^1)\\&= (r.e_p + r^1.e_p,\ m + r.(d.e_p) + m^1 + r^1.(d.e_p))\\&= ((r + r^1)e_p,\ (m + m^1) + (r + r^1)(d.e_p))\end{aligned}$$

The modified additive ElGamal scheme was used in this paper because it is simpler to implement rather than EC-ElGamal It will be is explained in section 3.2.3

3.1.4 Robust Threshold ElGamal Cryptosystem

According to [29], the purpose of threshold public-key cryptosystem is to share a private key among the authorities such that messages can be decrypted only when a substantial set of authorities cooperate. We need to change the key generation and the decryption protocol in the ElGamal cryptosystem. Messages will be encrypted as usual.

Key generation: The result of the key generation protocol is that each authority Aj will possess a share s_j of a secret s (a private key in the ElGamal cryptosystem) and the public key will be made public. The authorities are committed to their shares as the values $h = g^{s_j}$ are published. Furthermore, the shares s_j are such that the secret s can be reconstructed from any set of t+1 share. Any set of at most t shares can tell nothing about the secret s. To achieve this, Shamir's (t + 1, N) secret sharing scheme is used. Trusted third party is needed to compute and distribute these shares to authorities using untappable channel (key generation protocol without the trusted third party is presented [15]. Thus, it holds

$$s = \sum_{j\varepsilon A} s_j\, \lambda_{j,A} \text{ where } \lambda_{j,A} = \prod_{l\varepsilon A-\{j\}} \frac{L}{L-j}$$

The public key is (p, g, h), where $h = g^s$

Decryption: To decrypt a cipher text $(x, y) = (g^k, h^k m)$ without reconstructing the secret s, the authorities execute the following protocol:

1. Each authority A$_j$ broadcasts $w_j = x^{s_j}$ and proves in zero-knowledge that $\log_g h_j = \log_x s_j$
2. Let A is any set of (t+1) authorities who passed the zero-knowledge proof.

   The plaintext can be recovered as $m = \frac{y}{x^s}$

$$x^s = \sum_{j\varepsilon A} s_j\, \lambda_{j\varepsilon A} = \prod_{j\varepsilon A} w^{\lambda_{j\varepsilon A}}$$

At most t authorities' secrets s_j can be disclosed, as from the t +1 known values s_j a secret key s can be computed (using Lagrange interpolation), and the message can be directly recovered as in ElGamal decryption.

3.2 Architecture of the proposed E-voting scheme

Before the election process, some things need to be put in place (initial stage). Each party needs to register its candidate that will partake in the election with a trusted centre like one or two months before the stipulated time. The use of a single authority will sacrifice fairness in an election. A dishonest administrator can take advantage of his power to cast false votes. The election counter cannot distinguish between an eligible (or legitimate) vote from the one from an administrator because the votes cast is encrypted to ensure privacy The only way to detect the administrator is if the number of votes counted in the election is more than those that registered. Alternatively, the administrator can prohibit them from voting so that he can vote multiple times. In a real large-scale general election, some voters may abstain from voting after the registration phase. In this case, if the issue of votes is controlled by a single administrator, he/she may add extra ballots as he/she wishes. To overcome this problem, the issue of votes must be controlled by several administrators. [18] The solution to this problem is to employ a multi-authority voting scheme that will improve the security and fairness of the election so that a single authority cannot determine the overall election since he cannot decrypt the votes alone.

This scheme uses M voters *V1*, …, V_M, N authorities A_1, …, A_N, election candidates and a trusted centre that registers every one of them. The trusted centre's duty is to register them and verifies the election process, he cannot do the tallying. The Trusted centre shares the secret key among t-authorities. Each authority will compute $h_j = a^{x_j}$ from its x$_j$ share; this will be used to check if the authority passed the Zero knowledge proof before decryption of vote. The proposed e-voting scheme is divided into four major phases: Registration, Validation, Casting and Tallying.

The architecture of the proposed e-voting scheme is presented in Figure 1.

3.2.1 Registration Phase

Prior to the election, voters will have to prove their identity and eligibility. An electoral roll is created. The Trusted centre checks for the eligibility of each voter. The age of each person is checked and the national registration database to ensure he/she is not involved in crime before registration. All voters' information is sent to a database acting as the voters register which is kept safe by the trusted centre. Also, biometric features like fingerprint or face recognition can be very useful during registration of voters. The voter will provide a username along with a pass code that is randomly generated by the computer to log-in during the validation phase. This pass code is secured with a hash function such as SHA or MD5 to prevent any communications tampering and forgery. Therefore, the eligible voter must ensure that the username and pass code are safe. This will be used during the validation phase.

3.2.2 Validation Phase

During the election, voters are authenticated before casting their vote. This is similar to manual voter's verification in the traditional system of voting to ensure that the registration numbers are confirmed on the voters register. Each voter will have to supply the pair of username and pass code. When a voter is authenticated, he can now vote for the candidate of his choice, otherwise, he will be denied access. It should be noted that only one vote per voter is allowed in this e-voting system.

3.2.3 Vote Casting Phase

Voters cast their vote. Each voter's choice is directly transferred to the tallying phase. In this phase, we want to ensure anonymity, non-coercion and receipt-freeness. Anonymity ensures that each vote cannot be linked to the person that cast it. When there is receipt-freeness and no coercion, the voter will not be able to prove to the coercer the way he voted or to receive a receipt (bribe). The best way to do this is by encryption. Modified ElGamal cryptosystem that is additive homomorphic and satisfies threshold cryptography will be used. Each voter's ballot is digitally signed with EDSA (ElGamal DSA) and encrypted with the additive ElGamal scheme. The election counter verifies the ballot, and if it passes this stage, it will accept the voter's ballot because it is coming from the right source (to ensure non-repudiation of origin). The authorities monitor the voting process.

3.2.3.1 ElGamal DSA

$$sig(m, k) \; = \; (a, b)$$

$a \; = g^k \; mod \, p$ and $b \; = \; (m - \, x.a) \; (k^{-1} \; mod \; (p - 1)$

$$ver \; (m, a, b) => \; a^b \, . \, y^a \;\; = \; g^m \; mod \, p$$

3.2.3.2 Modified Additive Homomorphic ElGamal

Let G be a commutative group of order $|G| = q$, where q is a large prime. G can be constructed as a subgroup of Z_p^*, where p is a large prime. Let g be a generator of G, i.e. $G = \{g\}$ .The secret key x is chosen uniformly from Zq, and the public key is $h = g^x$. The key pair (x, h) is constructed in a way that each authority receives a share x_i of x in a (t, N)-threshold secret-sharing scheme and is publicly committed to this share by $h_i = g^{x_i}$. Also, γ is another (independent) generator of G. The set v of valid votes contains L values in Zq. An encryption of a vote $v \varepsilon V$ is given by $E(v) = (g^k, \, \gamma^v h^k)$, where ${}_R Zq$ is a random number and γ^v is the "message" in the context of ElGamal. γ^v is used instead of v in the cipher text. The secret key z is shared among the authorities such that any $t - 1$ authorities cannot compute z. Violating the secrecy of the scheme would mean to either break ElGamal or the secret-sharing scheme.

$$E(v_1)E(v_2) = (a_1, b_1).(a_2, b_2) = (a_1 a_2, \, b_1 b_2)$$

$$= (g^{k1}. g^{k2}, \gamma^{v1} h^{k1}. \gamma^{v2} h^{k2})$$

$$= \; (g^{k1+k2}, \gamma^{v1+v2}. h^{k1+k2}) = E(v_1 + v_2)$$

3.2.3.3 Proposed threshold ElGamal cryptosystem

Suppose the key generation protocol of Pedersen [20] is used to share x among those N servers. After the protocol is carried out successfully, each tallying authority t (1 ≤i≤ N) will get a share x ε Zq of the secret x, and has a commitment of its share computed as $h_i = g^{x_i}$ which is broadcast to other servers. The (group) public key is $h \; = g^x$. The secret x can be computed from any set A of size t as below:

$$x = \sum_{\mathrm{j\varepsilon A}} x_j \, \lambda_{j,A} \;\; \text{Where} \;\; \lambda_{j,A} = \prod_{\mathrm{L\varepsilon A-\{j\}}} \frac{\mathrm{L}}{\mathrm{L-j}}$$

The public key is (p, g, h), where is $h \; = g^x$

This is a Shamir (t, N)-threshold secret sharing, any set of less than t servers cannot recover the secret x. The cipher text is $(a, b) \; = \; (g^k, \gamma^v. h^k)$

3.2.3.4 1 – Out –Of- L Re-encryption

It is re-encryption technique that can be used to deal with coercion. The cipher text (a, b) produced will be re-encrypted. Let (a^1, b^1) be an encrypted vote of (a, b) is given by

$(a^1, b^1) = (g^\alpha \, . \, a, h^\alpha \, . \, b)$ for a random integer α ε ${}_R Zq$.

Clearly, if α is chosen uniformly in Zq, then (a^1, b^1) is uniformly distributed. 'α' serves as a witness of re-encryption. The re-encryption technique is the method that can be used to achieve a receipt free election because he can neither obtain nor be able to construct a receipt proving the content of his vote.

3.2.4 Tallying Phase

In this phase, all encrypted votes for all voters are decrypted and counted since each vote is sent to this phase for n-voters. At the end of the election process, there is need for audit trail where voters' results are verified by the trusted centre and the whole result is made known. The authenticator publishes the list containing the encrypted ballots and the ballot ID. The election counter publishes its version of the same list and the verifier confirms that these lists are identical to ensure fairness.

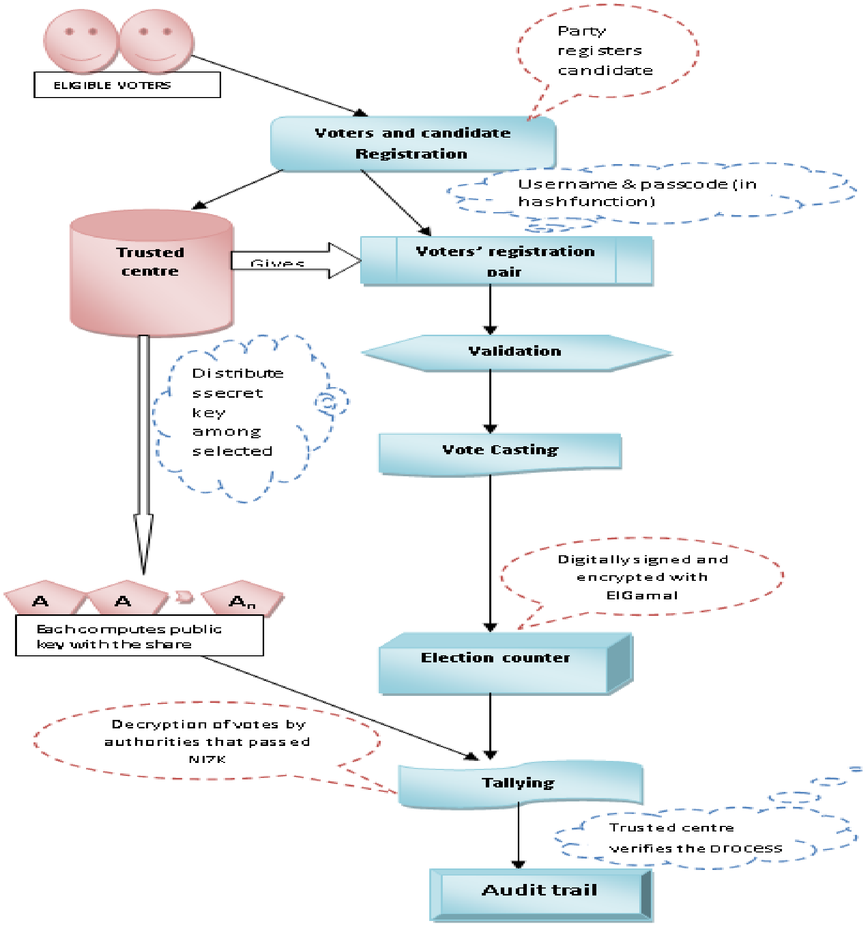
ELIGIBLE VOTERS
Party registers candidate
Voters and candidate Registration
Username & passcode (in hashfunction)
Trusted centre
Gives
Voters' registration pair
Validation
Distribute ssecret key among selected
Vote Casting
Digitally signed and encrypted with ElGamal
A
A
A_n
Each computes public key with the share
Election counter
Decryption of votes by authorities that passed NIZK
Tallying
Trusted centre verifies the process
Audit trail

Figure 1: ARCHITECTURE OF MULTI-AUTHORITY E-VOTING

3.2.4.1 Decryption

1. First thing to do is to decipher the re-encrypted vote by recovering (a, b) from (a^1, b^1) by $(a^1, b^1) = (g^\alpha . a, h^\alpha . b)$, since it is a discrete logarithm problem, we need to find an inverse to get (a, b), all computations will be in *mod p*. i.e.

$$a = a^1 . g^{-\alpha} \; mod \; p \qquad\qquad b = b^1 . g^{-\alpha} \; mod \; p$$

2. In order to verify correctness of ballots, each ballot must be accompanied by a zero-knowledge proof, proving that the ballot is an encryption of a legal value. Zero-knowledge proofs are essential parts of any homomorphic election system. Let A ε A_n represents the authorities that passed the zero-knowledge proof, each authority A_j broadcasts $w_j = a^{x_j}$ and proves in zero-knowledge that $\log_g h_i = \log_a x_j$

3. To decrypt a cipher text $(a, b) = (g^k, \gamma^v . h^k)$ without reconstructing the secret x. Let A is any set of t authorities who passed the zero-knowledge proof.

The plaintext can be recovered as $\gamma^v = \frac{b}{a^x}$

$$a^x = \sum_{j\varepsilon A} x_j \, \lambda_{j\varepsilon A} = \prod_{j\varepsilon A} w^{\lambda_{j\varepsilon A}}$$

To compute ballot v from γ^v is also a discrete problem which can only be solved if v is of moderate size. This can be solved if the candidates C_1, ... , C_n is encoded with a small value before encryption. Let $R = \gamma v$, then the ballot can be computed by

From discrete algebra, $R = \gamma v$ implies $v = \log_\gamma R$

So, the ballot is finally decrypted to get our vote.

After the decryption of votes; the authenticator publishes the list containing the encrypted ballots and the ballot ID, the counter publishes its version of the same list and the verifier confirms that these lists are identical. The trusted centre will verify the whole process and send it to the audit trail where the result will be published.

4. STEPS TO IMPLEMENT AN E-VOTING SYSTEM

I-voting will become fully electronic (from registration to tallying) only when a secure and uniform Public Key Infrastructure for digital signatures becomes available. Accuracy and privacy over the Internet should be protected with strong digital signatures and encryption techniques. Browsers that allow both the encryption and digital signing at the browser level should be designed. Furthermore, technologies such as Secure Socket Layer (SSL) and digital certificates should be adopted to deal with spoofing attacks [5].

The proposed e-voting architecture can be implemented with any object oriented programming language like Java, C#, PHP, VB.Net by creating a secure e-voting web application. The encryption algorithm that protects vote is on the server machine, the communication with clients using browsers need to be secured with the SSL technology. Java applet is advised to be used for vote casting (encryption of votes) and tallying (decryption) for two reasons: Java is more secured and it is platform independent (can be used on any operating system unlike C#). Though C# could be easier to program and provide more robust and beautiful interface but our concern is its accessibility to voters online regardless of their OS rather than Microsoft OS and its security (Java applet is secured). We need the following web pages or modules;

Candidate registration: Each party registers their candidates with the trusted centre.

Authority registration: The trusted centre registers each authority that will supervise the election and share the secret key with threshold cryptosystem.

Voter registration: each voter registers with the trusted centre in an interface. The voting system should allow only eligible voters (someone that is less than 18years and/or is involved in crime cannot register or vote). Each voter will have a unique username and pass code that will be encrypted with MD5.

Voter's validation: An interface that will authenticate each user is created. Voters (username, pass code) pair will be compared with the one in the database to authenticate users on the Election Day.

Vote Casting: After authentication, the voter casts his/ her ballot which is encrypted and digitally signed with ElGamal and re-encrypted to ensure receipt freeness. The votes move to the election counter (database) where the legitimacy of the vote is determined. If it is not from an eligible voter, the ballot is rejected. The authorities monitor the process.

Vote tallying: The voting system will stop the election after a specified time; all the votes are decrypted by the authorities that pass the zero-knowledge proof; it is counted and posted to the audit trail.

5. SECURITY ANALYSIS AND PERFORMANCE MEASUREMENT

In this section, we will show that the proposed e-voting scheme is secure, i.e., it satisfies completeness, privacy, No vote duplication, eligibility, fairness, verifiability, receipt-freeness, and non-coercion.

1. *Completeness*: No fake vote and sum of valid ballots are accurately counted in the proposed e-voting scheme.

Proof: All encrypted ballots posted on the bulletin board or database cannot be erased and any party can verify the validity of the ballots. Therefore, no valid encrypted ballot posted on it can be removed and invalid ballots cannot be added. Due to the homomorphic properties of the ElGamal encryption method, the final tally is the sum of all valid ballots (all ballots are accurately counted). Hence, the proposed e-voting scheme satisfies completeness.

2. *Privacy:* In the proposed e-voting scheme, all ballots are secret (not linked to voters)

Proof: Since the ballot is encrypted with the public key shared by the voting authorities, the encrypted ballot cannot be individually decrypted from its corresponding ballot. This can only be done by using the private key jointly shared by voting authorities with a robust threshold cryptosystem. ElGamal of probabilistic encryption produces several cipher text for a single vote. Therefore, decryption can be performed only by t-authorities that passed the zero-knowledge proof. Therefore, the proposed e-voting scheme ensures privacy.

3. *No vote duplication:* in the proposed e-voting scheme, a voter can vote twice.

Proof: Once a voter cast his votes, he has a record in the database; any attempt to vote the second time, his additional encrypted ballot will be rejected because it cannot enter the database. In addition, since each encrypted ballot should be accompanied with a proof that it contains a valid ballot, he cannot cast an encrypted ballot containing an invalid value. Therefore, the proposed e-voting scheme satisfies 'no vote duplication'.

4. *Eligibility:* In the proposed e-voting scheme, only eligible voters can vote.

Proof: The voter's identity must be registered and checked before he/she can enter the voting booth. Everyone can verify that the voter who has cast a ballot is included in the list of all eligible voters.

5. *Fairness*: No one can know the intermediate results of the voting in the proposed e-voting scheme.

Proof: An attacker can decrypt the ballot messages only if, he/she has the knowledge of the secret Key, "x" of the system and how to recover "x". In this case, if the votes are controlled by a single administrator, he/she may add extra ballots as he/she wishes. To overcome this problem, the issue of votes was controlled by several administrators. Hence, no one can learn partial results of an election and the entire voted ballots are kept secret until the end of the voting process. The final tally is obtained; only by the voting authorities that passed the zero-knowledge proof. A single authority or the trusted centre cannot do tallying.

$$\frac{b}{a^x} = \frac{\gamma^v . h^\propto}{(g^\propto)^x} = \gamma^v$$

Then the authorities will find T using discrete logarithm approach. Hence, the proposed e-voting scheme provides fairness to voters.

6. *Universal verifiability and Correctness*: In the proposed e-voting scheme, the public can verify the voting system.

Proof: The final ballot and the proof of validity are posted on the bulletin board and hence, anyone can verify the validity of the final ballots, the correctness of the ballot collection and the final result. Thus, valid votes are counted correctly.

7. *Receipt-freeness*: In the proposed e-voting scheme, the voter cannot reveal his ballot to others.

Proof: 1-out-of-L re-encryption scheme is used to ensure that no one is able to construct a receipt and no voter can prove how he/ she have voted. By encrypting an encrypted ballot, it will be difficult to construct a receipt. In addition, the voter must be given a proof of correctness of the encryption performed by the voting booth before the encrypted ballot is submitted to the bulletin board. $(a^1, b^1) = (g^\alpha . a, h^\alpha . b)$ for a cipher text, $(a, b) = (g^k, \gamma^v . h^k)$

Hence, the proposed e-voting scheme satisfies receipt-freeness.

8. *Non-coercion*: In the proposed e-voting scheme, a voter cannot be coerced into casting a particular ballot by a coercer.

Proof: By employing voting booths with guards, no one can monitor the voting process of others. Thus, the only way for the coercer to know the content of a ballot is checking its voter's receipt. Since the proposed voting scheme satisfies receipt-freeness, non-coercion is also satisfied.

Theorem: The proposed e-voting scheme is secure.

6. CONCLUSION AND FUTURE WORK

Many countries have not fully implemented e-voting systems because of the associated security challenges. Any little security flaw in the design of a secure e-voting can cause a very severe electoral fraud more than the conventional voting system. In our proposed scheme, we have ensured that all the requirements to design a secure e-voting are kept in mind. The scheme ensures eligibility, completeness, privacy, efficiency, universal verifiability, no vote duplication, non-coercion and receipt-freeness. The scheme is also practical to be used for real election.

It might be necessary for researchers to look at the implications of multi-authority scheme on the overall voting process. It is also necessary for researchers to develop methodology for assessing the usability of e-voting scheme by countries in which larger percentage of the population are ICT-illiterates.

7. REFERENCES

[1] Baraani-Dastjerdi A., Pieprzyk, J. and Safavi-Naini, R. 1995, A practical electronic voting protocol using threshold schemes, In Proc. 11th Ann. Computer Security Applications Conf., New Orleans, LA, December, pp. 143–148. IEEE Computer Security Press.

[2] Baudron O., Fouque P. A., Pointcheval D., Poupard G., and Stern J. 2001, Practical multi-candidate election system, Distributed Computing Journal 2001, pages 274–283, ACM Press.

[3] Benaloh, J. 1987, Verifiable Secret-Ballot Elections. PhD Thesis, Yale University.

[4] Benaloh, J., and Tuinstra, D. 1994, Receipt-Free Secret-Ballot Elections", In 26th Annual ACM Symposium on Theory of Computing, ACM, pp. 544-553.

[5] Burmester M., Magkos E. 2003, Towards Secure and Practical e-Elections in the New Era (chapter) In: Advances in Information Security- Secure Electronic Voting, Kluwer Academic Publishers pp.63-76.

[6] Chaum, D. 1982, Blind Signatures for Untraceable Payments, In CRYPTO '82, Plenum Press, pp. 199-203.

[7] Chaum, D. 1981, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. In Communications of the ACM, 24(2), pp. 84-88.

[8] Chinniah P., Ramalingam A., and Krishnasamy V. 2010, Multi-authority Electronic Voting Scheme Based on Elliptic Curves. PSG College of Technology Peelamedu, Coimbatore, Tamilnadu- 641 004, India International Journal of Network Security, Vol.12, No.2, PP.84-91

[9] Chow S. M., Liu J. K. and Wong D. S. 2008, Robust Receipt-Free Election System with Ballot Secrecy and Verifiability. In proceedings of Network and IT Conference: NDSS 2008.

[10] Cohen J. and Fischer M. 1985, A robust and verifiable cryptographically secure election scheme, Proceedings of 26th IEEE Symposium on Foundations of Computer Science (FOCS '85), pp. 372-382,

[11] Cramer, R., Gennaro, R., and Schoenmakers, B. 1997, A Secure and Optimally Efficient Multi-Authority Election Scheme. In EUROCRYPT '97, LNCS 1233, Springer-Verlag, pp. 103-118.

[12] El Gamal T. 1985, A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31:469-472, 1985.

[13] Fujioka, A., Okamoto, T., and Ohta, K. 1993, A Practical Secret Voting Scheme for Large Scale Elections. In AUSCRYPT '92, LNCS 718, Springer-Verlag, pp. 244-251.

[14] Geir R. 2004, Remote Electronic Voting. Universitas Bergensis

[15] Gennaro R., Stanislav J., Hugo K., and Rabin T. 1999, Secure distributed key generation for discrete-log based cryptosystems". EUROCRYPT'99.

[16] Ibrahim S., Kamat M., Salleh M., Rizan S. and Aziz A. 2004, Secure E-Voting With Blind Signature. University

Technology Of Malaysia, 81310 Skudai, Johor Bharu, Johor, Malaysia.

[17] Jakobsson, M. 1999, Flash Mixing. In 18th ACM Symposium on Principles of Distributed Computing PODC '99, ACM, pp. 83-89.

[18] Juang W., Lei C. and Liaw H. 2002, A Verifiable Multi-Authority Secret Election Allowing Abstention from Voting. British Computer Society

[19] Juels A., Catalano D., and Jakobsson M. 2005, Coercion-resistant electronic elections. In WPES 2005, pages 61–70. ACM Press.

[20] Hirt M. and Sako K. 2000, Efficient receipt-free voting based on homomorphic encryption. In B. Preneel, editor, EUROCRYPT '00, pages 539-556, LNCS no. 1807.

[21] Liaw H. T. (2004). A secure electronic voting protocol for general elections. Computers & Security, vol. 23, no. 2, pp. 107-119.

[22] Magkos E., Burmester M, and Chrissikopoulos M. 2001, Receipt-Freeness in Large-Scale Elections without Untappable Channels, Proc. 1st IFIP Conference on E-Commerce / E-business /E-Government, pp.683–693, Kluwer Academics Publishers.

[23] Michael R. C., Stephen C. and Andrew C. M. 2008, Civitas: Toward a Secure Voting System Department of Computer Science, Cornell University.

[24] Michels M. and Horster P. 1996, Some remarks on a receipt-free and universally verifiable mix-type voting scheme. In K. Kim and T. Matsumoto, editors, ASIACRYPT '96. Springer-Verlag, LNCS no. 1163.

[25] Moran T. and Naor M. 2006, Receipt-Free Universally-Verifiable Voting With Everlasting Privacy. In proceedings CRYPTO, pages 373-392. Springer-Velag.

[26] Niemi V. and Renvall A. 1994, How to prevent buying of votes in computer elections. In J. Pieprzyk and R. Safavi-Naini, editors, ASIACRYPT '94, pages 164 -170. Springer-Verlag, LNCS no. 917.

[27] Okamoto T. 1997, Receipt-free electronic voting schemes for large scale elections. In B. Christianson et al., editor, Security Protocols Workshop, pages 25-35. Springer-Verlag, LNCS no 1361.

[28] Orunsolu, A. A., Sodiya, A. S.,Onashoga, S. A. 2010, An Agent-based framework for secure e-voting, In proceedings of Nigeria Computer Society (NCS) Conference, pp 181-186.

[29] Rjaskova, Z. 2002, Electronic Voting Schemes. Comenius University, Bratislava

[30] Sako K. and Kilian J. 1995, Receipt-free mix-type voting scheme - a practical solution to the implementation of a voting booth. In L. Guillou and J.-J. Quisquater, editors, EUROCRYPT, pages 393-403. Springer-Verlag, 1995. LNCS no. 921.

[31] Schoenmakers B. 1999, A simple publicly verifiable secret sharing scheme and its application to electronic voting. In M. Wiener, editor, CRYPTO '99, pages 148-164. Springer-Verlag, LNCS no. 1666.

[32] Shamir A. 1979, How to share a secret, Communications of the Association for Computing Machinery, 22(11):612-613.

[33] Wang L., Guo J., and Luo M. 2006, A more effective voting scheme based on blind signature, International Conference on Computational Intelligence and Security, pp. 1507-1510.

[34] Wei-Chi K. and Chun-Ming H. 2004, An e-Voting Scheme with Improved Resistance to Bribe and Coercion. Taiwan: Catholic University, Taipei.

[35] Wei H., Chen K. and Zheng D. (2009) "Receipt-Freeness for Groth’s e-Voting Schemes", Shanghai Jiaotong University, Shanghai, 200240 P.R. China