



EIJEST

HOMOMORPHIC TALLYING OF ELECTRONIC VOTING SYSTEM USING RFID

Khaled A. Shehata, Nabil H. Shaker, Hanady Hussien, Hussien M. Abulnaga**

Arab Academy for Science and Technology and Maritime Transport,
Dept. of Electronics and Communication, Cairo, Egypt.

ABSTRACT

Electronic voting refers to the use of computers or computerized voting equipment to cast ballots in an election. Sometimes, this term is used more specifically to refer to voting that takes place over the Internet. Electronic systems can be used to register voters, tally ballots, and record votes [20]. In this paper, a software development in election procedure has been introduced in homomorphic tallying using Paillier cryptosystem with the confirmation of the electronic voting security requirements. Moreover, RFID technology has been embedded through the election procedure to identify a new role in identification of voters' eligibility through the voting process.

KEY WORDS: Cryptography E-voting system, Elgamal cryptosystem, Paillier cryptosystem, secret sharing scheme, Radio Frequency Identification (RFID), Mix-Nets, Homomorphic encryption and electronic voting scheme.

HOMOMORPHIQUE DECOMPTE DES SYSTÈME DE VOTE ELECTRONIQUE UTILISANT RFID

RÉSUMÉ

Le vote électronique se réfère à l'utilisation des ordinateurs ou du matériel de vote informatisé de voter à une élection. Parfois, ce terme est utilisé pour désigner plus spécifiquement au vote qui se déroule sur Internet. Les systèmes électroniques peuvent être utilisés pour inscrire les électeurs, les bulletins de pointage, et les votes d'enregistrement [20]. Dans cet article, un développement logiciel en mode d'élection a été introduit dans le décompte homomorphe utilisant Paillier cryptosystème à la confirmation des exigences de sécurité électroniques de vote. En outre, la technologie RFID a été intégré par la procédure d'élection d'identifier un nouveau rôle dans l'identification de l'admissibilité des électeurs dans le processus de vote.

MOTS CLÉS: Cryptographie système de vote électronique, Elgamal cryptosystème, Paillier cryptosystème, système de partage de secret, identification par radiofréquence (RFID), Mix-Nets, le chiffrement homomorphe et système de vote électronique.

* Received: 4/3/2012, Accepted: 26/8/2012 (Technical Report)

** Contact author (+2 012 22230575)

1. INTRODUCTION

An electronic-voting (e-voting) continues to grow as long as the world becomes more dependable on new technologies. E-voting tries to enable efficient and secure elections. Moreover e-voting provides a lot of benefits than traditional voting. The resources of e-voting schemes are reusable resulting in inexpensive elections. Also it does not require any geographical proximity of voters, and it provides better scalability for large elections [1]. Basically e-voting system contains software that defines the ballots, casts and counts the votes [2].

Any e-voting system contains mainly from three main entities, voter, registration authorities and tallying authorities [3]. Each entity has its role to conduct the election process. The process is starting with voter who has the right to vote. Then registration authority who registers the voters in the Election Day. In addition he should grantee only the registered voters are able to vote. Finally tallying authorities ensure cast votes are counted [3].

The security concern is one of the main challenges which faced any e-voting system. Most of e-voting systems in literature are based on one of three main cryptography protocols [4].

- E-voting based on Homomorphic Encryption [5, 6, 7, 8].
- E-voting based on Mixing Nets [9,10,11,12,13,14], and
- E-voting based on Blind Signatures [15, 16, 17].

In the systems which are based on homomorphic encryption algorithm a voter cooperates with the authorities in order to encrypt the voter's ballot. As a result both the voter information and ballot content are kept hidden.

A mix network or mixnet is a cryptographic construction that invokes a set of servers to establish private communication channels [9]. In a voting system, anonymity is a fundamental requirement. It means that the voter cannot be associated to her vote. To prevent the association, mixnets could be used in the electronic voting system [19].

In the systems using blind signatures, the voter firstly obtains a token – a blindly signed message unknown to anyone except himself. Next, the voter sends his token together with his vote anonymously. These schemes require voter's participation in more rounds.

This paper proposes an e-voting system based on both homomorphic and blind signature algorithms. The system uses RFID technology to satisfy some security concerns during identification step.

2. ELECTRONIC VOTING SECURITY REQUIREMENTS

Computerized voting will never be used for general elections unless there is a protocol that maintains individual privacy and prevents cheating [18]. Hence, any cryptographic protocol used in e-voting system it must satisfy at least seven security requirements [3, 18]

- Eligibility: ensure only authorized voters who satisfy pre-determined criterion can vote.
- Uniqueness: Only one vote for a voter so no one can vote more than once.
- Privacy: a vote kept secret and no one can determine for whom anyone else voted,
- Secrecy: election process is secure so no one can change anyone else's vote without being discovered. In addition no one can duplicate anyone else's vote.
- Accuracy: every voter can make sure that his vote has been taken into account in the final tabulation.
- Transparency: everyone knows who voted and who didn't.

3. PAILLIER CRYPTOSYSTEM

In 1999 Pascal Paillier has proposed an advanced encryption algorithm for public key cryptography. [ref brics-ds-039 pp 21]. Paillier algorithm is a probabilistic asymmetric encryption which is based on computations over the group $Z_{N^2}^*$, where n is an RSA modulus. This scheme provides many attractive algebraic properties which make it suitable for different applications such as electronic voting. The main appealing algebraic feature is homomorphic. This feature means if two ciphertexts are combined in a specific publicly commutable fashion, the resulting ciphertext encodes the combination of the underlying

plaintexts under a specific group operation, usually multiplication or addition [adida-phd2006 p 48].

The security of Paillier scheme comes from the concept of using the decisional composite residuosity assumption. This assumption provides many advantages such as

- It is hard to decide whether an element in $Z_{N^2}^*$ is an N -th power of an element in Z_N^* .
- No adaptive chosen-cipher text attacks recovering the secret key are known.

A brief description of Paillier cryptosystem algorithm is described below.

Key generation:

In this step both the public keys (n, g) and private keys (λ, μ) are generated.

Public key (n, g)

P, q prime ($\gcd(pq, (p-1)(q-1))=1$)
 $n=pq$
 $g \in Z_{n^2}^*$ where ($\gcd(\frac{g^{\lambda \bmod n^2} - 1}{n}, n)=1$) and
 $Z_n^* = \{z | z \in Z, 0 \leq z < n, \gcd(z, n) = 1\}$

Private key (λ, μ)

$\lambda = \text{lcm}(p-1, q-1)$ where ($\lambda = \frac{(p-1)(q-1)}{\gcd((p-1)(q-1)}$)
 $\mu = (L(g^\lambda \bmod n^2))^{-1} \cdot \bmod n$ where ($L(u) = \frac{u-1}{n}$)

Encryption:

Select random r where $r \in Z^*$
 c (ciphertext) = $g^m r^n \bmod n^2$

Decryption:

M (plaintext) = $L(c^\lambda \bmod n^2) \cdot \mu \bmod n$

To illustrate the homomorphic property consider two messages m_1 and m_2 , the encryption of each message is $E(m) = (g^m r^n \bmod n^2)$

Consequently, the product of cipher texts $E(m_1)$ and $E(m_2)$ produces the cipher of addition of m_1 and m_2 messages as follows:

$$\begin{aligned} E(m_1) \cdot E(m_2) &= (g^{m_1} r^n)(g^{m_2} r^n) \bmod n^2 \\ &= (g^{m_1+m_2} r^{2n}) \bmod n^2 \\ &= E(m_1 + m_2) \end{aligned}$$

4. PROPOSED E-VOTING SYSTEM COMPONENTS

The proposed system is based on three main components

- Voter's RFID card
- Local committee servers
- Central facility server

Each component has its role in this system. The RFID card is used to store all voters' data which required authenticating the voter eligibility. The local committee server represents a server for each city in the country. Each server comprises of several main voting terminals as shown in figure 1.

At the beginning of the voting process each voter is identified and checked his eligibility at the local committee. Then the voter casts his ballot through the main voting terminal which stores the voter ballot in encrypted form. Then all these encrypted ballots will be delivered to the central facility server in groups. The central facility server is now responsible for tallying all received ballots and announces the election result.

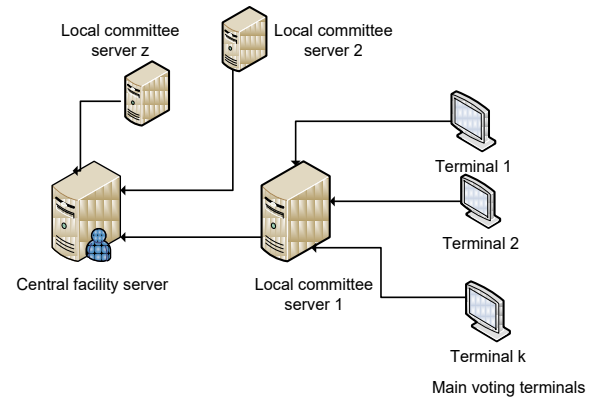
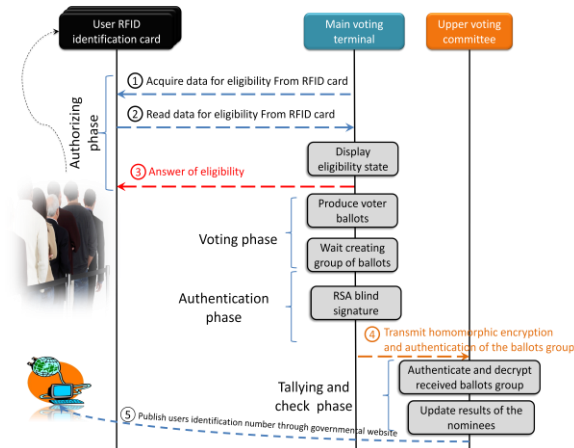


Figure 1: Components of Proposed System

5. PROPOSED E-VOTING SYSTEM

The proposed e-voting system procedure consists of five distinctive phases: authorizing, voting, authenticating, tallying and double checking phases. Each phase is detailed in the following sections



i. Authorizing phase:

This phase is the first step in the e-voting system. It performs in the local committee to check the voter eligibility.

To accomplish this phase both the voter national ID and his RFID card are required. The RFID card is prepared once before election process. It contains all information required to check voter eligibility as shown in table 1. The required data can be classified into three main groups. First one concerns voter eligibility data and the second one concern the type of election. Due to the limited storage area of the RFID all area needed is about 58 bytes (actually 466 bits). The eligibility section contains 40-byte which used to store the voter's name. One extra byte is needed to define all other voter eligibility information such as his nationality, age, criminal status...etc. as shown in table 1. Each bit in this byte is used as a flag which indicates if the voter is valid to vote or not.

Second group concerns the type of election. The proposed system contains eight different types of elections. This number could be increased to cover other types of elections. Each type needs 17-bit size. The first two bytes (16-bit) represent the date of election while the last bit is a flag bit which is used to specify if this is a first time for voter to elect or not. This group will be changed when a voter ends his voting process correctly. Moreover the flag bit is raised high to prevent a voter from revoke again.

Table 1: RFID contents

	Definition of data	Size
Eligibility Info	User Name	40-byte
	Nationality	1-bit
	Age	1-bit
	Criminal status	1-bit
	Armed forces	1-bit
	Quarantined status	1-bit
	Mental illness	1-bit
	Bankruptcy	1-bit
	Military status	1-bit
	Type of election	President election
Re-president elections		1-bit and 2-bytes
People's Council elections		1-bit and 2-bytes
Re-People's Council elections		1-bit and 2-bytes
Shura Council elections		1-bit and 2-bytes
Re-Shura Council elections		1-bit and 2-bytes
Local People's Councils		1-bit and 2-bytes
Re-Local People's Councils		1-bit and 2-bytes
Validity (Number of year)	2-bits	
Size=58 bytes & 2 bits (466 bit)		

The third group concerns the RFID validity time. This part needs 2-bit which limits the validation time to four years.

ii. Voting phase:

In this phase an eligible voter selects one of available candidates. This process accomplishes using software which shows all candidates and allows the voter to choose his nominee. Subsequently, the local committee starts to store all ballots generated by voters.

The local committee server stores the generated ballots in a table which consists of L columns where L is the number of nominees. Each row in this table represents a voter's ballot. The row contains a prime number representing vote YES in cell intersects with chosen nominee. The rest cells in same ballot (row) include another prime number that represents vote NO. As shown in table 2. Then each ballot is encrypted using Paillier cryptosystem in the local committee server.

Subsequently the encrypted ballot is concatenated with a corresponding voter's information. For a real time processing a group of encrypted ballots is sent to the central facility server during the Election Day. Based on additive homomorphic property of Paillier cryptosystem a group of ten or five ballots is counted in local committee.

Table 2 shows an example of stored ballots for a group contains five voters and five nominees. We choose a prime number 5 to represent “vote YES” and number 19 for “vote NO”. Then Paillier cryptosystem is implemented for each ballot as shown in table 3. For each nominee (column in our example) all encrypted votes are multiplied by each other as shown in table 4.

All these steps are repeated for the remaining ballots until the end of the Election Day.

Table 2: Plain text ballots of five voters (group =5)

	David	Jon	Carl	Arlond	Tom
Voter 1	5	19	19	19	19
Voter 2	5	19	19	19	19
Voter 3	19	5	19	19	19
Voter 4	19	5	19	19	19
Voter 5	19	19	5	19	19

Table 3: Encrypted ballot of each voter

	David	Jon	Carl	Arlond	Tom
Voter 1	E(5)	E(19)	E(19)	E(19)	E(19)
Voter 2	E(5)	E(19)	E(19)	E(19)	E(19)
Voter 3	E(19)	E(5)	E(19)	E(19)	E(19)
Voter 4	E(19)	E(5)	E(19)	E(19)	E(19)
Voter 5	E(19)	E(19)	E(5)	E(19)	E(19)

Table 4: Data to be transmitted to the central facility

David	Jon	Carl	Arlond	Tom
E(5)	*E(19)	E(19)	E(19)	E(19)
*E(5)	*E(19)	*E(19)	*E(19)	*E(19)
*E(19)	*E(5)	*E(19)	*E(19)	*E(19)
*E(19)	*E(5)	*E(19)	*E(19)	*E(19)
*E(19)	*E(19)	*E(5)	*E(19)	*E(19)
=ξ1	=ξ2	=ξ3	=ξ4	=ξ5

iii. Authentication phase:

Authentication means, It should be possible for the receiver of a message to ascertain its origin; an intruder should not be able to masquerade as someone else [18]. Many ways could be introduced to perform the authentication phase between the central facility and the local committee.

The used one is the RSA blind signature algorithm. Table 5 describes briefly the function of all committees participate in the election process to perform RSA blind signature algorithm.

Table 5 : Authentication procedure for each committee

Committee	Function	RSA blind signature implementation
Local committee.	Chooses a random value, k , between 1 and n Where $1 < k \leq n$	
	Blinds m	$t = m k^e \text{ mod } n$
	Signs t	$t^d = (mk^e)^d \text{ mod } n$
Central facility	Unblinds m with k	$S = t^d / k \text{ mod } n$

Where:
m is the final message sent to the central facility as mentioned in table 4.
k is a random number known by each authority “Central facility” and “Local Committees”
d is a private key
e is a public key
t is the blinded message.
S is the unblinded message.

The RSA blind signature algorithm is applied on the previous example shown in table 4. The resulted message will be blinded in the following table 6 after the selection of random number and generating the private and public key:

Table 6: Blinded Data to be transmitted to the central facility

David	Jon	Carl	Arlond	Tom
$B_{Kd}(\xi_1)$	$B_{Kd}(\xi_2)$	$B_{Kd}(\xi_3)$	$B_{Kd}(\xi_4)$	$B_{Kd}(\xi_5)$
* B_{Kd} : Blind message by random number k and private key d				

iv. Tallying phase:

Due to the additive homomorphic property of the Paillier cryptosystem, the tallying process could be performed on the data that sent in the table 7. After unblinding and decrypting the sent data for all voters by the end of Election Day the result will be the addition of the prime numbers as shown in table 7

Table 7 : Unblinding and Decryption result of the sent data

David	Jon	Carl	Arlond	Tom
Unblinding the sent message				
$UB_{Kp}(E(5*5*19*19*19))$	$UB_{Kp}(E(19*19*5*5*19))$	$UB_{Kp}(E(19*19*1*9*19*5))$	$UB_{Kp}(E(19*19*9*19*19))$	$UB_{Kp}(E(19*19*9*19*19))$
Decryption of the message				
$D(E(5*5*19*1))$	$D(E(19*19*5*5*19))$	$D(E(19*19*1*9*19*5))$	$D(E(19*19*9*19*19))$	$D(E(19*19*9*19*19))$

9*19))	5*19))	*19*5))	9*19))	9*19))
Result of decryption				
67	67	81	95	95
*UB _{KP} : Unblind message by random number k and public key P				

After decryption, the following equation will be applied to extract the number of votes for each nominee:

$$n = \frac{y - Nr_2}{r_2 - r_1}$$

Where,

n is number of “Vote Yes” for one nominee.

y is the result of the decryption of one nominee.

r₂ is the “Vote No” prime number.

r₁ is the “Vote Yes” prime number.

N is the number of voters in the group

Regarding to the example above, if it is required to find the number of “Vote Yes” and “Vote No” for the nominee 4, the equation will be:

$$n = \frac{95 - (5 * 19)}{5 - 19} = 0$$

And,

The number of “Vote No” = N - n = 5-0 = 0

Table 8 shows the final results for all nominees shown in table 7.

Table 8: Result of the election

NO of	David	Jon	Carl	Arlond	Tom
Yes Vote	2	2	1	0	0
No Vote	3	3	4	5	5

This process is re-performed for each data received from the local committee till the end of the election process to extract the result of the election.

v. Double check phase:

Double check phase means the same data sent every group should be the same data stored in the local committee.

After the end of the Election Day the stored data in the local committee which stored blindly will be sent to the central tabulating facility as the following in table 9:

Table 9: Blinded voter ballots

	David	Jon	Carl	Arlond	Tom
B _{Kd} (Voter 1)	B _{Kd} (E(5))	B _{Kd} (E(19))	B _{Kd} (E(19))	B _{Kd} (E(19))	B _{Kd} (E(19))
B _{Kd} (Voter 2)	B _{Kd} (E(5))	B _{Kd} (E(19))	B _{Kd} (E(19))	B _{Kd} (E(19))	B _{Kd} (E(19))
B _{Kd} (Voter 3)	B _{Kd} (E(19))	B _{Kd} (E(5))	B _{Kd} (E(19))	B _{Kd} (E(19))	B _{Kd} (E(19))
B _{Kd} (Voter 4)	B _{Kd} (E(19))	B _{Kd} (E(5))	B _{Kd} (E(19))	B _{Kd} (E(19))	B _{Kd} (E(19))
B _{Kd} (Voter 5)	B _{Kd} (E(19))	B _{Kd} (E(19))	B _{Kd} (E(5))	B _{Kd} (E(19))	B _{Kd} (E(19))

er 2))	9)	9)	9)	9)
B _{Kd} (Voter 3)	B _{Kd} (E(19))	B _{Kd} (E(5))	B _{Kd} (E(19))	B _{Kd} (E(19))	B _{Kd} (E(19))
B _{Kd} (Voter 4)	B _{Kd} (E(19))	B _{Kd} (E(5))	B _{Kd} (E(19))	B _{Kd} (E(19))	B _{Kd} (E(19))
B _{Kd} (Voter 5)	B _{Kd} (E(19))	B _{Kd} (E(19))	B _{Kd} (E(5))	B _{Kd} (E(19))	B _{Kd} (E(19))

The central tabulating facility unblinds the received messages as the following:

Table 10: Unblinded voter ballots

	David	Jon	Carl	Arlond	Tom
UB _{KP} (Voter 1)	UB _{KP} (E(5))	UB _{KP} (E(19))	UB _{KP} (E(19))	UB _{KP} (E(19))	UB _{KP} (E(19))
UB _{KP} (Voter 2)	UB _{KP} (E(5))	UB _{KP} (E(19))	UB _{KP} (E(19))	UB _{KP} (E(19))	UB _{KP} (E(19))
UB _{KP} (Voter 3)	UB _{KP} (E(19))	UB _{KP} (E(5))	UB _{KP} (E(19))	UB _{KP} (E(19))	UB _{KP} (E(19))
UB _{KP} (Voter 4)	UB _{KP} (E(19))	UB _{KP} (E(5))	UB _{KP} (E(19))	UB _{KP} (E(19))	UB _{KP} (E(19))
UB _{KP} (Voter 5)	UB _{KP} (E(19))	UB _{KP} (E(19))	UB _{KP} (E(5))	UB _{KP} (E(19))	UB _{KP} (E(19))

After unblinding the voter ballots the central tabulating facility decrypt each ballot to its plain text. The central tabulating facility compares the two results. If the result of the data that received from the local committee at the end of the day and the result of the data that sent along the Election Day are the same, this means the result is verified.

6. SOFTWARE IMPLEMENTATION:

Our implementation uses Microsoft visual C# 2008 for user interface and accesses voter RFID card with RFID card reader. Furthermore, The E-voting system is divided into two parts: ballot card issuing machine “Authorizing phase”, polling, counting and authentication machine “Voting and Tallying phase” as mentioned before in section V.

i. Ballot card issuing:

The ballot card issuing machine (shown as Fig. 2) reads the voter RFID card and checks its eligibility for election as introduced in section i table 1.

Voter Identification	-----
Voters' names	-----
Voters' nationality	-----
Voters' Criminal status	-----
Voters' Age	-----
Voters' eligibility	-----
Voters' place of residence	-----
Amed forces Officer	-----
Quarantined state	-----
Mental illness	-----
Bankruptcy	-----
Military service	-----

Fig. 2: Voter eligibility screen

Whenever the voter become valid for the election procedure, Language selection can be issued (Shown as Fig. 3).


	English
	عربي










Fig. 3: Language selection screen

ii. Polling, counting and authentication:

Polling, counting and authentication machine is the main unit of the election procedure. This machine accomplishes many valuable tasks described in section IV.

To elect one elector from a group (Shown as Fig. 4), Voter should select one elector and press end to confirm his selection or return back to the elector list and change his selection.

Please select one elector. To get valid ballot
if you selected two electors or more your ballot will be ignored.

David	John	Tom	Carl	Arlond
				
				
				

Please select one elector. To get valid ballot
if you selected two electors or more your ballot will be ignored.










David	John	Tom	Carl	Arlond
				
				
				

Fig. 4: Elector List

By the end of this screen the voter role has been finished and his vote stored in election database as following in Fig. 5 and Fig. 6.

	Vote	Voter ID
▶	5353475353	1234567
*	NULL	NULL

Figure 4: Database of voters' plain text ballots

	V...	David	John	Tom	Carl	Arlond
▶	3514\$	2635770...	102257...	327721...	16215...	2607168...

Figure 5: Database of voters' cipher text ballots.

The authentication double check and tallying phase begin as mentioned before in section V. These phases included in one screen as shown in figure 6.

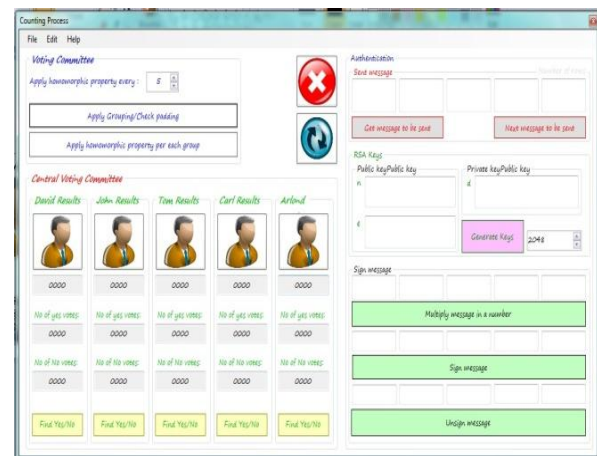


Figure 6: Tallying and authentication screen



Figure 7: The left hand side of figure 6.

Whenever tallying ballots is important, this screen does this job (Shown as figure 7). As mentioned in section V, to apply homomorphic property, Choose number of ballots and apply additive homomorphic property. The numeric up down counter is responsible about how many ballots will be grouped. Apply grouping/ check padding button check if the

number of ballots less than the number of group value to do padding or not as shown in figure 8.

	V...	David	John	Tom	Carl	Arlond
▶	35148	2635770...	102257...	327721...	16215...	2607168...
	12...	3637503...	153781...	276865...	39526...	3854888...
	12...	1544277...	210478...	365546...	51297...	4136796...
	12...	4000429...	315574...	355516...	65336...	1660540...
	12...	3588210...	271350...	245542...	13630...	2792878...
*	N...	NULL	NULL	NULL	NULL	NULL

Figure 8: Padding and check group database

Apply homomorphic property per each group button perform the additive homomorphic property per each group and sent it to the central facility as shown in figure 9.

	E1	E2	E3	E4	E5
▶	2500325163152361	1917726160282...	2301139878828...	2209721319340...	3387916989563...
*	NULL	NULL	NULL	NULL	NULL

Figure 9: Additive homomorphic of ballots group.

Before sending the additive homomorphic ballots group to the central facility to do tallying phase, the authentication phase should be done as shown in figure 10:

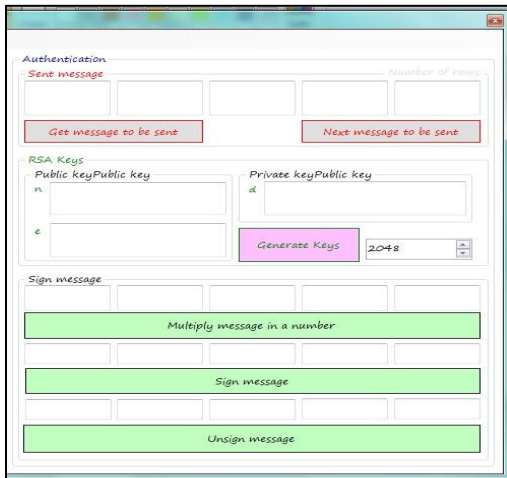


Figure 10: The right hand side of figure 6.

In this screen (Shown in figure 10) an RSA authentication phase is done. Firstly, by generate the keys of RSA blind signature algorithm from Generate keys button. Secondly, by import the message to be sent to the central facility from get message to be sent button. Thirdly, by multiply this message by a number by click the button multiply message in a number. Finally, by click the sign message to send it

to the central facility. To be sure that the message is signed well unsigned it by unsign message button and compare with the original one.

When the central facility received the signed message from the committee, it unsign the message and begin the tallying process as shown in figure 7 in central voting committee group box. By click in each voter picture its result will be displayed below his picture. As mentioned in section V regarding the tallying equation

$$n = \frac{y - Nr_2}{r_2 - r_1}$$

By click find yes/no vote for each elector the above equation is applied and the result displayed.

As mentioned in section V for double check phase, The RSA blind signature keys in figure 10 is used to sign all voter ballots to be send in the end of the election day to the central facility (shown in figure 11)

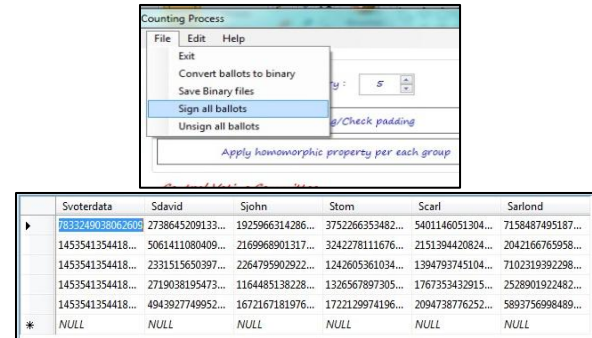


Figure 11: All voter ballot signing.

The central facility should be able to unsign all ballots to start the process of double check (Shown in figure 12)

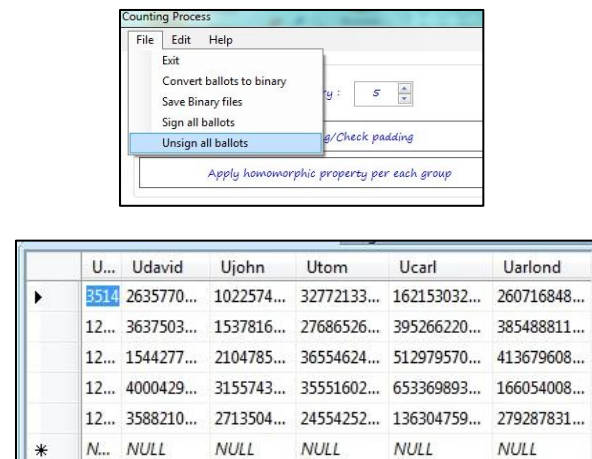


Figure 12: All voter ballot unsigning.

7. E-VOTING SECURITY REQUIREMENTS

The proposed e-voting system takes into consideration the security requirements mentioned in section II and satisfies them as following:

- Using the RFID for each voter satisfies eligibility and uniqueness requirements. The RFID contains all data needed to ensure the voter eligibility. Moreover, it contains flags which changed with authority party to prevent the voter from voting again.
- The secrecy requirement is accomplished by storing all votes as a cipher text. The advantage of the Paillier cryptosystem becomes clear as the Paillier cryptosystem encrypts each message by adding random number. This is called probabilistic encryption which means any information leaked will be eliminated with public key cryptography and no computation on the cipher text or on any other trial plaintexts can give the cryptanalyst any information about the corresponding plaintext [18].
- Because of there are two places storing the voter ballots but each one has its configuration as mentioned in section V, security requirement number five can be applied through the scheme. Regarding to the example mentioned in section V, if the five ballots changed after sending the total ballots summation to the central facility there will be a difference between the results among the central facility and local committee. This difference advertises the manipulation of the local committee in the ballots.
- As the voter data is concatenated to the voter ballot as mentioned in section v in voting phase, by the end of Election Day these data will be published on a governmental website, the accuracy and transparency requirements could be applied.

8. TESTS AND INVESTIGATIONS:

This scheme to be verified and become eligible to use in environmental societies many test suites and an

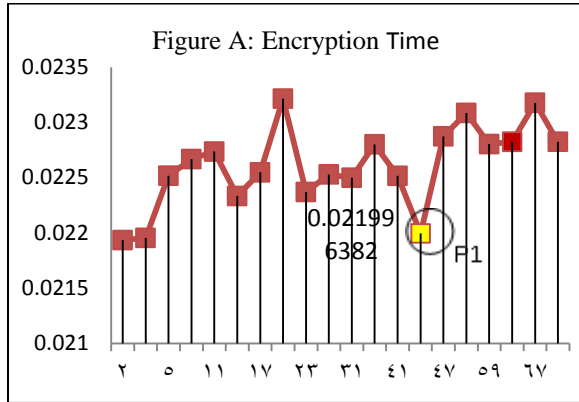
observation of computational complexity of prime number selection are done. Firstly to find the computation complexity of the prime numbers, the definition of the computational complexity becomes important. The computation complexity is defined as the measure of the complexity of the algorithm you could calculate time, space memory requirements, the communication bandwidth, the number of random bits, the amount of data and so on.

So a time and space measurements is applied to select the proper prime number for “Yes Vote” and “No Vote”. A prime numbers from 2 to 71 is encrypted for 50 times and at each time the time and space is calculated. At the end of 50 tests the average of the calculations was taken as shown in the following table:

The average value of the time and space complexity

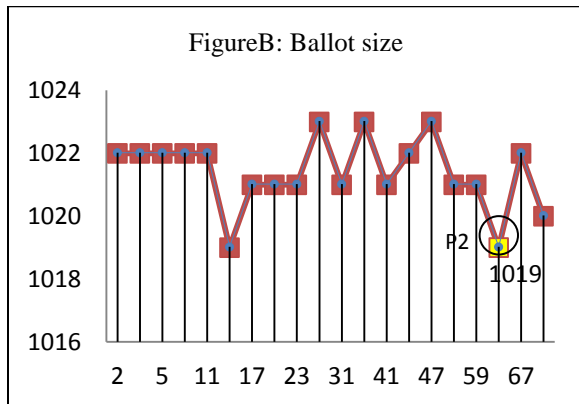
Prime number	Encryption time	Bit size
2	0.021935238	1022
3	0.021955202	1022
5	0.022518572	1022
7	0.022669281	1022
11	0.022737004	1022
13	0.022334453	1019
17	0.022548872	1021
19	0.023216597	1021
23	0.022371014	1021
29	0.022530683	1023
31	0.022500209	1021
37	0.022802971	1023
41	0.022517627	1021
43	0.021996382	1022
47	0.022874934	1023
53	0.023086981	1021
59	0.022804983	1021
61	0.022826364	1019
67	0.023179626	1022
71	0.022826086	1020

Figure A shows the time complexity of the prime number selectivity where the encryption time is figured out versus the corresponding prime number.



At point P1 the minimum time to encrypt the prime number equal 0.021996382 Sec at prime number equal 43.

Figure B shows the space complexity of the prime number selectivity where the bit size of the encrypted prime number is figured out versus the corresponding prime number.



At point P2 the minimum bit size of the encrypted prime number equal 1019 bit at prime number equal 61.

From figure 3 and 4, it is clear that the encryption time may be varied from 0.021996382 Sec (21.996 msec) at P equal 43 to 0.022826364 Sec (22.826 msec) at P equal 61 where the difference between two times equal 0.000829982. According to the bit size of the encrypted prime may be ranged from 1019 bit at P equal 61 to 1022 bit at P equal 43 where the difference between two sizes equal 3. As the time and space difference is comparably small. So, the selection of prime numbers could be selected from 43 to 61(In other words, Yes or No prime could be selected from 43 to 61).

9. CONCLUSIONS:

In this paper, we have developed an electronic voting scheme using Paillier cryptosystem and blind signature algorithm with the confirmation of electronic voting security requirement standards. RFID technology was implemented to satisfy eligibility concerns of voters. This scheme has been implemented by using Microsoft visual C# to take steps in the scheme performance. Besides, considerable tests and investigations have been used to fast up the scheme performance and reliability.

REFERENCES:

- [1] Electronic Voting Using Confirmation Numbers, 05346787
- [2] E-Voting System Security Optimization 2009.
- [3] Identity based Threshold Cryptography and Blind Signatures for Electronic Voting, 89-164, 2010
- [4] A survey on Cryptography Algorithms in Security of Voting System Approaches, 2008.
- [5] Josh Daniel Cohen and Michael J. Fischer, "A robust and verifiable cryptographically secure election scheme", in Proceedings of 26th Symposium on Foundations of Computer Science, pages 372–382, Portland, October 1985.
- [6] Josh Cohen Benaloh. "Verifiable Secret Ballot Elections". PhD thesis, Yale University, 1987.
- [7] Kazue Sako and Joe Kilian. "Secure voting using partially compatible homomorphisms". Advances in Cryptology - CRYPTO'94, Springer- Verlag, pages 411–424, 1994.
- [8] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. "A secure and optimally efficient multi-authority election scheme". Advances in Cryptology - EUROCRYPT, 1997.
- [9] David L. Chaum. Untraceable electronic mail, return address, and digital pseudonym. Communication of ACM 24, Feb 1981.
- [10] Choonsik Park, Kazutomo Itoh, and Kaoru Kurosawa, "Efficient anonymous channel and all/nothing election scheme", Advances in

Cryptology - EUROCRYPT'93, Springer-Verlag:248–259, 1993.

[11] Kazue Sako and Joe Kilian, “Receipt-free mix-type voting scheme – a practical solution to the implementation of a voting booth”. *Advances in Cryptology - EUROCRYPT'95*, 1995.

[12] Wakaha Ogata, Kaoru Kurosawa, Kazue Sako, and Kazunori Takatani, “Fault tolerant anonymous channel”, in *ICICS '97: Proceedings of the First International Conference on Information and Communication Security*, Springer-Verlag .pages 440–444, London, UK, 1997.

[13] Markus Jakobssen, “A practical mix”, lecture notes in *Computer Science*, 1403:448, 1998.

[14] Masayuki Abe, ”Mix-networks on permutation networks”, in *Asiacrypt'99*, volume 1716 of lecture notes in *Computer Science*, Springer-Verlag, pages 258 – 273, Berlin, 1999

[15] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta. “A practical secret voting scheme for large scale elections”. *Advanced in Cryptology - AUSCRYPT'92*, 1992.

[16] Kazue Sako. Electronic voting scheme allowing open objection to the tally (special section on cryptography and information security). *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 77(1):24–30, 1994.

[17] Tatsuaki Okamoto. “Receipt-free electronic voting scheme for large scale election”. *Proc. Of Workshop on Security Protocols'97*, LNCS(1361), 1997.

[18] Bruce Schneier, “Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C”, 1996.

[19] Johannes Buchmann, “Verifiable Mixnets Techniques and Prototype Implementation”, March 2007.

[20] “Electronic voting,” *Encyclopedia of Computers and Computer History*, prepared by Lorrie Faith Cranor and edited by Raul Rojas, published by Fitzroy Dearborn, 2001.