A New Proxy Electronic Voting Scheme Based on Proxy Signatures

Cheng-Chi Lee, Te-Yu Chen, Shu-Chen Lin and Min-Shiang Hwang

Abstract Electronic voting (e-voting) is used to solve the problems of traditional paper-based voting and to lower costs. So far, many researchers have offered their secure e-voting systems. However, the existing schemes do not seem to meet the requirement of delegation. For example, a stockholder may want to assign some other person in the company to vote by using a warrant, and the system should provide such service. In this paper, the authors propose a novel e-voting scheme called the proxy e-voting scheme that has the ability to delegate a proxy to vote. The proxy e-voting scheme can satisfy all the requirements we bring up. As a result, the scheme not only can be easily implemented but also has less computational cost for voters to cast the ballots.

Keywords Data security · Electronic voting · ElGamal cryptosystem · Proxy e-voting

C.-C. Lee
Department of Library and Information Science,
Fu Jen Catholic University, New Taipei City 24205,
Taiwan, ROC

T.-Y. Chen
Department of Information Networking Technology,
Hsiuping University of Science and Technology,
Taichung, Taiwan, ROC

S.-C. Lin
Department of Information Management,
Chaoyang University of Technology,
Taichung, Taiwan, ROC

M.-S. Hwang (✉)
Department of Computer Science and Information Engineering,
Asia University, Taichung, Taiwan, ROC
e-mail: mshwang@asia.edu.tw

James J. (Jong Hyuk) Park et al. (eds.), *Future Information Technology, Application, and Service*,
Lecture Notes in Electrical Engineering 164, DOI: 10.1007/978-94-007-4516-2_1,

1 Introduction

Each lawful citizen in a democratic country has the right and duty to participate in elections. Voting is a common approach used in elections. And a voter must cast a vote by himself/herself. In recent years, the stunning advancement of the Internet and other computer technologies have brought human communications to a new era, and such an important human value as democracy, carried out through voting, can now also be practiced electronically.

In 1983 [2], Chaum first proposed a concept called blind signature, and then many researchers developed and proposed their secure e-voting schemes on the basis of the blind signature scheme concept. Indeed, the blind signature mechanism enables many secure e-voting schemes to protect the privacy of the voters [10, 14, 15, 18, 19]. For example, Fujioka et al. [10] proposed a scheme where the privacy of the voters is ensured this way. Each voter encrypts his/her vote by using a random secret key and sends this vote to the counter center through an anonymous channel [1, 3], and this must be done again in the opening phase. In other words, in their scheme, the voter must send the same anonymous message twice. To reduce the communication cost, in the schemes in [14, 19], each voter only sends one anonymous message. Besides, Sako [19] also proposed a practical voting scheme where only a single center is involved. In the scheme, an open objection can be made to the tally without disclosing anyone's vote to other voters.

In 1998, Mu and Varadharajan [18] proposed two anonymous secure e-voting schemes that can not only protect the privacy of the voters, but also prevent double voting. One scheme assumes that the Authentication Server (AS) is trustworthy, and the other does not. Furthermore, if double voting occurs, the Ticket Counting Server (TCS) can compute the information from the two ballots and send the information to AS to identify the voters. However, in 2003, Chien et al. [5] and Lin et al. [15] showed that any voter could vote more than once without being detected in the Mu-Varadharajan scheme. Lin et al., on the other hand, improved the scheme to strengthen the protection against fraud while the Mu-Varadharajan scheme's advantage inherited from the blind signature concept still remains without any special voting channel needed.

In 2003, Yun and Lee proposed an e-voting scheme based on the undeniable blind signature scheme [22]. Assume that the Authorization Center is trustworthy when an untraceable communication channel is used. They follow the challenging/responding approach to verify the validity of the participants. The blind signature scheme is used to provide anonymity to the voters and to ensure that the intermediate voting results will not affect the entire election. However, their scheme does not support double voting detection. Recently, a lot of researchers proposed their e-voting schemes based on novel techniques [4, 9, 11, 12]. These schemes only addressed the traditional e-voting schemes. So far, there has been no e-voting scheme based on the blind signature scheme that supports double voting detection, and no voter can authorize a proxy to cast the ballot. Therefore, in this paper, we intend to propose a novel e-voting scheme, called the proxy e-voting scheme, to solve the above problems.

In 1996, Mambo et al. [17] first proposed the proxy signature concept. It allows a proxy signer to sign documents on behalf of the original signer. Several security requirements the proxy signature scheme has met [7, 16, 17, 20]:

- Verifiability: A valid proxy signature can be verified by anyone.
- Unforgeability: Only the original signer and designated proxy signer can create a valid proxy signature.
- Identifiability: Any proxy signer should be able to get identified by the proxy signature.

It is not hard to realize how closely such concepts as proxy signature and proxy e-voting are related to each other. In 2004, Dai et al. [6] proposed a privacy protecting proxy signature scheme and its application. Besides privacy protection, they also provided an application of proxy signatures to e-voting. However, there was no clear proxy e-voting protocol. A similar problem is found in [21]. In this paper, we propose a new proxy e-voting scheme based on the proxy signature scheme. The main contribution of this paper is that the voter can empower a proxy to cast the ballot. This delegation application can come in quite handy in our lives.

An ideal proxy e-voting scheme must satisfy the following requirements [13, 15, 18].

- Delegation: The original voter can either cast the ballot by himself/herself or grant his/her voting privilege to a proxy voter to do that for him/her.
- Unforgeability: Besides the original voter, the designated proxy voter can generate a valid proxy signature and act on behalf of the original voter. And nobody else can generate the valid proxy signature of the proxy voter.
- Anonymity: The identities of the original voter and the proxy voter are untraceable from the votes. When the votes are published in the electronic bulletin board, any third party can never obtain the voter's information from the votes.
- Vote uniqueness: Every voter is unique. The votes generated by them are also unique.
- Multi-value: In previous e-voting schemes, voters are mostly allowed only to click on either the yes or the no on the ballot. To make a difference, our scheme supports a ballot with much more flexibility. In addition, our scheme can also work smoothly when several elections are held at the same time.
- Verifiability:
  - Intentional Verifiability: the original voter can verify the content of the vote to see whether it is the candidate he/she intends to vote for that is chosen by the proxy voter.
  - Individual Verifiability: a proxy voter can verify his/her vote to see whether it has been counted by Ticket Counting Server.
- Tally correctness: The final tally must be equal to the total number of the valid votes.
- Double voting detection: When double voting occurs, the authority gets to know who the voters are.

The remainder of this paper is organized as follows. In Sect.2, we shall present our novel proxy e-voting scheme. In Sect.3, we shall analyze the security of our scheme. Finally, a conclusion is given in Sect.4.

2 The Proposed Scheme

In this section, we proposed our novel proxy e-voting scheme based on proxy signatures. Our new scheme supports not only proxy voting but also double-voting detection.

2.1 Notations

The system parameters of the proposed scheme are defined, and some notations are given as follows. t denotes timestamp; $\|$ denotes a concatenation; p denotes a large prime; q denotes a large prime factor of $(p - 1)$; g denotes a generator for $Z^*{}_p$; *flag* denotes a tag of proxy information; s_O denotes a signature of *flag* made by AS; $\{e_x, d_x\}$, n_x denotes a long-term RSA key pair of each participant x and a product of two large prime numbers n_x, where $e_x \times d_x \, mod \, \phi(n_x) = 1$; $\{x_o, y_o\}$ denotes the private key and public key of original voter, where $x_o \in Z^*{}_q, y_o = g^{x_o} \, mod \, p$; $\{x_p, y_p\}$ denotes the private key and public key of proxy voter, where $x_p \in Z^*{}_q, y_p = g^{x_p} \, mod \, p$; $h(.)$ denotes a one-way hash function; M_w denotes a warrant which records the identities of the original voter V_o, the proxy voter V_p, and the valid delegation time, etc.; C_{num} denotes the intention number of candidates; m denotes voting content including candidate's information; $Sign_A(B)$ denotes this is a digital signature of the message B. The signature is signed by the private key A using ElGamal-like digital signature scheme [8]. When a verifier wants to verify the correctness of the signature, he/she can use the corresponding public key $y = g^A \, mod \, p$ to verify the digital signature and check if B is correct.

There are four parties involved in the proposed scheme as follows. V_o denotes the original voter; V_p denotes the proxy voter; *AS* denotes the Authentication Server; *TCS* denotes the Ticket Counting Server.

2.2 The Proxy E-Voting Scheme

The novel proxy e-voting scheme is composed of five processes: delegation phase, registration phase, voting phase, counting phase and verifying phase. The framework of our proposed scheme is shown in Fig. 1.

(1) Delegation Phase:

(a) V_o chooses a random number $k_o \in Z^*{}_q$ and computes $r_o = g^{k_o} \, mod \, p$ and

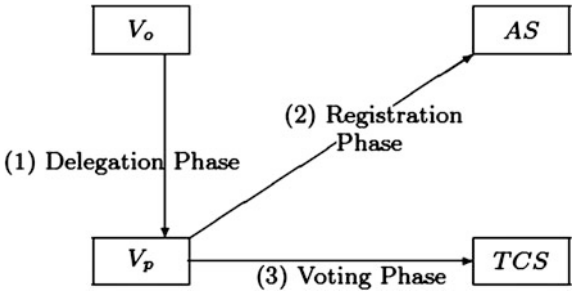

Fig. 1 The framework of novel proxy e-voting scheme

$$\sigma = x_o y_o + k_o \cdot h(M_w, r_o) \bmod q.$$

(b) V_o sends $\{\sigma, r_o, M_w, C_{num}\}$ to V_p over a secure channel.
(c) After receiving $\{\sigma, r_o, M_w, C_{num}\}$, V_p verifies whether the equation holds:

$$g^{\sigma}? = y^{yo} r_o^{h(M\,w,\,ro)} \bmod p.$$

If it holds, V_p computes an alternative proxy signature key $\sigma_p = \sigma + x_p h(M_w, r_o, y_p) \bmod q$.

(2) Registration Phase:

(a) V_p computes $u = g^{h(\sigma)} \bmod p$ and chooses three numbers $b_1, b_2,$ and $k_1 \in [1, p-1]$. The first two numbers b_1 and b_2 are the blind factors, and k_1 is a random number. With these parameters, V_p computes z_1 and z_2 by using the following equations.

$$\mathrm{z_1} = \mathrm{u^{*} b_1^{e\,AS}\ mod n_{AS}},$$
$$\mathrm{z_2} = \mathrm{g^{k1*} b_2^{e\,AS}\ mod\ n_{AS}}.$$

Then, V_p sends $\{V_p, AS, M_w, t, r_o, z_1, z_2, Sign_{\sigma p}(z_1||z_2||t)\}$ to AS.

(b) At first AS verifies the validity of the warrant and the proxy signature $Sign_{\sigma p}(z_1||z_2||t)$. AS verifies the validity of $Sign_{\sigma p}(z_1||z_2||t)$ by checking the verification function of a signature scheme with the newly generated public key $y = g^{\sigma p} \bmod p = y_o^{yo} r_o^{h(M\,w,\,ro)*} y_p^{h(M\,w,ro,yp)} \bmod p$.
(c) If the verification function is true, AS accepts that V_p is a valid voter on behalf of V_o. Then, AS chooses a random number k_2 that is unique to each voter and computes z_3, z_4, z_5, and z_6 as follows:

$$z_3 = (k_2||t)^{e\,vp} \bmod n_{vp},$$

$$z_4 = z_1^{dAS} \bmod n_{AS}$$
$$= u^{dAS} b_1 \bmod n_{AS},$$

$$\begin{aligned} z_5 &= (z_2 * g^{k2})^{dAS} \bmod n_{AS} \\ &= \left(g^{k1+k2}\right)^{dAS} b_2 \bmod n_{AS} \\ &= y_1^{dAS} b_2 \bmod n_{AS}, \end{aligned}$$

$$\begin{aligned} z_6 &= (z_2^{2*} g^{k2})^{dAS} \bmod n_{AS} \\ &= \left(g^{2k1+k2}\right)^{dAS} b_2^2 \bmod n_{AS} \\ &= y_2^{dAS} b_2^2 \bmod n_{AS}. \end{aligned}$$

where $u = g^{h(\sigma)}$, $y_1 = g^{k1+k2}$, and $y_2 = g^{2k1+k2}$. AS stores the k_2 that belongs to V_o and V_p in the database and sends $\{AS, V_p, z_3, (z_4||z_5||z_6||flag||s_0||t)^{e\,vp} \bmod n_{vp}\}$ to V_p.

(d) V_p firstly obtains k_2 by decrypting z_3 with d_{vp}. In the same way, he/she can obtain z_4, z_5, and z_6. Secondly, he/she can compute y_1 and y_2. At last, he/she can get signatures s_1, s_2 and s_3 by removing the blind factors in the following:

$$\begin{aligned} s_1 &= z_4 b_1^{-1} = u^{dAS} \bmod n_{AS}, \\ s_2 &= z_5 b_2^{-1} = y_1^{dAS} \bmod n_{AS}, \\ s_3 &= z_6 b_2^{-2} = y_2^{dAS} \bmod n_{AS}. \end{aligned}$$

(e) Let y_1 and y_2 be the public keys, $x_1 = k_1 + k_2$ and $x_2 = 2k_1 + k_2$ be the corresponding secret keys. V_p chooses a random number r and computes $r' = g^r \bmod p$. Then he/she generates two signatures, (r', s_4) and (r', s_5), of the voting content m in accordance with the original voter's intention C_{num}. The equations are as follows:

$$\begin{aligned} s_4 &= x_1^{-1}(mu - r) \bmod (p-1), \\ s_5 &= x_2^{-1}(mu - r) \bmod (p-1). \end{aligned}$$

Therefore, V_p can obtain the voting ticket $T = \{s_0||s_1||s_2||s_4||r'||flag||u||y_1||m\}$.

(3) Voting Phase:

(a) V_p sends $\left\{T||(s_3, s_5, y_2)^{e\,TCS} \bmod n_{TCS}\right\}$ to TCS.

(b) TCS obtains s_3, $s5$ and y_2 by decrypting $(s_3, s_5, y_2)^{eTCS} \bmod n_{TCS}$ with d_{TCS}. Then, it verifies the validity of u, y_1 and y_2 from T by checking the following verification equations:

$$\begin{aligned} u? &= s_1^{eAS} \bmod n_{AS}, \\ y_1? &= s_2^{eAS} \bmod n_{AS}, \\ y_2? &= s_3^{eAS} \bmod n_{AS}. \end{aligned}$$

If the above equations hold, TCS will verify the signatures *(r', s4)* and *(r', s5)* on m in addition. The verification equations of the signatures are as follows:

$$g^{mu}? = y_1 s_4 * r' \, mod \, p,$$
$$g^{mu}? = y_2 s_5 * r' \, mod \, p.$$

If the results of both equations are correct, *TCS* will accept that the voting ticket T is valid. Then, *TCS* will count the ballots in time.

(4) Counting Phase:
TCS publishes the tickets on the electronic bulletin board and counts them. Note that the electronic bulletin board is only for reading in public.

(5) Verifying Phase:
The ticket is verified by both the proxy voter and the original voter. The proxy voter checks his/her vote on the electronic bulletin board to see whether the vote-counting is correct. Besides, the original voter V_o can check if the proxy voter V_p casts the corresponding ticket and checks if it follows his/her intention. The verification equation is as follows.

$$g^{h(\sigma)} \, mod \, p? = u$$

Assume that a voter signs two different voting contents m and m' by using the same u, y_1, and y_2. This is when double voting occurs. In this situation, *TCS* can ask *AS* to find out who the voter is by computing the equations below:

$$x_1 = \frac{m'u - mu}{s'_4 - s_4} \, mod \, (p-1),$$
$$x_2 = \frac{m'u - mu}{s'_5 - s_5} \, mod (p-1),$$

TCS can obtain k_2 from computing $2x_1 - x_2 = 2(\mathrm{k}_1 + k_2) - (2k_1 + k_2) = k2$. Hence, *TCS* can tell *AS* the k_2 to find out the illegal voter from *AS*'s database.

3 Security Analysis

In this section, we analyze how our scheme can resist five different types of attacks as follows.

Attack 1: A malicious party wants to forge the legal identity and passes through the registration phase.
Analysis of Attack 1: A malicious party cannot generate any legal identity without a valid voter's private key. Moreover, if he wants to forge the valid proxy identity to register, he will fail. He must obtain the original voter's signature and the corresponding warrant and the proxy voter's signature. Because the identity of the voter is verified by *AS*, there exist the corresponding factors: the signature of the original voter, the proxy voter's secret key and the warrant that are used to

describe the proxy identity and the valid delegated period. Hence, the illegal voter cannot generate the valid proxy signature through the equation verified by *AS*.

Attack 2: A valid voter wants to forge one more ballot.
Analysis of Attack 2: The voter must pass through the verification equation and obtain the signature of *AS*. However, *AS* is permitted to sign the message one time for each voter. Hence, the voter can never generate another valid vote without verifying the equation of *AS*. If he/she wants to forge *AS*'s signature, he/she must face the problem of factoring large numbers, $S = M^{dAS} \ mod \ n_{AS}$.

Attack 3: Two or more voters conspire to get a new signature from individual signatures.
Analysis of Attack 3: Assume that there are two voters V_1 and V_2 who want to conspire to construct a new signature from individual signatures. They can obtain valid signatures (s_{11}, s_{12}, s_{13}) and (s_{21}, s_{22}, s_{23}). If they want to generate a new signature (s'_1, s'_2, s'_3), they have to try to generate s'_1 from s_{11} and s_{21}. In other words, they will also face the problem of factoring large numbers, $s_{11}^{dAS} = u_{11} \ mod \ n_{AS}$.

Attack 4: *AS* and *TCS* conspire to forge a valid ballot.
Analysis of Attack 4: Because tickets are public and the k1 is selected by the voter, everyone can check the number of voting tickets and that of registered voters to see whether they are equal or not. Hence, our scheme can resist the conspiracy attack.

Attack 5: A proxy voter wants to violate the original voter's intention.
Analysis of Attack 5: Because the original voter can check the ballot on the electronic bulletin board, no one can trace the voter's identity from u. Besides, because the original voter's signature σ is known only to himself and the proxy voter, anyone who wants to obtain σ must solve the discrete logarithms and face the difficulty of the one-way hash function $h(x) = y$. The function h is one-way in the sense that given x, it is easy to compute y. However, given y, it is hard to compute x.

4 Conclusion

In this paper, we have proposed a brand new proxy e-voting scheme. In our scheme, an original voter can delegate a proxy voter to vote on behalf of him/her. Furthermore, the original voter and the proxy voter can verify their ballot, respectively. When double voting occurs, the TCS can find out who the voter is. Our scheme not only can be easily implemented but also shortens the time voters need to cast their ballots.

In the future work, more experiments with different parameters will be considered. We also can apply the new cryptographic techniques to this environment or mobile environment.

Acknowledgments This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC 100-2221-E-030-015 and 100-2218-E-164-002.

References

1. Chaum, C.: Untracable electronic mail, return addresses, and digital pseudonyms. Commun. ACM **24**, 84–88 (1981)
2. Chaum, C.: Blind signatures system. Adv. Cryptol. CRYPTO'83, 153–156 (1983)
3. Chaum, C.: The dinning cryptographers problem: unconditional sender and recipient untraceability. J. Cryptol. **1**, 65–75 (1988)
4. Chen, W., Wu, Y., Pan, F., Lei, F.: An efficient electronic voting scheme based on quadratic residue. In: Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing, pp. 647–649 (2009)
5. Chien, H.Y., Jan, J.K., Tseng, Y.M.: Cryptanalysis on Muvaradharajan's e-voting schemes. Appl. Math. Comput. **139**, 525–530 (2003)
6. Dai, J.Z., Yang, X.H., Dong, J.X.: A privacy-protecting proxy signature scheme and its application. In: Proceedings of IEEE International Conference on Systems, Man and Cybernetics, vol. 1, pp. 203–206 (2004)
7. Das, M.L., Saxena, A., Phatak, D.B.: Proxy signature scheme with effective revocation using bilinear pairings. Int. J. Netw. Sec. **4**, 312–317 (2007)
8. ElGamal, T.: A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory **IT-31**, 469–472 (1985)
9. Flonta, S., Miclea, L.C., Enyedi, S.: Electronic vote scheme based on ring signature. In: Proceedings of the IEEE International Conference on Automation, Quality, and Testing Robotics, pp. 1–3 (2009)
10. Fujioka, A., Okamoto, T., Ohta, K.: A practical secret voting scheme for largescale elections. Adv. Cryptol. AUSCRYPT'92, 244–251 (1993)
11. Gallegos-Garcia, G., Gomez-Cardenas R., Salinas, R.M., Duchen-Sanchez, G.I.: A new and secure electronic voting protocol based on bilinear pairings. In: Proceedings of the International Conference on Electronics, Communications, and Computer, pp. 240–244 (2009)
12. Gallegos-Garcia, G., Gomez-Cardenas R., Salinas, R.M., Duchen-Sanchez, G.I.: Electronic voting using identity based cryptography. In: Proceedings of the Fourth International Conference on Digital Society, pp. 31–36 (2010)
13. Hwang, M.S., Lee, C.C., Lai, Y.C.: An untraceable blind signature scheme. IEICE Transactions on Fundamentals on Electronics, Communications and Computer Science, vol. E86-A, pp. 1902–1906 (2003)
14. Juang, W.S., Lei, C.L.: A secure and practical electronic voting scheme for real world environments. IEICE Trans. Fundam. **E80-A**, 64–71 (1997)
15. Lin, I.C., Hwang, M.S., Chang, C.C.: Security enhancement for anonymous secure e-voting over a network. Comput. Stand. Interfaces **25**, 131–139 (2003)
16. Lu, E.J., Huang, C.J.: A time-stamping proxy signature scheme using time-stamping service. Int. J. Newt. Sec. **2**, 43–51 (2006)
17. Mambo, M., Usuda, K., Okamoto, E.: Proxy signatures: delegation of the power to sign messages. IEICE Trans. Fundam. **E79-A**, 1355–1360 (1996)
18. Mu, Y., Varadharajan, V.: Anonymous secure e-voting over a network. In: Proceedings of the 14th Annual Computer Security Application Conference, CAC-SAC'98, 2936–2939 (1998)
19. Sako, K.: Electronic voting schemes allowing open objection to the tally. IEICE Trans. Fundam. **E77-A**, 24–33 (1994)
20. Tan, Z.W.: Improvement on nominative proxy signature schemes. Int J. Netw. Sec. **7**, 175–180 (2008)

21. Wang, S., Fan, H., Cui, G.: A proxy blind signature schemes based on DLP and applying in e-voting. In: Proceedings of the 7th International Conference on Electroni Commerce, pp. 641–645 (2005)
22. Yun, S.H., Lee, S.J.: An electronic voting scheme based on undeniable blind signature scheme. In: Proceedings of the 37th IEEE Carnahan Conference on Security, pp. 163–167 (2003)