A new secure and practical electronic voting protocol without revealing voters identity

Sadegh Jafari
Computer Engineering Department
Islamic Azad University, Zanjan Branch
Zanjan, Iran
jafari.s66@gmail.com

Jaber Karimpour
Computer Engineering Department
Tabriz University
Tabriz, Iran
karimpour.jaber@gmail.com

Nasour Bagheri
Electrical Engineering Department
Iran University of Science and Technology
Tehran, Iran
n_bagheri@iust.ac.ir

***Abstract*— E-voting systems are important tools for community participation in essential decisions of society. In comparison with traditional voting systems, e-voting systems have special advantages. Any e-voting system is based on an e-voting protocol. In this paper, a new secure and efficient e-voting protocol is proposed based on ElGamal cryptosystem which provide all security requirements of a practical electronic voting. One of the new properties of proposed protocol is protection of voter's identity against Authorities and adversary by using implementable physical assumptions. In this protocol, each voter distributes his/her secret key among the election Authorities and finally eligible voters are recognition from their public key. Also due to having low communication volume, the proposed protocol is suitable for internet voting and communication networks with less bandwidth.**

Keywords-component; Electronic Voting; ElGamal Cryptosystem; Homomorphic Encryption; Voter's Certificates, Voter's Identity.

I. INTRODUCTION

E-voting may provide many benefits to democratic societies. It may increase elections turnouts, afford convenience to the voters, and reduce costs, for instance. Any e-voting protocol must meet certain requirements. These requirements are divided into two categories: basic security requirements and extended security requirements.

Achieving the basic security requirements is necessary for each e-voting protocol and any protocol without these features is useless. The basic security requirements are:

- ***Eligibility:*** Only eligible voters can take part in voting and every voter can cast only one vote.
- ***Privacy:*** The fact that a particular voter voted in a particular way is not revealed to anyone.
- ***Individual verifiability:*** Each eligible voter can verify that his/her vote was really counted [21].
- ***Accuracy:*** Voting protocols must be error-free. The votes must be correctly recorded and tallied. Votes of invalid voters should not be counted in the tally.
- ***Fairness:*** No early results can be obtained which could influence the remaining voters.
- ***Robustness:*** Each voting protocol should be resistant against the attacks of active/passive corrupt authorities, voters and others. In addition, no coalition of voters and deceptive voter can disrupt the elections.

On the other hand, achieving the *extended security requirements* is important. These requirements are**:**

- ***Universal verifiability:*** After the counting result was announced, anyone can review functioning of all voting processes and the announced final result [21].
- ***Receipt-freeness:*** The voter cannot produce a receipt to prove that his/her vote's is special ballot. [5].
- ***Coercion-resistance:*** An extrinsic agent cannot influence the vote of a voter [12].
- ***Hiding voter's identity:*** The identity of those who have participated in election should be secret to all persons, even Authorities of elections. This makes each voter to decide about his/her or herself participation in elections [18].

Any e-voting system is based on an e-voting protocol. E-voting promises the possibility of a convenient, efficient and secure facility for recording and tallying votes. It can be used for a variety of types of elections, from small committees or on-line communities through to full-scale national elections. E-voting protocols are formal protocols that specify the messages sent between the voters and administrators.

In many designed e-voting protocols are used from hard physical assumptions to accomplish receipt-freeness and coercion-resistance. For example, in protocols [3, 7, 17] voting booth is used; in [10] and [21] untappable private channel are used; secret communication channel and smart cards are used in the protocol [4]; in [7] and [8] visual cryptography is used; the protocol [13] used from tamper-resistant randomizer etc. Some of these assumptions are not implementable and some others have challenging and are not acceptable to all participants in elections.

Recently, some e-voting protocols have weak physical assumptions. Juels and Jakobsson(JJ) [11] proposed a receipt-freeness and coercion-resistance protocol that requires anonymous channel at some point during the voting process. Later Juels et al.(JCJ) [12] presented a new version of the protocol. Their protocol is based on Mix Net, plaintext equivalence proof and zero knowledge proof. According to [15] their protocols have following problems: (1) do not defence against forced-abstention and simulation attacks; (2) cannot support write in ballot.

Also in the paper [22] Smith points out JCJ protocol is not secure against 1009 attack and time stamping attack, and then proposes an improved coercion-resistant protocol with weak physical assumptions: anonymous channel. Unfortunately, Ara´ujo and Traor´ in [2] and Clarkson et al. in [6] pointed out that the Smith's method is not secure and an adversary can use the ElGamal malleability to determine whether a coerced voter gave him a valid or a fake credential.

Applying some of the [12] ideas, Acquisti [1] proposes a coercion-resistant receipt-free voting protocol with weak physical assumptions: an anonymous channel. The idea is that election Authorities provide shares of credentials to each voter, along with designated verifier proofs of each share's validity. In this protocol voter can cheat the coercer by producing a false credential. Owning to designate verifier proof the coercer cannot verify the proof. Meng [14] points out that in this protocol not achieved receipt-freeness and coercion-resistance properties. He also using some of Acquisti ideas, presents a receipt-free coercion-resistant e-voting protocol based on designated verifier proof. His protocol has receipt-freeness and coercion-resistance and it with weak physical assumptions: a one way anonymous channel between voter and Authority. Also in the papers [15,16], Meng proposed another e-voting protocols based on non-interactive deniable authentication protocol and deniable encryption.

According to our analysis, we find that the protocols [1,14,15,16] do not meet robustness characteristics fully. In these protocols Authorities sends voter certification with deniable authentication protocol and designated verifier proof. By using these tools, nobody except the voter can specify accuracy of certifications. In such situation, if each of Authorities doesn't deliver valid certification to voter, the voter will not have any way to prove the wrong certification unless reveals his/her private key. Moreover, to our best knowledge up to now there is no e-voting protocol to meet the receipt-freeness and coercion-resistance and hiding voter's identity together. In these protocols voters to prove his/her eligibility, somehow introduces himself to Authorities. Therefore, Authorities are aware of who has participated in election. With this point of weakness, a corrupt Authority can forced certain voter to participate or not in elections.

In this paper, the proposed e-voting protocol not only provides all the security requirements, but also provides implementing requirements.

The paper in organized in such a way that, Section II, describes our method by presenting the new protocol. In this Section, firstly is introduced the definitions and assumptions. Then, discusses present protocol in three phases: Preparation phase, Voting phase and Tallying phase. Analysis of the proposed protocol will perform in section III. The paper is concluded in section IV.

II. THE PROPOSED E-VOTING PROTOCOL

Main Idea of the proposed protocol is recognition voter's eligibility from their public key. In this protocol, each voter distributes his/her secret key among Authorities to prove his eligibility. Finally, Authorities corporately make the public key without revealing voters secret key.

A. Definitions and assumptions

Voters: Eligible voters denoted by set $V = \{V_1, V_2, \dots, V_n\}$. We let index j be a public identifier for V_j. Our protocol requires a preestablished public key infrastructure based on ElGamal cryptosystem. This set of public keys denoted by set $h = \{h_1, h_2, \dots, h_n\}$, where the public key h_j belongs to the voters V_j and are made as:

$$h_j = g^{s_j}.$$

Where $s_j \in Z_P$ and s_j is the secret key of voter V_j, g is a generator in Z_P. Also we assume that, any voters can not reveal his secret key in the proposed protocol1. More related work about ElGamal Cryptosystem is in [9].

Authorities: In the proposed protocol m Authorities are used which are denoted by set $A = \{A_1, A_2, \dots, A_m\}$. We let index i be a public identifier for A_i; each of these Authorities is independent servers which have a lot of computing power where is used for managing election and implementing mix net. It is assumed that, each action assigned to the Authorities, at least $\lceil m/2 \rceil + 1$ Authorities of the m Authorities, accomplish the operation properly.

Operator φ(): This operator show mixing in mix net. Mix net carried out permute and modify the sequence of objects in order to hide the correspondence between elements of original and final sequence. If a batch of inputs be set of cipher text $x = \{E_{PK}(g^{s_1}), \dots, E_{PK}(g^{s_k})\}$, output of mix net is set of $y = \{E_{PK}(g^{s_{\varphi(1)}}), \dots, E_{PK}(g^{s_{\varphi(k)}})\}$; each of original texts $g^{s_{\varphi(i)}}$ in set y is corresponding with one of original texts g^{s_i} in set x, but how the mapping between two elements collection, is hidden for all.

Powering: In the proposed protocol, powering cipher text in ElGamal cryptosystem is done as follows:

$$\left(E_{PK}(m)\right)^x = (g^r, g^{S*r}m)^x = \left(g^{x*r}, g^{x*(S*r)}m^x\right) = \left(g^{r'}, g^{S*r'}m^x\right) = E_{PK}(m^x).$$

Where, symbol $E_{PK}(m)$ is encryption massage m with Authorities' public key.

Homomorphic property: An encryption algorithm $E_{PK}()$, is homomorphic, if for given $E_{PK}(m_1)$ and $E_{PK}(m_2)$, the property $E_{PK}(m_1) \otimes E_{PK}(m_2) = E_{PK}(m_1 \oplus m_2)$ will be established. The oprator $\otimes$, is applied on the cipher texts and operator $\oplus$ is applied on the original texts. In the ElGamal cryptosystem we have:

$$E_{PK}(m_1) \times E_{PK}(m_2) = (g^{r_1}, g^{S*r_1}m_1) \times (g^{r_2}, g^{S*r_2}m_2) = \left(g^{(r_1+r_2)}, g^{S*(r_1+r_2)}m_{1*}m_2\right) = \left(g^{r'}, g^{S*r'}m_1 * m_2\right)$$
$$= E_{PK}(m_1 * m_2).$$

In the proposed protocol is used from this property on several occasions.

B. Details of the proposed Protocol

The proposed protocol has three phases: Preparation phase, Voting phase and Tallying phase.

Preparation phase: In the beginning of preparation phase, Authorities use the introduced protocol in [19, 20] and generate a threshold public/private ElGamal key. In this key, threshold is assumed $t = \lceil m/2 \rceil$. This key is denoted by $(PK = g^S, SK_i = s_i, PK_i = g^{s_i}, VK, VK_i)$, where PK is the shared Authorities public key, S is shared Authorities private key, SK_i is private key of i-th Authority, PK_i is Public key of i-th Authority, VK is verification of created shared key and VK_i is verification of any Authorities private key. Authorities' public key and its verification are posted on bulletin board.

The Authorities prepare list of candidates that is participated in the election. In the list of candidate, profile of each candidate is recorded with a unique ID. This list is signed by the Authorities and sent to bulletin board. Also in this phase, Authorities prepare list of eligible voters. This list consists of three columns. In the first column, profile of each eligible voter is appeared and voter's public keys are recorded in the second column. Also, in the third column of list, the encrypted with Authorities public keys are appeared. Structure of eligible voters list is shown in Figure 1. This list also is signed and recorded in the bulletin board by the Authorities.

profile of voter V_j	public key of voter V_j	Encrypted public key of voter V_j

[1] This assumption is set through election low of each country and done by election committee.

$\boldsymbol{identity_{V_1}}$	$h_1 = g^{s_1}$	$E_{PK}(g^{s_1})$
⋮	⋮	⋮
$\boldsymbol{identity_{V_n}}$	$h_N = g^{s_n}$	$E_{PK}(g^{s_n})$

Figure1. Structure of the eligible voter's table.

Voting phase: Each voter V_j in set V, needs create a ballot for participating in voting phase and sending his vote. We denote a ballot of voter V_j with $ballot_j$. Each $ballot_j$ ecomposes of two parts: certificate of voter V_j where is denoted by C_j and encrypted vote of voter V_j. Each voter V_j, to create certificate C_j, receives Authorities public key (PK, PK_i, VK, VK_i) from bulletin board and verifies it. If the verification of Authorities' public key is success, creation of certification will be as follow:

1. At first step, each voter V_j divides his/her private key s_j to m section $s_j^1, \dots, s_j^m$. This classification is based on introduced threshold cryptosystem (t, k) in [20]. Here we assume that threshold t is equal to $t = \lceil m/2 \rceil$. For eny t element of this sections, the following relationship will establish:
$$s_j = \sum_{i=1}^{t} (\lambda_t * s_j^t).$$
Where, λ_i is Lagrange's coefficient.
2. In the second step, each voter V_j creates certificate C_j as follow:
$C_j = \left(E_{PK_1}(s_j^1), \dots, E_{PK_m}(s_j^m)\right)$.
Where, s_j^i is i-th portion of private key of voter V_j, and $E_{PK_i}(m)$ is encryption of message m with public key of Authority A_i.

Then each voter V_j prepares lists of candidates from bulletin board and choice her vote B_t from the list of permissible candidates and encrypt with Authorities public key as:$E_{PK}(B_t)$. Each voter V_j creates his/her ballot as: $ballot_j = \left(C_j, E_{PK}(B_t)\right)$. Finally, each voter V_j encrypts $ballot_j$ with Authorities public key as: $E_{PK}(ballot_j)$ and sends it to bulletin board.

Tallying phase:

When the voting deadline is met, the bulletin board is signed by Authorities. The following stages are performed by Authorities set A for counting valid votes of eligible voters:

1. In the first step of voting phase, third column of eligible voters table (encrypted public key of voter V_j) are mixed through a mix net and output stored in the first column of the table T_1. In order to verify correctness of mixing by people, Authority stores the proof of correctness of decryption in second column of table T_1. Structure of table T_1 is shown in Figure 2.

$E_{PK}(g^{s_{\varphi(j)}})$	$Zero-knowledge\ proof_j$

Figure 2. Structure of table T_1.

2. We assume that the number of stored encrypted ballot on bulletin board is equal to w. The value of w can be more[1] or less[2] from the number of eligible voter n. All stored encrypted ballot on the bulletin board decrypt by Authorities and each field is stored in the table T_2 in corresponding column. Structure of table T_2 is shown in Figure 3.

Submitted ballot $(ballot_j)$										
$\boldsymbol{j}$	$\boldsymbol{C_j}$	$\boldsymbol{E_{PK}(B_t)}$	$\boldsymbol{A_1}$	…	$\boldsymbol{A_m}$	$\boldsymbol{E(R_j)}$	$\boldsymbol{E_{PK}(R_j) \times Com_j}$	$\boldsymbol{D_{sk}(E_{PK}(R_j) \times Com_j)}$	$\boldsymbol{proof_j}$	$\boldsymbol{E_{pk}(g^{s_j})}$
	C_1	$E_{PK}(B_t)$	$E_{PK}(g^{s_1^1})$	…	$E_{PK}(g^{s_1^m})$	$E(R_1)$	$E_{PK}(R_1) \times Com_1$	$D_{sk}(E_{PK}(R_1) \times Com_1)$	$proof_1$	$E_{pk}(g^{s_1})$
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
w	C_w	$E_{PK}(B_t)$	$E_{PK}(g^{s_w^1})$	…	$E_{PK}(g^{s_w^m})$	$E(R_w)$	$E_{PK}(R_w) \times Com_w$	$D_{sk}(E_{PK}(R_w) \times Com_w)$	$proof_w$	$E_{pk}(g^{s_w})$

Figure 3. Structure of table T_2.

For each recorded ballots in table T_2, the following steps are done by Authorities:

[1] When, some of voter sent several ballot.
[2] When, some of voter abstains from voting.

a. Each Authority A_i in set A decrypts section $E_{PK_i}(s_j^i)$ from certificate C_j with his/her private key s_i and gets share s_j^i private key of sender's ballot. Then Authority A_i computes $\left(g^{s_i^j}\right)$ and encrypts it with Authorities public key as $E_{PK}\left(g^{s_i^j}\right)$. Then the results are inserted in table T_2 in columns A_i of row j-th.

b. To make sender's encrypted public key of ballot $ballot_j$, are needed, $t = \lceil m/2 \rceil$ numbers Authority. Each collection of t honest Authorities, perform the following act to make encrypted public key:

$$\prod_{k=1}^{t}\left(E_{PK}\left(g^{s_j^k}\right)\right)^{\lambda_k} = \prod_{k=1}^{t} E_{PK}\left(g^{\lambda_k * s_j^k}\right) = E_{PK}\left(\prod_{k=1}^{t}\left(g^{\lambda_k * s_j^k}\right)\right) = E_{PK}\left(g^{\sum_{k=1}^{t}\left(\lambda_k * s_j^k\right)}\right) = E_{PK}(g^{s_j}).$$

But since t honest Authorities are not clear, for detecting valid encrypted public key corresponding with $ballot_j$, for each compounds of Authorities $\binom{m}{t}$, is run up process and make $\binom{m}{t}$ different encrypted public key. This set denoted by:

$$Com_j = \left(E_{PK}(x_1), \dots, E_{PK}\left(x_{\binom{m}{t}}\right)\right).$$

On the other hand, each A_i creates random number r_j^i and encrypts it with Authorities public key as $E_{PK}(r_j^i)$. Encrypted shared random number of Authorities is created as follow:

$$E(R_j) = \prod_{i=1}^{m} E(r_j^i).$$

The results inserted in table T_2 and columns $E(R)$ and row j-th. Since was assumed at least $\lceil m/2 \rceil + 1$ Authority of the m Authorities are honest and to make any elements of set Com_j, is required $t = \lceil m/2 \rceil$ Authorities, number of encrypted public key $E_{PK}(g^{s_j})$ in set Com_j will be:

$$\binom{\lceil m/2 \rceil + 1}{\lceil m/2 \rceil} = \lceil m/2 \rceil + 1 = t + 1.$$

Where, each of $t + 1$ these encrypted elements is encrypted with different random number, to verify these elements, all elements in the set Com_j are multiplied in encrypted shared random number $E_{PK}(R_j)$. Using homomorphic property in ElGamal cryptosystem will be:

$$E_{PK}(R_j) \times Com_j = \left(E_{PK}(R_j * x_1), \dots, E_{PK}\left(R_j * x_{\binom{m}{t}}\right)\right).$$

Then Authorities working together decrypt all these elements and t he result stored in the column $D_{sk}(E_{PK}(R_j) \times Com_j)$ of table T_2, and proof of correctness of decryption is stored in the column $proof_j$ of table T_2. Authorities with a simple search algorithm among these elements, find elements that is repeated $t + 1$ time and one of the corresponding value in the set Com_j, insert in table T_2 and columns $E_{PK}(g^{s_j})$ in row j-th.

3. The columns $E_{PK}(B_t)$ and $E_{PK}(g^{s_j})$ of the table T_2 is mixed by Authorities with mix net and the output with a proof of correctness of mixing is stored in the table T_3. Structure of table T_2 is shown in Figure 4.

$E_{PK}(g^{s_{\varphi(j)}})$	$E_{PK}(B_{\varphi(t)})$	$proof_j$

Figure 4. Structure of the table T_3.

4. In this step, Authorities run a search algorithm with a set of operations and distinguished valid votes of the table T_3 from T_1 elements. In this algorithm, index j is used for the table T_1 and index k is used for the table T_3. Detail of the search algorithm is described as follow:

a. Row j is selected from T_1 and value of forth column $E_{PK}(g^{s_{\varphi(j)}})$ is used for computing $\left(T_1.E_{PK}(g^{s_{\varphi(j)}})\right)^{-1}$ as:

$$\left(T_1.E_{PK}(g^{s_{\varphi(j)}})\right)^{-1} = T_1.E_{PK}(g^{-s_{\varphi(j)}}).$$

b. Result of previous step is multiplied in column $E_{PK}(g^{s_{\varphi(j)}})$ of all rows of table T_3 and the result is stored in the first column of table $temp_j$. Structure of the table $temp_j$ is shown in Figure 5.

$E_{PK}(g^{-T_1.s_{\varphi(j)}+T_2.s_{\varphi(w)}})$	A_1		...	A_m	
	$x^1 = (E_{PK}())^{l_k^1}$	$proof_k^1$	...	$x^m = \left(E_{PK}(x)\right)^{l_k^m}$	$proof_w^m$

$E_{PK}(g^{-T_1.S_{\varphi(j)}+T_2.S_{\varphi(1)}})$	$x_1^1 = (E_{PK}())^{l_1^1}$	$proof_1^1$	...	$x_1^m = \left(E_{PK}(x)\right)^{l_1^m}$	$proof_1^m$
⋮	⋮	⋮	...	⋮	⋮
$E_{PK}(g^{-T_1.S_{\varphi(j)}+T_2.S_{\varphi(w)}})$	$x_w^1 = (E_{PK}())^{l_w^1}$	$proof_w^1$	...	$x_w^m = \left(E_{PK}(x)\right)^{l_w^m}$	$proof_w^m$

Figure 5. Structure of the table $temp_j$.

c. For each row in the table $temp_j$, each Authority A_i creates hidden random number l_k^i and compute:

$$x_k^i = \left(E_{PK}\left(g^{-T_1.S_{\varphi(j)}+T_2.S_{\varphi(k)}}\right)\right).l_k^i$$

Also, each Authority A_i creates a Non-Interactive proof for correctness of x_k^i. The proof is denoted by $proof_k^i$. Each Authority A_i stores x_k^i and $proosf_k^i$ in the section A_i in row k-th of table $temp_j$.

d. After completing contents of the table $temp_j$, the election Authorities, compute X_k for each row $k = 1, \dots, w$ of $temp_j$ as:

$$X_k = \prod_{i=1}^{m} x_k^i = \prod_{i=1}^{m} \left(E_{PK}\left(g^{-T_1.S_{\varphi(j)}+T_2.S_{\varphi(k)}}\right)\right)^{l_k^i} = E_{PK}\left(g^{\left(-T_1.S_{\varphi(j)}+T_2.S_{\varphi(k)}\right)\sum_{i=1}^{m} l_k^i}\right)$$
$$= E_{PK}\left(g^{\left(-T_1.S_{\varphi(j)}+T_2.S_{\varphi(k)}\right)*L}\right).$$

Where let $L = \sum_{i=1}^{m} l_k^i$.

e. Each X_k with $k = 1, \dots, w$ from the previous step jointly is decrypted by the Authorities. If between the decrypted texts only one element equal to one, corresponding encrypted vote from table T_3 is added to list of valid votes in the table T_4. Otherwise, if the number of one element is more than one or no exists any one, the certificate $T_1.E_{PK}(g^{S_{\varphi(j)}})$ will be declared invalid.

f. For all rows in T_1, steps a. to e. is repeated. After finishing all rows in the table T_1, Authorities decrypt all encrypted votes in the table T_4 by using a threshold system. The result with the proof of correctness of decryption is stored in table T_4. Everyone can account result of the election from contents of the table T_4.

$E_{PK}(B_{\varphi(t)})$	$B_{\varphi(t)}$	***proof of correct decryption***

Figure 6. Structure of the table T_4.

III. ANALYSIS OF THE PROPOSED PROTOCOL

Theorem 1: The proposed protocol provides all basic security requirements.

- ***Demonstrate of Eligibility:*** The authorities prepare the list of eligible voters before voting phase and register it in the bulletin board. In this list, each profile of voters is placed along with their public key. Correctness of this list can be investigated by all people. On the other hand in tallying phase of the proposed protocol, only ballots will be confirm that encrypted public key of those exist in table T_1. So only eligible voters can send a valid vote. On the other hand, if eligible voters try to vote several times, in the search algorithm of tallying phase for encryption public key of them in the table T_1, several number of one obtain in the table $temp_j$ that will cause the encrypted public key in table T_1 for voters V_j will invalidate. Therefore, the proposed protocol provides eligibility features.
- ***Demonstrate of Privacy:*** Authorities after decrypting sent ballots to the bulletin board will make encrypted public key of sender's ballot. In any step of making encrypted public key, not reveal sender's public key for none authorities. The encryption public key with posted encrypted vote from table T_2, mix with mix net and store in the table T_3; with this mixing, remove link between casted votes and voters. On the other hand list of encrypted public of eligible voter mix with mix net and store in the table T_1. In the mixing, the link between voters and reliable encrypted keys is removed. Finally, in the search algorithm presented in tallying phase, does not appear public key of voters in any of the step. Therefore the proposed protocol maintains voter privacy.
- ***Demonstrate of individual verifiability:*** Each voter V_j can view his/her sent encrypted ballot in the table T_2. Also each voter V_j can verify created encryption public key by authorities via the proof $proof_j$. From this point onwards the link between voters and their votes is eliminated and each voter can check with presented proofs in tables T_1, T_3, $temp_j$ and T_4, and certain from his/her votes counted in the final outcome.
- ***Demonstrate of Accuracy:*** When a voter uses his private key s_j to sending $ballot_j$, create an encrypted public key as $E_{PK}(g^{s_j})$ in T_2 for himself. The encrypted public key is mixed by mix net and transferred to

T_3. In searching valid encrypted public keys of the table T_1 from the table T_3, since only a valid encrypted public key exist on the table T_1 as $E_{PK}(g^{s_j})$, in the search algorithm we will have:

$$T_1.E_{PK}(g^{-s_j}) \times T_3.E_{PK}(g^{s_j}) = E_{PK}(g^{-s_j+s_j}) = E_{PK}(1), \prod_{i=1}^{m} E_{PK}(1)^{l_k^i} = E_{PK}(1)^{\sum_{i=1}^{m} l_k^i} = E_{PK}(1).$$

On the other hand, if the voter uses an invalid secret key as s', the above result for any encrypted public key of the table T_1 not reach and the submitted ballot not affect the final outcome.

- ***Demonstrate of Fairness:*** All operations in tallying phase only are done in cooperation of authorities and authorities begin tallying phase after reaching deadline. So no one can be aware of the intermediate results.
- ***Demonstrate of Robustness:*** Since voter's certificate and his/her selected vote encrypt by the authorities public key, no one can change the content of encrypted ballot and since any set lower than $t = \lceil m/2 \rceil$ of Authority cannot do alone any step of tallying phase, corrupt authorities could not disrupt the elections. On the other hand, if voter's encoded ballot is removed among way by an aggressive, his/her certificate was not recorded in the table T_2, so the voter with verifying this table, can send own encoded ballot to the bulletin board again.

Theorem 2: The proposed protocol provides all extended security requirements.

- ***Demonstrate of Universal verifiability:*** In the proposed protocol all people could check list of eligible voters and the public key of them. Also everyone can verify encrypted public key with presented proofs in table T_2. Also in tables T_1 and T_3 is recorded correctness of mixing and in table $temp_j$, correctness of Authorities function is recorded and in the table T_4 proved correct decrypting. Since correctness of all processes can be investigate by all people, so the proposed protocol meet universal verifiability features for public.
- ***Demonstrate of Receipt-freeness:*** Each submitted ballot by the voters composed of two parts: voter's certificate and encrypted votes. Submitted voters certificate, is distributing of voter's private key which each of them encrypt by Authorities public keys. After making voter's encrypted public key, the encrypted public key with corresponding encrypted vote is mixed via mix net and the result record in T_3. This mixing remove link between encrypted ballot and voter. So voter cannot use any of them as a receipt. Thus the proposed scheme is receipt-freeness.
- ***Demonstrate of Coercion-resistance:*** Since the identity of all participants is protected in all steps and for all people including Authorities, any coercers cannot aware from identity of valid or invalid voters and forced certain voter to reveal his/her vote. So the proposed scheme is coercion-resistance. The features "Hiding voter's identity" is investigated in the next section.
- ***Demonstrate of Hiding voter's identity:*** In the proposed scheme voter's identity is their public key. Here is shown that the public key participants remain hidden in the tallying phase.

  For each submitted $ballot_j$, encrypted public key of set com_j, directly is made from the cipher text $E_{PK}\left(g^{s_j^i}\right)$, So the encrypted public keys remain hidden from Authorities. For detection valid encrypted public key of set com_j, this set is multiplied to the encrypted shared random member $E_{PK}(R_j)$. Then the result set is decrypted by Authorities. In the obtained set, valid public keys appears in the form of $(g^{s_j}R_j)$. With having random parameter R_j no one can obtain the public key g^{s_j}. Also in table T_3 and $temp_j$, used from mixed encrypted public keys $E_{PK}(g^{s_j})$. On the other hand the link between encrypted public key and the eligible voters is removed in mixing and sending to T_1. For detecting valid encrypted public key of the table T_1 from encrypted public key of T_3, first each of the encrypted public key $E_{PK}(g^{s_j})$ is will be powered -1 and then the result is multiplied to all encrypted public keys of table T_3 and so:

  - For encrypted public key $E_{PK}(g^{s_j})$, on the table T_3 we have:

    $$T_1.E_{PK}(g^{-s_j}) \times T_3.E_{PK}(g^{s_j}) = E_{PK}(1).$$

    And so:

    $$\prod_{i=1}^{m} E_{PK}(1)^{l_k^i} = E_{PK}(1)^{\sum_{i=1}^{m} l_k^i} = E_{PK}(1).$$

    Where with decryption $E_{PK}(1)$, no one can detect the public key of sender's ballot.

- For other encrypted public key $E_{PK}(g^{s_k})$ on the table T_3we have:

$$T_1.E_{PK}(g^{-s_j}) \times T_3.E_{PK}(g^{s_k}) = E_{PK}(g^{-s_j+s_k}).$$

And so:

$$\prod_{i=1}^{m} E_{PK}(g^{-s_j+s_k})^{l_k^i} = \prod_{i=1}^{m} E_{PK}\left(g^{(-s_j+s_k)*l_k^i}\right) = E_{PK}\left(g^{(-s_j+s_k)*\sum_{i=1}^{m} l_k^i}\right) = E_{PK}\left(g^{(-s_j+s_k)*L_k}\right).$$

Since l_k^i select secret and randomly by the Authorities, no one cannot detect the public key g^{s_j} or g^{s_k} from $g^{(-s_j+s_k)*L_k}$.

So in the proposed protocol voter's identity or his/her public key remain hidden in the all steps of tallying phase.

Performance evaluation of the proposed protocol:

In the proposed protocol only one connection is need for each voter and that is sending encrypted ballot to the bulletin board.

On the other hand each voter to make his/her encrypted ballot, needs $(m + k + 1)$ encryption. Required time for $(m + k + 1)$ encryption is minimal and minor.

Authorities' computational complexity steps of tallying phase than number of voters is linear except in two cases:

- ***Build the set com_j and detection valid encrypted public key:*** In this case for each ballot is required $\left(\left\lceil\frac{m}{2}\right\rceil * \binom{m}{\left\lceil\frac{m}{2}\right\rceil}\right)$ multiplication operator and $\binom{m}{\left\lceil\frac{m}{2}\right\rceil}$ decrypting operator.
- ***Making table $temp_j$ in the search algorithm:*** If the number of sent ballot to bulletin board be $w \cong n$, for each encrypted public key in table T_1 all operator will be of order $O(n)$. So the search algorithm is will be of order $O(n^2)$.

In general, computational complexity in the proposed protocol for authorities will be in order $O(n * m! + n^2)$, and since number of authorities is very smaller than number of voters, therefore in practice, the algorithm order will be $O(n^2)$.

We compare security properties and complexity properties of Acquisti [1], Juels et al. [11, 12], meng [14, 15, 16] protocols with our present protocol. A briefly result of comparing is shown in the Table 1.

TABLE I. COMPARING THE EARLIER SEVERAL TYPICAL PROTOCOLS WITH OUR PRESENT PROTOCOL. THE MARK "T" REPRESENTS THE ROTOCOL HAS THE PROPERTY; THE MARK "F" REPRESENTS HAS NOT THE PROPERTY.

Properties \ **Protocols**			**Acquisti [1]**	**Juels et al. [11, 12]**	**Meng [14, 15, 16]**	**Our present**
Basic security requirements	***Privacy***		T	T	T	T
	Eligibility		F	F	T	T
	Individual verifiability		T	T	T	T
	Accuracy		T	T	T	T
	Fairness		T	T	T	T
	Robustness against	***Authority***	F	F	F	T
		Others	T	T	T	T
Extended security requirements	***Universal verifiability***		T	T	T	T
	Receipt-freeness		F	T	T	T
	Coercion-resistance		F	T	T	T
	Hiding voter's identity against	***Authority***	F	F	F	T
		Others	F	T	T	T
Authority computational complexity			$O(n^2 * L)$	$O(n^2)$	$O(n^2)$	$O(n^2)$
Voter's communication complexity			$O(m)$	$O(m)$	$O(m)$	$O(1)$

IV. CONCLUSION

In this paper, is proposed a new e-voting protocol. The novelty of this protocol, in addition to providing basic security requirements, is that the voter's identity remains hidden and requires nonphysical assumptions for implementation. Also, the proposed protocol support write in ballot and it is easily generalizable for K-out-of-L voting. At the end of this paper, we have proved that the proposed protocol has provided all security features of election. In addition, it is shown that the

communication size of our new protocol is very efficient and authorities computation's order is $O(n^2)$. Due to having low communication volume, the proposed protocol is suitable for internet voting and communication networks with less bandwidth. Finally, security properties and complexity properties of the proposed protocol are compared with the earlier several typical protocols in this field.

REFERENCES

[1] A. Acquisti, "Receipt-Free Homomorphic Elections and Write-in Voter Verified Ballots", *Technical Report* 2004/105, CMU-ISRI-04-116 (2004).

[2] S.F. Ara´ujo and J.A. Traor´, "Practical and secure coercionresistant scheme for remote elections", *Frontiers of ElectronicVoting* (2008).

[3] J. Benaloh, "Verifiable secret-ballot elections", *PhD Thesis*, Yale University, Department of Computer Science (1987).

[4] Baudron, Olivier, Fouque, Pierre-Alain, David Pointcheval, Guillaume Poupard and Jacques Stern, "Practical multi-candidate election system", *In PODC* '01, pages 274–283. ACM (2001).

[5] J. Benaloh and D. Tuinstra, "Receipt-free secret-ballot elections", In *STOC* '94, pages 544–553 (1994).

[6] M. Clarkson, S. Chong and A.C. Myers, "Civitas: A Secure Remote Voting System", *Technical report, Cornell University Computing and Information Science Technology Report* (2007).

[7] D. Chaum, "Secret-ballot receipts and transparent integrity", (2002), *http://www.vreceipt.com/article.pdf*.

[8] D. Chaum, "Secret-ballot receipts: true voter-verifiable elections", *IEEE Security & Privacy* Magazine (2004).

[9] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", In *CRYPTO* '84, pages 10–18. Springer-Verlag, LNCS 196 (1984).

[10] M. Hirt and S. Kazue, "Efficient receipt-free voting based on homomorphic encryption", In *EUROCRYPT* '00, pages 539–556. Springer-Verlag, LNCS 1807 (2000).

[11] A. Juels and M. Jakobsson, "Coercion-resistant electronic elections", (2002), *http://www.citeseer.nj. nec.com/555869.html* .

[12] A. Juels, D. Catalano, and M. Jakobsson, "Coercionresistant electronic elections", (2005), *http://www.rsasecurity.com/rsalabs/node.asp?id=2030* .

[13] B. Lee and K. Kim, "Receipt-free electronic voting through collaboration of voter and honest verifier", (2000), *http://www.citeseer.nj.nec.com/lee00receiptfree.html* .

[14] B. Meng, "An internet voting protocol with eceipt-free and Coercion-resistant", In *Proceedings of IEEE 7th International Conference on Computer and Information Technology*, Japan, pp.721-726, October 16 to 19 (2007).

[15] B. Meng, "A Secure Non-Interactive Deniable Authentication Protocol with Strong Deniability Based on Discrete Logarithm Problem and its Application on Internet Voting Protocol", *Information Technolog Journal* , 8(3), pp.302-309 (2009).

[16] B. Meng and J.Q. Wang, "An efficient receiver deniable encryption scheme and its applications", *Journal of Networks*, VOL. 5, NO. 6, pages 683– 690 (2010).

[17] A. Neff, "Detecting malicious poll site voting clients", (2003), *http://www.votehere.net/*.

[18] M. Rezvani, M. Jahromi and H. Lashkari, "Security Considerations in Electronic Voting Protocols", *Proceedings of the 2nd Conference* on E-City, Tehran (2009).

[19] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting", *Advances in Cryptology - CRYPTO*, 1666 of Lecture Notes in Computer Science:148–164 (1999).

[20] A. Shamir, "How to share a secret", *Communications of the ACM*, 22:612–613 (1979).

[21] K. Sako and J. Kilian, "Receipt-free mix-type voting scheme", In *EUROCRYPT* '95, pages393–403, Springer-Verlag, LNCS 921 (1995).

[22] W.D. Smith, "New cryptographic voting scheme with best-known theoretical properties", In *Workshop on Frontiers in Electronic Elections* (2005).