European Journal of Scientific Research
ISSN 1450-216X / 1450-202X Vol. 112 No 3 October, 2013, pp.387-393
http://www.europeanjournalofscientificresearch.com

Proposed Secured Remote E-Voting Model Based on Blind Signature

Reham Mohamed Kouta
Arab Academy for Science and Technology
E-mail: mmkouta@gmail.com
Tel: 01006439141

Essam-Eldean F. Elfakharany
Arab Academy for Science and Technology
E-mail: essam.fakharany@gmail.com
Tel: 01117722018

Wafaa Boghdady Mohamed
Arab Academy for Science and Technology
E-mail: wafae.boghdady@gmail.com
Tel: 01001633533

Abstract

We proposed a secured e-voting system model by using blind signature. Our proposed model achieved all security requirements which are: (authentication, privacy, integrity, non repetition).

Our proposed model depends on these main entities that are involved within the voting processes

(voters registration, voting, counting, audit), these entities are: certificate authority, ministry of interior, voter, high committee of elections(investigator), counter)

The voter can vote from any remote where with secured data transfer (ballot) by using the blind signature to blinded ballot and then sign it, when it sent to the high committee of elections (investigator) for checking the voter eligibility there is encrypting random value r that attached with the blind ballot, using for removing blind the ballot which is encrypted by counter's public key.

The high committee of elections checks the signature of voter and checks that if he eligible voter or not. Then remove the voter's digital signature and put his digital signature and then sends to counter party.

The counter party checks the signature of high committee of election and extracts the random value r by decrypting with his private key and removing blind the ballot and counts the vote.

Keywords: Secured e-voting system, blind ballot, certificate authority, ministry of interior.

1. Introduction

Election is a fundamental instrument of democracy that provides an official mechanism for people to express their views to the government. Traditionally, the process of voting is quite complicated because voter must come in person to vote.

This problem resulting low participation rate at elections. Electronic voting system can overcome those problems in national election, by enabled the voter to vote from his home or office or from any remote place.

Although remote electronic voting is more flexible and easier for voters than the traditional voting, but also it more vulnerable than traditional voting due to the nature of digital processing of election data which can be easily spread, manipulated within the network, hence may result in widespread fraud and corruption [1, 2].

For theses, we will propose a prototype of the remote electronic voting In this research, that may

Satisfy the security requirements of voting process [3, 4]. Which can reduce human errors that occurred in traditional voting process and also reduce the fraud of voting with making the process of voting easier and more reachable for the voters (citizens)?

2. Preliminaries

Let E= {V, VA, T, CA, MOI} be the set of entities involved where V voter, VA investigator, T counter, CA certificate authority and MOI ministry of interior. Let X Є E, X is represented as follows. X= (PK[x], SK[$_x$], n_x), PK[x]is the public key of Entity X, SK[$_x$] is the private key of X, and n_x is the RSA constant. Recall that pub_x and privx are multiplicative inverses to each other mod Φ (n_x), where Φ (.) is the Euler totient function. We assume $priv_x$ Є {MAX (p_x, q_x), Φ (n_x)-1} is a large prime for two large primes p_x, q_x, and $n_x = p_x * q_x$. We also assume for message M the following holds:

$(M^{PK[x]}) \bmod n_x)^{SK[x]}) \bmod n_x =$

$(M)^{SK[x]} \bmod n_x)^{PK[x]}) \bmod n_x = M.$

We also assume for X Є E, X does not knows $priv_y$ of Y Є E, Y ≠ X but knows the rest of Y parameters and DC_x denotes the digital certificate of X Є E. Thus we can represent the entities involved as follows:

1. V= (PK [$_{Vo}$], SK [$_{vo}$], n_v).
2. VA= (PK [$_{VA]}$, SK [$_{vA}$], n_{vA}).
3. T= (PK [$_{TA}$], SK [$_{TA}$], n_{TA}).

For two entities X, Y Є E, Y ≠ X, a message m from X to Y is sent over a secure channel that follows the secure socket protocol as follows:

X signs on m, generating encrypt $_{privx}$(H(m)) where H is a hashing one way function, X generates a session key SK, X generates the encrypted message encrypt $_{SK}$ (m ||encrypt $_{privx}$(H(m))|| DC_x), X generates the digital envelop encrypt $_{puby}$(SK) to achieve privacy, and finally X sends both the encrypted message and the digital envelop to Y. Y opens the envelop as follows: SK= decrypt $_{privy}$ (encrypt $_{puby}$(SK)), Y gets m ||encrypt $_{privx}$(H(m))|| DC_x =decrypt$_{SK}$ encrypt $_{SK}$(m ||encrypt $_{privx}$(H(m))|| DC_x), Y verifies H(m) = decrypt$_{pubx}$(encrypt $_{privx}$(H(m)) achieving authenticity, non repudiation, and message integrity [5].

3. The Proposed Protocol

The procedures and steps that occurred at any elections must be divided into three stages:

1. The pre-voting stage (preparation).
2. The voting stage (the casting of the votes).
3. The post-voting stage (counting, auditing).

1. The pre-voting stage: this phase include all preparations that occurs before the period of elections, at proposed model this stage include these 2 steps:
   a) Voter registration.
   b) Ballot preparations.
2. The voting stage: these phase include all the chain of steps that occurred within the period of elections until the voter casting his vote and send it, at proposed model these stage include 3 steps:
   a) Voter getting ballot.
   b) Blind ballot.
   c) validating & signed blind ballot
3. The post-voting stage: these phase include all the chain of steps that occurred after the period of elections ended, which include all these steps:
   a) Unblind ballot.
   b) Counting the unblind ballots.
   c) Auditing.

3.1. Pre-Voting Stage

3.1.1. Voter Registration

An individual must register to be an eligible voter. This is done before the voting period. Voter registration for E-Voting is done as follows:

I. The individual generates key pair in smart card. And then generates certificate request during generates certificate request the system asks his information like name, ID and address, e-mail etc.
II. The individual sends his certificate request to CA to issue digital certificate.
III. The CA inquires the information of voter from MOI to check if the individual are eligible or not, if eligible the CA issues digital certificate and sends to voter's email.
IV. The voter downloads his digital certificate from his email and imports to his smart card.
V. The voter download ballot from organized election website. The ballot contains unique id to prevent from multiple cast.

3.1.2. Ballot Preparations

I. At this stage the high committees of elections (investigator) starts to generate ballots with different and unique IDS which include list of candidates names.
II. High committee of elections will send the numbers of the ballots' IDS that generated to the counter as list of the ballots ready for casting votes, make these for purpose if counter received any ballot it's id number not included at these list these mean that ballot is invalid,
III. High committee of elections(investigator) will sign each ballot of these ballots using their secret key, so the voter must get the ballot(**B**) signed, which can represent into these equation:
$\mathbf{B}^{\mathbf{SK\,[VA]}}\ \mathbf{mod}\ (\mathbf{n}_{\mathbf{va}})$
IV. High committee of elections will upload these signed ballots into the official website of the elections as preparation step for voters to cast their votes.

3.2. Voting Phase

3.2.1. Voter Getting Ballot

I. Voter will download the ballot from the high committee of elections (investigator) website and it must be signed also.
II. Voter will unsigned this ballot using the high committee of election's public key, then will cast his vote, and then will cast his vote into the ballot.

3.2.2. Blind Vote

I. The voter cast his ballot and then blind ballot as Fig (1) by generates a random value r such that *r* is relatively prime to *N* (i.e. *gcd*(*r*, *N*) = 1). *r* is raised to the public exponent *e* modulo *N*, and the resulting value r^emodN is used as a blinding factor [6].

II. Voter will encrypt these random no. r in two different ways:

1. Voter will encrypt these random no. r using the investigator 's public key, which will be the blind factor(**BF**), so the blind factor can be represented into these equation:
   BF = ($\mathbf{r^{PK\,[va]}}$ **mod (**$\mathbf{n_{va}}$**)).**
2. Voter will encrypt this random no. r using the counter's public key, which will be used in the unblind factor(**UBF**), so the unblind factor can be represented into this equation:
   UBF = ($\mathbf{r^{PK\,[TA]}}$ **mod (**$\mathbf{n_{TA}}$**)).**

III. Voter will blind his ballot using the blind factor by multiply his ballot with the blind factor, so the blind ballot (**BB**) can be represented into these equation:
BB = B* BF

IV. Voter will attached the blind ballot (BB) with the unblind factor (UBF), so these will resulted B'' which can be represented into these equation B'' = (BB || UBF), SO
B'' = (BB || UBF)

V. Voter will sign these B''using his secret key, so these will resulted the signed B'' (**SB''**), which can be represented into these equation **SB''= (B'')**$^{\mathbf{Sk[vo]}}$**mod(**$\mathbf{n_{vo}}$**).**

3.2.3. Validating & Signed Ballot

I. Voter send the SB'' to the high committee of elections (investigator) for authenticate the voter and check the voter's signature eligibility and also to check if voter voted before or not.

II. Investigator will verify the voter's signature as Fig (2) by using his public key:
SB'' = ((B)* ($r^{pk[va]}$ mod (n_{va})),
($r^{PK[TA]}$ mod (n_{TA})))$^{SK[vo]}$$\cancel{mod(n_{vo}}$))$^{PK[vo]}$mod($n_{vo}$)., which will resulted
B'' = (BB $\cancel{\| UB}$**F)**

I. Investigator after verifying the voter signature and check these the first time for voter to vote will sign these B'' using his secret key so these will resulted investigator signed B'' (**VSB''**), This can be represented into this equation:
VSB'' = (B'') $^{\mathbf{SK\,[va]}}$ **MOD (**$\mathbf{n_{va}}$**)**

While investigator using this secret key to sign the ballot, this secret key will decrypt the random no. that encrypted by the investigator public key (BF) which will resulted.

VSB''= ((B) $^{\mathbf{SK\,[va]}}$ **MOD (**$\mathbf{n_{va}}$**) * (r)) ||**
(UBF)$^{\mathbf{SK\,[va]}}$ **MOD (**$\mathbf{n_{va}}$**)**

II. Then investigator will send the VSB'' to the counter party.

3.3. Post-Voting Stage

3.3.1. Unblind Votes

I. Counter will received ballots from the investigator (VSB'') then do these process as Fig (3) into each VSB '':

A Counter will insert each VSB'' into separator function, to get:

1) The unblind factor but signed from investigator (VSUF**).**
VSUF = UBF$^{SK\,[VA]}$**, SO**
VSUF = ($\mathbf{r^{PK[TA]}}$**)**$^{\mathbf{SK[VA]}}$

2) The Investigator signed ballot (VSBB).
VSBB = r * (B) $^{\mathbf{SK\,[VA]}}$

note the random no. r no longer encrypted by the investigator public key, coz these encryption removed while the investigator sign the blind ballot using his secret key.

B Counter will verify the signature of investigator on the blind facto, which will resulted the unblind factor:
$(UBF) = (r^{PK[TA]} \text{ mod } (n_{TA}))$

C Counter will decrypt the random no. using his secret key:
$\cancel{(r}^{PK[TA]} \text{ mod } (n_{TA})^{\cancel{SK[TA]}} \text{mod}(n_{TA}) = (R)$
So will get the random no. r

D Counter will use the random no. to unblind the vote by multiply the blind ballot by the random no. versa:
$(r * B^{SK\,[va]} \text{mod}(n_{va}) \cancel{*} 1/ r$, which will resulted the ballot unblind and signed from investigator:
Vote = $B^{SK\,[va]} \text{ mod } (n_{va})$

3.3.2. Counting the Unblind Ballots

II. Counter after unblinding the vote will count it according to the voter selection.

III. Counter will declare the result about the candidates that take the highest number of ballots counted.

3.3.3. Audit

I. It's phase of auditing and reviewing the counting phase, these phase occurred especially at the case of when any one of the candidates appealed about the counted number of the votes that he got, after declaring the result of elections.

II. audit phase occurred under the supervision of high committee of elections (investigator) which will compare the number of ballots that generated by them and the numbers of the ballots IDS receives by counter (check the ID number of each valid ballot that counted by counter).

III. High committee of elections also checking the ballots that counted as invalids' ballots must apply one of 3 conditions:

   a. Ballot no. ID not identical to the serial ids numbers of ballots that generated by the investigator, which means these ballot not coming from investigator, its fraud by any hacker.
   b. Ballot received by counter is not signed from the high committee of elections (investigator), which means that ballot was attaced by attacker.
   c. Ballot receives by counter is not blind(unblind) which means also these ballot, hacked by hacker, into these 3 cases the ballot counted as unvalid vote.

IV. The audit phase at our proposed model depends on the ballot's ID'S, at these phase the declaration of results not only about the number of votes that each candidate got, but also about the IDS numbers of ballots that each candidate take, which will make the candidate check random sample of his supporters (voters), that they know their ballot's id's, they can check their ballots counted for which candidate.

4. Tables and Figures

The bellowing tables contain the abbreviations used in paper. The table (1) contains the abbreviations of key pairs of entities used in proposed model and the table (2) contains the abbreviations of data items used in proposed model.

Table 1: key pairs of entities at our proposed model.

Sk[va]	Investigator (high committee of elections) secret key
Pk[va]	Investigator (high committee of elections) public key
Sk[vo]	Voter's secret key
Pk[vo]	Voter's public key
Sk[ta]	Counter's secret key
Pk[ta]	Counter's public key

Table 2: main data items at our proposed model.

R.	Random no. generated by voter application
B	Ballot
BF	Blind factor, which is (random no.) encrypted by investigator public key PK[VA]
UBF	Unblind factor, which is (random no.) encrypted by counter public key PK[TA]
BB	Blind ballot, which the ballot multiply by random no., these no. encrypted by investigator public key PK[VA]
B’’	Blind ballot concatenate the unblind factor(BB ‖UBF)
SB’’	B’’ signed by voter secret key
VSB’’	B’’ signed by investigator secret key
VSUF	unBlind factor that signed from the investigator, using investigator secret key SK[VA]
VSBB	Blind ballot that signed from the investigator, using investigator secret key SK[VA]
Vote	Ballot signed from investigator (unblind)

Figure 1: blind phase

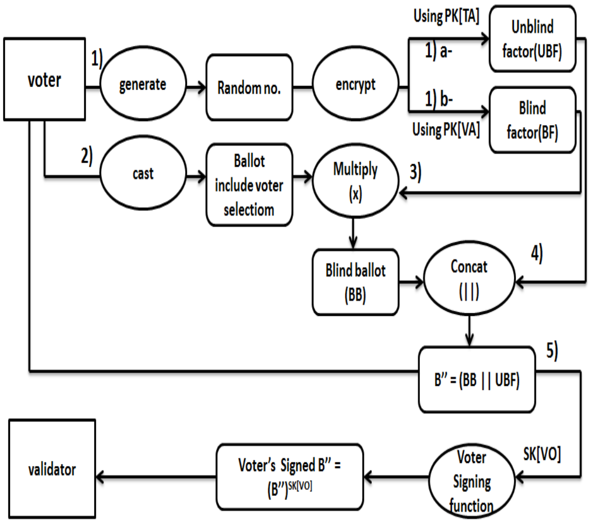


Figure 2: validating phase

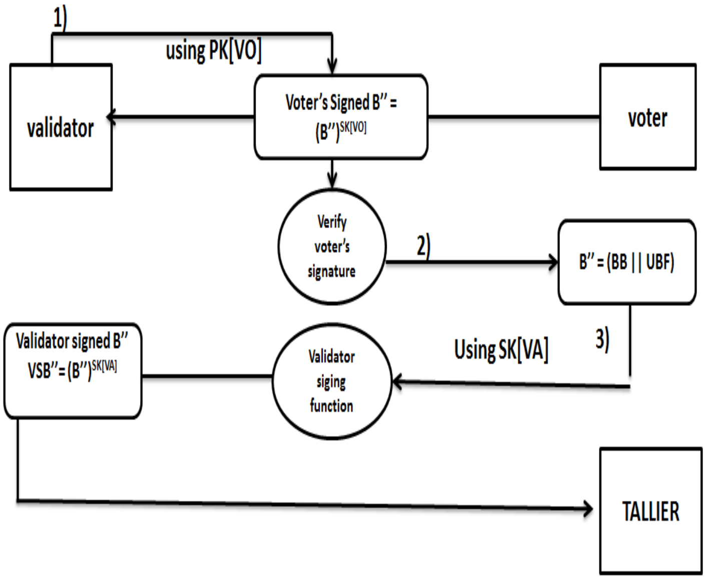
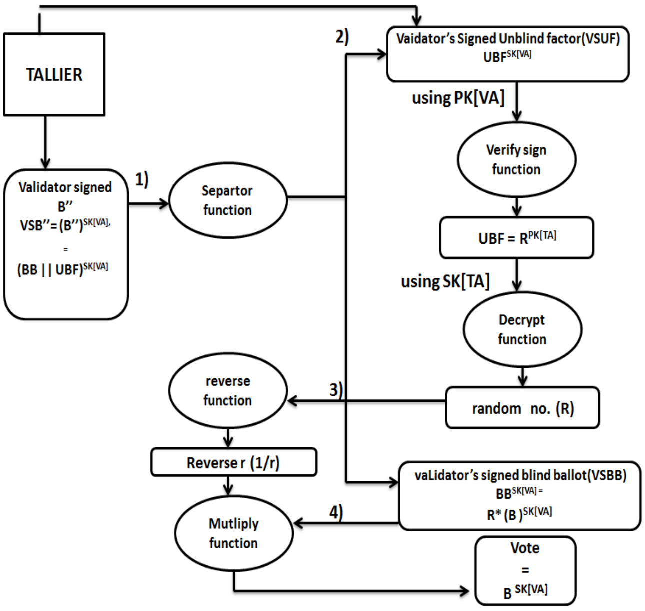


Figure 3: unblind phase



4. Conclusion

We have proposed electronic voting system that satisfied security requirements and we expect the participations rate is increased because the voters will not pending in long queue. With electronic voting the voting will be faster than the traditional voting.

References

[1] Subariah Ibrahim, Mazleena Salleh and Maznah Kamat, "Electronic Voting System: Preliminary Study, " *Jurnal Teknologi Maklumat*, Vol. 12, pp. 31-40, 2000.

[2] Subariah Ibrahim, Mazleena Salleh and Maznah Kamat, "Design of a Secure Web-Based Electronic Voting System, " in *Proceedings of Malaysian Science and Technology Congress*, 1999.

[3] R. Cramer, R. Gennaro, and B. Schoenmakers, and M. Yung, "Multi-Authority Secret-Ballot Elections with Linear Works." *Eurocrypt '96, LNCS 1070*, pp 72 – 83, 1996.

[4] L.R. Cranor, and R.K. Cytron, "Design and Implementation of a Practical Security-Conscious Electronic Pollind System, " *Washington University: Computer Science Technical Report*, 1996.

[5] Stalling, W., Cryptography and Network Security, 3rd Edition, Prentice Hall, New Jersey, 2003.

[6] Subariah Ibrahim, Maznah Kamat, Mazleena Salleh, Shah Rizan Abdul Aziz, Secure E-Voting With Blind Signature, "*Faculty Of Computer Science & Information Technology, University Technology Of Malaysia".*

[7] Robling Denning, Cryptography and Data Security, 1982.