A Secure and Anonymous Electronic Voting Scheme Based on Key Exchange Protocol[§]

Chun-Ta Li[1] and Min-Shiang Hwang[2,*]

[1]*Department of Information Management, Tainan University of Technology*
529 Zhongzheng Road, Tainan City 71002, Taiwan (R.O.C.)
th0040@mail.tut.edu.tw

[2]*Department of Computer Science and Information Engineering, Asia University*
500 Lioufeng Road, Taichung City 41354, Taiwan (R.O.C.)
[*]*Corresponding author: mshwang@asia.edu.tw*

Abstract

Voter anonymity and voting correctness are important issues for electronic voting mechanisms. Compared electronic voting with traditional 1elections, an electronic voter is able to cast his/her ballot through the Internet in any place and at any time if he/she can access the network. Therefore, convenience and mobility make electronic voting become more and more popular and electronic voting can be adopted in the real world with higher feasibility. Recently, Chang and Lee presented an electronic voting (e-voting) scheme based on the blind signature and the Diffie-Hellman key exchange methods for ensuring voter anonymity and performance efficiency. They claimed that numerous essential requirements of general electronic voting can be ensured in their e-voting scheme. Unfortunately, we found that Chang-Lee's e-voting scheme suffers from susceptibility to security attacks and some critical security requirements of their e-voting scheme may be compromised. To prevent security weaknesses of Chang-Lee's e-voting scheme, in this paper, an improved version on their e-voting scheme is proposed that not only keeps the merits of Chang-Lee's e-voting scheme but also enhances the security of their e-voting scheme.

Keywords: *Voter anonymity, blind signature, electronic voting (e-voting), information and network security, Diffie-Hellman key exchange*

1. Introduction

With the continuous development of computer networks and democratic societies, it is important to facilitate easy access for voters to the election polls. Recent advances in cryptographic techniques have made possible to provide Internet based voting as a feasible alternative to conventional elections [11, 12, 15, 16, 17, 18, 19, 21, 29, 30, 31]. Chaum [3] proposed the first electronic election mechanism in 1981. The scheme enables people to electronically cast his/her ballot over insecure network. In order to ensure voting security, many electronic voting (e-voting) schemes [1, 2, 7, 8, 9, 10, 13,

[§] Portions of this paper were presented at International Journal of Smart Home, Vol. 6, No. 2, 2012 and at the 6th International Conference on Information Security and Assurance (ISA 2012), April 28-30, Shanghai, China, 2012.

14, 23, 24] are proposed and the following criteria are important for securing e-voting schemes. Major design goals include:

Anonymity: A voter’s real identity cannot be traced by any adversary and no one can identify the relation between a ballot and the voter who cast it.

Fairness: Adversaries cannot learn or reveal any information about the progress of the election until the final voting results are published by administration.

Convenience: A voter does not need to have complicated knowledge or be able to perform special techniques and no additional voting equipment. In other words, it is voter-friendly.

Uniqueness: During the election phase, a legal voter can only cast his/her ballot once and all double voting ballots will be detected and eliminated.

Accuracy: All valid ballots must be counted correctly and adversaries cannot remove, duplicate or alter a valid ballot.

Unforgeability: Adversaries cannot fake or forge a valid ballot.

Verifiability: A legal voter can check that his/her legitimate ballot has been correctly counted or not.

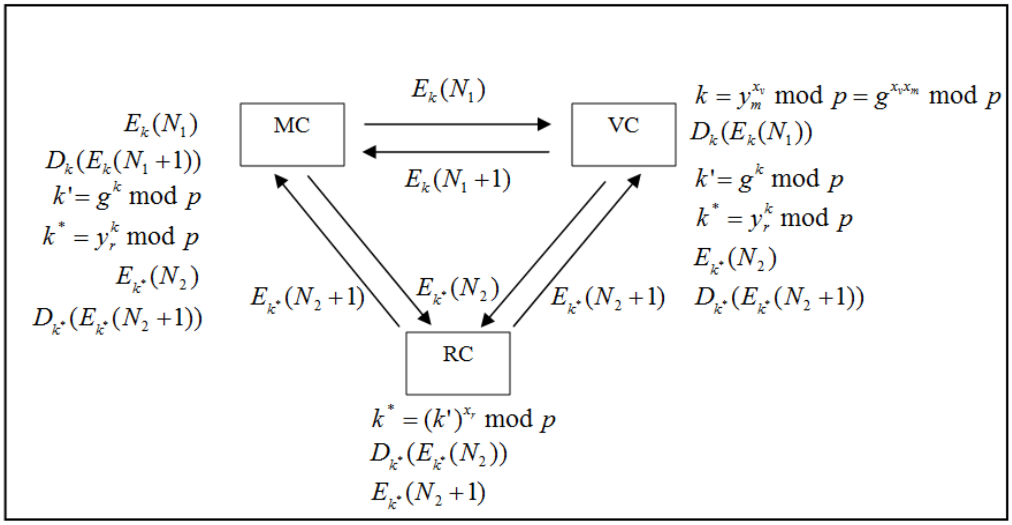


Figure 1. Initial Phase of Chang-Lee’s e-voting Scheme

Recently, Chang and Lee [2] proposed an e-voting scheme with voter anonymity. In order to achieve the above-mentioned criteria, they adopt many cryptographic techniques [5, 25, 26], including: Diffie-Hellman key exchange [6] and blind signature [4]. Moreover, a proxy server is used in their e-voting scheme. Their scheme not only provides an anonymous link from the voter to the voting authority but also enhances the performance such that it can be practically applied over the Internet. Chang-Lee’s e-voting scheme consists of three phases: initial phase, voting phase and publishing phase. The handshakes between participants in Chang-Lee’s e-voting scheme are depicted in Figure 1, 2 and 3. Unfortunately, we found that

Chang-Lee's e-voting scheme is insecure to some security attacks [22] and thus some essential criteria of e-voting cannot be satisfied in their scheme. Chang-Lee's scheme has five weaknesses as follows.

Attack 1. An adversary may replace the valid ballot with another one and on one knows this attack.

Attack 2. An adversary may send the same serial number to many legal voters and only one voter's ballot will be counted correctly. This attack damages the correctness of e-voting system.

Attack 3. An adversary may send an invalid timestamp to legal voters and their ballots will be ignored by voting center later. This attack damages the correctness of e-voting system.

Attack 4. A denial of vote attack may happen in their scheme because it does not provide mutual authentication [27, 28] between voter and proxy server.

Attack 5. An adversary may transmit multiple ballots with multiple serial numbers for double voting attack.

As a result, we propose an improvement on Chang-Lee's scheme in this paper. To shorten the length of this paper, we omit the review of Chang-Lee's e-voting scheme. Please refer to [2]. The remainder of this paper is organized as follows. In Section 2, we propose our improved scheme and analyze its security and performance in Section 3 and 4, respectively. Finally, we conclude this paper in Section 5.

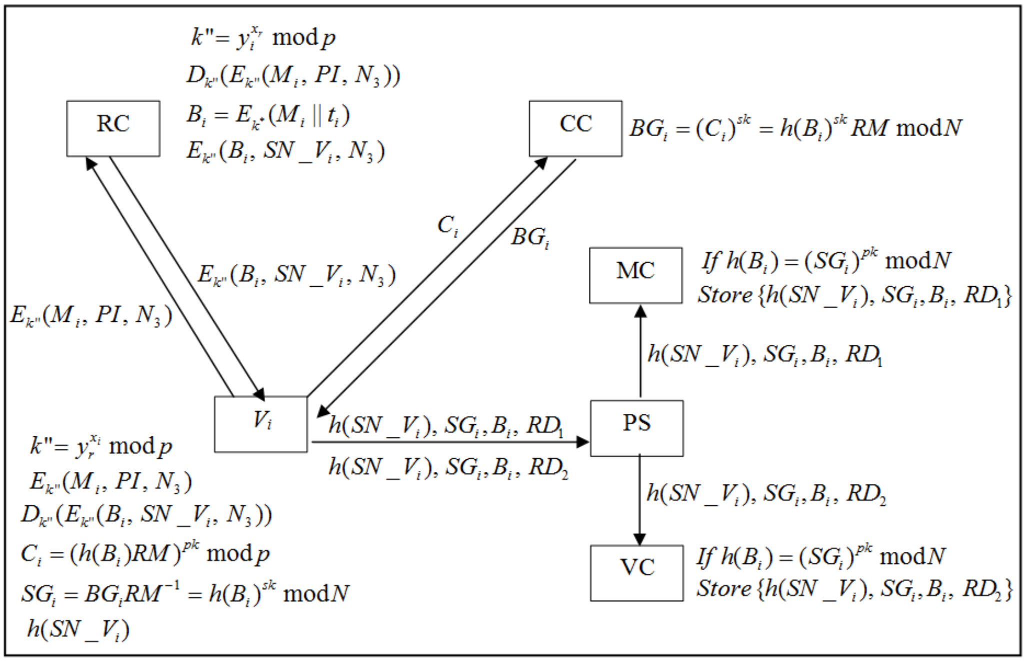

$k" = y_i^{x_r} \bmod p$
$D_{k"}(E_{k"}(M_i, PI, N_3))$
$B_i = E_{k^*}(M_i \| t_i)$
$E_{k"}(B_i, SN\_V_i, N_3)$
RC
CC
$BG_i = (C_i)^{sk} = h(B_i)^{sk} RM \bmod N$
C_i
BG_i
MC
$If\ h(B_i) = (SG_i)^{pk} \bmod N$
$Store\ \{h(SN\_V_i), SG_i, B_i, RD_1\}$
$E_{k"}(B_i, SN\_V_i, N_3)$
$E_{k"}(M_i, PI, N_3)$
$h(SN\_V_i), SG_i, B_i, RD_1$
V_i
$h(SN\_V_i), SG_i, B_i, RD_1$
PS
$h(SN\_V_i), SG_i, B_i, RD_2$
$k" = y_r^{x_i} \bmod p$
$E_{k"}(M_i, PI, N_3)$
$D_{k"}(E_{k"}(B_i, SN\_V_i, N_3))$
$C_i = (h(B_i)RM)^{pk} \bmod p$
$SG_i = BG_i RM^{-1} = h(B_i)^{sk} \bmod N$
$h(SN\_V_i)$
$h(SN\_V_i), SG_i, B_i, RD_2$
VC
$If\ h(B_i) = (SG_i)^{pk} \bmod N$
$Store\ \{h(SN\_V_i), SG_i, B_i, RD_2\}$

Figure 2. Voting Phase of Chang-Lee's e-voting Scheme

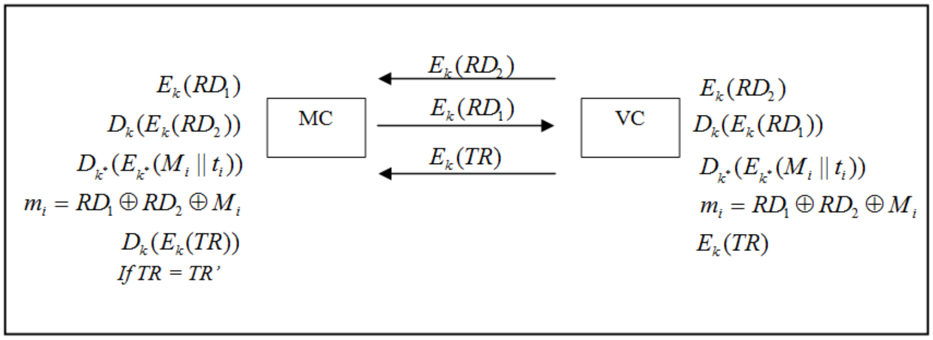

$E_k(RD_1)$
$D_k(E_k(RD_2))$
$D_{k^*}(E_{k^*}(M_i \| t_i))$
$m_i = RD_1 \oplus RD_2 \oplus M_i$
$D_k(E_k(TR))$
$If\ TR = TR'$
MC
$E_k(RD_2)$
$E_k(RD_1)$
$E_k(TR)$
VC
$E_k(RD_2)$
$D_k(E_k(RD_1))$
$D_{k^*}(E_{k^*}(M_i \| t_i))$
$m_i = RD_1 \oplus RD_2 \oplus M_i$
$E_k(TR)$

Figure 3. Publishing Phase of Chang-Lee's e-voting Scheme

2. The Improved Scheme

In this section, we propose an improvement on Chang-Lee's e-voting scheme. Chang-Lee's e-voting scheme consists of the following participants: Registration Center (RC), Certification Center (CC), Monitor Center (MC), Vote Counter (VC), Voter and a proxy server (PS). Some notations used in Chang-Lee's and our improved scheme are defined in Table 1. The notations of the improved scheme are the same as those in Chang-Lee's scheme. To overcome the above-mentioned attacks in Chang-Lee's scheme, we introduce the RSA public-key cryptosystem for participants RC and the proxy server and the details of the improved scheme are described as follows.

2.1. Initial Phase

In this phase, the proposed steps are almost the same as that in Chang-Lee's scheme and the only difference between ours and Chang-Lee's scheme is MC and VC have to use k' to negotiate a new session key $\hat{k}$ with the proxy server (PS), where $k' = g^k \bmod p = g^{x_m x_v} \bmod p$. Thus, we assume that PS's private key and public key are x_p and $y_p = g^{x_p} \bmod p$, respectively. To shorten the length of this paper, we only demonstrate the key exchange procedure between MC and PS. First, MC computes $\hat{k} = y_p^k \bmod p = g^{x_p k} \bmod p = g^{x_p x_m x_v} \bmod p$ and sends $E_{\hat{k}}(N_3)$ to PS, where N_3 is a nonce generated by MC. Upon receiving the message from MC, PS computes $\hat{k} = k'^{x_p} \bmod p$ and $D_{\hat{k}}(E_{\hat{k}}(N_3))$ and reveals N_3 for freshness checking. If it is valid, PS sends $E_{\hat{k}}(N_3 + 1)$ to MC. Upon receiving the message from PS, MC computes $D_{\hat{k}}(E_{\hat{k}}(N_3 + 1))$ and reveals $N_3 + 1$ for freshness checking. If it holds, MC and PS generate a session key $\hat{k}$ by using authenticated Diffie-Hellman key exchange procedure and $\hat{k}$ can be used for securing latter sensitive communications. The handshakes between MC, VC, PS and RC in the proposed scheme are depicted in Figure 4.

Table 1. Notations

Symbol	Decryption
(pk_i, sk_i)	The RSA public/private key pair of entity i
p	A large prime number
g	A primitive element in $GF(p)$
V_i	The voter
PI	Personal information of V_i
RC	Registration center
CC	Certification center
MC	Monitor center
VC	Vote counter
PS	Proxy server
x_r	RC's private key
y_r	RC's public key, where $y_r = g^{x_r} \bmod p$
x_m	MC's private key
y_m	MC's public key, where $y_m = g^{x_m} \bmod p$
x_v	VC's private key
y_v	VC's public key, where $y_v = g^{x_v} \bmod p$
x_p	PS's private key
y_p	PS's public key, where $y_p = g^{x_p} \bmod p$
x_i	V_i's private key
y_i	V_i's public key, where $y_i = g^{x_i} \bmod p$
$h(.)$	A public one-way hashing function
m_i	V_i's marked ballot
t_i	A timestamp generated by RC
$\{.\}^{pk}$	The asymmetric computation with public key pk
$\{.\}^{sk}$	The asymmetric computation with private key sk
$E_k(.)$	The symmetric encryption with encryption key k
$D_k(.)$	The symmetric decryption with decryption key k
TR/TR'	The tally result of all votes

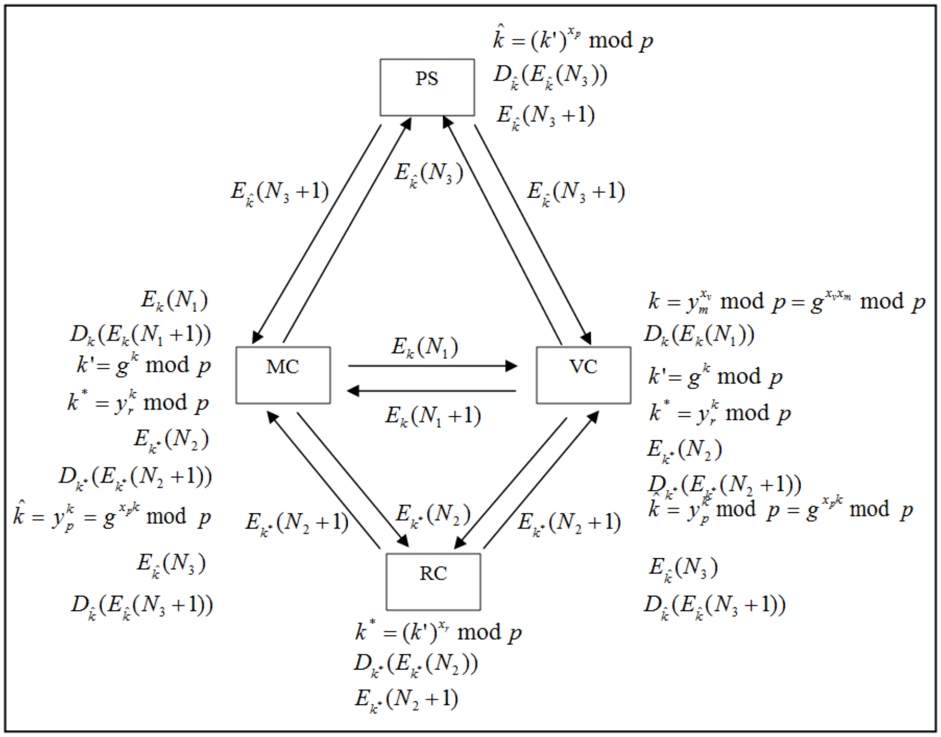


Figure 4. Initial Phase of the Improved Scheme

2.2. Voting Phase

In this phase, Step 1 is the same as Chang-Lee's scheme and the major differences from Step 2 to Step 7 are shown as follows.

Step 2: Upon receiving the message from V_i, RC decrypts the message and reveals (M_i, PI, N_3). Then, RC checks the identification of V_i. If it is valid, RC computes $B_i = E_{k^*}(M_i \| SN\_V_i \| t_i)$ and sends $E_{k''}(B_i, \{M_i \| t_i \| SN\_V_i\}^{sk_r}, N_3)$ to V_i, where SN_V_i is an unique serial number for V_i and sk_r is the RSA private key of RC.

Step 3: V_i computes $D_{k''}(E_{k''}(B_i, \{M_i \| t_i \| SN\_V_i\}^{sk_r}, N_3))$ and reveals N_3 for freshness checking. If $\{\{M_i \| t_i \| SN\_V_i\}^{sk_r}\}^{pk_r} = (M_i \| t_i \| SN\_V)$ is true, V_i sends C_i to CC, where $C_i = \{h(B_i)RM\}^{pk_c}$.

Step 4 and 5: In Step 4 and 5, our improved scheme is the same as Chang-Lee's scheme.

Step 6: V_i sends $MV_i = \{h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, RD_1 / RD_2, N_4\}^{pk_p}$ to PS, where pk_p is the public key of PS and it is generated by RSA cryptosystem. Moreover, upon receiving the messages from V_i, PS reveals the messages $h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, RD_1 / RD_2, N_4$ by computing $\{MV_i\}^{sk_p}$ and sends $\{N_4+1\}^{sk_p}$ to V_i for further checking. If it is valid, V_i convinces that the voting message is received by PS. Then, PS replaces the network address of the ballot of V_i by another network address for voter anonymity and sends $MV_{i1} = E_{\hat{k}}(h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, RD_1, N_4)$ and $MV_{i2} = E_{\hat{k}}(h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, RD_2, N_4)$ to MC and VC, respectively. Finally, MC and VC will send the response message $E_{\hat{k}}(N_4)$ to PS for mutual authentication.

Step 7: MC and VC checks the validity of V_i by checking whether $h(B_i) = \{SG_i\}^{pk_c}$. If yes, MC and VC stores $MV_{i3} = h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, RD_1$ and $MV_{i4} = h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, RD_2$ in their databases, respectively. Besides, MC and VC need to ensure that parameters $h(SN\_V_i)$ and $h(SN\_V_i)^{x_i} \bmod p$ are stored in their database only once.

The handshake between MC, VC, PS, CC, RC, and V_i in the proposed scheme are depicted in Figure 5.

2.3. Publishing Phase

In publishing phase, RC first computes $E_{k^*}(All\ valid\ serial\ numbers)$ and transmits it to MC and VC.

Step 1: Upon receiving all valid serial numbers from RC, MC and VC checks whether computed $h(SN\_V_i)$ is equal to stored serial number or not. If $h(SN\_V_i)$ does not appear in valid serial number, a double voting incident is detected and the ballot will be ignored. Next, MC and VC mutually send and exchange the random number of each valid ballot.

Step 2: MC and VC verify the validity of SN_V_i and t_i by computing $D_{k^*}(E_{k^*}(M_i \| SN\_V_i \| t_i))$. If the above condition holds, MC and VC reveal the choice of marked ballot by computing $m_i = RD_1 \oplus RD_2 \oplus M_i$ and count TR, where TR is the tally result of all marked ballots. Finally, VC sends TR to MC.

Step 3: Upon receiving TR from VC, MC checks whether VC's TR is equal to its TR'. If it does not hold, MC cannot announce the final result of voting. Otherwise, the final result, all legal voters' $h(SN\_V_i)^{x_i} \bmod p$ and the session key k^* will be published by MC.

Step 4: V_i can first check whether published $h(SN\_V_i)^{x_i} \bmod p$ is equal to stored $h(SN\_V_i)^{x_i} \bmod p$ or not. Moreover, V_i reveals B_i with decrypting key k^* to check the validity of B_i. If $h(SN\_V_i)^{x_i} \bmod p$ appears and the content of B_i is valid, it means V_i's ballot has been correctly counted. Otherwise, V_i presents $(B_i, \{M_i \| t_i \| SN\_V_i\}^{sk_r}, h(SN\_V_i)^{x_i} \bmod p)$ and inquires the electoral unit to check and recount his/her ballot.

The handshake between MC, VC, RC and V_i in the proposed scheme are depicted in Figure 6.

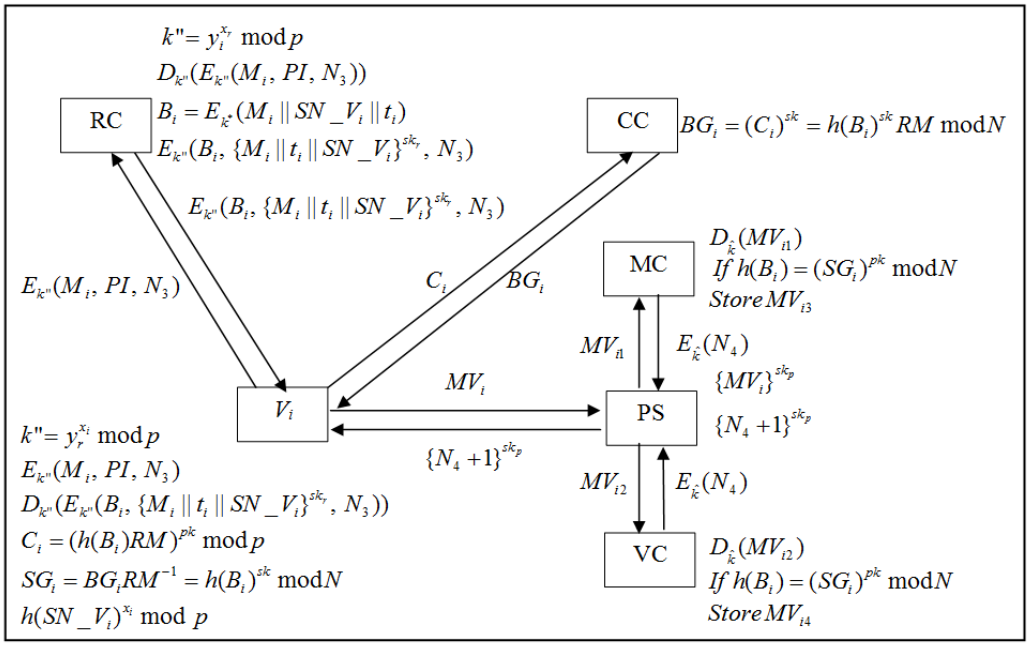

$k" = y_i^{x_r} \bmod p$
$D_{k"}(E_{k"}(M_i, PI, N_3))$
$B_i = E_{\hat{k}}(M_i \| SN\_V_i \| t_i)$
$E_{k"}(B_i, \{M_i \| t_i \| SN\_V_i\}^{sk_r}, N_3)$
RC
CC
$BG_i = (C_i)^{sk} = h(B_i)^{sk} RM \bmod N$
$E_{k"}(B_i, \{M_i \| t_i \| SN\_V_i\}^{sk_r}, N_3)$
$D_{\hat{k}}(MV_{i1})$
$If\ h(B_i) = (SG_i)^{pk} \bmod N$
$Store\ MV_{i3}$
MC
$E_{k"}(M_i, PI, N_3)$
C_i
BG_i
MV_{i1}
$E_{\hat{k}}(N_4)$
MV_i
$\{MV_i\}^{sk_p}$
V_i
PS
$\{N_4 + 1\}^{sk_p}$
$k" = y_r^{x_i} \bmod p$
$E_{k"}(M_i, PI, N_3)$
$D_{k"}(E_{k"}(B_i, \{M_i \| t_i \| SN\_V_i\}^{sk_r}, N_3))$
$C_i = (h(B_i)RM)^{pk} \bmod p$
$SG_i = BG_i RM^{-1} = h(B_i)^{sk} \bmod N$
$h(SN\_V_i)^{x_i} \bmod p$
$\{N_4 + 1\}^{sk_p}$
MV_{i2}
$E_{\hat{k}}(N_4)$
VC
$D_{\hat{k}}(MV_{i2})$
$If\ h(B_i) = (SG_i)^{pk} \bmod N$
$Store\ MV_{i4}$

Figure 5. Voting Phase of the Improved Scheme

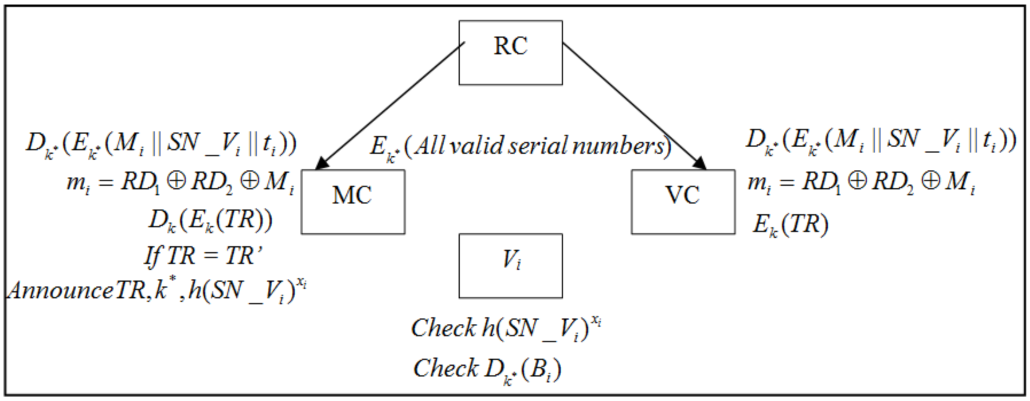

RC
$D_{\hat{k}^*}(E_{\hat{k}^*}(M_i \| SN\_V_i \| t_i))$
$m_i = RD_1 \oplus RD_2 \oplus M_i$
$D_{\hat{k}}(E_{\hat{k}}(TR))$
$If\ TR = TR'$
$Announce\ TR, k^*, h(SN\_V_i)^{x_i}$
$E_{\hat{k}^*}(All\ valid\ serial\ numbers)$
MC
VC
$D_{\hat{k}^*}(E_{\hat{k}^*}(M_i \| SN\_V_i \| t_i))$
$m_i = RD_1 \oplus RD_2 \oplus M_i$
$E_{\hat{k}}(TR)$
V_i
$Check\ h(SN\_V_i)^{x_i}$
$Check\ D_{\hat{k}^*}(B_i)$

Figure 6. Publishing Phase of the Improved Scheme

3. Security Analysis

In this section, we will show that how our improved scheme withstands the attacks described in [22] as follows.

Attack 1 resistance: In attack 1 of [22], if an adversary E in RC tries to replace V_i's valid ballot with another one, E needs to know the parameters $h(SN\_V_i)^{x_i} \bmod p$, SG_i and N_4 to generate the message in Step 6 of the voting phase. Unfortunately, under the protection of

PS's public key pk_p , E cannot decrypt ($h(SN\_V_i)^{x_i} \bmod p$, SG_i , N_4) from $\{h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, RD_1, N_4\}^{pk_p}$ and $\{h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, RD_2, N_4\}^{pk_p}$ to convince the voter V_i. Therefore, attack 1 cannot be work in our improved scheme unless E knows the private key sk_p of PS.

Attack 2 resistance: In attack 2 of [22], E uses the same serial number SN_V_i repeatedly that were used by many legal voters in the voting phase. However, the serial number SN_V_i is signed by using RC's private key sk_r in the voting phase and $h(SN\_V_i)^{x_i} \bmod p$ will be published in the publishing phase. Therefore, V_i can know that his/her ballot has been counted or not. Finally, it appears that the adversary E cannot use the same serial number to cheat the V_i and attack 2 can be prevented in our improved scheme unless E knows the private key x_i of V_i.

Attack 3 resistance: In our improved scheme, RC must sign the generated timestamp by using its private key sk_r and send it to V_i in the voting phase. If V_i 's ballot does not counted for the reason of invalid timestamp, V_i can show the signed timestamp $\{t_i\}^{sk_r}$ to the electoral administration and ask it to recount his/her ballot. Finally, attack 3 cannot be work in our improved scheme.

Attack 4 resistance: For denial of vote attack, we introduce mutual authentication between V_i, the proxy server, MC and VC during the proposed voting phase and E cannot generate the valid signature $\{N_4+1\}^{sk_p}$ to V_i for further checking unless he/she knows the private key sk_p of PS. As a result, attack 4 of [22] can be detected when V_i 's voting ballot has been discarded by E. On the other hands, during the publishing phase of our improved scheme, Steps 3 and 4 are introduced for each voter to check whether his/her ballot has been correctly counted or not. If it does not count, V_i still can ask the electoral administration to recount his/her ballot and the requirement of verifiability is achieved in our improved scheme.

Attack 5 resistance: In attack 5 of [22], since RC transmits $E_{k^*}(All\ valid\ serial\ numbers)$ for MC and VC in the publishing phase. Thus, the voter V_i cannot cast his/her ballot more than once by generating invalid serial numbers. If V_i is dishonest, both MC and VC will detect these invalid serial numbers in their databases and delete them. Finally, prevention of double voting and requirement of unforgeability can be provided in the improved scheme.

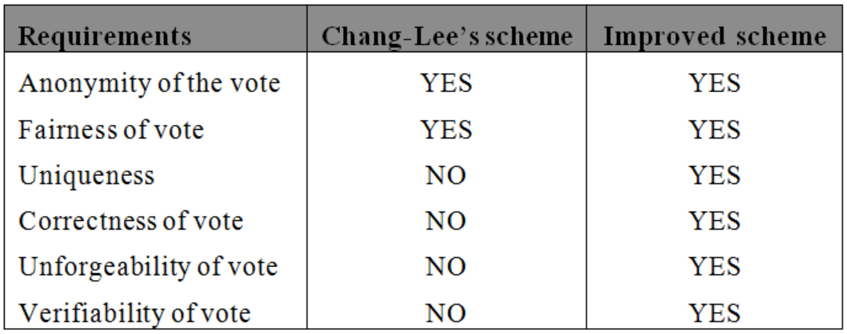
The e-voting requirements of Chang-Lee's scheme and our improved scheme are summarized in Table 2. In comparison with Chang-Lee's scheme, the improved scheme is more secure.

4. Performance Analysis

In this section, we evaluate the performance of the improved scheme and compare it with original Chang-Lee scheme in terms of efficiency. For evaluation of performance, we defined some evaluation parameters in Table 3. Table 4 gives evaluative values for computation and communication analysis of our improved scheme and compares it with [2]. With regard to communication rounds, our improved scheme introduces a mutual authentication mechanism and a verifiability requirement for securing whole e-voting procedure. Therefore, the necessity to add nine additional communication rounds for involved voter and voting authorities per vote.

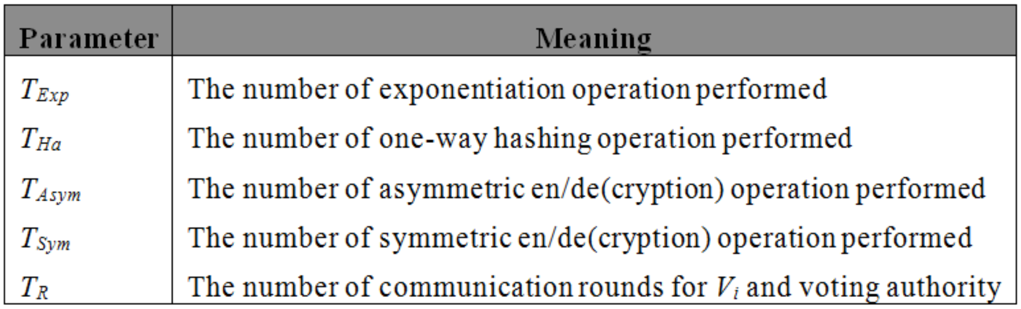
In addition, to compare the computational cost of the improved scheme against Chang-Lee's scheme, we measured the cryptographic operations needed to secure the communication channels for initial phase, voting phase, and publishing phase. During the initial phase of our scheme, MC/VC must negotiate a new session key with PS for resisting attack 4 presented in [22]. As a result, it is necessity to add three additional T_{Exp} and eight additional T_{Sym} for MC, VC, and PS in this phase. Next, during the voting phase of our scheme, in order to prevent attacks 1, 2, and 3 presented in [22], the necessity to add four additional T_{Sym} and eight additional T_{Asym} for involved parties in this phase. Finally, during the publishing phase of our scheme, in order to ensure the verifiability of voting and resist double voting, the necessity to add two additional T_{Sym} for RC and V_i in this phase. Note that we assumed there is one voter involved in a vote. It is clear that the overhead of additional computations for a vote is negligible, especially in view of the level of security the improved e-voting scheme offers.

Table 2. Comparisons of e-voting Criteria between Chang-Lee's Scheme and our Improved Scheme



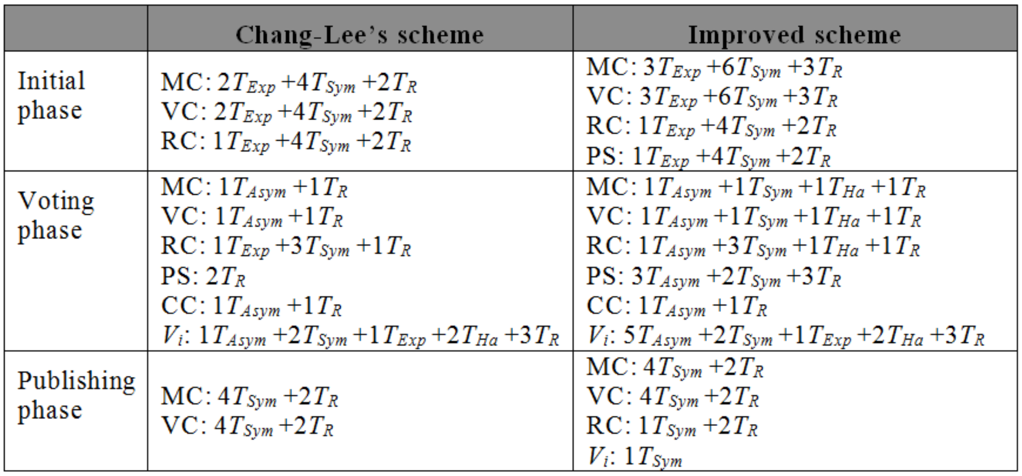
Requirements	Chang-Lee's scheme	Improved scheme
Anonymity of the vote	YES	YES
Fairness of vote	YES	YES
Uniqueness	NO	YES
Correctness of vote	NO	YES
Unforgeability of vote	NO	YES
Verifiability of vote	NO	YES

Table 3. Evaluation Parameters



Parameter	Meaning
T_{Exp}	The number of exponentiation operation performed
T_{Ha}	The number of one-way hashing operation performed
T_{Asym}	The number of asymmetric en/de(cryption) operation performed
T_{Sym}	The number of symmetric en/de(cryption) operation performed
T_R	The number of communication rounds for V_i and voting authority

Table 4. Efficiency Comparisons



	Chang-Lee's scheme	Improved scheme
Initial phase	MC: $2T_{Exp}+4T_{Sym}+2T_R$ VC: $2T_{Exp}+4T_{Sym}+2T_R$ RC: $1T_{Exp}+4T_{Sym}+2T_R$	MC: $3T_{Exp}+6T_{Sym}+3T_R$ VC: $3T_{Exp}+6T_{Sym}+3T_R$ RC: $1T_{Exp}+4T_{Sym}+2T_R$ PS: $1T_{Exp}+4T_{Sym}+2T_R$
Voting phase	MC: $1T_{Asym}+1T_R$ VC: $1T_{Asym}+1T_R$ RC: $1T_{Exp}+3T_{Sym}+1T_R$ PS: $2T_R$ CC: $1T_{Asym}+1T_R$ V_i: $1T_{Asym}+2T_{Sym}+1T_{Exp}+2T_{Ha}+3T_R$	MC: $1T_{Asym}+1T_{Sym}+1T_{Ha}+1T_R$ VC: $1T_{Asym}+1T_{Sym}+1T_{Ha}+1T_R$ RC: $1T_{Asym}+3T_{Sym}+1T_{Ha}+1T_R$ PS: $3T_{Asym}+2T_{Sym}+3T_R$ CC: $1T_{Asym}+1T_R$ V_i: $5T_{Asym}+2T_{Sym}+1T_{Exp}+2T_{Ha}+3T_R$
Publishing phase	MC: $4T_{Sym}+2T_R$ VC: $4T_{Sym}+2T_R$	MC: $4T_{Sym}+2T_R$ VC: $4T_{Sym}+2T_R$ RC: $1T_{Sym}+2T_R$ V_i: $1T_{Sym}$

5. Conclusions

Security, fairness, accuracy, verifiability and privacy are essential issues for online e-voting applications. Recently, Chang and Lee proposed an anonymous voting scheme based on Chaum's blind signature and Diffie-Hellman key exchange. However, with deep insight into Chang-Lee's e-voting scheme, we found that their scheme has some security weaknesses, and is not easily reparable. To solve security flaws of Chang-Lee's e-voting scheme, in this paper, we propose an improvement on their scheme to solve security problems found in Chang-Lee's e-voting scheme. Security analysis shows that our improved scheme not only prevents various attacks but also provides mutual authentication between system participants. In addition, the overhead of additional computations for securing e-voting is negligible in the improved scheme. Therefore, it is suitable for e-voting applications with high security criteria.

Acknowledgement

Authors would like to thank the publishing editors of International Journal of Smart Home and the reviewers of our previous conference paper published in ISA 2012 for their valuable comments and suggestions. In addition, this paper was partially supported by the National Science Council of the Taiwan under grant NSC 101-2221-E-165-002.

References

[1] A. Azadmanesh, A. Farahani and L. Najjar, "Tolerant weighted voting algorithms", International Journal of Network Security, vol. 7, **(2008)**, pp. 240-248.

[2] C. C. Chang and J. S. Lee, "An anonymous voting mechanism based on the key exchange protocol", Computers and Security, vol. 25, **(2006)**, pp. 307-314.

[3] D. Chaum, "Untraceable electronic mail, return address and digital pseudonyms", Communications of the ACM, vol. 24, **(1981)**, pp. 84-88.

[4] D. Chaum, "Blind signature systems", In Proceedings of advances in Crypto'83, New York, USA, **(1983)**.

[5] J. Choi and H. Kim, "A novel approach for SMS security", International Journal of Security and Its Applications, vol. 6, **(2012)**, pp. 373-378.

[6] W. Diffie and M. E. Hellman, "New directions in cryptology", IEEE Transactions on Information Theory, IT-12, **(1976)**, pp. 644-654.

[7] C. I. Fan and C. L. Lei, "An unlinkably divisible and intention attachable ticket scheme for runoff elections", Journal of Network and Computer Applications, vol. 25, **(2002)**, pp. 93-107.

[8] C. I. Fan and W. Z. Sun, "An efficient multi-receipt mechanism for uncoercible anonymous electronic

voting", Mathematical and Computer Modelling, vol. 48, **(2008)**, pp. 1611-1627.

[9] D. A. Gritzalis, "Principles and requirements for a secure e-voting system", Computers and Security, vol. 21, **(2002)**, pp. 539-556.

[10] W. C. Ku and S. D. Wang, "A secure and practical electronic voting scheme", Computer Communications, vol. 22, **(1999)**, pp. 279-286.

[11] C. C. Lee, C. T. Li and R. X. Chang, "A simple and efficient authentication scheme for mobile satellite communication systems", International Journal of Satellite Communications and Networking, vol. 30, **(2012)**, pp. 29-38.

[12] C. C. Lee, Y. M. Lai and C. T. Li, "An improved secure dynamic ID based remote user authentication scheme for multi-server environment", International Journal of Security and Its Applications, vol. 6, **(2012)**, pp. 203-209.

[13] C. T. Li, M. S. Hwang and Y. C. Lai, "A verifiable electronic voting scheme over the Internet", In Proceedings of Sixth International Conference on Information Technology: New Generations, Las Vegas, USA, **(2009)**, pp. 449-454.

[14] C. T. Li, M. S. Hwang and C. Y. Liu, "An electronic voting scheme with deniable authentication for mobile ad hoc networks", Computer Communications, vol. 31, **(2008)**, pp. 2534-2540.

[15] C. T. Li and M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks", Information Sciences, vol. 181, **(2011)**, pp. 5333-5347.

[16] C. T. Li, C. C. Lee, L. J. Wang and C. J. Liu, "A secure billing service with two-factor user authentication in wireless sensor networks", International Journal of Innovative Computing, Information and Control, vol. 7, **(2011)**, pp. 4821-4831.

[17] C. T. Li, C. Y. Weng and C. I. Fan, "Two-factor user authentication in multi-server networks", International Journal of Security and Its Applications, vol. 6, **(2012)**, pp. 261-267.

[18] C. T. Li, "A more secure and efficient authentication scheme with roaming service and user anonymity for mobile communications", Information Technology and Control, vol. 41, **(2012)**, pp. 69-76.

[19] C. T. Li and C. C. Lee, "A novel user authentication and privacy preserving scheme with smart cards for wireless communications", Mathematical and Computer Modelling, vol. 55, **(2012)**, pp. 35-44.

[20] C. T. Li, C. C. Yang and M. S. Hwang, "A secure routing protocol with node selfishness resistance in MANETs", International Journal of Mobile Communications, vol. 10, **(2012)**, pp. 103-118.

[21] C. T. Li, C. C. Lee and C. W. Lee, "An improved two-factor user authentication protocol for wireless sensor networks using elliptic curve cryptography", Sensor Letters, **(2012)**, article in press.

[22] C. T. Li and M. S. Hwang, "Security enhancement of Chang-Lee anonymous e-voting scheme", International Journal of Smart Home, vol. 6, **(2012)**, pp. 45-51.

[23] H. T. Liaw, "A secure electronic voting protocol for general elections", Computers and Security, vol. 23, **(2004)**, pp. 107-119.

[24] S. Maus, H. Peters and T. Storcken, "Anonymous voting and minimal manipulability", Journal of Economic Theory, vol. 135, **(2007)**, pp. 533-544.

[25] K. Rhee, W. Jeon and D. Won, "Security requirements of a mobile device management system", International Journal of Security and Its Applications, vol. 6, **(2012)**, pp. 353-358.

[26] G. Swain and S. K. Lenka, "A technique for secret communication using a new block cipher with dynamic steganography", International Journal of Security and Its Applications, vol. 6, **(2012)**, pp. 1-12.

[27] L. Yang, J. F. Ma and Q. Jiang, "Mutual authentication scheme with smart cards and password under trusted computing", International Journal of Network Security, vol. 14, **(2012)**, pp. 153-163.

[28] F. Zhu, M. W. Matka and L. M. Ni, "Private entity authentication for pervasive computing environments", International Journal of Network Security, vol. 14, **(2012)**, pp. 86-100.

[29] C. T. Li, C. C. Lee, C. Y. Weng and C. I. Fan, "An extended multi-server-based user authentication and key agreement scheme with user anonymity", KSII Transactions on Internet and Information Systems, **(2012)**, article in press.

[30] C. T. Li, "A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card", IET Information Security, **(2012)**, article in press.

[31] C. T. Li, C. C. Lee, C. Y. Weng and C. I. Fan, "A RFID-based macro-payment scheme with security and authentication for retailing services", ICIC Express Letters, **(2012)**, article in press.