Secure Internet Voting System based on Public Key Kerberos

Hussein Khalid Abd-alrazzq[1], Mohammad S. Ibrahim[2] and Omar Abdulrahman Dawood[3]

**[1] College of Administration and Economic-Ramadi, Anbar University,
Ramadi, Anbar, Iraq**

**[2] College of Computer, Anbar University
Ramadi, Anbar, Iraq**

**[3] College of Education for Humanities Sciences, Anbar University
Ramadi, Anbar, Iraq**

Abstract

Electronic voting system is an important tool which allows voters to vote over the Internet without the geographical restrictions with considers important criteria in evaluating electronic voting schemes such as the mobility, democracy, and privacy. In this paper secure remote voting system has been presented. The proposed system uses public key Kerberos which is another form of traditional Kerberos as infrastructure deal with voters. The public key is used in all steps of Kerberos (not only in initial). The proposed system utilizes the advantages of threshold cryptography to prevent anyone to decrypt or sign the ballot alone without agreement all authorities, and use threshold blind signature to prevent discovers the vote or the identity of voter and protect the content of the ballot during casting and provide verifiable and discourages ballot buying.

Keywords: *Internet Voting System, Kerberos, Elliptic Curve, Blind Signature, Threshold Cryptography.*

1. INTRODUCTION

The wide spread of democracy concepts in several countries especially in this time lead to introduce new methods in management the elections which is the main tool in democracy systems that ensure to each eligible person to be responsible to detect his fate.

The traditional voting system is depending on basic concepts which are ballot paper, poll-sites, supervisors and others. These concepts have some disadvantage such as the cost of establish the sites of voting and restrict the voter such the employers and students or any eligible voter whose are far from their voting sites to be near of their sites in election time. The Internet voting system is a practicable alternative on account of the swift computer network and the benefits from cryptographic techniques. Every voter can participate in the election over the Internet, eliminating the geographical restrictions and thus increasing the rate of voting. The main goal of a secure electronic voting system is to ensure the privacy of the voters and the accuracy of votes [1].

Internet voting can by divided into two broad categories: (a) Remote internet voting, and, (b) Poll-site internet voting [2].

Category (b) solved the distance problem for employers and students whose are far from their ballot stations but the cost of establishing poll-sites is not solved. Our e-voting system focus on the category (a) which is solved the cost and distance problems.

In our system we depend on criteria that must be available at any electronic voting system proposed, these criteria are [3, 4]:

1. Eligibility***:*** Only eligible voters can take part in voting and every voter can cast only one vote.
2. Uniqueness: No voter should be able to vote more than once.
3. Accuracy: Voting systems should record the votes correctly.
4. Integrity: Votes should not be able to be modified without detection.
5. Verifiability: Should be possible to verify that votes are correctly counted for in the final tally.
6. Auditability: There should be reliable and demonstrably authentic election records.
7. Reliability: Systems should work robustly, even in the face of numerous failures.
8. Secrecy: No one should be able to determine how any individual voted.
9. Non-coercibility: Voters should not be able to prove how they voted.
10. Flexibility: Equipment should allow for a variety of ballot question formats.

In our proposal internet voting system we attain some of these criteria.

In Proposed system we use Kerberos, which is one of authentication mechanisms that used by companies, organizations and institutions that deal with its clients in secure and authenticated manner.

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users [5]. We use the Kerberos with public key cryptography concepts to increase the security, verifiability and efficiencyof the system. Elliptic Curve (EC) Arithmetic operations were used in generating public and private keys for public key cryptography, the principle of EC compared to RSA or ElGamal are offer the same security but with smaller bit size, thereby reducing processing overhead.

In our proposed system we proposed new Blind signature which is a special form of digital signature, which was introduced by David Chaum in 1982 [6], in which the content of a message is blinded before signature. In blind signature scheme, signer signs on the blind message using his/her private key and anyone can verify the legitimacy of the signature using signer's public key [7]. The concept of Blind Signature which is first proposed by Dr. Chaum's based on RSA while the proposed scheme for our Blind Signature is based on Elliptic curve.

The rest of this paper is organized as follows: Section 2 provide general description of the proposed system and its parts. Section 3 presents the proposed security techniques that are used in this system. Section 4 presents the proposed system. System evaluation has been achieved in Section 5. At end, theconclusionin section 6.

2. Description of the Proposed System

To have a tour for our proposed system, we will introduce an overview depending on the following two subsections:

2.1. Parts of the Proposed System

Our internet votingsystemcomprises of five partsrepresented by Initialization Setup Center (ISC), Voter (V),Key Distribute Center (KDC), Ticket Granting Server (TGS),and Application Server (AppS). See fig. 1 which illustrates how the parts of proposed system.

The Kerberos considered the core of the system which generated key for voters, permission them to voting, and collect the votes in order to tallying it later. Our Proposal's five parts participants will be explained as follow:

- Initialization Setup Center (ISC) generates the public parameters and generates public/threshold private keys ECC for the system parts.
- Public key Kerberos:
  - ✓ $KDC$is response to register the voters and generate the pair keys (public and private) for the voters with public key's certification depending on the public parameters and his public/private keys.
  - ✓ TGS is response to authenticate the voter. Itis similar to the central election commission in a traditional election, and it is responsible for verifying whether each voter registered with the KDC or not. If the voters have passed the registering then itsign the vote and ID (without read it) using blind signature to prevent revote.
  - ✓ $AppS$ receive the votes form voters and store them. AppS is similar to the polling station in a traditional election and is responsible for supervising the procedure election through verifying the voter cast vote properly to enable the Tallying Center counting the ballot correctly.
- Tallying Center (TC) retrieve the votes from the AppS in order to collecting the cast ballots and tallying the result of the election. When the tally center has collected one cast ballot, it must verify the legality of the ballot. Only legal ballots can be tallied in the counting phase.

In our model, we shall use public cryptosystems to ensure the security of transmission on a public channel, use threshold public-key cryptosystem to share a private key among the authorities such that messages can be decrypted only when a substantial set of authorities cooperate, and use the blind signature technique to protect the private information.

2.2. Proposed System Overview

In the registration phase the user request his/her pair keys by send hash of his identity with the random number to include in his certification in order to prevent uncovering the voter's identity in next phases. The user can obtain only one pair key because the voter have one identity (such as the national civic registration number) and password.

The voter is not able to create the token by himself, only during the interactivity with the authority, which is the TGS, in the authentication phase. The authority helps the eligible voter to construct the token only once, so the voter could obtain only one token. The authority has no idea how the voter's token looks like. Moreover, the validity of the token is verifiable to anyone. This concept is realized via blind signatures.

In the voting phase, the voter sends a ballot containing the token and his vote to the authority. The authority will not accept the ballot with invalid token or with the token that has already been used. This ensures that only eligible voters can vote, and that they can vote once because the voters cannot obtain more than one token. Also no one can deduce anything about how the voter voted except the tallying center but without know the voter's identity. The only restriction is that it should be hard or impossible to extract the voter's identity from the token and that each voter has to have different token.

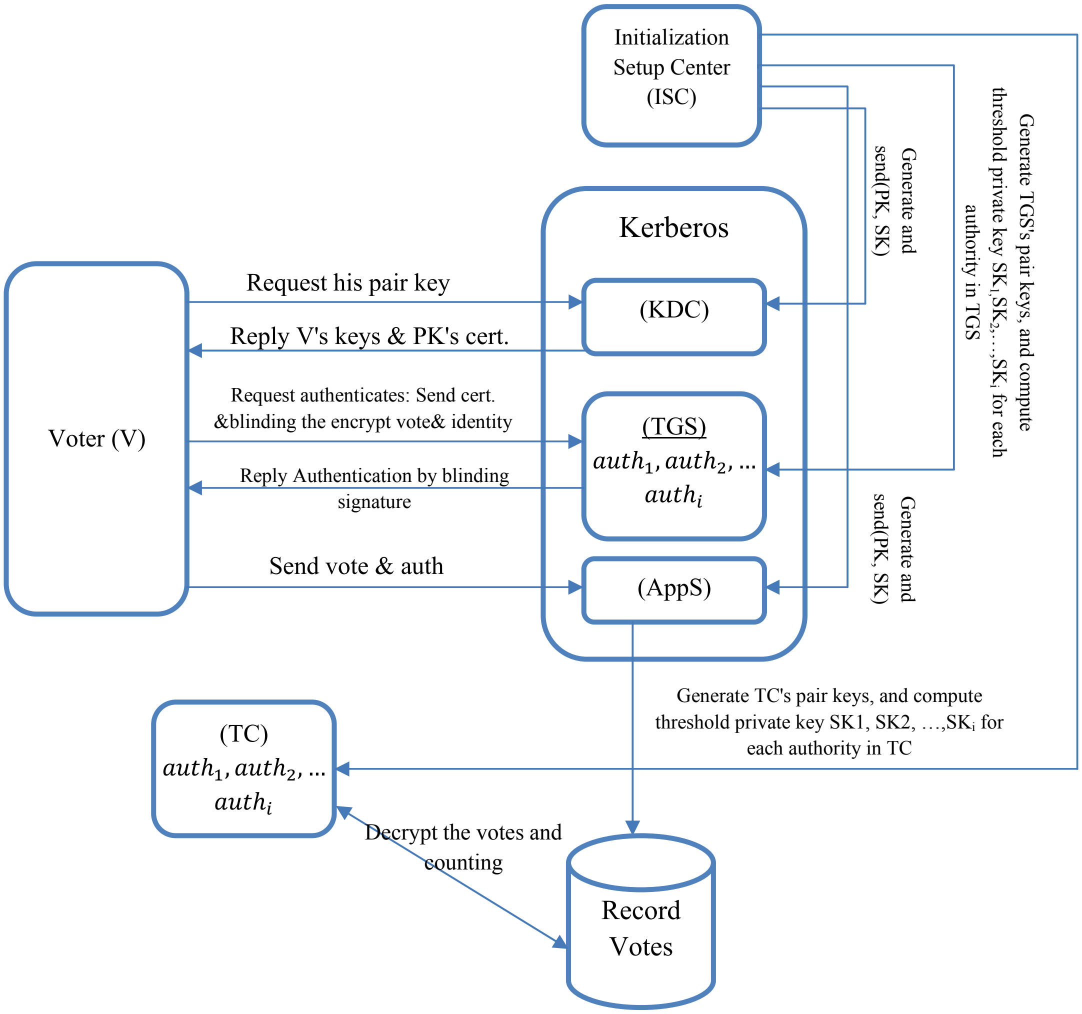
Initialization Setup Center (ISC)
Kerberos
(KDC)
(TGS)
$auth_1, auth_2, \dots$
$auth_i$
(AppS)
Voter (V)
Request his pair key
Reply V's keys & PK's cert.
Request authenticates: Send cert. &blinding the encrypt vote& identity
Reply Authentication by blinding signature
Send vote & auth
Generate and send(PK, SK)
Generate TGS's pair keys, and compute threshold private key SK1,SK2,…,SKi for each authority in TGS
Generate and send(PK, SK)
Generate TC's pair keys, and compute threshold private key SK1, SK2, …,SKi for each authority in TC
(TC)
$auth_1, auth_2, \dots$
$auth_i$
Decrypt the votes and counting
Record Votes

Fig.1 Proposed internet voting system.

The TGS and TC consist many of authorities, they must cooperate to be able achieve the decrypt or sign the message. For that, no one can reconstruct the private key alone without agreement the other authorities. In The proposed Internet Voting System applies the encryption technologies which include proposed threshold Elliptic Curve Integrated Encryption Scheme (ECIES) and threshold Blind Signature based on Elliptic Curve.

3. The Proposed Security Techniques

Before starting our proposed system we will introduce some of the most important concepts that used in our proposed system.

3.1. Threshold Elliptic Curve Cryptography

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 Elliptic Curve Integrated Encryption Scheme (ECIES). Messages will be encrypted as usual.

Setup: the parties should establish elliptic curve domain parameters *T* (*p, a,b, P, n, h*), let *KDF* denote the key derivation function chosen such as SHA-1, let ENC/DEC is the encryption/decryption function for a symmetric-key encryption scheme such asthe AES, and DEC is the decryption function.

Key Deployment

The users should have the elliptic curve key pair associated with the elliptic curve domain parameters *T*, as follow:

1. Choose the random number d as the private key
2. Compute$Q = dP$ as public key
3. Divide the private key to *i* part
    1) Choose the random number $1 < d_1 < d$ as private key for first party.
    2) Choose the random number $1 < d_2 < d - d_1$ as private key for second party.

3) Choose the random number $1 < d_3 < d - (d_1 + d_2)$ as private key for third party.
4) Repeat this operation for all parties, but must $d = d_1 + d_2 + d_3 \ldots + d_j$

4. Send public key for all parties with own private key.

Encryption: the encryption scheme is similar the original.

INPUT: Domain parameters *D* = *(p,a, b, P, n, h)*, recipient's public key Q_R, plaintext *m*.

1. Select $k \in R\,[1, n-1]$.
2. Compute $R = kP$ and $Z = hkQ$. If $Z = \infty$then go to step 1.
3. $(k1, k2) \leftarrow KDF(xZ\,, R)$, where *xZ* is the *x*-coordinate of *Z*.
4. Compute $C = ENC_{k1}(m)\ and\ t = MAC_{k2}(C)$.
5. Ciphertext(*R*, *C*, *t*).

Decryption:

INPUT: Domain parameters *D* = *(p,a, b, P, n, h)*, recipient's private key *d*, ciphertext *(R, C, t)*.

1. The *j* parties cooperate together to enable compute
$$Z = \sum_{i=1}^{j} hd_iR$$
If $Z = \infty$ then Reject the ciphertext.
2. $(k1, k2) \leftarrow KDF(xZ\,, R)$, where *xZ* is the *x*-coordinate of *Z*.
3. 4. Compute $\grave{t} = MAC_{k2}(C).\, If\ \grave{t} \neq t$ then Reject the ciphertext.
4. Compute $m = DEC_{k1}(C)$.

3.2. Blind Signatures (BS)

In our proposed system we proposed new BS. The concept of BS which is first proposed by Dr. Chaum's based on RSA while the proposed scheme for our BS is based on Elliptic curve.

The parties should establish elliptic curve domain parameters *T* (*p, a,b, P, n, h*), *P* a point with large prime order *n* which generates the whole additive group of *E* , the private key is denoted as a number *d* and the public key is denoted as $Q = dP$ and.

Blinding Phase: The requester picks a blinding factor *a, b*, where $1 < a, b < n$, and computes:

1. $R_1 = bP\quad and\ r_1 = x(R_1)$
2. $R_2 = aP\quad and\ r_2 = x(R_2)$
3. $R = abP\quad and\ r = x(R)$
4. $\overline{m} = (mr_1r_2^{-1}a^{-1}) mod\ n$
5. $e = H(r||m)\ mod\ n$

Where $x(R_1)$ *x*-coordinate of R_1, the requester sends $\overline{m}, r_1$ to the signer

Signing Phase: The signers cooperate together to signs the message $\overline{m}$ using his/her private key *d* after reconstruction as below:

1. each signer picks random number $k_i$and compute $T_i = k_iP$
2. $\bar{s} = \left(\sum_{i=1}^{j} d_j\overline{m} + r_1k_i\right) mod\ n$
3. $T = \sum_{i=1}^{j} T_j$

The signer returns $\bar{s}, T$ to the requester as the blind signature.

Extraction Phase: The requester after receiving the $\bar{s}$, he/she extracts the signature *s* as follows:

1. $s = (\bar{s}r_1^{-1}r_2a + ab)\ mod\ n$
2. $\bar{T} = aT$

The pair ($\bar{T}$, r_2, *s*) is the valid digital signature of message *m*

Verification Phase: Any one can verify the legitimacy of the digital signature ($\bar{T}$, *r*, *s*, *and e*) of message *m* as follow

$$e = H(x(sP - r_2\bar{T} - mQ)||m)$$

Correctness

The correctness of this scheme can be easily verified as follows.

The sign

$$\bar{s} = \sum_{i=1}^{j} d_j\overline{m} + r_1k_i$$

$$\bar{s} = (d_1\overline{m} + r_1k_1) + (d_2\overline{m} + r_1k_2) + \cdots + (d_j\overline{m} + r_1k_j)$$
$$= d\overline{m} + r_1k)$$

Where $d = d_1 + d_2 + \cdots + d_j$ *, and let* $k = k_1 + k_2 + \cdots + k_j$

The verifier has only digital signature (*T*, *r*, *s*) of message *m* for verification

$s = \bar{s}r_1^{-1}r_2a + ab$
$= (d\overline{m} + r_1k)r_1^{-1}r_2a + ab$
$= (d(mr_1r_2^{-1}a^{-1}) + r_1k)r_1^{-1}r_2a + ab$
$= (dmr_1r_2^{-1}a^{-1} + r_1k)r_1^{-1}r_{21}a + ab$
$= dm\, r_1r_2^{-1}a^{-1}r_1^{-1}r_2\, a + r_1\, k\, r_1^{-1}r_2\, a + ab$
$= dm\ + r_2ak + ab$

Finally $s = dm\ + r_2ak$

In the verification$e = H(x(sP - r_2\bar{T} - mQ)||m)$

Where $sP = (dm\ + r_2ak + ab)P$ and $mQ = mdP$ and $\bar{T} = aT$

$\because T = T_1 + T_2 + \cdots + T_j\ =\ k_1P + k_2P + \cdots + k_jP$

$\because k = k_1 + k_2 + \cdots + k_j$

$r_2akP =\ r_2ak_1P + r_2ak_2P + \cdots + r_2ak_jP$
$= r_2aT_1 + r_2aT_2 + \cdots + r_2aT_j = r_2aT$

$= dmP\ + r_2akP + abP$

$e = H(x(mdP\ + r_2aT + abP - r_2aT - mdP)||m)$

$e = H(x(abP)||m)$ Where $R = abP$

As the requester randomly selects two blinding factors (a, b) to compute the blind message $(\overline{m}, e)$ so from the blind messages $(\overline{m}, r_1)$, the signer cannot compute the original message as it is based on ECDLP, so that the blindness is verify. And the signer cannot link the signature to the message as the signer only has the information $(\overline{m}, r_1)$, for all blinded messages. If the requester reveals the signatures of a message and its signature (*a*,*b*) to public, from this information the signer can retrieve the original message. Therefore, without the knowledge of the secret information (*a*, *b*) of therequester, anyone cannot trace the blind signature, so that the untraceability is verify

4. The Proposed Internet Voting System

Our internet voting system consists of five phases, namely: preparation phase, the registering phase, the authentication phase, the voting phase, and the tallying phase. The details of our system are described as follows:

i. **Preparation Phase**: the preparation phase executed by ISC in beginning operating the system to generate the public parameters and public/private keys, as follow.

A. Public Parameters:

1. q: Select a large prime number, q, which Defines the underlying finite field Fq. The field size is defined by use q as the module.
2. *FR*: Field representation of the method used for representing field elements in ∈*Fq*, with *E*(*Fq*)
3. Select the curve order, #*E*(*F*q), such that:
   $q+1-2q \leq \# E(Fq) \leq q+1+2q$
4. *a, b*: The coefficients defining the elliptic curve *E*, elements of *Fq*.
5. *G*: A point, *G* = (*x*, *y*), on an elliptic curve called the *base point* or *generating point*; it is defined by two field elements *x* and *y* in *F*q.
6. *n*: The order of the base point *G*, normally a large prime.

B. Participants' keys

1. Selects a random or pseudorandom integer *d* in the interval (1, n – 1)
2. Computes $Q = d * G$
3. Makes Q the public key, Pub, and d the private key, $Priv$
4. Threshold private key based on elliptic curve cryptography is Divided the private key to *ith* authorities, $1 < d_1, d_2, \dots, d_i > d - 1$, where
   $$d = d_1 + d_2 + \cdots + d_i.$$

The steps 1-3 executed to generate the Apps and KDC's keys. Repeat the steps 1-4 executed to generate the TGS and TC's keys.

The public key of KDC, TGS, and TC with public parameter are posted on bulletin board to be able every voter reach it.

ii. **Register Phase:** the register phase executed by KDC (in Kerberos) to generate the public/private keys for voters (V), as follow

A. Identification :

In this phase only the people eligible to vote should be able to do so, secure online identification of the voters must be feasible. This presupposes, first, that it is practicable to require ID particulars from voters when they log on and, secondly, that each voter has a unique, personal password. At present, the KDC has the election database contains the national civic registration number of everyone; it is similar to the electoral register. In an Internet voting system, the electoral register needs supplementing with the voter's personal password or code, to permit reliable identification. One alternative that may be considered is whether, as in Finland, to introduce a citizen's smart card on which the holder's ID particulars are stored on a microchip in a plastic card. Introducing such a card would permit the problem of identification (authentication) in online voting to be solved.

B. Generate voter's pair keys:

1. Voter pick a as random number.
2. $Voter \rightarrow KDC$:
   $E_{PK_{KDC}}[ID_V, VPP, H(ID||a)]$
   $VPP = Voter\ Personal\ Password$
3. $KDC \rightarrow Voter$: $E_{VPP}[K_V, Cert_V]$
   $V = Voter$
   K_V =Voter's public keyPK_V, voter's private keySK_V
   $Cert_V$
   $= E_{SK_{KDC}}[PK_V, H(ID||a), LifeTime$
   $, TimeStamp]$

iii. **Authentication Phase:** the authentication phase executed by TGS (in Kerberos) to sure the voter is register in KDC and has the own his keys, and it signs the identity of voter and the own his vote. At first The voter download the blank ballot M from KDC and then picks out one candidate to mark on the blank ballot, as follow

A. Voter compute:

1. Encrypt the ballot by TC's public key $C = E_{PK_{TC}}[M]$
2. Choose random number $r\ where\ 1 < r < n$
3. Encrypt $C\ and\ H(ID||a)$ with the random number as blind signature
   (Use elliptic curve) $X = BS_{rq}[C]$, $Y = BS_{rq}[H(ID||a)]$
   Where BS_{rq} is the request blinding signature (blinding phase).
4. Sign the $X\ and\ Y$ with voter' s private key$X_1 = E_{SK_V}[X]$, $Y_1 = E_{SK_V}[Y]$
5. Encrypt the result with TGS' s public key $Z = E_{PK_{TGS}}[X, X_1, Y, Y_1]$

$Voter \rightarrow TGS$: $Z, Cert_V$

B. TGS compute

1. Decrypt Z using its private key$(X, X_1, Y, Y_1) = D_{SK_{TGS}}[Z]$
2. Retrieve the voter's public key from certification $PK_V = D_{PK_{KDC}}[Cert_V]$, and verify the validity of the key and lifetime according to Timestamp
3. check if $X \equiv D_{PK_V}[X_1]\ and\ Y \equiv D_{PK_V}[Y_1]$then continue

4. Sign the X and Y with TGS's private key without know what is contain

$$X_2 = \sum_{i=1}^{j} BS_{S_{SKtgs_j}}[X] \ , \quad Y_2 = \sum_{i=1}^{j} BS_{S_{SKtgs_j}}[Y]$$

Where $BS_{S_{SKtgs}}$ is blind sign by private key of TGS (signing phase), and j the number of authorities in TGS.

5. Encrypt theX_2 and $Y_2$with voter's public key $w = E_{PK_V}[X_2, Y_2]$

$TGS \rightarrow Voter$: w

C. Voter compute:

1. Decrypt the w using his private key$(X_2, Y_2) = D_{SK_V}(w)$
2. Use r to remove blinding (use elliptic curve)

   $SG_1 = BS_{ex}[X_2] = S_{SK_{TGS}}[C]$

   $SG_2 = BS_{ex}[Y_2] = S_{SK_{TGS}}[H(ID||a)]$

   Where BS_{ex} is remove the blinding (Extraction phase) and $S_{SK_{TGS}}$ is sign by private key of TGS
3. $Check\ if C = D_{PK_{TGS}}[SG_1] and\ H(ID||a) = D_{PK_{TGS}}[SG_2]$

iv. **Voting Phase:** To cast a vote, after the voter is authenticated, the Validator sends the confirmation message, vote, and certification, encrypt by AppS' public key, to the Application Server to verify the validand record the vote with hash of identity.

$Voter \rightarrow AppS\ :\ E_{PK_{AppS}}[SG_1, SG_2, C, Cert_V]$

A. AppS:

1. Retrieve $(SG_1, SG_2, C, Cert_V) = D_{SK_{AppS}}[SG_1, SG_2, C, Cert_V]$
2. Retrieve the voter's public key and hash of identity $(PK_V, H(ID||a)) = D_{PK_{KDC}}[Cert_V]$
3. Check if $H(ID||a) = D_{PK_{TGS}}[SG_2]\ and\ C = D_{PK_{TGS}}[SG_1]$
4. record $H(ID||a)$as voted and record $[H(ID||a), SG_1, SG_2, C]$ $in\ counting\ list$

v. **Counting Phase:** When the voting time is up, AppS (Voting phase) stops collecting ballots, This part is completely hidden to the voter, After receiving the encrypted vote the Tallying Center performs the following operations during counting phase:

1. Check if $H(ID||a) = D_{PK_{TGS}}[SG_2]$
2. Decrypt the vote

$$M = \sum_{i=1}^{nTC} D_{SK_{TC_i}}[C]$$

nTC: Number of authorities in Tallying Center

3. Record M, C, SG_2 , $H(ID||a)$ in result list to publish.

5. System Evaluation

The proposed internet voting system evaluated depending on criteria that must be available at any electronic voting system. So we will explain each requirement in these criteria and how the proposed system has been attaining it:

1. **Eligibility:** The authorities prepare the keys of eligible voters before voting phase and register it in the bulletin board; each profile of voters is placed along with their public key and certification. On the other hand in Authentication phase of the proposed system, only ballots will be confirmed that encrypted public key of those has the certification. So only eligible voters can send a valid vote. On the other hand, if eligible voters try to vote several times, in the voting phase detected this voter is ineligible because the hash of identity is record $H(ID||a)$ in counting list where the Server checks the list by computing $H(ID||a) = D_{PK_{TGS}}[SG_2]$before the ballot record. The voter cannot replace $H(ID||a)$ because it exist in certification.
2. **Privacy:** In anonymous voting, no one can find out the relationship between a cast ballot and a specific voter, and the voting strategy cannot be known during the whole voting procedure. In our internet voting system, we use the blind signature based on elliptic curve scheme to protect the privacy. In the authentication phase, the voter generates a unique name to produce $H(ID||a)$ and the voted ballot C, and then he/she uses the blinding (using elliptic curve) to calculate X and Y,
3. **Verifiability**: Each voter can view his/her sent encrypted ballot in the result list. Also each voter can verify created signature by authorities. TC announces the counting result list which includes M, C,SG_2 , $H(ID||a)$. For that, any voter can check whether his/her cast ballot was counted correctly or not by $H(ID||a) = D_{PK_{TGS}}[SG_2]$ and $C = E_{PK_{TC}}[M]$.
4. **Coercion-resistance**: Since the identity of all participants is protected in voting, authentication, and tallying phase 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. If anyone wants to prove that a specific $H(ID||a)$ represents ID, the parameter a must be known.
5. **Accuracy**: In this voting system, the blank ballot is a free document for anyone to download. In other

words, blank ballot isn't has any identity information. In the voting phase, only an eligible ballot can be cast. Then, TC checks the list by computing $H(ID||a) = D_{PK_{TGS}}[SG_2]$ before the ballot counting is started. Also the cast ballot M was encrypted by using the TC's public key therefore, no one can decrypt it only the TC.

6. **Fairness*:***the authentication token operation, which is blinding signature in authentication phase, and the counting votes operation in tallying phase only are done in cooperation of authorities by using threshold cryptography. So no one can be aware of the intermediate results.
7. **Robustness*:*** Since voter's certificate encrypted by KDC's private key and his/her selected vote encrypt by the TC public key, no one can change the content of encrypted ballot and certification, since any set lower than j of Authority cannot do alone any step of tallying phase.

6. Conclusion

The proposed scheme is an efficient electronic voting scheme that provides basic security requirements and the voter's identity remains hidden. It utilizes the advantages of the threshold cryptography to make the counting votes submit to group of authority. The secure internet voting system should not only allow all voters to verify the voting result but also avoid ballot buying. Therefore the proposed internet voting system uses proposed threshold blind signature to protect the content of the ballot during casting, the proposed internet voting system is verifiable and discourages ballot buying at the same time. So our scheme is expected to serve as efficient and secure. At the end of the proposed protocol has been provided some of the most important security criteria for the electronic voting systems.

References

[1]. Chun-Ta Li, Min-Shiang Hwang, Yan-Chi Lai, "A Verifiable Electronic Voting Scheme over the Internet", Sixth International Conference on Information Technology: New Generations, 2009.

[2]. P. Akritidis, Y. Chatzikian, M. Dramitinos, and Nikolaos V. ,"The VoteSecure Secure Internet Voting System", Springer-Verlag Berlin Heidelberg, pp. 422 – 425, 2005

[3]. Dimitris Gritzalis, "Secure Electronic Voting", Seventh Computer Security Incidents Response Teams Workshop Syros, Greece, 2002

[4]. Sadegh Jafari, Jaber Karimpour, Nasour Bagheri, " A new secure and practical electronic voting protocol without revealing voters identity", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 6 June 2011.

[5]. William Stallings: Cryptography and Network Security: Principles and Practices, Fourth Edition, Prentice Hall, 2006.

[6]. D. Chaum, "Blind Signature Systems", U.S. Patent 4,759,063, 19 Jul 1988.

[7]. Zuowen Tan, Zhuojun Liu, Chunming Tang, "Digital Proxy Blind Signature Schemes Based on DLP and ECDLP", MM Research Preprints, 212–217, 21, December 2002.

Hussein Khalid Abd-Alrazzaq was born in Basra, Iraq (1986), now live in Ramadi, Anbar. He obtained B.Sc. (2008), M.Sc. (2011) in Computer Science from the College of Computer, Anbar University. He is teaching staff member in Public of Administration Department in College of Administration and Economic-Ramadi, Anbar University. His research interests data and network security, cryptography.

Mohammed Salah Ibrahim was born in Anbar, Iraq (1985), now live in Fallujah, Anbar. Complete study of secondary school in Fallujah (2005). He obtained B.Sc. (2008), M.Sc. (2011) in Computer Science from the College of Computer, Anbar University. Mohamed worked as an administrator in the Department of calculating in Al-SafaCo. to oversee the reconstruction work in Fallujah (2007), and worked with Afaq Co. as accountant (2010). Now, He is teaching staff member in Computer Science Department in College of Computer, Anbar University.

Omer Abdulrahman Dawood was born in Habanyah, Anbar, Iraq (1986), now live in Ramadi, Anbar. He obtained B.Sc. (2008), M.Sc. (2011) in Computer Science from the College of Computer, Anbar University. He is teaching staff member in English Department in College of Education and humanities sciences, Anbar University. His research interests data and network security, cryptography.