A Verifiable Electronic Voting Scheme Over the Internet

Min-Shiang Hwang[1], Yan-Chi Lai[2], and Chun-Ta Li[3]

[1] Department of Management Information Systems, National Chung Hsing University, 250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
mshwang@nchu.edu.tw

[2] Department of Information Management, Chaoyang University of Technology, 168 Gifeng E. Rd., Wufeng, 413 Taichung, Taiwan, R.O.C.

[3] Department of Computer Science, National Chung Hsing University, 250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.

Abstract. The electronic election allows voters to vote over the Internet without the geographical restrictions. The mobility, democracy, and privacy are important criteria in evaluating electronic voting schemes. Moreover, researchers have suggested that the supervision of ballot counting is necessary and that electronic voting systems should allow all voters to confirm the result of voting. In the light of this viewpoint, many electronic voting schemes have emphasized that the voters can verify the voting result. We called it the verifiability. Unfortunately, the property of the verifiability might encourage ballot buying. In this paper, we shall propose an electronic voting protocol that can satisfy all security requirements and allow the voter to verify whether the cast ballot has been counted correctly or not, and further, it will not encourage ballot buying.

1 Introduction

In the real world, private information protection is a very crucial task in occasions such as anonymous voting systems and anonymous payment systems [6, 7, 12]. In a true democracy, the constitution grants every citizen the right to vote. Accordingly, every voter can select the right officials for the country. Conventional paper-based voting system is inconvenient for voters and therefore is responsible for decreasing the rate of voting. The main reason is that all legal voters, especially students or businessmen, do not live in their domiciled homes, and each may relinquish their voting right because of the geographical restrictions. The electronic election 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.

D. Chaum introduced the first blind signature scheme [2, 3] to ensure that the user's private information would not be revealed when he/she was proceeding with casting or purchasing over the Internet. Up to now, many researchers have proposed a variety of electronic voting schemes [1, 4, 5, 8–11, 13].

The main goal of a secure electronic voting system is to ensure the privacy of the voters and the accuracy of votes. In general, a secure electronic voting system should satisfy such requirements as follows:

- **Accuracy**: A secure electronic voting system must prevent the cast ballot from being altered, duplicated, or removed by anyone. Each legitimate ballot must be counted correctly. Furthermore, the possibility must be absolutely eliminated for anyone to forge an illegitimate ballot to cast.
- **Simplicity**: The voting process should be as simple as possible. In other words, a user-friendly electronic election interface does not need to learn complex techniques and either additional equipments.
- **Privacy**: In order to achieve anonymous electronic election, anyone besides the voter her-/himself cannot link to a specific voter when he/she is going through the voting procedure. Private information protection is one of the most important requirements in electronic voting systems.
- **Democracy**: Only legitimate voters can cast their ballots. Each voter can cast at most one ballot in an election.
- **Verifiability**: Each legitimate voter should be able to verify the validity of the cast ballot. Each voter must be allowed to check whether her/his ballot has been counted. As the same time, the election result should be verifiable by everyone. The verifiability requirement can be viewed as a means to assure correctness.
- **Uncoercibility**: Each voter must be able to cast the vote according to her/his own conscience and no voter can be forced to vote in a particular way thanks to the prevention of ballot buying and extortion.

Moreover, some researchers have suggested that the supervision of ballot counting is necessary and that system should allow all the voters to confirm the result of voting. In the light of this viewpoint, many electronic voting schemes have emphasized that the voters in their systems can verify the voting result. We called it the verifiability. Unfortunately, the property of the verifiability might encourage ballot buying. For this reason, some electronic voting schemes have recommended that the voter should not be allowed to verify whether his/her ballot has been counted correctly or not. However, since the voters cannot verify their ballots, the electronic voting system must get the trust of the voters some other way. In order to avoid ballot buying and get the trust of the voters, the design of supervision facilities should be established in a secure electronic voting system on behalf of all voters to monitor the whole election process and to prevent the voting center from defrauding. However, there does not exist any single trusted organization in a real world situation. Therefore, the supervision facilities should involve parties of different political points of view. In our opinion, the trust supervision facilities are necessary in the electronic voting system, but the verifiability should still remain. We believe that a secure electronic voting system should not only allow all the voters to verify the voting result but also avoid ballot buying. In the next section, we shall propose an electronic voting protocol that satisfies all the requirements described above.

The remainder of our paper is organized as follows. In Sections 2, we will show the familiar primitives which provides the formidable security for our scheme. In Section 3, the details of our scheme will be presented. In Section 4, we shall analysis the scheme that satisfies all the requirements described above. Finally, we shall present our conclusion in Section 5.

2 Preliminaries

In the following, we define some secure definitions which the security of our scheme rely on.

Definition 1. A secure public-key system $\Gamma = (K, E, D)$ is defined as follows.

- Key generation algorithm K: The algorithm K produces a pair (PK, SK) of matching public key PK and private key SK. Algorithm K is probabilistic.
- Encryption algorithm E: Given a plaintext m and a public key PK, E encrypts m using PK, and produce a ciphertext c, i.e. $c = E_{PK}(m)$. On the other hand, given a message m and a private key SK, E encrypts m using SK, and produce a signature S, i.e. $S = E_{SK}(m)$. Algorithm E is probabilistic. Given PK, it is computationally infeasible to find SK.
- Decryption algorithm D: Given a ciphertext c and private key SK, D decrypts c using SK, and outputs the plaintext m, i.e. $m = D_{SK}(c)$. On the other hand, given a signature S, a message m and a public key PK, any one who can verify the equation $m = D_{PK}(S)$. If it holds, the signature S is generated by that owning the corresponding public key PK. Without knowing SK, anyone has no ability to find another SK' to satisfy $m = D_{SK'}(c)$ and generate a signature S' to satisfy $m = D_{PK}(S')$.

Definition 2. A secure blinding function, $B(m, r)$, without knowing the blind factor r, no one can use the unblinding function $B^{-1}(m, r)$ to get the signature S on the message m. In Chaum's blind signature scheme, there are five phases: initializing, blinding, signing, unblinding, and verifying. The procedures describe as below:

- *Initializing phase:*
  The signer randomly chooses two large primes p and q, and computes $n = p{\cdot}q$ and $\phi(n) = (p-1)(q-1)$. The signer chooses two large numbers e and d such that $ed \equiv 1 \bmod \phi(n)$ and $gcd(e, \phi(n)) = 1$. Let $(e,\, n)$ be the signer's public key and d be the signer's secret key. The signer keeps (p, q, d) secure and publishes $(e,\, n)$ and a one-way hash function $H(\cdot)$.
- *Blinding phase:*
  The requester has a message m, and he/she wishes to have it signed by the signer. The requester randomly selects an integer r as the blinding factor. The requester computes and submits the integer $m' = r^e \cdot H(m) \bmod n$ to the signer.

- *Signing phase:*
  After receiving m' from the requester, the signer computes and sends the integer
- *Unblinding phase:*
  After receiving S' from the signer, the requester computes $S = S' \cdot r^{-1} \bmod n$.
- *Verifying phase:*
  The S is a signature on the message m. Any one can verify the legitimacy of the signature by checking whether $s^e \equiv h(m) \bmod n$.

3 Our Electronic Voting Model

Our electronic voting model comprises of four phases and five participants: voters, a certificate authority (CA), an authentication center (AC), a tally center (TC), and a supervisor center (SC). In our model, we shall use public cryptosystems to ensure the security of transmission on a public channel and use the blind signature technique to protect the private information. The responsibilities of these facilities are described as follows:

- **Voters**: People who have eligibility to participate in an election.
- **Certificate Authority (CA)**: The certificate authority is responsible for registering each voter before the deadline of the election. To offer a true democracy, the certificate authority must ensure the constitutionality of each voter. In the meantime, the certificate authority should also get the trust of each voter. Hence, we recommend that the certificate authority should be composed of parties from the different parts of political spectrum.
- **Authentication Center (AC)**: The authentication center is similar to the central election commission in a traditional election, and it is responsible for verifying whether each voter registered with the certificate authority or not. If the voters have passed the registering phase, the authentication center will transmit the "voting certificate" to the registered voters. Any voter who has the voting certificate can cast his/her ballot in the voting phase, and the voting certificate is the main solution to prevent the voter from voting twice or more in an election.
- **Supervisor Center (SC)**: The supervisor center is similar to the polling station in a traditional election and is responsible for supervising all tasks through the election and verifying whether tally center counting the ballot correctly or not in the counting phase. As stated earlier, the supervisor center should also be composed of parties of different political points of view.
- **Tally Center (TC)**: The tally center is similar to the polling station in a traditional election and is responsible for 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.

3.1 Notations

In our electronic voting scheme, we shall use the following notations.

ID_i: the unique identity of each voter such as the identity card number.
EM_i: the unique e-mail account of the $voter_i$.
(PK_i, SK_i): the public key and its corresponding private key of the $voter_i$.
PK_{se}: the public key for encrypting the ballot by the $voter_i$. It was published by the certificate authority.
SK_{se}: the private key for decrypting the ballot by tally center. It was also published by the certificate authority.
(M, M'): a blank ballot and a marked ballot of $voter_i$.
$E_x(m)$: an encryption function for message m by using the key x.
$D_x(m)$: a decryption function for message m by using the key x.
$B(m, r)$: a blinding function for message m by using a blind factor r.
$B^{-1}(m, r)$: an unblinding function for message m by using a blind factor r.
$H(m)$: a one-way hash function for message m.

3.2 Our Electronic Voting Scheme

Our electronic voting protocol consists of four phases, namely: the registering phase, the authentication phase, the voting phase, and the tally phase. The details of our scheme are described as follows.

Registering Phase

Step 1: First, CA generates a unique pair of public key PK_{se} and private key SK_{se} for every eligible voter to encrypt the voted ballot M' and for the tally center to decrypt the cast ballot. Note that the private key SK_{se} will be kept secure until the voting time is up.

Step 2: Every voter must first register with the CA by using his/her unique identity information ID_i such as the identity number and inform CA which e-mail account EM_i he/she wants to use in the following procedures. CA must ensure that the e-mail account is not repeatedly used. In our protocol, every eligible voter must have a unique e-mail account.

Step 3: CA generates a unique pair of public key PK_i and private key SK_i for the registered voter after the voter passes the identity verification. And then CA will set up an "eligible registered voters list" that records the e-mail accounts EM_i and the public keys PK_i of the registered voters.

Step 4: CA should offer a secure way in which each registered voter can acquire the public key PK_i and private key SK_i. Furthermore, the key for encrypting the ballot PK_{se} should also follow the same way to be delivered to every eligible voter.

Step 5: When the registering time is up, CA will deliver the eligible registered voters list to AC and SC for the authentication phase.

Authentication phase

Step 1: The voter starts with downloading the blank ballot M from AC and then, according to his/her free will, picks out one candidate to mark on the blank ballot. This marked ballot is called a voted ballot M'. Finally, the voter encrypts the voted ballot by computing $C = E_{PK_{se}}(M')$.

Step 2: The voter randomly selects a blind factor r_1 and blinds the encrypted ballot by using the blinding function to compute $X = B(C, r_1)$. Additionally, the voter signs the blinded message X by using his/her privacy key SK_i to compute $X_1 = E_{SK_i}(X)$.

Step 3: In the next voting phase, the voter needs a rightful login name and password pair, which we call the "voting certificate". Hence, he/she gets the login name by computing $H(ID_i||a)$. Here, the argument a denotes a random number or a fictitious name chosen by the voter, and $||$ denotes the concatenation operator. And then the voter blinds $H(ID_i||a)$ by using the blinding function with another blind factor r_2 to compute $Y = B(H(ID_i||a), r_2)$. The same as Step 2, the voter signs the blinded message Y by using the encryption function with the privacy key SK_i to compute $Y_1 = E_{SK_i}(Y)$.

Step 4: Before the voter transmits the blinded message (X, Y) and the signature (X_1, Y_1), for the reason of security, he/she uses AC's public key PK_{AC} to encrypt these messages by computing $Z = E_{PK_{AC}}(X, X_1, Y, Y_1)$. Finally, the voter can use his/her e-mail account EM_i, which has been registered with CA to send the ciphertext Z to AC for requesting a voting certificate.

Step 5: After receiving the ciphertext Z, AC uses the decryption function with its privacy key SK_{AC} to obtain the requested information by computing $(X, X_1, Y, Y_1) = D_{SK_{AC}}(Z)$. And then AC, according to the voter's e-mail account EM_i, can find the public key PK_i of the voter in the eligible registered voter list, and hence AC can use the public key PK_i to verify the signature (X_1, Y_1) by verifying $X = D_{PK_i}(X_1)$ and $Y = D_{PK_i}(Y_1)$. If the signatures (X_1, Y_1) is validated, AC signs the blinded message (X, Y) with its private key SK_{AC} by computing $X_2 = E_{SK_{AC}}(X)$ and $Y_2 = E_{SK_{AC}}(Y)$. Then, AC encrypts the blind signatures (X_2, Y_2) by using the encryption function with the voter's public key PK_i and sends $W = E_{PK_i}(X_2, Y_2)$ back to the voter. Finally, in order to avoid double certification, AC marks on the eligible registered voter list according to the e-mail account EM_i of the voter.

Step 6: When the voter has received W, he/she uses the private key SK_i to reveal (X_2, Y_2) by computing $D_{SK_i}(W)$. And then the voter uses the unblinding function with the blind factor r_1 and r_2 to obtain the true signatures of message C and $H(ID_i||a)$ as follows.

$$SG_1 = B^{-1}(X_2, r_1) = E_{SK_{AC}}(C).$$
$$SG_2 = B^{-1}(Y_2, r_2) = E_{SK_{AC}}(H(ID_i||a)).$$

Step 7: After successfully authenticated by AC, the voter must also be authenticated by SC in order not only to obtain another signature of the voted ballot but also to ensure that the voted ballot will be counted correctly in the counting phase. For this reason, the voter generates a new blind factor r_3 to blind the voted ballot C by computing $X_3 = B(C, r_3)$. And then the voter sends $Z_1 = E_{PK_{SC}}(X_3, H(ID_i||a), SG_2)$ to SC.

Step 8: After receiving Z_1, SC uses its privacy key SK_{SC} to reveal $(X_3, H(ID_i||a), SG_2)$ by computing $D_{SK_{SC}}(Z_1)$. And SC verifies whether $H(ID_i||a)$ was signed by AC or not by validating $H(ID_i||a) = D_{PK_{AC}}(SG_2)$. Then, SC signs the blinded message X_3 by computing $X_4 = E_{SK_{SC}}(X_3)$. In addition, SC generates another random number or an identity name b and injects it into $H(ID_i||a)$ by computing $H(H(ID_i||a)||b)$. And then SC signs $H(H(ID_i||a)||b)$ by computing $SG_3 = E_{SK_{SC}}(H(H(ID_i||a)||b))$. Eventually, SC sends $H(H(ID_i||a)||b)$, SG_3, and X_4 to the voter.

Step 9: After $H(H(ID_i||a)||b)$, SG_3, and X_4 are received from SC, the voter verifies whether or not $H(H(ID_i||a)||b)$ was signed by SC by validating $H(H(ID_i||a)||b) = D_{PK_{SC}}(SG_3)$. Finally, the voter uses the unblinding function with the blind factor r_3 to obtain the true signature of the voted ballot C signed by SC by computing $SG_4 = B^{-1}(X_4, r_3) = E_{SK_{SC}}(C)$.

Voting Phase

Step 1: Before the voter casts the voted ballot C, he/she uses the voting certificate $(H(ID_i||a), SG_2)$ to login TC, where $H(ID_i||a)$ and SG_2 denote the voter's login name and password, respectively.

Step 2: TC checks the login name and its password by verifying $H(ID_i||a) = SG_2$.

Step 3: After the voter logs into TC successfully, he/she casts the voted ballot C, SG_1, SG_3, $(H(H(ID_i||a)||b)$, and SG_4 through a secure channel.

Step 4: After receiving the ballot information, TC starts with verifying the validity of the ballot by computing $M_1' = D_{PK_{AC}}(SG_1)$ and $M_2' = D_{PK_{SC}}(SG_3)$, and checking whether $C = M_1' = M_2'$. Furthermore, TC verifies $(H(H(ID_i||a)||b)? = D_{PK_{SC}}(SG_4)$ to see whether $(H(H(ID_i||a)||b)$ was signed by the SC or not. If the ballot information passes the verification procedure, then TC records $H(ID_i||a)$ as a voted voter. This prevents double voting. Finally, TC records $H(H(ID_i||a)||b)$, SG_4, and M' on the counting result list.

Counting Phase

Step 1: When the voting time is up, TC stops collecting ballots, and CA announces the privacy key SK_{se}.

Step 2: After getting the private key SK_{se}, TC decrypts the encrypted ballot C by computing $M' = E_{SK_{se}}(C)$.

Step 3: Then, TC records the ballot M' on the counting result list as $H(H(ID_i||a)||b)$, SG_4, C, and M'.

Step 4: Finally, TC announces the election result and makes the counting result list public.

4 Analyses and Discussions

In this section, we prove that the proposed protocol satisfies all general requirements of an electronic voting system mentioned earlier and show the functionality comparisons between our scheme and other related schemes in Table 1.

Table 1. Comparisons of functionality requirements between our scheme and other related schemes

	Protocols		
Requirement	Liaw's protocol [11]	Chang-Lee's protocol [4]	Our protocol
Accuracy	Yes	Yes	Yes
Simplicity	No	Yes	Yes
Privacy	Yes	Yes	Yes
Democracy	Yes	Yes	Yes
Verifiability	Yes	No	Yes
Uncoercibility	No	Yes	Yes

Accuracy: In our electronic voting protocol, the blank ballot is a free document for anyone to download. In other words, AC cannot mark any identity information on the blank ballot. In the voting phase, only an eligible ballot can be cast to TC, and AC will announce a counting result list which includes $H(H(ID_i||a)||b)$, SG_4, and C when the voting time is up. Then, SC checks the list by computing $H(H(ID_i||a)||b) = D_{PK_{SC}}(SG_4)$ before the ballot counting is started. Note that the cast ballot M' was encrypted by using the public key PK_{se}. When the time has come to count the cast ballots, CA announces the private key SK_{se}, and now TC has the ability to decrypt C to get M'. Next, TC records M' on the counting result list. Hence, the cast ballots can be counted successfully. Moreover, SC can supervise the counting by checking the list.

Simplicity: Our electronic voting system can be implemented via any system development software and Internet. A user-friendly interface can make it very easy for voters to use the system and no additional equipment is required such as smart cards and card readers.

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 electronic voting protocol, we adopt the blind signature technique to protect the privacy. In the authentication phase, the voter generates a unique name to produce $H(ID_i||a)$ and the voted ballot C, and then he/she uses the blinding function with the blind factor r_1 and r_2 to calculate X and Y. AC signs the blinded message (X, Y) by using the encryption function along with its private key SK_{AC} and then sends it back to the voter. Finally, the voter obtains the true signatures of C and $H(ID_i||a)$ by unblinding the blind signature (X_2, Y_2) as follows.

$$SG_1 = B^{-1}(X_2, r_1) = E_{SK_{AC}}(C).$$
$$SG_2 = B^{-1}(Y_2, r_2) = E_{SK_{AC}}(H(ID_i||a)).$$

Moreover, the voter follows the same path to obtain the signature of $SG_3 = E_{SK_{SC}}(H(H(ID_i||a)||b))$ signed by SC. After TC announces the result of election, neither AC nor SC can find out the relationship among the $H(H(ID_i||a)||b)$, C, and M' on the counting result list.

Democracy: There are three parties responsible for verifying the eligibility of each voter. First, in the registering phase, each voter has a unique identification name such as an identification card number and an e-mail account. When the registering time is up, CA records all registered voters' PK_i and EM_i on the eligible registered voters list, and then transmits this list to AC and SC for the further authentication. Hence, AC can check the eligibility of a voter when it receives Z from the voter. Also, AC can obtain the corresponding public key PK_i through the eligible registered voters list. After the authentication is successful, AC marks the result on the eligible registered voters list. For the security reason, each voter must also be authenticated by SC. After receiving X_3, $H(ID_i||a)$ and SG_3 from the voter, SC then checks $H(ID_i||a)$ to see whether it was signed by AC or not by verifying $H(ID_i||a) = D_{PK_{AC}}(SG_2)$. Finally, just like what is done in the previous authentication process, SC records $H(ID_i||a)$ to avert the voter from authenticating again. Therefore, each voter can cast only one ballot.

Verifiability: In order to prevent ballot buying, some electronic voting systems do not allow the voter to verify the result of voting and check whether the ballot was counted correctly by TC or not. However, how can TC get the trust of all voters is a big problem if verifiability is not provided. In our scheme, TC announces the counting result list which includes $H(H(ID_i||a)||b)$, SG_4, C, and M'. Thus, any voter can check whether his/her cast ballot was counted correctly or not.

Uncoercibility: If a voter wants to prove that a specific $H(H(ID_i||a)||b)$ represents himself, the parameter b must be known to the voter. However, the parameter b was generated by the SC and is kept secure all the time. Any voter has no way to get the parameter. Therefore, our electronic voting system not only maintains the verifiability but also keeps ballot buying from happening.

5 Conclusions

In this paper, we proposed an electronic voting protocol. The proposed electronic voting protocol adopts blind signature to protect the content of the ballot during casting. Because we believe that a secure electronic voting system should not only allow all voters to verify the voting result but also avoid ballot buying, the proposed electronic voting protocol is verifiable and discourages ballot buying at the same time. Any malicious candidate or party can still try to buy ballots during the election. However, no voter can prove exactly which ballot was cast by him/her after the announcement of the election result. In other words, ballot buying may still exist, but the ballot buyer cannot be assured that the voter will mark the ballot as the buyer wishes.

Acknowledgements

This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under the grants NSC 95-2218-E-001-001, and NSC95-2218-E-011-015.

References

1. Pierluigi Bonetti, Stefano Ravaioli, and Simone Piergallini. The Italian academic community's electronic voting system. *Computer Networks*, 34(6):851–860, December 2000.
2. D. Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology, CRYPTO'82*, pages 199–203, 1982.
3. D. Chaum. Blind signatures system. In *Advances in Cryptology, CRYPTO'83*, pages 153–156, 1983.
4. C. C. Chang and J. S. Lee. An anonymous voting mechanism based on the key exchange protocol. In *Computers & Security*, 25(4):307-314, 2006.
5. R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung. Multi-authority secret bollat elections with linear work. In *Advances in Cryptology, EUROCRYPT'96*, pages 72–83, Lecture Notes in Computer Science, 1070, 1996.
6. Min-Shiang Hwang, Iuon-Chung Lin, and Li-Hua Li. A simple micro-payment scheme. *Journal of Systems and Software*, 55(3):221–229, 2001.
7. Min-Shiang Hwang, Eric Jui-Lin Lu, and Iuon-Chung Lin. Adding timestamps to the secure electronic auction protocol. *Data & Knowledge Engineering*, 40(2):155–162, 2002.
8. Jinn-Ke Jan and Chih-Chang Tai. A secure electronic voting protocol with IC cards. *Journal of Systems and Software*, 39(2):93–101, November 1997.
9. Wei-Chi Ku and Sheng-De Wang. A secure and practical electronic voting scheme. *Computer Communicarions*, 22(3):279–286, 1999.
10. C. L. Lei and C. I. Fan. A universal single-authority election system. *IEICE Transactions on Fundamentals*, E81-A(10):2186–2193, 1998.
11. H. T. Liaw. A secure electronic voting protocol for general elections. *Computers & Security*, 23(2):107-119, 2004.
12. Y. Mu and V. Varadharajan. Anonymous secure e-voting over a network. In *Proceedings of the 14th Annual Computer Security Applications Conference, CACSAC'98*, pages 2936–2939, 1998.
13. Andreu Riera, Josep Rifà, and Joan Borrell. Efficient construction of vote-tags to allow open objection to the tally in electronic elections. *Information Processing Letters*, 75(5):211–215, October 2000.