IMPROVED ANONYMOUS SECURE E-VOTING OVER A NETWORK

Chou-Chen YANG, Ching-Ying LIN, and Hung-Wen YANG

Abstract: In a democratic country voting is one of the most important activities. However, many eligible voters do not exercise their right simply because they do not want to visit a public booth where they can vote. In 1981, David Chaum first introduced the concept of electronic voting and attempted to overcome the problems associated with the traditional voting environment. Hereafter, Mu and Varadharajan proposed in 1998 an anonymous secure e-voting scheme over a network. They claimed that the proposed scheme is not only capable of preventing double voting but it can also protect the privacy of voters. However, many researchers afterwards have discovered that Mu and Varadharajan's scheme is not secure. Attackers can easily forge a valid ballot and can vote more than once. In this paper, an e-voting scheme based on Mu and Varadharajan's scheme is proposed that meets the following e-voting requirements: democracy, accuracy, anonymity, mobility and efficiency.

Keywords: Anonymity, Blind Signature, ElGamal Public Key Crypto-System, e-Voting.

In a democratic society voting is one of the most important activities. In such a traditional voting environment, the voting process sometimes becomes quite ineffective and inconvenient due to the fact that the eligible voters have to visit a voting booth to cast their votes. Very often the eligible voters do not exercise their right to vote simply because they do not have time to visit a voting booth. Besides, the traditional voting method requires more expenses and involves more social resources, social cost and human resources. Therefore, the effort of many researchers has been put into finding solutions to the problems inherent in traditional voting environment. The development of computer networks and the elaboration of the cryptographic techniques facilitate the implementation of electronic voting.

Electronic voting is very convenient for the voters due to the fact that they can cast their ballots through a network. Even if the voters do not have time to go to the voting booth they can still cast they vote through a computer with Internet connection. Thus,

they can exercise their right to vote. Furthermore, this electronic voting method can reduce the expenses and avoid errors. The first electronic election scheme was proposed by David Chaum;[1] then the same author suggested the concept of blind signatures.[2] Later on, many researchers have worked and proposed various developments in e-voting.[3,4,5,6,7,8,9,10,11,12,13] The existing e-voting systems can be divided into two types. One type of systems is based on homomorphic functions,[14] and the other is based on blind signatures.[15] The e-voting systems based on blind signatures are preferable in practice in comparison with those based on homomorphic functions due to the fact that the system of homomorphic functions is less flexible and it only provides YES or NO function on the ballot. The other system based on blind signatures provides more flexibility on the ballot. In other words, it can allow more formats on the ballot. The general requirements of e-voting are listed in Table 1.

Table 1: Requirements of e-Voting.

Property	*Definition*
Democracy	Only eligible voters can participate in election.
Convenience	Voters can cast their ticket easily and quickly.
Mobility	No restrictions imposed on the location where voters can cast their ballots.
Efficiency	The voters cast their ballot in a reasonable amount of time and he/she is not required to wait for others to complete the process.
Robustness	No one can disrupt or disturb the election because of the independence of the voting processes.
Anonymity	No one can trace the identity of the voter from the ballot.
Authentication	The authorities and voter should verify each other during the process of voting.
Validation	The authorities are able to check whether the ballots are valid or not.
Uniqueness	No voters can vote more than once.
Completeness	An eligible voter is always accepted by the authorities.
Fairness	The authorities are prohibited to cheat, even if they attempt to collude.

In 1998, Mu and Varadharajan proposed an anonymous secure electronic voting scheme,[16] which is based on ElGamal's digital signature algorithm.[17] In essence, the authors claimed that their scheme can ensure the secrecy of voters and prevent the occurrence of double voting. However, Lin, Hwang, and Chang[18] and Chien, Jan, and Tseng[19] pointed out that there are flaws in Mu and Varadharajan's scheme. They outlined problems such as a voter can vote more than once without being detected, the

voter's identity can be revealed by the authorities, and the valid ballot can be forged without being authenticated.

To enhance the security of Mu and Varadharajan's scheme, in 2003 Lin, Hwang, and Chang[20] proposed an improved scheme. Later, Chien, Jan, and Tseng[21] also pointed out some limitations existing in Mu and Varadharajan's scheme. In turn, the authors of the current paper have observed that the improved scheme reported by Lin, Hwang, and Chang cannot resist to the attack proposed by Chien, Jan, and Tseng. Therefore, this paper proposes an improved scheme that can overcome the deficiencies existing in Mu and Varadharjan's scheme.

The paper is structured as follows. First, the environment and the scheme and process of general e-voting will be introduced. Then, Mu and Varadharajan's scheme will be briefly reviewed. The section that follows shall present the general act of attacking of an e-voting scheme and the Chien, Jan, and Tseng's scheme. After that, an improved scheme that overcomes the weakness of Mu and Varadharajan's scheme will be proposed, followed by a security analysis. Conclusions and future research directions are given in the last section.

E-Voting Environments and Processes

E-voting Environments

This section introduces the environments for e-voting. In general, there are five parties in anonymous e-voting environments,[22] which are listed as follows:

- *Voter*: Citizens who are qualified to vote.
- *Authentication Server (AS)*: AS is responsible for authenticating the voters and granting voting tickets.
- *Voting Servers (VS)*: It collects voting tickets from voters.
- *Tickets Counting Server (TCS)*: Responsible for tallying the votes.
- *Certificate Authority (CA)*: Provides a certificate service provider for all voters enrolled.

The e-voting activities are:

(1) 〔Voter→CA〕: Before voting, all voters should register at CA as valid voters.

(2) 〔CA→Voter〕: After a voter completes the enrollment, the CA signs and issues a certificate to the voter.

(3) 〔Voter→AS〕: Voter sends a request to AS for a voting ticket.

(4) 〔AS→Voter〕: AS sends a blindly signed ticket to voter.

(5) 〔Voter→VS〕: Voter sends the voting ticket via network to VS.

(6) 〔VS→TCS〕: VS sends voting tickets to TCS once the voting box is full. The counting of tickets is done by TCS.

Figure 1 provides an illustration of the anonymous e-voting environment and its process.

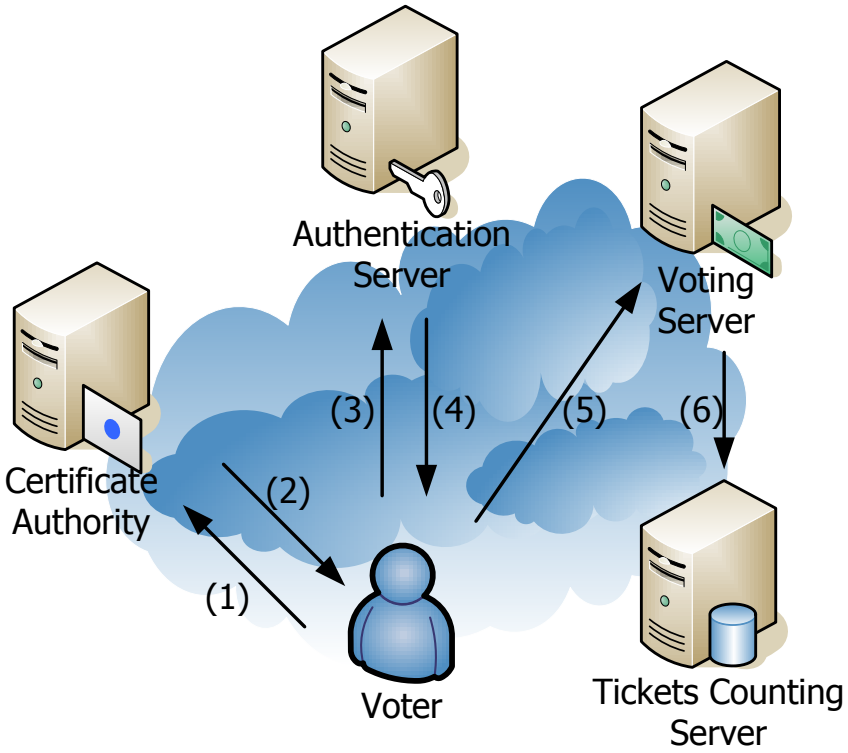

Figure 1: The Anonymous e-Voting Environment and its Process.

e-Voting Processes

In general, the e-voting process involves at least three phases: a registration phase, a voting phase, and a counting phase.

In 1998, Mu and Varadharajan proposed two anonymous secure electronic voting schemes[23] based on ElGamal's digital signature algorithm.[24] Both schemes have five parties involved and three processes as described above. However, the first scheme proposed by Mu and Varadharajan assumes that the Authentication Server (AS) is trustworthy; the second scheme assumes that the trusted AS is unnecessary. The second scheme is more efficient, secure and practical as compared with the first scheme.

However, as Lin, Hwang, and Chang[25] and Chien, Jan, and Tseng[26] showed the second scheme of Mu and Varadharajan is insecure. The following section provides a brief review.

First, we define the notations used is this paper.

- ID_x: The identity of X.
- $Cert_x$: The certificate of X, which includes X's identity, public key, serial number, valid period, and CA's signature.
- (d_x, e_x): The RSA secret/public key pair of X.
- p: A large prime number.
- n_x: A product of two large prime numbers.
- g: A generator for Z_p^*.
- t: The current timestamp.
- $||$: Concatenation of bits.

Registration Phase

The registration phase includes two procedures: getting a voting certificate from CA and obtaining a voting ticket from AS. The procedures are shown in Figure 2.

1. Getting a Voting Certificate:

A voter generates a key pair first, and then s/he sends it to CA. In order to achieve the e-voting requirements of democracy and completeness, CA has to check the identity of the voter and issue a certificate.

2. Obtaining a Voting Ticket:

Step 1: Before voting, the voter has to send a request to AS for getting a voting ticket. In order to meet the requirement of anonymity, the voter chooses a blind factor b and two secret parameters r and $k_1 \in Z_{p-1}$. Then $a \equiv g^r \bmod p$, $x_1 \equiv gb^{e_{AS}} \bmod n_{AS}$, $x_1' \equiv g^{k_1} b^{e_{AS}} \bmod n_{AS}$, and $x_2 \equiv ab^{e_{AS}} \bmod n_{AS}$ are computed. After that, the voter sends $\{ID_v, ID_{AS}, Cert_V, (x_1 || x_1' || x_2 || t)^{d_v} \bmod n_v\}$ to AS in order to request a voting ticket.

Step 2: When AS receives the message from the voter, the voter's signature has to be verified first; then a random parameter $k_2 \in Z_{p-1}$ is chosen; $x_3 = (k_2 || t)^{e_v} \bmod n_v$ and $x_4 \equiv (x_1^{k_2} x_1' x_1^{2k_2} x_1' x_2)^{d_{AS}} \bmod n_{AS}$ are computed; and k_2 is stored in a database. Finally, the AS sends the message

$\{ID_{AS}, ID_V, x_3, (x_4 \,||\, t)^{e_v} \bmod n_v\}$ to the voter.

Step 3: When the voter receives the message from AS, he uses his secret key to decrypt x_3 and get k_2. Then, the parameters k, k', y_1, and y_2 are computed for the voter, where $k = k_1 + k_2$, $k' = k_1 + 2k_2$, $y_1 = g^k$, and $y_2 = g^{k'}$. Moreover, the blind factor $b^{3(k_2+1)}$ can be removed in order to obtain $x'_4 \equiv (y_1 y_2 a)^{d_{AS}} \bmod n_{AS}$, and compute $s_1 = k^{-1}(ma - r) \bmod p\text{-}1$ and $s_2 = k'^{-1}(ma - r) \bmod p\text{-}1$. Finally, the voting ticket is composed as $T \equiv \{a \,||\, g \,||\, y_1 \,||\, y_2 \,||\, x'_4 \,||\, s_1 \,||\, s_2 \,||\, m\}$.

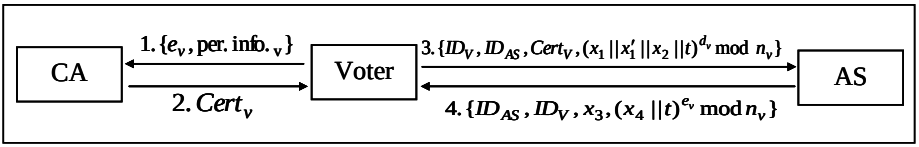

Figure 2: Registration Phase of Mu and Varadharajan's Scheme.

Voting Phase

On the voting day, the voter sends a voting ticket $\{ID_{VS}, (T \,||\, t)^{e_{VS}} \bmod n_{VS}\}$ to the Voting Server, where *T* is the ticket and *t* denotes the real timestamp. After VS receives the voting ticket, it decrypts $(T \,||\, t)^{e_{VS}} \bmod n_{VS}$ using its secret key d_{VS} to obtain *T*. Then VS verifies whether the signature of AS is valid or not. If valid, then VS verifies the voter's signatures s_1 and s_2 by $y_1^{s_1} a = g^{ma} \bmod p$ and $y_2^{s_2} a = g^{ma} \bmod p$. If valid, VS casts the voting ticket into voting boxes.

Counting Phase

After voting is over, TCS executes the procedures of counting tickets and checking whether double voting has occurred by examining whether (a, g, y_1, y_2) are used more than once. In the case of double voting, the AS could compute $k = k_1 + k_2$ and $k' = k_1 + 2k_2$ to get k_2 and trace the voter's identity back.

Attacks

In general, the attacks on the e-voting systems can be divided into three types:

- *Forge ticket*: The malicious attacker can forge a valid ticket without being detected.

- *Trace voter's identity*: The identity of a voter can be traced from the cast voting ticket.
- *Double voting*: An eligible voter can vote more than once.

We have reviewed the Mu and Varadharajan's e-voting scheme in a previous section. Unfortunately, their scheme is vulnerable to attacks as mentioned above. In 2003, Chien, Jan, and Tseng[27] pointed out the weaknesses of Mu and Varadharajan's e-voting scheme as follows.

Attack 1: Forge Ticket

Assume that an attacker chooses three random numbers k_1, k_2, and r (let $k_1, k_2, r < p$), and computes the following equations:

$$a = g^{re_{AS}},\ y_1 = g^{k_1 e_{AS}},\ y_2 = g^{k_2 e_{AS}},$$
$$s \equiv_{n_{AS}} g^{k_1 + k_2 + r} \bmod n_{AS},$$
$$s_1 = (k_1 + k_2)^{-1}(ma - r) \bmod np - 1,$$
$$s_2 = (k_1 + 2k_2)^{-1}(ma - r) \bmod p - 1$$

Then, the attacker can construct the ticket $T = \{a \| g \| y_1 \| y_2 \| s \| s_1 \| s_2 \| m\}$, and VS and TCS cannot detect whether the ticket is forged. This attack can also be found in the work of Lin, Hwang, and Chang.[28]

Attack 2: Trace Voter's Identity

In Mu and Varadharajan's scheme, the parameter k_2 indicates a unique identity for each voter. However, TCS can trace the voter's identity back from the voting ticket even the situation of double voting has not occurred. To get the parameter k_2 TCS computes the following equation:

$$\frac{y_2}{y_1} \equiv \frac{g^{k_1 + 2k_2}}{g^{k_1 + k_2}} \equiv g^{k_2} \bmod p$$

Thus, the Mu and Varadharajan's scheme cannot meet the requirement of anonymity.

Attack 3: Double Voting

The definition of double voting is the situation where a voter or an attacker can vote more than once in the same election process. In Mu and Varadharajan's scheme, the

eligible voter can perform the voting process correctly and compose the voting ticket as follows. First, the voter chooses $g = g'^{k}$, r, and k_1; then the voter sends $\{ID_v, ID_{AS}, Cert_V, (x_1 || x_1' || x_2 || t)^{d_v} \bmod n_v\}$ to AS for obtaining a voting ticket. In this way, the voter can construct the voting ticket $T = \{a || g || y_1 || y_2 || s || s_1 || s_2 || m\}$, where $a = g^r$, $y_1 = g^{k_1+k_2}$, $y_2 = g^{k_1+2k_2}$, and $s \equiv (y_1 y_2) a^{d_{AS}} \bmod n_{AS}$. Moreover, the voter can construct another valid voting ticket as follows. The voter lets $a' = g^{r+k_1+k_2}$, $y_1' = g^{k_1}$, and $y_2' = g^{2k_2}$; it becomes obvious that $\{a', g', y_1', y_2', s\}$ can still satisfy $s \equiv_{n_{AS}} (y_1' y_2' a')^{d_{AS}}$, and the voter can compose a new ticket using these parameters as $T' = \{a' || g' || y_1' || y_2' || s || s_1' || s_2' || m\}$. VS and TCS are not able to detect the double voting.

Improvements

In this section, a new improved scheme is presented to enhance the security and prevent the above-mentioned attacks. The proposed scheme consists also of three phases and there are five parties involved, very much the same as in Mu and Varadharajan's scheme. The voting process will be described in what follows.

Registration Phase

The registration phase involves two procedures: requesting a voting certificate from CA and obtaining a valid voting ticket from AS. The voter should provide his identity when requesting a voting ticket from AS. The procedures are shown in Figure 3.

1. Requesting a Voting Certificate:

Each voter generates a key pair (d_v, e_v) and a large number n_v to request a voting certificate from CA. After checking the identity of a voter, CA issues a certificate to the voter to achieve the e-voting requirement of democracy and completeness.

2. Obtaining a Voting Ticket

Step 1: The voter has to send a request to AS for getting a voting ticket. In order to achieve the e-voting requirement of anonymity and authentication, the voter chooses a blind factor b_1 and four random numbers b_2, q, r and $k_1 \in Z_{p-1}$. With these parameters, a, x_1, x_2 and x_2 can be computed for the voter using the following equations:

$$a = g^r \bmod n,$$
$$x_1 = g b_1^{e_{AS}} \bmod n,$$
$$x_1' = g^{2k_1+q} b_1^{e_{AS}} \bmod n,$$
$$x_2 = a b_2^{e_{AS}} \bmod n$$

where $g \in Z_p^*$ is the system's public parameter. Finally, the voter sends the message $\{ID_V, ID_{AS}, Cert_v, (x_1 || x_1' || x_2 || t)^{d_v} \bmod n_v\}$ to AS for getting parameters to compose the voting ticket.

Step 2: Upon receiving the message, for authentication, AS verifies whether the signature $(x_1 || x_1' || x_2 || t)^{d_v} \bmod n_v$ is valid or not. If valid, AS chooses a random number k_2, that is different for each voter in order to meet the property of uniqueness and to compute the following equations:

$$x_3 = (k_2 || t)^{e_v} \bmod n_{AS},$$
$$x_4 = (x_1^{k_2}\ x_1'\ x_1^{2k_2}\ x_1'\ x_2)^{d_{AS}} \bmod n_{AS}$$
$$= (y_1\ y_2\ a)^{d_{AS}} b_1^{3k_2+2} b_2 \bmod n_{AS}$$

where $y_1 = g^{k_1+2k_2+2q}$, and $y_2 = g^{3k_1+k_2}$. In order to achieve the e-voting requirement of validation, AS will store k_2 in the database, compute the value of $h(x_2)$ and publish it so it can detect double-voting. Finally, AS sends the message $\{ID_{AS}, ID_V, x_3, (x_4 || t)^{e_v} \bmod n_V\}$ to the voter.

Step 3: When the voter receives the message, x_3 is decrypted to get k_2 and the blind factor $b_1^{3k_2+2} b_2$ is removed to obtain the signature (s'); then the following equations are computed:

$$s' = (y_1\ y_2\ a)^{d_{AS}} \bmod n_{AS},$$
$$s_1 = (k_1 + 2k_2 + 2q)^{-1}(ma - r) \bmod p - 1,$$
$$s_2 = (3k_1 + k_2)^{-1}(ma - r) \bmod p - 1.$$

Finally, the voter can compose the voting ticket as follows: $T = \{a || g || y_1 || y_2 || s' || s_1 || s_2 || m || b_2\}$.

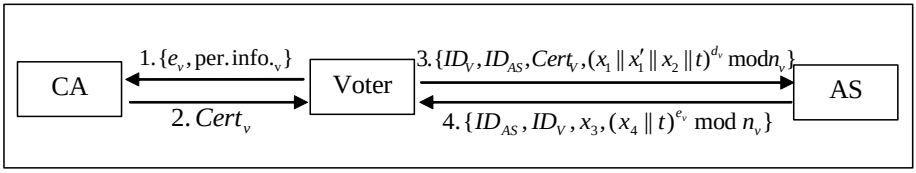

Figure 3: Registration Phase of the Proposed Scheme.

Voting Phase

After obtaining a valid voting ticket from AS, the voter can send the voting ticket. The procedure is shown in Figure 4.

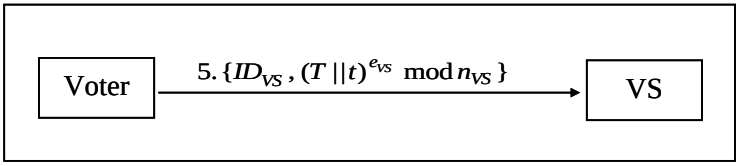

Figure 4: Voting Phase of the Novel Scheme.

Step 1: The voter sends $\{ID_{VS}, (T \| t)^{e_{VS}} \bmod n_{VS}\}$ to VS, where T is the voting ticket and t denotes the current timestamp.

Step 2: VS decrypts $(T \| t)^{e_{AS}} \bmod n_{VS}$ with its secret key (d_{AS}) to achieve the e-voting requirement of authentication. VS verifies the validity of a, y_1, and y_2 using AS's signature from the equation $(s')^{e_{AS}} = (y_1 y_2 a) \bmod n_{AS}$. If the result is true, then VS checks the correctness of s_1 and s_2 using voter's signatures from the following equations:

$$y_1^{s_1} a = g^{ma} \bmod p$$

$$y_2^{s_2} a = g^{ma} \bmod p.$$

If the results are true, VS can be sure that the ticket is valid. Finally, VS stores all the voting tickets and sends them back to TCS via a network.

Counting Phase

After voting is over, TCS checks whether the parameters (a, g, y_1, y_2) have been used more than once and checks $h(ab_2^{e_{AS}}) \bmod n_{AS} = ? h(x_2)$ to detect double voting,

where $h(x_2)$ is published by AS to be used to confirm the authentication of the ticket. If the results are positive, then TCS will calculate the valid ballot and announce the result obtained from this electronic election.

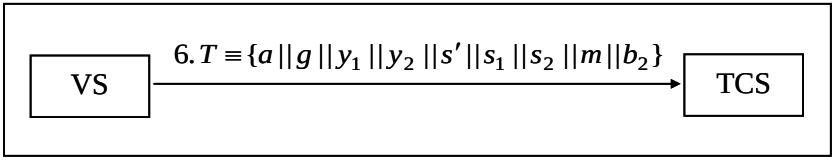

Figure 5: Counting Phase of the Proposed Scheme.

Security Analysis

In this section, it will be illustrated that the proposed scheme can enhance the security and overcome the limitations of Mu and Varadharajan's scheme.

Prevent Tracing the Voter's Identity

Chien, Jan, and Tseng's work[29] points out that the authorities can obtain a voting ticket from the public network and compute the following equation to get the value of k_2.

$$\frac{y_2}{y_1} \equiv \frac{g^{k_1+2k_2}}{g^{k_1+k_2}} \equiv g^{k_2} \bmod p$$

Thus, the authorities can easily trace the identity of the voting ticket. However, in our improved scheme, no one can trace the identity from the voting ticket. The authorities cannot employ the above equation to obtain k_2 since the parameters y_1 and y_2 contain the secret value k_1 and q chosen by the voter. In consequence, in the proposed scheme, attacking using the trace from the voter's identity as reported by Chien, Jan, and Tseng cannot be successful. In what follows it will be demonstrated why:

$$y_1 = g^{k_1+2k_2+2q},$$
$$y_2 = g^{3k_1+k_2},$$
$$\frac{y_2}{y_1} \equiv \frac{g^{k_1+2k_2+2q}}{g^{3k_1+k_2}} \bmod p$$

It is obvious that:

$$\left(\frac{y_2}{y_1} \bmod p\right)$$

cannot give k_2. Therefore, the authorities cannot find the identity from the voting ticket.

Prevent Forging Ticket and Double Voting

In the improved scheme the authors propose, the public value of $h(x_2)$ is used to detect forged tickets and double voting, where $(x_2 = ab_2^{e_{AS}} \bmod n)$ and b_2 are chosen by the voter. In the registration phase, AS has to confirm the identity of the voter first, and then publish $h(x_2)$, where x_2 is received from the voter. However, in the counting phase, in order to detect forged tickets, TCS will check $h(ab_2^{e_{AS}}) \bmod n_{AS} = ? h(x_2)$. If TCS computes a value of $h(ab_2^{e_{AS}}) \bmod n_{AS}$ which is not in the list published by AS, TCS can determine whether the ticket is valid or not. So, if the voter wants to forge another ticket, he has to send another x_2 to AS. Obviously, it is not possible, since the CA will not issue another certificate to the same voter. So, if the voter cannot get another certificate, then AS will not accept the identity of the voter and will not publish the value of $h(x_2)$.

On the other hand, if an attacker attempts to forge $h(x_2)$ in the list published by AS, then he/she will discover that this is not possible due to the property of the hash function, i.e. that there is no way to find the value of x_2 from $h(x_2)$. Besides, it is difficult to find other parameters such as a' and b_2' that can allow through $h(a'b_2'^{e_{AS}} \bmod n) = h(x_2)$ passing the validation of signature. As a result, the proposed scheme can resist forged attack and prevent double voting.

Conclusion

In this paper, the authors have introduced an anonymous secure e-voting environment, together with its processes and common attacks. Furthermore, the authors have also proposed an improved scheme that can enhance the security of Mu and Varadharajan's scheme.

Acknowledgement

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract No. NSC92-2213-E-324-005.

Notes:

[1] David L. Chaum, "Untraceable Electronic Mail, Return Address and Digital Pseudonyms," *Communictions of the ACM* 24, no. 2 (1981): 84-88.

[2] David L. Chaum, "Blind Signatures System," in *Advances in Cryptology, CRYPTO'83* (1983), 153– 156.

[3] Josh D. Cohen and Michael J. Fischer, "A Robust and Verifiable Cryptographically Secure Election Scheme," in *Proceedings of the 26th IEEE Symposium on Foundations of Computer Science (FOCS)* (Portland, OR, 21-23 October 1985), (New York, USA: IEEE Computer Society, 1985), 372-382.

[4] Josh C. Benaloh and Dwight Tuinstra, "Receipt-Free Secret-Ballot Elections (extended abstract)," in *Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing STOC'94* (Montreal, Quebec, Canada, 23-25 May 1994), (New York, USA: ACM, 1994), 544-553.

[5] Josh C. Benaloh and Moti Yung, "Distributing the Power of a Government to Enhance the Privacy of Voters," in *Proceedings of the 5th Annual ACM Symposium on Principles of Distributed Computing (PODC)* (Calgary, Alberta, Canada, August 1986), (New York, USA: ACM, 1986), 52-62.

[6] Hung-Yu Chien, Jinn-Ke Jan, and Yuh-Min Tseng, "Cryptanalysis on Mu-Varadharajan's e-Voting Schemes," *Applied Mathematics and Computation* 139, no. 2-3 (July 2003): 525-530.

[7] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta, "A Practical Secret Voting Scheme for Large-Scale Elections," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology - AUSCRYPT'92* (Gold Coast, Queensland, Austrailia, 13-16 December 1992), *Lecture Notes in Computer Science* 718, ed. Jennifer Seberry and Yuliang Zheng (Berlin: Springer-Verlag, 1993), 244-251.

[8] Martin Hirt and Kazue Sako, "Efficient Receipt-Free Voting based on Homomorphic Encryption," in *Advances in Cryptology, EUROCRYPT'00*, *Lecture Notes in Computer Science* 1807, ed. B. Preneel (Berlin: Springer-Verlag, 2000), 539-556.

[9] Wen-Shenq Juang and Chin-Laung Lei, "A Secure and Practical Electronic Voting Scheme for Real World Environments," *IEICE Transactions on Fundamentals* E80-A, no. 1 (January 1997): 64-71.

[10] Horng-Twu Liaw, "A Secure Electronic Voting Protocol for General Elections," *Computers and Security* 23, no. 2 (March 2004), 107-119.

[11] Iuon-Chang Lin, Min-Shiang Hwang, and Chin-Chen Chang, "Security Enhancement for Anonymous Secure e-Voting over a Network," *Computer Standards & Interfaces* 25, no. 2 (May 2003): 131-139.

[12] Yi Mu and Vijay Varadharajan, "Anonymous Secure e-Voting over a Network," in *Proceedings of the 14th Annual Computer Security Applications Conference (ACSAC'98)* (Scottsdale, AZ, USA, 7-11 December 1998), (IEEE Computer Society, 1998), 293–299.

[13] Kazue Sako and Joe Killian, "Secure Voting Using Partially Compatible Homomorphisms," in *Advances in Cryptology--CRYPTO'94*, *Lecture Notes in Computer Science* 839, ed. Yvo G. Desmedt (Berlin: Springer-Verlag, 1994), 411-424.

[14] Benaloh and Fischer, "A Robust and Verifiable Cryptographically Secure Election Scheme;" Benaloh and Tuinstra, "Receipt-Free Secret-Ballot Elections;" Benaloh and Yung,

"Distributing the power of a government to enhance the privacy of voters;" Hirt and Sako, "Efficient Receipt-Free Voting based in Homomorphic Encryption;" Sako and Killian, "Secure Voting Using Partially Compatible Homomorphisms."

[15] Fujioka, Okamoto, and Ohta, "A Practical Secret Voting Scheme for Large-Scale Elections;" Juang and Lei, "A Secure and Practical Electronic Voting Scheme for Real World Environments;" Liaw, "A Secure Electronic Voting Protocol for General Elections;" Lin, Hwang, and Chang, "Security Enhancement for Anonymous Secure e-Voting over a Network;" Mu and Varadharajan, "Anonymous Secure e-Voting over a Network."

[16] Mu and Varadharajan, "Anonymous Secure e-Voting over a Network."

[17] ElGamal, "A Public-Key Cryptosystem and a Signature Scheme based on Discrete Logarithms."

[18] Lin, Hwang, and Chang, "Security Enhancement for Anonymous Secure e-Voting over a Network."

[19] Chien, Jan, and Tseng, "Cryptanalysis on Mu-Varadharajan's e-Voting Schemes."

[20] Lin, Hwang, and Chang, "Security Enhancement for Anonymous Secure e-Voting over a Network."

[21] Chien, Jan, and Tseng, "Cryptanalysis on Mu-Varadharajan's e-Voting Schemes."

[22] Mu and Varadharajan, "Anonymous Secure e-Voting over a Network."

[23] Mu and Varadharajan, "Anonymous Secure e-Voting over a Network."

[24] ElGamal, "A Public-Key Cryptosystem and a Signature Scheme based on Discrete Logarithms."

[25] Lin, Hwang, and Chang, "Security Enhancement for Anonymous Secure e-Voting over a Network."

[26] Chien, Jan, and Tseng, "Cryptanalysis on Mu-Varadharajan's e-Voting Schemes."

[27] Chien, Jan, and Tseng, "Cryptanalysis on Mu-Varadharajan's e-Voting Schemes."

[28] Lin, Hwang, and Chang, "Security Enhancement for Anonymous Secure e-Voting over a Network."

[29] Chien, Jan, and Tseng, "Cryptanalysis on Mu-Varadharajan's e-Voting Schemes."

CHOU-CHEN YANG received his B.S. in Industrial Education from the National Kaohsiung Normal University in 1980. He received his M.S. in Electronic Technology from the Pittsburg State University in 1986, and his Ph.D. in Computer Science from the University of North Texas in 1994. He is an associate professor at the Department of Management Information Systems at National Chung Hsing University. His current research interests include network security, mobile computing, and distributed system. *Address for correspondence:* Department of Management Information System, National Chung Hsing University, 250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.; *E-mail:* cc.yang@nchu.edu.tw.

CHING-YING LIN received her B.S. in Information Management from Chaoyang University of Technology in 2004. She is pursuing her M.S. in Networking and Communication Engineering from Chaoyang University of Technology. Her current research interests include information security and mobile communications. *Address for correspondence:* Graduate Institute of Networking and Communication Engineeing, Chaoyang University of Technology, 168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.; *E-mail:* s9330601@mail.cyut.edu.tw.

HUNG-WEN YANG received his B.S. in Information Management from Taichung Healthcare and Management University in 2003. He is pursuing his M.S. in Information Management from Chaoyang University of Technology. His current research interests include information security and mobile communications. *Address for correspondence:* Department of Information Management, Chaoyang University of Technology, 168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.; *E-mail:* s9214605@mail.cyut.edu.tw.