# Secure E-Voting System with Secure Storage Media

Shaikh Muhammad Allayear* and Sung Soon Park**
Dept. of Computer Science & Engineering, Anyang University
**e-mail**:*allayear@anyang.ac.kr,**sspark@aycc.anyang.ac.kr

**Abstract**

The Global IT revolution is growing rapidly. Government and business have to be ready to meet the increased demand for effective and secure online services. With the E-Government practicing, day-by-day the public demand is also increasing simultaneously. Now this present moment, one of important research part is secure E-Voting for E-Government service, but for this important factor or Government Issue, it needs information privacy for secure information transaction of citizen's opinions and secure authentication. This paper has analyzed several approaches E-voting protocols, those are implemented with many digital signature mechanism and maintained many types of cryptographic rules, which are main factor for information privacy. In this paper we have discussed them with a view to voter anonymity and protection from manipulations. The paper then developed an algorithm designed to guarantee anonymity of the voter and to avoid the risk of manipulation of votes. In this paper the proposed algorithm is based upon the strict separation of voter's registration and submission of votes, which means that certain information has to be stored on a secure storage media.

## 1. Introduction

Each legal citizen has the right and has duty to elect senators by the election for their country. Voting is a common approach used in the election. And a voter must cast a vote by himself. Because of the convenience of Internet, communication through the network becomes a vital part of people's life. The E-Voting is an important issue to promote the rate of voting in an election process. So, citizen can fulfill their democratic rights by the E-Voting.

In this paper, we have tried to focus on voter's privacy, anonymity and manipulation's protection with Secure E-Voting system with secure storage media, because E-Voting is one of the main issues where information transaction and privacy is needed. With the help of crypto algorithm and blind signature mechanism, in this paper we have focused on our Secure Two-Doors E-Voting algorithm, which is not only helpful for developing E-Voting systems but also useable with many kinds of application that needs secure transaction and digital authentication.

In this paper, in **Section 2** we have discussed several E-Voting protocols in different approaches. In **Section 3,** we described our proposed secure E-Voting algorithm, which is offering voter's anonymity, risk of manipulation and storage idea for storing tokens which will keep the secure authentication for voter and, in **Section 4**, we have discussed our proposed method's performance and also a comparison with several types of secure E-Voting schemes.

## 2. E-Voting Protocols in Different Approaches

Chaum proposed an Anonymous Channel (MIX NET) [1] protocol for E-Voting where the original message is encrypted with the public keys from several servers and then passed from one server to the next server, each decrypting with its private key and passing the message on the next server in large batches with different order. Anonymous Channel also gives a solution to the problem of anonymous users but in this case at least one server has to be honest. On the other hand, when the number of server is large the protocol can become slow and also have the possibility to fake the vote.

Extensions of the original scheme can be found in Park et al.[2] and in Sako and Kilian [3]. However, both schemes were broken [4,5]. Later approaches by Abe [6] and Jakobsson [7,8], apart from algorithmic improvements, add much to the stability and performance of the protocol and the computational effort in the client is reduced considerably (one collective key instead of several consecutive keys); however, it still has to be analyzed and tested in prototype implementations, whether the basic difficulties in MIX nets have been completely addressed.

The Homomorphism protocol, as Homomorphic based protocols in generally has limited scalability, as they tend to limit the poll to several options, which the voter has two options to choose from {1, -1}. The vote is cast as a binary YES/NO vote, encoded following a homomorphism scheme, and submitted to a number of ballot box servers. Due to the homomorphism, the summary count of YES/NO votes is possible without having to know the individual votes [9]. This advantageous property is also the main problem of the approach: only binary votes can be cast. Although its privacy is good and follows homomorphic encrypt algorithm but it is not suitable for real environment for E-Voting because of its two options YES/NO.

ANDOS protocols provide a sender-anonymous channel. They emulate the anonymous purchase of a bit string [10]. In the *Two Agency Protocol* developed by Nurmi, Salomaa, and Santean [11], the responsibilities of validating registered voters and computing and publishing the results of the

election are divided between two agencies. One of the biggest problems with this protocol is that if the validator and tallier collude they can determine the mapping between voter and vote.

The *One Agency Protocol* is identical to the Two Agency Protocol, except for the tag distribution procedure. When voters is not satisfied or cannot see their vote then they could be challenge their vote to tallier and tallier then distributes the secret tags to justifying the votes. This could be solves the collusion problem, but not the vote-buying[1] problem.

Fujioka, Okamoto and Ohta proposed in 1993 [12], blind signature based E-Voting protocol called FOO's protocol. Previously, Chaum invented the blind signature method in 1982. The registrar has no way of tracing the ballot even if the tallier publishes it and back to the voter for blinded signature mechanism. So, this blind signature method is so secured and can give guarantee of voter's anonymity.

Blind signature protocol is famous and we also followed this protocol. Nevertheless, although FOO's one-stage smart card based E-voting system is well formatted and well secured in application side, a problem arises when the administration of the registration and the ballot box servers collude. In this case, it is possible to break the anonymity as well as to vote for voters that are entitled to vote but do not do so. Another problem is if the browser based application (e.g. a java applet provided by the registration to perform the registration step) fraudulently stores the IP address for each blindly signed ballot paper and passes this information to the ballot box and, thus, vote can be forged.

## 3. Proposed algorithms for Secure Two-Doors E-Voting

From the above discussion [Section 2] we can realize that secure anonymity and secure data protection is necessary for E-Voting. For maintaining anonymity of the voter and to avoid the risk of manipulation of votes we propose an algorithm that is divided into two processes. One is for secure registration and another for secure voting. For both processes voters need to authenticate and have some crypto key mechanisms. Here, any type of fraud on the operating system level has to be considered as well. That's why the algorithm strictly separates into the registration and the voting process. Before that let us introduce some notations:

*BP* : Ballot Paper
*B* : Ballot box Server
*R* : Registration Server
*V* : voter
*m* , '*m*: Symmetric crypto key
$S^{\{V,R,B\}}_{\{priv,pub\}}$ : The voter's, the registration's and the ballot box server's signature key pair.
$K^{\{V,R,B\}}_{\{priv,pub\}}$ :The voter's, the registration's and the ballot box server's key pair for encryption.

### 3.1. Registration Process (First Door)

Before the Election Day, voters should have to complete the registration process. Voters can register even at a time when the list of candidates is not complete yet.

- **Step 1.** Voter generates a random token *t.*
- **Step 2.** Prepare the *t* for blind signature and add a text for applying the E-Vote.
- **Step 3.** Sign it with voters private signature key: $S^{V}_{priv}(blinded(t), \text{"I want to give E-Vote"})$.
- **Step 4.** Then the message is encrypted with *R***'s** (Registration server) public key and sent it to registration server: $K^{R}_{pub}[S^{V}_{priv}(blinded(t), \text{"I want to give E-Vote"})]$.
- **Step 5.** Registration server verifies the voter by resolving the public signature key of the voter's. If verification is successful then the registration server signs the blinded *t* and makes $\sigma_R(blinded(t))$.
- **Step 6.** Then the registration server signs $\sigma_R(blinded(t))$ with *R*'s private signature key and again encrypt the message with voter's public encryption key and send it to the voter: $KV_{pub}[SR_{priv}\ \sigma_R\ (blinded(t)))]$.
- **Step 7.** Voter gets the token $t,\sigma_R(t)$.
- **Step 8.** Voter issued a second token **τ,** blind it and obtains the blindly signed $\sigma_T(\tau)$ from the trust center followed by same mechanism [**Step 1** to **Step 7**].

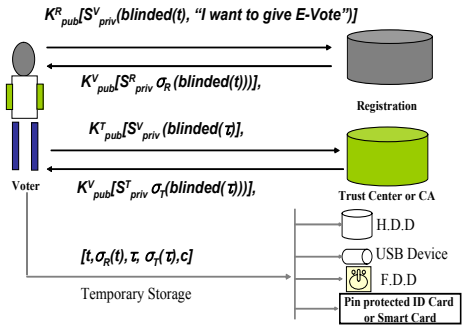


**Fig. 1.** Registration Process (First Door).

- **Step 9.** At the end of registration process voter obtains the temporary tokens and constituency information $[t,\sigma_R(t),\tau,\ \sigma_T(\tau),c]$ both tokens are needed to cast a vote on election day.

In most elections, voters will be organized in constituencies ***c***, this information is also sent back to the voter and has to be submitted on election day to indicate in which constituency the vote is to be counted. To avoid possible manipulation of *c* the blind signature keys used for $\sigma_R(t)$can be made specific to the constituency. Hence the clear-text *c* submitted on Election Day and the authentication token issued by the registration have to point to the same *c*.

### 3.2. Voting Process (Second Door)

On the Election Day the voter sends the tokens to the ballot box server to obtain a ballot paper. The voter does not sign this submission and the only means of authentication are the two tokens obtained earlier.

- **Step 1.** Voter generates an asymmetric key *m* , '*m* for secure communication**.**
- **Step 2.** Voter adds *T*, the identification of the trust center or CA, for resolving the blind signature.
- **Step 3.** Voter encrypts the temporary token with ballot server's public encryption key and send it to ballot server: $K^{B}_{pub}\ [c,T,m,t,\sigma_R(t),\tau,\ \sigma_T(\tau)]$.

[1] The last issue was addressed by Niemi and Renvall in a later paper, but the algorithm pre-supposes the use of a secure voting booth and involves high computational efforts [13]

- **Step 4.** Ballot box decrypts the message to resolve the signatures $\sigma_R(t)$and $\sigma_T(\tau)$.
- **Step 5.** If the token is OK to authenticate the voter then the ballot server issues an empty ballot sheet and encodes it with the symmetric key *(m(BP))* and sends it to the voter: $m(S^B_{priv}(BP))$.
- **Step 6.** Voter decrypts it with '*m* and fills out the ballot paper.
- **Step 7.** Voter again send the ballot sheet with tokens by encrypting with the Ballot servers public key: $K^B_{pub}$ *[c,T,m,t,*$\sigma_R(t)$*,*$\tau$*,* $\sigma T(\tau)$*,BP]*.

After authentication of the tokens, the ballot box server stores the ballot paper and the others information receives from the voter.

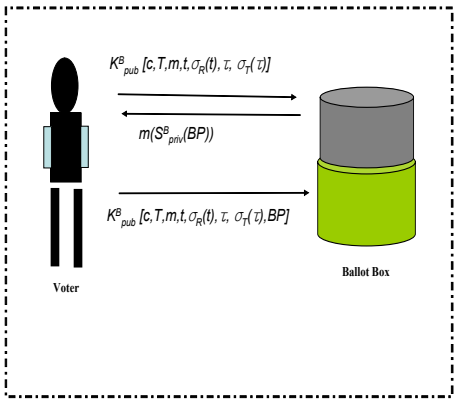


**Fig. 2.** Voting Process (Second Door).

### 3.3. Secure Storage Media

As the algorithm uses a secure E-Voting system, there is a need to temporarily store the token on a secure, anonymous medium. In particular, if rises the issue of where to store the election token between registration and Election Day, when the token is used to request a ballot paper and to eventually cast a vote. General storage media, such as diskettes, hard drives, USB keys etc. are readily available, however, they are not linked to a person, they offer no or limited protection of the data stored, and most are error-prone and may result in loss of data.

Hence, the logical storage media seems to be the digital signature card or the National ID card. As a suitable storage media it has to fulfill certain privacy criteria:

- The election token has to be stored in a PIN-protected. For example, Government can offers at least 2 "info-boxes" which are 2K storage areas in the file system of the card, which can be PIN-protected. Industry standard card readers can write and read these, once they have been created on card initialization. Since after the election the token and all others data associated with the election protocol can be deleted from the card, and then the info boxes could be used for other purposes.

## 4. Performances and Evaluation

Here we have described performances, evaluations (according to the voting principles) and comparisons of our Two-Doors E-voting scheme with different types of E-Voting protocols or schemes that have been mentioned above, in Section 2.

### 4.1 Discussions

In this section, we have discussed that our proposed Two-Doors E-Voting algorithm satisfies Anonymity, Avoid the issue of multiple tokens, Forged vote, Risk of manipulation:

**Anonymity** In the registration process, both parties (Registration server and Voter) use blind signature. Voter generates random number *t* and blinds it. Then the voter signs it with voter's Private signature key $S^V_{priv}$ and then be encrypts it again with Registration server's public key $K^R_{pub}$. On the other hand, Registration server does the same mechanism and sends to the voter $\sigma_R(t)$ with blindly. So, this blind signature strictly maintains voters anonymity, because blind signature hides the voter's identity.

**Avoid the issue of multiple tokens** The registration stores the $\sigma_R(t)$; if the original signed token is lost and the voter re-applies for another token, the registration server will always respond with original $\sigma_R(t)$, to avoid the issue of multiple tokens.

**Forged Vote** Our scheme can be guaranteed to the voter, if he uses different terminal (IP address) for registration and submission of vote, votes cannot be forged, as a valid vote also has to be authenticated by the trust center.

**Manipulation** To avoid possible manipulation of *c* the blind signature keys used for $\sigma_R(t)$can be made specific to the constituency. Hence the clear-text *c* submitted on Election Day and the authentication token issued by the registration have to point to the same *c*.

### 4.2. Performance Analysis

For making public key and private key and authentication and also for encryption and decryption we have followed RSA cryptography mechanism. In simulation, the scheme is implemented and got the average time by using the 512 and 1024 bit key length. When the 512 bits key length is adopted, the voter needs $3092x10^{-3}$ seconds for registration process and $48x10^{-3}$ for voting process. When the 1024 bits key length is used, the voter needs $30008x10^{-3}$seconds for registration process and $356x10^{-3}$ for voting process. For Trust Center process, its processing time is same as registration process.

| Key length (bit) | Registration Process (sec) | Trust Center Process (sec) | Voting Process (sec) | Total Time (Sec) |
|---|---|---|---|---|
| 512 bit | $3092x10^{-3}$ | $3092x10^{-3}$ | $48x10^{-3}$ | $6232x10^{-3}$ |
| 1024 bit | $30008x10^{-3}$ | $30008x10^{-3}$ | $356x10^{-3}$ | $60372x10^{-3}$ |

**Table 1.** Computation time of our proposed Two-Doors E-Voting scheme [14]

Performance of the scheme has shown in Table 1 and the total time of computations are needed $6.232x10^{-3}$ and $60.372x10^{-3}$ seconds by using 512 bits and 1024 bits key length, respectively.

#### 4.2.1. Comparision with Existing E-voting Schemes

In this section, we have compared our approach with exiting E-Voting protocols or schemes [See section 2]. The following properties are included in table 2: Anonymity

(Com1), Avoid manipulation of vote (Com2), Collusion freedom (Com3), Avoid Multi Token (Com4), Variability (Com5), Vote buy (Com6), for running Real Environment (Com7) and Storage (Com8).

For showing the comparison with existing E-Voting protocol and schemes, we can use "X" where any property is not satisfied with E-voting schemes; "M" is for medium level of satisfaction and "H" indicates for full satisfaction with following properties.

| | Com1 | Com2 | Com3 | Com4 | Com5 | Com6 | Com7 | Com8 |
|---|---|---|---|---|---|---|---|---|
| MIX- Net | M | M | M | M | H | X | H | X |
| Homomorphism | H | H | M | H | M | X | X | N |
| ANDOS | M | H | M | H | M | H | M | X |
| Blind Signature FOO | H | M | M | H | H | X | H | X |
| Our Method | M | M | M | H | H | H | H | H |

**Table 2.** Comparison our E-Voting scheme with several types of E-Voting protocol and scheme's [14]

On the above Table 2, we have compared the results according to our E-Voting method with the existing E-Voting protocol and schemes that we have discussed at section 2.1. If we overlook on the Com 3 (Collusion freedom) then we see that we have used "M" for all E-Voting systems. Though our Two-Doors E-Voting System can give guaranteed the anonymity of the voters and also others above existing methods can give security and maintain anonymity of voters but in Com3 case we cannot be sure, because everything depends on Trust Center. If trust center collude then Com3 property will not satisfy with any E-Voting schemes. It can be solved if we choice a right and reliable trust center or CA. In our method, there has another advantages is "Storage" in the table 2 known as Com8. Before voting day a voter can registered and in voting day (another day) he/she can use his/her identity tokens, which were found from registration process and stored them to storage. This storage facility is helpful for maintaining the privacy of voter's information.

## 5. Conclusions

In this paper we proposed an algorithm for secure E-Voting (the two Two-Doors E-Voting system) and discussed about possible secure storage media. One of the main concerns in E-Voting is the possibility of fraudulent manipulations of the voter's PC or voting terminal. Our proposed algorithm mainly based on blind signature's mechanism can protect and give guarantee of voters' anonymity and has the capability to avoid the risk of manipulation of votes. This mechanism can efficiently satisfy the need of keeping privacy of the citizen's information. The Government can make National ID cards with Pin protected digital signature, which is affiliated by Trust Center or CA (Certificate Authority). This link is implemented by the combining the public key of digital certificate and the registry number, where the Government digitally signs the combination. Then, there is no need for voters to specific register for election and it could be more secured.

**Future works.** Secure Two-Doors E-Voting with PIN based Card Reader and Writer storage system.

## References


[1] Chaum, D.: Untraceable electronic mail return addresses and digital pseudonyms in: communications of the ACM, Vol.24(2), pp.84-88, 1981.

[2] Park, C., Itoh, K., Kurosawa, K.: All/Nothing Election Scheme and Anonymous Channel. In: Lecture Notes in Computer Science 765, Advances in Cryptography Euro crypt 93,Berlin, Springer Verlag, pp.248-259, 1994.

[3] Sako, K., Kilian, J.: Receipt-Free, Mix-Type Voting Scheme. In: Lecture Notes in Computer Science 921, Advances in Cryptology Eurocrypt 95, Berlin, Springer- Verlag, pp. 393-403, 1995.

[4] Pfitzmann B., Pfitzmann A.: How to Break the Direct RSA-Implementation of Mixes. In: Eurocrypt 89, Springer-Verlag, Berlin, pp. 373-381, 1989.

[5] Horster P., Michels M.: Some Remarks on a Receipt-Free and Universally Verifiable Mix- Type Voting Scheme. In: Asiacrypt´96, LNCS163, Springer-Verlag, Berlin, pp. 125-132, 1996.

[6] Abe M.: Universally Verifiable Mix-Net with Verification Work Independent of the Number of Mix-Centers. In: Advances in Cryptology - EUROCRYPT '98, Springer-Verlag, Berlin, pp. 437-447, 1998.

[7] Jakobsson M.: A Practical Mix. In: Advances in Cryptology - EUROCRYPT '98, Springer- Verlag, Berlin, pp. 448-461, 1998.

[8] Jakobsson M.: Flash Mixing. In: Information Sciences Research Center, Bell Labs, New Jersey, http://www.bell-labs.com/user/markusj 2002.

[9] Cramer R., Gennaro R., Schoenmakers B.: A Secure and optimally Efficient Multi-Authority Election Scheme. In: Advances in Cryptology-EUROCRYPT'97, Lecture Note in Computer Science 1233, Springer-Verlag, Berlin, pp.103-118, 1997.

[10] Brassard, G., Crepeau, C., Robert, J.-M.: All-or- Nothing Disclosure of Secrets. In: Lecture Notes in Computer Science 263, Advances in Cryptology; Crypto 86, Berlin, Springer Verlag, pp. 234-238. 1987.

[11] Salomaa, A.: Verifying and Recasting Secret Ballots in Computer Networks. In: Maurer, H.A. (ed.): New Results and New Trends in Computer Science, Springer-Verlag, Berlin pp.283 –289, 1991.

[12] Fujioka, A., Okamoto, T., Ohta, K.: A Practical Secret Voting Scheme for Large Scale Elections. In: Advances in Cryptology – AUSCRYPT92. Springer-Verlag, Berlin pp.244 –251, 1993.

[13] Niemi V., Renvall A.: How to prevent the buying a votes. In: advance cryptology Asiacrypt'94, Springer-Verlag, Berlin, pp.164-170, 1995.

[14] Shaikh Muhammad Allayear. Security Aspects For E-Government Services, Masters Thesis Paper, Anyang University. 2004.