Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080556

A Secure Anonymous E-Voting System based on Discrete Logarithm Problem

Chin-Ling Chen[1,∗], *Yu-Yi Chen*[2], *Jinn-Ke Jan*[3] *and Chih-Cheng Chen*[4]

[1] Department of Computer Science and Information Engineering, Chaoyang University, 168 Jifeng E. Road, Wufeng District, Taichung, 41349, Taiwan, R.O.C.
[2] Department of Management Information Systems, National Chung Hsing, University, 250 Kuo-Kwang Road, Taichung 40227, Taiwan, R.O.C.
[3] Department of Computer Science and Engineering, National Chung-Hsing, University, 250 Kuo-Kwang Road, Taichung 40227, Taiwan, R.O.C.
[4] Department of Health Policy and Management, Chung Shan Medical University, Taichung 40201, Taiwan, R.O.C

Received: 28 Sep. 2013, Revised: 26 Dec. 2013, Accepted: 27 Dec. 2013
Published online: 1 Sep. 2014

Abstract: In this paper, we propose a practical and secure anonymous Internet voting protocol. This method integrates Internet reality and cryptology. Issues such as the kinds of “certificate authority” and “public proxy server” are integrated in our scheme to solve the Internet identification and anonymity problems. To combine and make up a series of ElGamal blind signature and secret sharing cryptosystem, this protocol can be applied to a secure, practical, and fair voting system.

Keywords: E-Voting, Blind signature, Secrete sharing, Anonymous

1 Introduction

The first electronic election scheme was proposed by David Chaum[1]. Anonymous voting involves making sure that voters can vote of their own free will. The voting system must guarantee that voters remain anonymous during the entire voting process. A good electronic voting system should be at minimum as secure as traditional voting systems. The most important privacy issue is making sure that the voting process is untraceable; a ballot cannot be traced to an individual. In 1981, David Chaum [1] proposed a solution that employed a series of honest “mixers” on the network. Any mixer could be chosen by the voter as a transmitter to send the ballot and cut off the network address on the way. As to cut the link between the voters and the ballots, the theorem of “blind signature” is used in many proposals [2,3,4,5,6,7,8,9] to solve such a problem.

Anonymity and coercion-free issues were often mentioned e-voting systems[10,11] in recent years. In fact, implementing a secure anonymous channel is not a problem on the current Internet. Suppose we want to construct a voting system on the Internet, this means that all of the voting centers should be set up as web sites. We know that any web site can make a secure communication channel under the “Secure Socket Layer (SSL)” infrastructure. We propose applying the SSL for secure communications between the voters and the voting centers. Moreover, for cutting off the network address as a voter casts his ballot, we introduce the existing “public proxy server” to play the role of “mixer” [4]. The network address for the ballot can then be replaced by a proxy server address. As to cut the link between the voters and the ballots, we also introduce how the signature for valid ballots can be signed blindly using the ElGamal blind signature[12,13,14] scheme where a malicious voter cannot cheat the system and a malicious center cannot determine how any individual voted.

According to the other important verifiability issue, many proposals [1,15,16,17,18,19,20] emphasized that their schemes allow the voters to verify the voting result. When a voter finds that his/her vote has not been properly counted by the tally center, he/she can accuse the tally center. However, such a design will encourage bribery. That is, some candidates could force voters to change their voting intention using money or threats. This would

[∗] Corresponding author e-mail: clc@mail.cyut.edu.tw

also make it easy for bribers to verify the bribed vote.
We advocate that voters should not be allowed to verify their votes by themselves. The voting process supervision should have the responsibility for supervising centers constructed by the various political parties. The tally center cannot falsify a tally because all of the votes are counted under the supervision of the supervision center. In our scheme, to be sure that all of the votes are counted correctly we employed a secret sharing mechanism [16, 17].

2 Preliminaries

In this section, we will state the related preliminaries about secret sharing and ElGamal blind signature which will be adapted in our scheme.

2.1 Secret sharing

A secret sharing mechanism was proposed by Shamir[16]and Blakley[17].The idea of secret sharing schemes is to start with a secret, and divide it into pieces, which are distributed to users, such that the pooled shares of specific subsets of users allow reconstruction of the original secret. We find this technology extremely suitable to construct the "separation of duties" concept; it is the key in achieving trustworthy voting. We will give the famous scheme-Shamir's (t, n) threshold scheme[16]to illustrate this technology as follows.
Shamir's threshold scheme is based on polynomial interpolation, and the polynomial $y = f(x)$ of degree t-1 is uniquely defined by t points $(x_i\ y_i)$ with distinct x_i A trusted party T distributes shares of a secret integer S to n users. Any t users which contribute their shares can recover S. The setup phase is described as follows.
(1) T chooses a prime $P > max(S,n)$, and define $a_0 = S$.
(2) T chooses t-1 random coefficients $a_1, \ldots, a_{t-1}$from a uniform distribution over the integers in [0,P) , defining the random polynomial over Z_p , $f(x) = \sum_{j=0}^{t-1} a_j x^j$.
(3) T computes $S_i = f(i)$ mod p, $1 \leq i \leq n$, and securely transfers the share S_i to user P_i.
Any group of t or more users contribute their shares. Their shares provide t distinct points $(x,y) = (i,S_i)$, allowing computation of the coefficients a_j, $1 \leq j \leq t-1$ of f(x) by Lagrange interpolation. The secret is recovered by noting $f(0) = a_0 = S$, the shared secret maybe expressed as:
$S = \sum_{i=1}^{t} c_i y_i$, where $c_i = \prod_{1 \leq j \leq t, j \neq i} \frac{x_j}{x_j - x_i}$

2.2 ElGamal blind signature scheme

In this section, we describe ElGamal blind signature scheme briefly. Suppose p and q be large prime numbers, q|p-1 and g is an element of Z_p^* of order q. Let Alice's public key be y=g^x mod p where x∈ Z_p^* is her private key. Suppose Bob wants to send a message m to Alice.

Step 1: Alice chooses a random number k∈ Z_q^* and computes r′=g^k mod p, then sends r′ to Bob;
Step 2: Bob chooses two blind factors $\alpha, \beta \in Z_q^*$.
The message m is then blinded as follows.
r=r′ $^\alpha$ g$^\beta$ mod p
m′=α m r′ r^{-1} mod q
The blind message m′ is then transmitted to Alice.
Step 3: After Alice receives the blind message m′, Alice signs the message m′ using its secret key SK_{Alice}.
Step 4: After Bob receives the blind signature s′, the real signature s can be unblinded as follows.
s=s′ r r $'^{-1}$ + β m mod q.
Thus the signature of the message m is the pair (r,s).

3 Our e-voting scheme

In this paper, we discuss the security of the secure anonymous e-voting system using the following criteria to sketch a good electronic voting system.

3.1 Requirements

Only eligible voters are permitted to vote and they can vote only once.

- **Anonymity** : There is no way to derive the link between the voter's identity and the marked ballot. The voter remains anonymous.
- **Accuracy** : All valid votes are counted correctly. A voter's vote cannot be altered, duplicated, or removed.
- **Verifiability** : Voters can make sure that their votes are counted correctly.
- **Mobility** : A system is mobile if there are no restrictions on the location from which voters can cast their ballots.
- **Convenience** : The voter does not need to learn sophisticated technique, and no additional equipment is needed. An e-voting system must be practical in that it must be easy to implement.
- **Uncoercibility:** No voter can prove his/her choice to others must be achieved in electronic voting. That is, only a voter can decide his/her intention.

- **Efficiency** : The computation loads of the whole election must be light enough to have the voting result obtained within a reasonable period of time.

3.2 General description

The structure of our scheme is illustrated in figure 1. There are six parties in our scheme as follows:

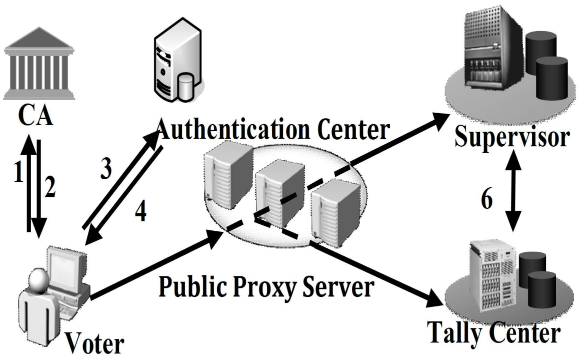

Figure 1: The structure of our scheme

- **Voter:**The people who have the right to vote.
- **Certificate Authority (CA):**A trusted certificate provider.
- **Authentication Center (AC):**A web site that is responsible for verifying a voter's certification. It is subordinated to the central election committee.
- **Public Proxy Server:**Voters can choose any public proxy server to forward anonymous ballot without the self IP address.
- **Tally Center (TC):**A web site that is responsible for counting the votes.
- **Supervision Center (SC):**A web site that is responsible for supervising the tallying task.

1. **Voter** → **CA:**Before the election, all of voters should be enrolled in a register of electors.
2. **CA** → **Voter :**After the voter completes the enrollment, the CA signs and issues a "personal certificate" to the voter.
3. **Voter** → **AC :**Only voters that have a verified legal "personal certificate" embedded into their web browser can login to the AC web site.
4. **AC** → **Voter :**The AC issues the corresponding "voter-pseudonym signature" to the voter for the next voting phase.
5. **Voter** → **TC, SC :**The voter casts his "voter-pseudonym signature" and "encrypted secret-sharing ballot" through a trusted public proxy server to the TC and SC, respectively, without forwarding any information about the location from where the voter voted.
6. **TC** ↔ **SC :**Under TC and SC cooperation, each "encrypted secret-sharing ballot" can be decrypted and counted for the voting result.

3.3 The proposed e-voting scheme

The following notations are used to explain how our scheme is constructed.
SK_x :the secret key of X.
PK_x :the public key of X.
v_i :the voter-pseudonym for voter i.
m :marked ballot.
w : encrypted ballot.
p,q :two large prime numbers , where q|p-1 .
α,β :blind factors; $\alpha,\beta \in Z_q^*$.
r_i,s_i :the ElGamal signature of v$_i$.
a,b,k :the random number.
Y_a :a part of the ballot that is held by the TC for revealing half of m.
Y_b :a part of the ballot held by SC for revealing the other half of m.
λ_a :a secret sharing parameter that is held by the TC.
λ_b :another secret sharing parameter that is held by SC.
$A?=B$:compare whether A is equal to B.
Now, we introduce how our scheme is implemented on the Internet. It is divided into the following four phases.

3.4 Initialization phase

Step 1: Initially, there are a large prime number p, a prime factor q of (p-1), and a primitive number g (mod p) which are known to all users in our scheme.

Step 2: The AC, TC, and SC choose their secret keys SK$_{AC}$, SK$_{TC}$, and SK$_{SC}$ from numbers in the range [1,q-1] and compute the corresponding public keys PK$_{AC}$, PK$_{TC}$, and PK$_{SC}$.

$$PK_{AC} = g^{SK_{AC}} \ mod\ p \tag{1}$$

$$PK_{TC} = g^{SK_{TC}} \ mod\ p \tag{2}$$

$$PK_{SC} = g^{SK_{SC}} \ mod\ p \tag{3}$$

Step 3: Before the election each voter is enrolled with a register of electors and issued a "personal certificate" from the CA to be embedded into the voter's browser. This "personal certificate" can be used for a number of elections.

3.5 Authentication phase

Step 1: On the voting day, only the voter whose legal "personal certificate" has been embedded into his web browser can pass the verification and login to the AC website. Each voter has only one chance to ask the AC to run the following steps to get the "voter-pseudonym signature".

Step 2: The AC selects a random number $\widetilde{K_i}$, where $\widetilde{K_i} \in Z_q^*$, and computes.

$$\widetilde{r_i} = g^{\widetilde{k_i}} \ mod\ p \tag{4}$$

which is then sent back to the voter.

Step 3: The voter selects a pseudonym v$_i$ and two blind factors $\alpha, \beta \in Z_q^*$. The voter-pseudonym v$_i$ is then blinded as follows.

$$r_i = \widetilde{r_i}^{\alpha} g^{\beta} \ mod\ p \tag{5}$$

$$\widetilde{v_i} = \alpha v_i \widetilde{r_i} r_i^{-1} \ mod\ q \tag{6}$$

The blind voter-pseudonym $\widetilde{v_i}$ is then transmitted to the AC.

Step 4: After the AC receives the above message, the AC signs the voter-pseudonym $\widetilde{v_i}$ using its secret key SK$_{AC}$.

$$\widetilde{s_i} = SK_{AC} \cdot \widetilde{r_i} + \widetilde{k_i} \cdot \widetilde{v_i} \ mod\ q \tag{7}$$

The blind signature $\widetilde{s_i}$ is then sent back to the voter.

Step 5: After the voter receives the blind signature, the real signature s$_i$ can be unblinded as follows.

$$\widetilde{s_i} = SK_{AC} \cdot \widetilde{r_i} + \widetilde{k_i} \cdot \widetilde{v_i} \ mod\ q \tag{8}$$

Now the complete voter-pseudonym signature, v$_i$ is the pair(r$_i$, s$_i$).

3.6 Voting phase

Step 1: As the voter makes a voting decision the marked ballot m is generated and encrypted as follows.

$$w = PK_{TC}^{a} \cdot PK_{SC}^{b} \cdot \ m\ mod\ p \tag{9}$$

The above two numbers a and b are randomly chosen by the voter to randomize m. Two corresponding numbers Y$_a$ and Y$_b$ are also generated as follows.

$$Y_a = g^a \ mod\ p \tag{10}$$

$$Y_b = g^b \ mod\ p \tag{11}$$

The voter casts (v$_i$, r$_i$, s$_i$, w, Y$_a$) and (v$_i$, r$_i$, s$_i$, w, Y$_b$) through one trusted public proxy server to TC and SC, respectively, without forwarding any information about the voter's location.

Step 2: To confirm that a voter is certified, the TC and SC verify the validity of the "voter-pseudonym signature" based on the following equality holding.

$$g^{s_i} ? = PK_{AC}^{r_i} \cdot r_i^{v_i} \ mod\ p \tag{12}$$

Without the cooperation of the TC and SC, no one can decrypt w to get m until the next phase. The TC and SC just record the received (v$_i$, r$_i$, s$_i$, w, Y$_a$) and (v$_i$, r$_i$, s$_i$, w, Y$_b$) into their respective database.

3.7 Announcement phase

Step 1: When the deadline for vote casting is reached, the TC and SC stop accepting ballots and publish their secret keys to one another. Upon receiving the SC's secret key SK$_{SC}$, the TC verifies the TC's secret key as follows.

$$PK_{SC} ? = g^{SK_{SC}} \ mod\ p. \tag{13}$$

On the other hand, the SC can use the TC's public key PK$_{TC}$ to verify the TC's secret key as follows.

$$PK_{TC} ? = g^{SK_{TC}} \ mod\ p. \tag{14}$$

Step 2: With the cooperation of the TC and SC, each ballot will be decrypted. The TC and SC release the corresponding Y$_a$ and Y$_b$ used to reveal half of each marked ballot using their secret keys SK$_{TC}$ and SK$_{SC}$, respectively.

$$\lambda_a = (Y_a)^{SK_{TC}} \ mod\ p \tag{15}$$

$$\lambda_b = (Y_b)^{SK_{SC}} \ mod\ p \tag{16}$$

Only with the cooperation of the TC and SC, the marked ballot m can be decrypted as follows.

w/($\lambda_a \cdot \lambda_b$) mod p
=w/(Y$_a^{SK_{TC}}$· Y$_b^{SK_{SC}}$) mod p
=w/(g$^{a \cdot SK_{TC}}$. g$^{b \cdot SK_{SC}}$) mod p
=w/(PK$_{TC}^{a}$· PK$_{SC}^{b}$) mod p
=(PK$_{TC}^{a}$· PK$_{SC}^{b} \cdot m$) / (PK$_{TC}^{a}$· PK$_{SC}^{b}$) mod p
=m

Every ballot is revealed in this way and announced. This design guarantees that the ballot counting occurs under the supervision of the SC and TC. The ballot miscounting cannot occur in our scheme.

4 Analysis

In this section, we will present that our proposed scheme can achieve the requirements mentioned in section 3.1 and make a comparison between some related electronic voting schemes and ours in sections 4.1 and 4.2, respectively.

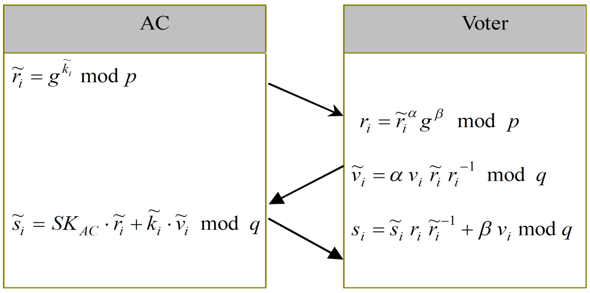
AC
Voter
$\widetilde{r}_i = g^{\widetilde{k}_i} \bmod p$
$r_i = \widetilde{r}_i^{\alpha} g^{\beta} \bmod p$
$\widetilde{v}_i = \alpha\, v_i\, \widetilde{r}_i\, r_i^{-1} \bmod q$
$\widetilde{s}_i = SK_{AC} \cdot \widetilde{r}_i + \widetilde{k}_i \cdot \widetilde{v}_i \bmod q$
$s_i = \widetilde{s}_i\, r_i\, \widetilde{r}_i^{-1} + \beta\, v_i \bmod q$

Figure 2: The scenarios of the blind signature

4.1 Requirements analyses

4.1.1 Fairness issues

According to the fairness issue, only eligible voters are permitted to vote and they can vote only once. In our scheme, the AC plays the key role of authenticating voter identification. Only a voter whose legal "personal certificate" has been embedded into his web browser can pass the AC website verification and login. Each voter has only one chance to ask the AC for a "voter-pseudonym signature" for the next voting phase. In this way, the AC can prevent eligible voters from voting more than once.
As we know, a "personal certificate" is used to sign digital messages like email or to encrypt information. Once you exchange a certificate with others, you can correspond over the Internet in complete privacy. In more Internet Commerce applications a user's "personal certificate" is used as his/her digital identity. We point out that the "personal certificate" can also be used as the digital identity of a voter in our e-voting system on the Internet.

4.1.2 Anonymity Issues

Voters must remain anonymous during the entire voting process. We will describe how to meet these criteria in the following three parts.

(1) Anonymity in the authentication phase
To cut the link between a voter's identity and ballot, the voter selects a pseudonym by himself, and the "voter-pseudonym signature" is signed by the AC blindly. AC cannot derive the link from the voter's identity and the "voter-pseudonym signature". The whole process is described as Figure 2.

The voter pseudonym complete signature v$_i$ is the pair (r$_i$, s$_i$), used as the identity for the next voting phase without any link to the voter. The AC cannot derive the link between the voter's identity and the voter-pseudonym signature.

(2) Anonymity in the voting phase
There are two kinds of anonymity problems in the voting phase. To make it impossible to trace a ballot to an individual, the voter's network address must be cut off on the way to the AC. To cut off the network address as a voter casts his ballot we introduce the existing "public proxy server" to play the role of "mixer". As we know, the network address of a packet on the Internet can be replaced by a proxy address. For example: an enterprise (or university) can set up a public proxy server for the employee (or staffs) to access outside valuable resource. Once the employee (or staffs) setup the proxy connection, their original IP address is hidden and replaced. In our scheme, each voter casts his "voter-pseudonym signature" and "encrypted secret-sharing ballot" to TC and SC through a trusted public proxy server that can be freely selected by the voter. Then each vote is impossible to be traced to the location of the voter.
The TC and SC receive the "voter-pseudonym signature" (v$_i$, r$_i$, s$_i$). To confirm that a voter is certified or not, the TC and SC can verify the validity of the "voter-pseudonym signature" based on the following equality holding.
$g^{s_i}?{=}PK_{AC}^{r_i}\cdot r_i^{v_i} \bmod p$
It is shown in the Theorem 1.

Theorem 1. Upon receiving the triplet (v$_i$, r$_i$, s$_i$), the receiver can correctly verify the equation $g^{s_i}?{=}PK_{AC}^{r_i}\cdot r_i^{v_i}$ mod p is equivalent.
Proof. We first drive the left side of the equation as follows:

$$g^{s_i}{=}g^{\widetilde{s}_i r_i \widetilde{r}_i^{-1}+\beta v_i}$$
$$=g^{(SK_{AC}\widetilde{r}_i+\widetilde{k}_i\widetilde{v}_i)r_i\widetilde{r}_i^{-1}+\beta v_i}$$
$$=g^{SK_{AC}r_i+\widetilde{k}_i\widetilde{v}_i r_i\widetilde{r}_i^{-1}+\beta v_i}$$
$$=g^{SK_{AC}r_i+\widetilde{k}_i(\alpha v_i\widetilde{r}_i r_i^{-1})r_i\widetilde{r}_i^{-1}+\beta v_i}$$
$$=g^{SK_{AC}r_i+\widetilde{k}_i\alpha v_i+\beta v_i}\ (\text{mod p})$$

And the right side of the equation as follows:

$$PK_{AC}^{r_i}r_i^{v_i}{=}(g^{SK_{AC}})^{r_i}(\widetilde{r}_i^{\alpha}g^{\beta})^{v_i}$$
$$=(g^{SK_{AC}})^{r_i}((g^{\widetilde{k}_i})^{\alpha}(g^{\beta}))^{v_i}$$
$$=(g^{SK_{AC}})^{r_i}(g^{\widetilde{k}_i\alpha v_i}g^{\beta v_i})$$

$=g^{SK_{AC}r_i+\widetilde{k}_i\alpha v_i+\beta v_i}$(mod p)

Therefore it is clearly to prove the both sides of the equation are equivalent.
The TC and SC can confirm that the voter was certified using the "voter-pseudonym signature". However, the TC and SC do not know the voter's real identity. There is no way to derive the voter's identity from the vote in our scheme.

(3) Anonymity in the Announcement phase
As we mentioned before, other systems allow the voters to verify the voting result. This will encourage bribery because bribers will also be able to verify bribed votes. We advocate that a supervision center comprised of members from all of the political parties must control and verify the voting process. Only with the cooperation of TC and SC, each vote can be decrypted. A secure supervision facility will win the voter's trust. It is not necessary to allow voters verify (or show to bribers) their votes in the announcement phase. There is no anonymity problem in the announcement phase in our scheme.

4.1.3 User's privacy

All valid votes must be counted correctly. A vote cannot be altered, duplicated, or removed in our scheme because the secret sharing mechanism is applied to each vote.
As a voter makes a voting decision, the marked ballot m is generated and encrypted into w as follows.
$w=PK^b_{TC}\cdot PK^b_{SC}\cdot m \bmod p$
Two corresponding numbers Y_a and Y_b are generated as follows
$Y_a=g^a \bmod p$
$Y_b=g^b \bmod p$

The secret marked ballot m is then hidden in the two parts of (w, Y_a) and (w, Y_b) which are transmitted to the TC and SC, respectively. Only with the cooperation of the TC and SC using their secret keys can a ballot m be revealed.

$w/(\lambda_a\cdot\lambda_b) \bmod p$
$=w/(Y_a^{SK_{TC}}\cdot Y_b^{SK_{SC}}) \bmod p$
$=w/(g^{a\cdot SK_{TC}}\cdot g^{b\cdot SK_{SC}}) \bmod p$
$=w/(PK^a_{TC}\cdot PK^b_{SC}) \bmod p$
$=(PK^a_{TC}\cdot PK^b_{SC}\cdot m) / (PK^a_{TC}\cdot PK^b_{SC}) \bmod p$
$=m$

Every ballot will be revealed in this way and announced. This design guarantees that ballot counting is under the supervision of the SC and TC. A ballot miscount cannot occur in our scheme.

There is another point is worth noting. Some schemes [15,18,19,21] do not ensure that the election is fair, i.e., the voting center knows the intermediate result from the voting. The voting center can therefore affect the election by leaking the intermediate result to the public. Those schemes that allow voters to recast their votes before the election deadline create a very serious problem. In our scheme, no one can get any information about the tally result before the voting deadline.

4.1.4 Verifiability issues

According to the verifiability issue, let voters can make sure that their votes are counted correctly; we advocate that voters should not be allowed to verify their votes by themselves. Since some candidates may enforce voters to change their intentions by money or threat. And the bribers will be easy to verify the bribed vote as voters can verify their votes. Therefore, we involve the secret sharing mechanism in our scheme to be sure all of the votes can be counted correctly. The tally center cannot falsify a false tally since all votes are counted under the supervision of the supervision center. Such a kind of concept should be the general definition of verifiability.

4.1.5 Mobility issues

Our scheme involves setting up those web sites, applying the existing certificate authority and public proxy servers and secure and anonymous voting. The voting process is reasonable and easy for voters on the Internet. Our scheme can easily be implemented by connecting personal computers to those web sites, allowing voters to vote from anywhere. The voters are not restricted to a given physical location to cast their votes.

4.1.6 Convenience issues

The proposed scheme needs not any additional equipment, such as smart card or card readers for voters. Except for a proxy server, the voter does not need to learn too many sophisticated techniques. The design is suitable for implementation on the Internet.

4.1.7 Uncoercibility issues

In our scheme, a secret sharing mechanism is involved to ensure that all votes can be counted correctly. Only with the cooperation of the TC and SC using their secret parameters λ_a and λ_b, a ballot m can be revealed. The tally center cannot falsify a tally because all votes are counted under SC supervision. Any influence such as threats or vote-buying, the voter is not allowed to prove to others he/she has voted.

4.1.8 Efficiency issues

In our proposed scheme, the voter only needs to take a little time to perform the voting procedure. Most of the computation operations are performed by TC and SC. Each legal voter needs to perform only four exponential operations in the voting phase. Hence, our proposed electronic voting scheme can be applied in the real world.

4.2 Comparisons between electronic voting schemes

In this subsection, we will present the comparisons between our proposed scheme and other related scheme. As shown in table 1, our scheme not only conform the mentioned requirements, but also has better performance than other works [5,6,8]. The proposed scheme can be applied in general election.

Table 1: The comparisons between our scheme and other related schemes

Methods Issue	Our Scheme	Fjioka et al. [6]	Dini [5]	Liaw [8]
Fairness	Yes	No	Yes	Yes
Anonymity	Yes	Yes	Yes	Yes
Accuracy	Yes	Yes	Yes	Yes
Verifiability	Yes	Yes	Yes	Yes
Mobility	Yes	No mention	Yes	Yes
Convenience	Yes	No mention	Low	Mid
Uncoercibility	Yes	No	Yes	No
Efficiency	High	Low	Low	Mid

5 Conclusions

We proposed a secure anonymous e-voting scheme that uses a modified ElGamal digital signature algorithm. According to the concepts mentioned above, our scheme not only solves the fairness, privacy, accuracy and verifiability problems, but also uses current network technology to implement a mobile e-voting system. This design is suitable for implementation on the Internet.

Our e-voting system is not difficult to implement. Our scheme is designed to meet the demands of the future.

Acknowledgement

This research was supported by the National Science Council, Taiwan, R.O.C., under contract number NSC 101 - 2622 - E324 - 003 - CC3 and NSC 101 - 2221 - E - 324 - 005 - MY2.

References

[1] D. Chaum, Untraceable Electronic Mail, Return Address and Digital Pseudonyms, Communications of the ACM, **24** 84-88 (1981).

[2] Y.Y. Chen, The Study of Employing the Cryptography in the Network Society, Ph. D. theses, National Chung Hsing University, Taiwan, R.O.C, (1998).

[3] F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi and A.Vaccarelli, SEAS, A Secure E-voting Protocol: Design and Implementation, Computers & Security, **24**, 642-652 (2005).

[4] C.C. Chang and J.S. Lee, An Anonymous Voting Mechanism Based on the Key Exchange Protocol, Computers & Security, **25**, 307-314 (2006).

[5] G. Dini, A Secure and Available Electronic Voting Service for A Large-Scale Distribution System, Future Generation Computer Systems, **19**, 69-85 (2003).

[6] A. Fujioka, T. Okamoto, and K. Ohta, A practical Secret Voting Scheme for Large Scale Elections, Advances in Cryptology AUCRYPT'92 Proceedings 6.15-6.19 Springer-Verlag, (1993).

[7] J.K. Jan, Y.Y. Chen and Y. Lin, The Design of Protocol for e-Voting on the Internet, Proceedings of the IEEE International Carnahan Conference on Security Technology, London, England, 180-189 (2001).

[8] H.T. Liaw, A Secure Electronic Voting Protocol for General Elections, Computers & Security, **23**, 107-119 (2004).

[9] Yi. Mu and V. Varadharajan, Anonymous secure e-voting over a network, Proceedings of the 14_{th} Annual on Computer Security Applications Conference (ACSAC'98), 7-11 Dec, 293-299 (1998).

[10] C.I. Fan and W.Z. Sun, An efficient multi-receipt mechanism for uncoercible anonymous electronic voting, Mathematical and Computer Modelling, **9-10**, 1611-1627 (2008).

[11] Y.F. Chung, and Z.Y. Wu, Approach to designing bribery-free and coercion-free electronic voting scheme, Journal of Systems and Software, **12**, 2081-2090 (2009).

[12] J. L. Camenisch, J. M. Piveteau and M. A. Stadler, Blind Signature Schemes based on the discrete logarithm problem, Rump session of Eurocrypt '94 (5 pages), (1994).

[13] T. ElGamal A Public Key Cryptosystem and A Signature Scheme Based on Discrete Logarithms, IEEE Trans., IT-31, 469-472 (1985).

[14] P. Hoster, M. Michaels and H. Petersen, Meta-Message Recovery and Meta-Blind Signature Based on The Discrete Logarithm Problem and Their Applications, Proc. Asiacrypt '94, Lecture Notes in Computer Science, **917**, 224-237 (1995).

[15] D. Chaum, Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA, Advances in Cryptology - EUROCRYPT'88 Proceedings, Springer-Verlag, 177-182 (1989).

[16] A. Shamir, How to share a secret, Communications of the ACM, **11**, 612-613 (1979).

[17] G. Blakley, Safeguarding cryptographic keys, Proceeding of AFIPS 1979 National Computer Conference, AFIPS Press, New York, 313-317 (1979).

[18] W.S. Juang and C.L. Lei, A Collision-Free Secret Ballot Protocol for Computerized General Elections, Computers & Security, **4**, 339-348 (1996).

[19] H. Nurmi, A. Salomaa, and L. Santean, Secret Ballot Elections in Computer Networks, Computers & Security, **6**, 553-560 (1991).

[20] P. H. Slessenger, Socially Secure Cryptographic Election Scheme, Electronics Letters, **27**, 955-957 (1991).

[21] R. Saltman, Accuracy, Integrity and Security in Computerized Vote-tallying, Communications of the ACM, **10**, 1181-1191 (1998).

Chin-Ling Chen was born in Taiwan in 1961. He received the B.S. degree in Computer Science and Engineering from the Feng Chia University in 1991; the M.S. degree and Ph.D. in Applied Mathematics at National Chung Hsing University, Taichung, Taiwan, in 1999 and 2005 respectively. He is a member of the Chinese Association for Information Security. From 1979 to 2005, he was a senior engineer at the Chunghwa Telecom Co., Ltd. He is currently a professor of the Department of Computer Science and Information Engineering at Chaoyang University of Technology, Taiwan. His research interests include cryptography, network security and electronic commerce.

Yu-Yi Chen was born in Kaohsiung, Taiwan, in 1969. He received the B.S., M.S., and Ph.D. in Applied Mathematics from the National Chung Hsing University in 1991, 1993, and 1998, respectively. He is presently an associate professor of the Department of Management Information Systems, National Chung Hsing University, Taiwan. His research interests include computer cryptography, network security, and e-commerce.

Jinn-Ke Jan was born in Taiwan in 1951. He received the B.S. degree in physics from the Catholic Fu Jen University in 1974 and the M.S. degree in information and computer science from University of Tokyo in 1980. He studied Software Engineering and Human-Computer Interface in the University of Maryland, College Park, MD, during 1984-1986. He is presently a professor in the institute of Computer Science at National Chung Hsing University. He is currently also an editor of Information and Education, an editor of Journal of Computers, and an executive member of the Chinese Association for Information Security. He is a member of IACR and member of IEEE. From 1995 to 1997, he was the Director of the Counseling Office for Overseas Chinese and Foreign Students. From 1997 to 2000, he was the Director of the Computer Center at National Chung Hsing University. His research interests include computer cryptography, human factors of designing software and information systems, ideograms I/O processing , data structures and coding theory.

Chih-Cheng Chen is an assistant professor in Department of Industrial Engineering and Management in National Chin-Yi Institute of Technology. From 1996 to 2004, he was a senior engineer of Syntegra Tech. Company, which is an integration application software provider for the enterprise. He earned a Master and Ph.D. Degrees in Department of Mechatronics Engineering from National Changhua University of Education in 2005 and 2011 respectively. He has been practicing the RFID application system in many fields such as the patrol system and the long-term care of elders. His research interests include mobile technology and RFID applications.