Security Enhancement of Chang-Lee Anonymous E-Voting Scheme

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

[1] *Department of Information Management, Tainan University of Technology*
529 Zhongzheng Road, Tainan City 710, TAIWAN (R.O.C.)
th0040@mail.tut.edu.tw

[2] *Department of Computer Science and Information Engineering, Asia University*
500 Lioufeng Road, Taichung City 413, TAIWAN (R.O.C.)
[*] *Corresponding author: mshwang@asia.edu.tw*

Abstract

In recent years, several electronic voting (e-voting) schemes for communication networks have been proposed. In 2006, Chang and Lee presented an anonymous electronic voting scheme which can be applied in real-world elections. However, this paper shows that Chang-Lee's e-voting scheme suffers from susceptibility to security attacks. As a result, some essential security requirements of their e-voting scheme may be compromised. An improved scheme is suggested to enhance the security of their scheme.

Keywords: *Anonymity; Blind signature; E-voting; Security; Key exchange.*

1. Introduction

In 1981, Chaum [4] proposed the first electronic election mechanism that enables people to electronically cast his/her ballot over insecure network. Recently, a lot of electronic voting (e-voting) schemes [1, 2, 3, 5, 7, 8, 9, 10, 11, 12, 13, 14] are proposed and a secure e-voting scheme should satisfy the following requirements:

1. **Anonymity of voter**: No one can identify the relation between a ballot and the voter who cast it.
2. **Fairness of vote**: No one can learn any information about the progress of the election until the final voting results are published.
3. **Convenience of vote**: The 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.
4. **Perceptibility of double voting (Uniqueness)**: Each legal voter cannot cast his/her ballot more than once and all double voting ballots will be detected and eliminated.
5. **Correctness of vote**: All valid ballots must be counted correctly and no one can remove, duplicate or alter a valid ballot.
6. **Unforgeability of ballot**: No one can fake or forge a ballot.
7. **Verifiability of vote**: For this requirement, each voter should be able to independently check that his/her legitimate ballot has been counted correctly.

In 2006, Chang and Lee [3] proposed an anonymous e-voting scheme. In order to satisfy the above requirements, in their scheme, they combine the techniques of Diffie-Hellman key exchange [6], blind signature and a proxy server in their e-voting scheme. This 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. However, we find that Chang-Lee's e-voting scheme is vulnerable to some security attacks and thus some essential requirements of e-voting cannot be achieved in their scheme. As a result, we propose an improved scheme to solve the security weaknesses of Chang-Lee's scheme in this paper.

2. Review of Chang-Lee E-Voting Scheme

In this section, we will review 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 (V_i) and a Proxy Server (PS). Some notations used in Chang-Lee's and our e-voting scheme are defined in Table 1. Chang-Lee's e-voting scheme is divided into three phases: initial phase, voting phase, and publishing phase. To shorten the length of this paper, we omit the review. Please refer to [3].

Table 1. Notations Used Through this Paper

Symbol	Meaning
(pk_i, sk_i)	The RSA public/private key pair of participant i
p	A large prime number
g	A primitive element in $GF(p)$
(x_r, y_r)	RC's private key and public key, where $y_r = g^{x_r} \bmod p$
(x_m, y_m)	MC's private key and public key, where $y_m = g^{x_m} \bmod p$
(x_v, y_v)	VC's private key and public key, where $y_v = g^{x_v} \bmod p$
(x_i, y_i)	V_i's private key and 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

3. Security Problems of Chang-Lee's E-Voting Scheme

Attack 1 - RC compromise attack: Suppose that there is a traitor E in RC, E could replace the valid ballot M_i with another one, said $M_i^{'}$ in the voting phase and no one knows that V_i's valid ballot has been replaced by another one. In the voting phase, E first generates a new ballot $M_i^{'}$ (with new $m_i^{'}$, $R_1^{'}$ and $R_2^{'}$) to replace the original M_i in Step 2 and the following steps are continued until Step 5. Next, in order to convince the MC and VC, in Step 6, before the messages are sent through a proxy server, E must alter the messages ($h(SN\_V_i)$, SG_i, B_i, R_1) and ($h(SN\_V_i)$, SG_i, B_i, R_2) sent by V_i with another ($h(SN\_V_i)$, SG_i, B_i, $R_1^{'}$) and ($h(SN\_V_i)$, SG_i, B_i, $R_2^{'}$), respectively. MC and VC will store $R_1^{'}$ and $R_2^{'}$ in their own databases, respectively. Finally, the requirement of correctness cannot be achieved in Chang-Lee's scheme.

Attack 2 - RC compromise attack: In this attack, E could send the same serial number SN_V_i repeatedly to many legal voters in the voting phase. Thus, only one voter's ballot will be counted correctly and other voters who used the same serial number would be cancelled because of duplications. Finally, the requirement of correctness is also not achieved in Chang-Lee's scheme.

Attack 3 - RC compromise attack: Like above-mentioned attacks, E could send an invalid timestamp $t_i^{'}$ to many legal voters in voting phase. Next, in publishing phase and Step 2, these voter's ballots will be ignored by MC and VC because $t_i^{'}$ will not pass the procedure of freshness checking. Again, the requirement of correctness will not be achieved in Chang-Lee's scheme.

Attack 4 - Denial of vote attack: In the voting phase, before the messages are sent through the proxy server in Step 6, any adversary can intercept the messages ($h(SN\_V_i)$, SG_i, B_i, R_1) and ($h(SN\_V_i)$, SG_i, B_i, R_2) sent by V_i and thus V_i is unable to cast his/her ballot to MC and VC. Undoubtedly, it can be said that a denial of vote attack can occur in Chang-Lee's scheme because it lacks mutual authentication between V_i and the proxy server. Similarly, this attack might occur in communications between the proxy server and MC/VC and, as a result, their scheme is unable to resist an adversary to remove a valid ballot from the final tally. Finally, the requirements of correctness and verifiability are not achieved in Chang-Lee's scheme.

Attack 5 - Double voting attack: In the voting phase, any crafty voter can generate n fake serial numbers (SN_V_i, $j = 1,2,...,n$) for double voting in Step 6. Before the crafty voter sends the messages for double voting, he/she only needs to change the message $h(SN\_V_i)$ leaving the messages (SG_i, B_i, R_1) and (SG_i, B_i, R_2) unchanged. So, a crafty voter could transmit n ballots with n serial numbers. Moreover, because MC and VC only have to check that $h(SN\_V_i)$ is stored in its database only once. Therefore, the requirements of perceptibility of double voting and unforgeability of ballot cannot be achieved in Chang-Lee's scheme.

4. The Improved Scheme and Security Analysis

To overcome the susceptibility to above-mentioned attacks in Section 3, we propose an improvement on Chang-Lee's e-voting scheme in Section 4.1. Moreover, we analyze the security requirements of the improved scheme in Section 4.2.

4.1. The Improved Scheme

The notations of the proposed scheme are the same as those in Chang-Lee's scheme. However, we also introduce the RSA public-key cryptosystem for participants RC and the proxy server. The details of the improved scheme are described as follows.

4.1.1. Initial Phase

In the improved scheme, the steps of this phase are almost the same as that in Chang-Lee's scheme. The only difference between the proposed scheme and Chang-Lee's scheme is MC and VC would also need to use k' (where $k' = g^k \bmod p = g^{x_m x_v} \bmod p$) to negotiate a new session key k'' with the proxy server (PS), respectively. Thus we assume that x_p is PS's private key and y_p is the public key of PS, where $y_p = g^{x_p} \bmod p$. To simplify the exposition, we only show the key exchange procedure related to MC and PS as follows. First, MC generates a nonce N_3 and computes $k'' = y_p^k \bmod p = g^{x_p k} \bmod p = g^{x_p x_m x_v} \bmod p$. Then, MC sends $E_{k''}(N_3)$ to PS. After receiving the message sent by MC, PS computes $k'' = k'^{x_p} \bmod p$ and $D_{k''}(E_{k''}(N_3))$ to reveal N_3 for freshness checking. If it holds, PS computes $E_{k''}(N_3+1)$ and sends it to MC. Finally, MC computes $D_{k''}(E_{k''}(N_3+1))$ to reveal N_3+1 for freshness checking. If it is valid, the session key k'' can be used for securing latter communications between MC and PS.

4.1.2. Voting Phase

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

Step 2: After receiving the message sent by V_i, RC decrypts the message to reveal (M_i, Personal information, N_3) and checks the identification of V_i. If it holds, RC generates a unique serial number SN_V_i for V_i and computes $B_i = E_{k*}(M_i \| SN\_V_i \| t_i)$. Then, RC sends $E_{k''}(B_i, \{M_i \| t_i \| SN\_V_i\}^{sk_r}, N_3)$ to V_i, where sk_r is the RSA private key of RC.

Step 3: After receiving the message sent by RC, V_i computes $D_{k''}(E_{k''}(B_i, \{M_i \| t_i \| SN\_V_i\}^{sk_r}, N_3))$ to reveal N_3 for freshness checking and checks $\{\{M_i \| t_i \| SN\_V_i\}^{sk_r}\}^{pk_r} = (M_i \| SN\_V_i \| t_i)$. If the above conditions hold, V_i computes $C_i = \{h(B_i)RM\}^{pk_c}$ and sends C_i to CC.

Steps 4 and 5: In these two steps, the improved scheme is the same as Chang-Lee's scheme.

Step 6: In this step, 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, generated by RSA cryptosystem. Then, after receiving the messages sent by V_i, PS reveals the messages $h(SN\_V_i)^{x_i}, h(SN\_V_i), SG_i, B_i, R_1/R_2, N_4$ with its private key sk_p and sends the message $\{N_4+1\}^{sk_p}$ to V_i for further checking. If it holds, V_i confirms that the message is received by PS. Then, PS will replace the network address of the ballot of V_i by another network address for anonymity and sends $E_{k''}(h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, R_1, N_4)$ and $E_{k''}(h(SN\_V_i)^{x_i} \bmod p, h(SN\_V_i), SG_i, B_i, R_2, N_4)$ to MC and VC, respectively. Now, in order to confirm that the messages sent by PS are received by MC and VC, both MC and VC will send the message $E_{k''}(N_4)$ to PS for mutual authentication.

Step 7: In this step, both MC and VC will first check the validity of V_i by computing $h(B_i) = \{SG_i\}^{pk_c}$. If it holds, MC and VC will store $(h(SN\_V_i)^{x_i}, h(SN\_V_i), SG_i, B_i, R_1)$ and $(h(SN\_V_i)^{x_i}, h(SN\_V_i), SG_i, B_i, R_2)$ in their databases, respectively. Besides, both MC and VC must confirm that both parameters $h(SN\_V_i)$ and $h(SN\_V_i)^{x_i} \bmod p$ are stored in their database only once.

4.1.3. Publishing Phase

After the voting time expires and before counting the ballots, RC must transmit all the valid serial numbers to MC and VC to prevent attacks. Thus, RC computes E_{k*}(*All valid serial numbers*) and sends it to MC/VC.

Step 1: Upon receiving all valid serial numbers from RC, MC/VC first compares stored $h(SN\_V_i)$ with valid serial numbers for every ballot to see whether they have been maliciously used. If $h(SN\_V_i)$ does not appear in valid serial numbers, then a double voting incident is detected and the ballot is ignored. Next, just as in Step 1 of Chang-Lee's scheme in publishing phase, MC and VC mutually exchange the random number of each valid ballot.

Step 2: In this step, MC/VC decrypts the message $D_{k*}(E_{k*}(M_i \| SN\_V_i \| t_i))$ to check the validity of SN_V_i and t_i. If the above conditions hold, MC and VC compute $m_i = R_1 \oplus R_2 \oplus M_i$ to get the choice of marked ballot and calculate the tally result of all marked ballots. Finally, VC sends the tally result TR to MC.

Step 3: Upon receiving the tally result sent by VC, MC compares TR with TR'. If they are not equivalent, MC cannot announce the final result of voting. Otherwise, MC publishes the final result, all legal voters' $h(SN\_V_i)^{x_i} \bmod p$ and the session key k^*.

Step 4: V_i can first check whether $h(SN\_V_i)^{x_i} \bmod p$ does appear or not and further decrypts B_i with decrypting key k^* to check the content of B_i. If $h(SN\_V_i)^{x_i} \bmod p$ appears and the content of B_i is confirmed, it is convinced that V_i's ballot has been correctly counted. Otherwise, V_i can ask the electoral unit to recount his/her ballot by showing these messages ($B_i, \{M_i \| t_i \| SN\_V_i\}^{sk_r}, h(SN\_V_i)^{x_i} \bmod p$).

4.2. Security Analysis of the Improved Scheme

In this subsection, we will show that how our improved scheme withstands the attacks described in Section 3 as follows.

1. In Attack 1, if a traitor *E* in RC wants to replace the valid ballot with another one, *E* must know the values $h(SN\_V_i)^{x_i} \bmod p$, SG_i and N_4 to forge the message in Step 6 of the voting phase. However, *E* has no way to derive these values 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. Thus, *E* cannot apply the Attack 1 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. So, V_i would know that his/her ballot has been counted or not. Therefore, it appears that the traitor E has no way to use the same serial number to cheat the voter.

3. In our improved scheme, RC has to sign the generated timestamp and sends it to V_i in the voting phase. Therefore, 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 unit and ask it to recount his/her ballot. Then, attack 3 can be prevented in our scheme.

4. With regard to the denial of vote attack, during the proposed voting phase, we introduce mutual authentication between V_i, the proxy server, MC, and VC and an adversary cannot generate the valid signature $\{N_4+1\}^{sk_p}$ to V_i for further checking. Thus, this attack can be detected when V_i 's voting ballot has been discarded by attackers. 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 hold, V_i still can ask the electoral unit to recount his/her ballot. As a result, the verifiability requirement is provided in our mechanism. Hence, this attack will be detected and eliminated from our improved scheme.

5. Since RC transmits all valid serial numbers for MC and VC in the publishing phase, 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. As a result, the requirements of perceptibility of double voting and unforgeability of ballot can be achieved in our improved scheme.

5. Conclusions

In this paper, we have shown that Chang-Lee's e-voting scheme is vulnerable to some attacks and the essential requirements of general electronic voting cannot be achieved in their scheme. We propose an improvement on Chang-Lee scheme to solve these problems and demonstrate that it is suitable for e-voting applications with high security requirements.

References

[1] A. Azadmanesh, A. Farahani and L. Najjar, "Fault tolerant weighted voting algorithms", International Journal of Network Security, 7(2), **(2008)**, pp. 240-248.

[2] F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi and A. Vaccarelli, "SEAS, a secure e-voting protocol: design and implementation", Computers & Security, 24(8), **(2005)**, pp. 642-652.

[3] C. C. Chang and J. S. Lee, "An anonymous voting mechanism based on the key exchange protocol", Computers & Security, 25(4), **(2006)**, pp. 307-314.

[4] D. Chaum, "Untraceable electronic mail, return addresses and digital pseudonyms", Communications of the ACM, 24(2), **(1981)**, pp. 84-88.

[5] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "Cryptanalysis on Mu-Varadharajan's e-voting schemes", Applied Mathematics and Computation, 139(2-3), **(2003)**, pp. 525-530.

[6] W. Diffie and M. E. Hellman, "New directions in cryptology", IEEE Transactions on Information Theory, IT-22(6), **(1976)**, pp.644-654.

[7] G. Dini, "A secure and available electronic voting service for a large-scale distributed system", Future Generation Computer Systems, 19(1), **(2003)**, pp. 69-85.

[8] D. A. Gritzalis, "Principles and requirements for a secure e-voting system", Computers & Security, 21(6), **(2002)**, pp. 539-556.

[9] S. Y. Hwang, H. A. Wen and T. Hwang, "On the security enhancement for anonymous secure e-voting over computer network", Computer Standards & Interfaces, 27(2), **(2005)**, pp. 163-168.

[10] 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.

[11] C. T. Li, M. S. Hwang and C. Y. Liu, "An electronic voting scheme with deniable authentication for mobile ad hoc networks", Computer Communications, 31(10), **(2008)**, pp. 2534-2540.

[12] H. T. Liaw, "A secure electronic voting protocol for general elections", Computers & Security, 23(2), **(2004)**, pp. 107-119.

[13] I. C. Lin, M. S. Hwang and C. C. Chang, "Security enhancement for anonymous secure e-voting over a network", Computer Standards & Interfaces, 25(2), **(2003)**, pp. 131-139.

[14] F. Rodiguez-Henriquez, D. Ortiz-Arroyo and C. Garcia-Zamora, "Yet another improvement over the Mu-Varadharajan e-voting protocol", Computer Standards & Interfaces, 29(4), **(2007)**, pp. 471-480.