A Secure and Anonymous Electronic Voting Scheme Based on Key Exchange Protocol*

Chun-Ta Li
Department of Information Management, Tainan University of Technology
529 Zhongzheng Road, Tainan 710, Taiwan
th0040@mail.tut.edu.tw

Min-Shiang Hwang⋆
Department of Computer Science and Information Engineering, Asia University
500 Lioufeng Road, Taichung 413, Taiwan
⋆Corresponding author: mshwang@asia.edu.tw

Abstract

Recently, Chang and Lee presented an anonymous electronic voting (e-voting) scheme based on the key exchange protocol. Unfortunately, in this paper, 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. As a result, an improved version on their scheme is proposed to enhance the security of their scheme.
Keywords : Anonymity, blind signature, e-voting, security, key exchange

1 Introduction

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, 9, 8, 11] 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.

*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.

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.

Correctness: 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.

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, 12, 13], 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. Unfortunately, we found that Chang-Lee's e-voting scheme is insecure to some security attacks [10] 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 no 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 [14, 15] 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.

Table 1: Notations

(pk_i, sk_i)	the RSA public/private key pair of participant i
p	a large prime number
g	a primitive element in $GF(p)$
V_i	the voter
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_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 function with the public key pk
$\{.\}^{sk}$	the asymmetric computation function with the private key sk
$E_k(.)$	the symmetric encryption function with the encryption key k
$D_k(.)$	the symmetric decryption function with the decryption key k
TR/TR'	the tally result of all votes

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.

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 $(M_i, \text{Personal information}, N_3)$. 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: Upon receiving the message from RC, 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 $\{\{M_i||t_i|| SN\_V_i\}^{sk_r}\}^{pk_r} = (M_i||t_i||SN\_V_i)$ 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 $\{h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, R_1/R_2, N_4\}^{pk_p}$ 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 $h(SN\_V_i)^{x_i} \bmod p$, $h(SN\_V_i), SG_i, B_i, R_1/R_2, N_4$ by using its private key 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 $E_{\hat{k}}(h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, R_1, N_4)$ and $E_{\hat{k}}(h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, R_2, N_4)$ 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 $h(B_i)$ is equal to $\{SG_i\}^{pk_c}$. If it holds, MC and VC stores $(h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, R_1)$ and $(h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, R_2)$ 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.

2.3 Publishing Phase

In publishing phase, RC first computes $E_{k^*}(\textit{All valid serial numbers})$ 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/VC verifies 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 $m_i = R_1 \oplus R_2 \oplus M_i$ 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.

3 Security Analysis

In this section, we will show that how our improved scheme withstands the attacks described in [10] as follows.

1. In attack 1, if an adversary E in RC wants to replace the valid ballot with another one, E have to know the parameters $h(SN\_V_i)^{x_i} \bmod p$, SG_i and N_4 to make the message in Step 6 of the voting phase. However, E cannot derive these parameters from $\{h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, R_1, N_4\}^{pk_p}$ and $\{h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, R_2, N_4\}^{pk_p}$ 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 the proxy server.

2. In attack 2, E may try to use the same serial number SN_V_i repeatedly that were used by many legal voters in the voting phase. Note that 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. Thus, V_i would 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 voter.

3. In our improved scheme, RC must sign the generated timestamp 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.

4. 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. As a result, attack 4 can be detected when V_i's voting ballot has been discarded by E. Moreover, 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

Table 2: Comparisons of e-voting criteria between Chang-Lee's scheme and our improved scheme

Requirements	Chang-Lee's scheme [2]	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

still can ask the electoral administration to recount his/her ballot and the verifiability requirement is provided in our mechanism.

5. In attack 5, since RC transmits 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, the double voting prevention and unforgeability can be achieved in our 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 Evaluation

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 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 [10]. 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 [10], 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

Table 3: Evaluation parameters

Parameter	Meaning
T_{Exp}	The number of exponentiation operation performed
T_{Ha}	The number of 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: Comparisons of the efficiency

	Our improved scheme	Chang-Lee's scheme [2]
Initial Phase	MC: 3 T_{Exp}+6 T_{Sym}+3 T_R VC: 3 T_{Exp}+6 T_{Sym}+3 T_R RC: 1 T_{Exp}+4 T_{Sym}+2 T_R PS: 1 T_{Exp}+4 T_{Sym}+2 T_R	MC: 2 T_{Exp}+4 T_{Sym}+2 T_R VC: 2 T_{Exp}+4 T_{Sym}+2 T_R RC: 1 T_{Exp}+4 T_{Sym}+2 T_R
Voting Phase	MC: 1 T_{Asym}+1 T_{Sym}+1 T_{Ha}+1 T_R VC: 1 T_{Asym}+1 T_{Sym}+1 T_{Ha}+1 T_R RC: 1 T_{Asym}+3 T_{Sym}+1 T_{Exp}+1 T_R PS: 3 T_{Asym}+2 T_{Sym}+3 T_R CC: 1 T_{Asym}+1 T_R V_i: 5 T_{Asym}+2 T_{Sym}+1 T_{Exp}+ 2 T_{Ha}+3 T_R	MC: 1 T_{Asym}+1 T_{Ha} VC: 1 T_{Asym}+1 T_{Ha} RC: 1 T_{Exp}+3 T_{Sym}+1 T_R PS: 2 T_R CC: 1 T_{Asym}+1 T_R V_i: 1 T_{Asym}+2 T_{Sym}+1 T_{Exp}+ 2 T_{Ha}+3 T_R
Publishing Phase	MC: 4 T_{Sym}+2 T_R VC: 4 T_{Sym}+2 T_R RC: 1 T_{Sym}+2 T_R V_i: 1 T_{Sym}	MC: 4 T_{Sym}+2 T_R VC: 4 T_{Sym}+2 T_R

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.

5 Conclusion

In this paper, we propose an improvement on Chang-Lee 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 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.

References

[1] Azadmanesh A., Farahani A., and Najjar L., Fault Tolerant Weighted Voting Algorithms, *International Journal of Network Security*, 7(2008), 240-248.

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

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

[4] Chaum D., Blind Signature Systems, In *Proceedings of advances in Crypto'83*, page 153, New York, USA, 1983.

[5] Choi J. and Kim H., A Novel Approach for SMS Security, *International Journal of Security and Its Applications*, 6(2012), 373–378.

[6] Diffie W. and Hellman M. E., New Directions in Cryptology, *IEEE Transations on Information Theory*, IT-22(1976), 644-654.

[7] Gritzalis D. A., Principles and Requirements for A Secure E-Voting System, *Computers & Security*, 21(2002), 539-556.

[8] Li C. T., Hwang M. S., and Lai Y. C., A Verifiable Electronic Voting Scheme over The Internet, In *Proceedings of Sixth International Conference on Information Technology: New Generations*, pages 449–454, Las Vegas, USA, April 2009.

[9] Li C. T., Hwang M. S., and Liu C. Y., An Electronic Voting Scheme with Deniable Authentication for Mobile Ad Hoc Networks, *Computer Communicarions*, 31(2008), 2534–2540.

[10] Li C. T. and Hwang M. S., Security Enhancement of Chang-Lee Anonymous E-Voting Scheme, *International Journal of Smart Home*, 6(2012), 45–51.

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

[12] Rhee K., Jeon W., and Won D., Security Requirements of a Mobile Device Management System, *International Journal of Security and Its Applications*, 6(2012), 353–358.

[13] Swain G. and Lenka S. K., A Technique for Secret Communication Using a New Block Cipher with Dynamic Steganography, *International Journal of Security and Its Applications*, 6(2012), 1–12.

[14] Yang L., Ma J. F., and Jiang Q., Mutual Authentication Scheme with Smart Cards and Password under Trusted Computing, *International Journal of Network Security*, 14(2012), 156-163.

[15] Zhu F., Matka M. W., and Ni L. M., Private Entity Authentication for Pervasive Computing Environments, *International Journal of Network Security*, 14(2012), 86-100.