An Electronic Voting Scheme Based on LUC Secret System and Secret Sharing

Hongquan Pu[1,2,3], Zhe Cui[1,2], Ting Liu[1,2,3], Zhihan Wu[1,2], and Hongjiang Du[1,2]
(Corresponding author: Hongquan Pu)

Chengdu Institute of Computer Applications, Chinese Academy of Sciences[1]
No. 9, South Renmin Road, Section 4, Chengdu 610041, China
School of Computer and Control Engineering, University of Chinese Academy of Sciences[2]
No. 19 (A), Yuquan Road, Shijingshan District, Beijing 100049, China
Guangxi Key Laboratory of Hybrid Computation and IC Design Analysis[3]
No. 188, East University Road, Nanning, 530006, China
(Email: 774149765@qq.com)

(Received Aug. 31, 2019; Revised and Accepted Dec. 6, 2019; First Online Apr. 8, 2020)

Abstract

The security of electronic voting systems is an essential factor restricting its development. This paper proposes an electronic voting scheme based on LUC secret system and secret sharing. This scheme uses LUC to verify and identify voters' identities. Furthermore, it adopts Shamir's secret sharing to divide votes into multiple secret sharings, which are shared with all vote counters. The vote counters use the homomorphism of secret sharing to perform additional operations on the secret sharings received and then recover the final result of the voting. The proposed scheme meets the security requirements of anonymity, no receipt, verifiability and fairness, and so on. At the same time, it can obtain the final result without restoring the vote of each voter and there is an optimum number of vote counters, which guarantees the efficiency of the voting process. At last, it performs the voting process hierarchically. These advantages make our method suitable for electronic voting of different scales.

Keywords: Electronic Voting; Homomorphism; LUC; Secret Share; Vote Counters

1 Introduction

With the development of information technology, voting has been changed from paper voting to electronic voting. The security of electronic voting has always been the bottleneck restricting its development. The privacy protection in electronic voting systems has attracted more and more attention from scholars and engineers [21]. The most important feature of electronic voting based on cryptography is to provide end-to-end verifiability. All submitted votes are published in the ciphertext. Trusted third parties can verify the results of the voting, and different voters can also verify and supervise the whole voting process. These advantages are not available to non-cryptographic electronic voting.

After Chaum [5] presented the first electronic voting scheme based on an anonymous letter channel in 1981, a large number of electronic voting schemes based on cryptography have been proposed, which can be divided into the following four categories.

The first kind of electronic voting scheme is based on a hybrid network. Encrypted votes are confused through the hybrid network, which can shield the correlation between output and input, thus achieving the purpose of protecting the vote information. Chaum's scheme [5] uses an anonymous channel to transmit votes, which is a typical voting scheme based on the hybrid network. Sako and Killian [34] proposed an obfuscation scheme based on re-encryption and random permutation for voting. Neff [29] proposed a mathematical structure to shuffle the votes, which is only suitable for ElGamal encryption. Groth [14] gived a scheme to extend Neff's scheme to general homomorphic encryption in public key cryptosystem. Electronic voting scheme based on the hybrid network usually requires multiple confusion calculations, encryption and decryption operations and zero-knowledge proof. Therefore, the implementation efficiency is generally low, and it is difficult to be applied to large-scale voting activities.

The second kind of electronic voting scheme is based on homomorphic encryption. Cohen [7] in 1985 proposed the first electronic voting scheme based on homomorphic encryption, which requires all voters to vote at the same time. Cramer *et al.* [8] proposed a 1-out-of-many electronic voting scheme based on ELGamal encryption and zero-knowledge proof. This method needs an exhaustive search when decrypting, and it leads to a high computational cost. Damgard *et al.* [11] proposed a many-out-of-many electronic voting scheme based on Pailier encryption [30]. When the set of possible votes contains a large number of elements, the efficiency of this scheme is reduced sharply. Damgard, Groth and Solomonsen [10] designed a scheme to code votes by using homomorphic commitment and homomorphic encryption, which is more efficient. Chen *et al.* [6] proposed a receipt-free homomorphic encrypted electronic voting scheme based on semi-trust model. This scheme achieves the result of confidentiality, generalized verifiability and fairness. However, it has high requirements for the voters which is difficult to be used in practice.

The third kind of electronic voting scheme is based on the blind signature. In 1992, Fujiaka *et al.* [13] proposed the famous electronic voting scheme based on the blind signature (FOO scheme). This scheme achieves the security goal in large-scale electronic voting activities. However, it still exists some problems, such as the voters cannot abstain and the votes collision. The proposed scheme makes electronic voting enter a practical stage. Some electronic voting systems developed later are basically based on FOO scheme, *e.g.*, the Sensus system of the University of Washington [9]. Shilbayeh *et al.* [35,38] proposed EV-APS scheme based on the blind signature and improved the scheme, both of which are based on REVS [19] and Evox-MA [12]. Fenfen Luo *et al.* [27] proposed a receipt-free electronic voting scheme based on FOO, which theoretically solved the problems of ballot collision and non-abstention, but still failed to achieve overall verifiability.

Shamir [37] proposed the first secret sharing scheme in 1979. This scheme is based on Lagrange difference polynomial, which is easy to implement and has high security. Many improved versions, such as the multi-stage secret sharing scheme (MSS) [16,22], have emerged to realize multiple secret sharing. The secret sharing scheme [23,31], introducing the one-way function, solves the problem of secret share reuse and improves the practicability. Benaloh *et al.* [2,4] began to use secret sharing in electronic voting. There are two main types of electronic voting schemes based on secret sharing: one is based on the difference method in Shamir's (t, n) threshold [26,28,36], the other is based on the Chinese Remainder Theorem [18,40].

This paper applies the LUC secret system to authenticate voters and Shamir's (t, n) secret sharing technology to realize the voting process. Finally, based on the homomorphism of Shamir secret sharing, the final results of voting are counted, and the feasibility and the security of our scheme are compared with other methods through security analysis.

The organizational structure of this paper is as follows. The second part introduces the information of the LUC secret system, secret share, and homomorphism of secret sharing.The third part introduces the security requirements, the composition and the form of the electronic voting system. The fourth part presents our proposed scheme. The fifth part carries on the security analysis to the proposed scheme. The last part concludes this paper.

2 Preliminaries

This part mainly introduces the knowledge needed in this paper, including: The Shamir's (t, n) secret sharing, the LUC cryptosystem, and the homomorphism of secret sharing.

2.1 Shamir's (t, n) Secret Sharing

Shamir's (t, n) secret sharing is based on Lagrange interpolation polynomials, which consists of three phases [37].

2.1.1 Initialization Phase

Secret Distributor (SD) randomly selects n different nonzero elements x_1, x_2, $\ldots$, x_n, Identifies each participant $P_r \in \{P_1, P_2, \ldots, P_n\}(r = 1, 2, \ldots, n)$, orders $P = \{P_1, P_2, \ldots, P_n\}$, SD and assigns x_r to the corresponding $P_r(r = 1, 2, \ldots, n)$, where the value of x_r is public.

2.1.2 Secret Distribution Phase

If SD intends to have a participant $P_r \in P(r = 1, 2, \ldots, n)$ sharing secret $s \in \mathbb{Z}_m$(m is a large prime), SD randomly chooses t-1 elements a_1, a_1, $\ldots$, a_n in $GF(q)$ and constructs t-1 polynomial, by the formula as follows:

$$f(x) = (s + \sum_{i=1}^{t-1} a_i x^i) \ mod \ q$$

where $q > s$ and $s = f(0)$. Then SD generates secret shares for all participants:

$$s_r = f(x_r) = (s + \sum_{i=1}^{t-1} a_i x_r^i) \ mod \ q.$$

SD sends s_r to the corresponding participant P_r through the secure channel.

2.1.3 Secret Recovery Phase

Any t participants in the n participants may be set as P_1, P_2, $\ldots$, P_t, showing their secret shares, which can reconstruct polynomial $f(x)$.

$$f(x) = (\sum_{i=1}^{t} f(x_i) \prod_{j=1,j\neq i}^{t} \frac{x - x_j}{x_i - x_j}) \ mod \ q.$$

By Ordering $x = 0$, the following formulas is obtained.

$$s = (\sum_{i=1}^{t} f(x_i) \prod_{j=1,j\neq i}^{t} \frac{-x_j}{x_i - x_j}) \ mod \ q.$$

In Shamir'(t, n) secret sharing scheme, any secret shares of not less than t can recover secret s, and no information of s can be obtained if less than t secret shares. This secret share scheme is a one-time scheme and can only be used once in the process of secret share, because after t participants give secret shares, the secret share can be disclosed at the same time. The polynomial $f(x)$ constructed by D is also made public. This feature just meets the characteristics of electronic voting. The electronic voting scheme should be a one-time scheme; otherwise, the scheme itself will be questioned.

2.2 LUC

LUC is a double cryptosystem proposed by P.Smith [24, 32, 39]. This method uses Lucas sequence to realize encryption and decryption.

2.2.1 Lucas Sequence

Definition 1. *Choosing two non-negative integers P and Q, Constructing quadratic equation $x^2 - Px + Q = 0$, the two roots of the equation are:*

$$x_1, x_2 = \frac{P \pm \sqrt{P^2 - 4Q}}{2}.$$

If $P^2 - 4Q \neq 0$, then the Lucas sequence can be defined as:

$$\begin{aligned} U_n(P,Q) &= \frac{x_1^n - x_2^n}{x_1 - x_2},\ n \geqslant 0 \\ V_n(P,Q) &= x_1^n + x_2^n,\ n \geqslant 0. \end{aligned}$$

LUC cryptosystem is only interested in $V_n(P,Q)$ sequences, Lucas sequence has the following properties:

- Let a and b be arbitrary positive integers, $V_{ab}(P,1) = V_a(V_b(P,1),1)$; The proof is available in reference [39].

- Let a and b be arbitrary positive integers, $V_b(V_a(P,1),1) = V_a(V_b(P,1),1)$.

  Proof. $V_b(V_a(P,1),1) = V_{ba}(P,1) = V_{ab}(P,1) = V_a(V_b(P,1),1)$. □

2.2.2 LUC Cryptosystem

Let $N = pq$, for the product of two odd prime numbers, we choose an integer e and let$(e, \phi(N)) = 1$, then $(e, \phi(N)) = 1$ is an Euler function, which determines another integer d by $ed \equiv 1\ mod\ \phi(N)$. The construction method is as follows:

- Public key: N, e;

- Private key: d;

- Plaintext: P is an integer less than N;

- Ciphertext: $C = V_e(P,1)\ mod\ N$;

- Decrypt: $P = V_d(P,1)\ mod\ N$.

This paper implements voter authentication through the LUC cryptosystem.

2.3 Homomorphism of Secret Sharing

The concept of homomorphism of secret sharing is given in [1]. S is the main secret space and T is the secret sharing space corresponding to the main secret. The function $F_I : T \to S$ is the induced function of (t,n) secret sharing. This function defines the secret s based on any subset of $\{s_1, s_2, ..., s_t\}$ containing t secret shares as $s = F_I(s_1, s_2, ..., s_t)$, where $\{I = s_1, s_2, ..., s_t\}$. Definition: Suppose $\oplus$ and $\otimes$ are two functions on set S and T elements, respectively. For any subset I, if there exists $s = F_I(s_1, s_2, ..., s_t)$, $s' = F_I(s_1', s_2', ..., s_t')$ satisfies $s \oplus s' = F_I(s_1 \otimes s_1', s_2 \otimes s_2', ..., s_t \otimes s_t')$, then it is considered that a $(t,\ n)$ secret sharing scheme has $(\oplus,\ \otimes)$ homomorphism.

According to the above definition, Shamir's $(t,\ n)$ is $(+, +)$ homomorphic.

The proof is as follows: suppose two participants A and B share the secret s_A and s_B with Shamir's $(t,\ n)$, For A, the secret s_A can be decomposed into multiple secret shares by the following polynomial $s_A = F_I(a_1, a_2, ..., a_t)$; for B, the secret s_B can be decomposed into multiple secret shares by the following polynomial $s_B = F_I(b_1, b_2, ..., b_t)$. The following formulas can be obtained through mathematical variations:

$$s_A + s_B = F_I(a_1 + b_1, a_2 + b_2, ..., a_t + b_t).$$

This indicates that Shamir's $(t,\ n)$ share sharing is $(+, +)$ homomorphic.

3 Electronic Voting System

This part includes the security requirements of electronic voting, the form of electronic voting and the composition of electronic voting.

3.1 Security Requirements for Electronic Voting

Fujioka *et al.*[11] defined seven security requirements of electronic voting, which are considered as the basic security requirements of electronic voting schemes.

1) Completeness: All legitimate and valid votes should be counted correctly.

2) Soundness: Illegal or malicious voters cannot affect or disrupt the voting process.

3) Privacy: The identity and voting information of all voters must be kept confidential.

4) Unreusability: All voters can vote only once, not many times.

5) Eligibility: All voters need to be authenticated before voting. If the authentication fails, they are not allowed to vote.

6) Fairness: Voting is fair to all, and nothing can affect the fairness of voting.

7) Verifiability: The voting results are verifiable, and no one can change the voting results.

With the emergence of new network technologies and attack methods, electronic voting needs to meet higher security requirements besides the above seven basic security requirements [3, 15, 33]:

8) Receipt-Freeness: Voters cannot prove what they voted for during the voting process.

9) Universal Verifiability: Not only can voters verify that their votes have been counted correctly, but any third parties can also verify that the results are correct

10) Coercion-Resistance: Voters cannot coerce others to prove their voting information during the voting process.

3.2 Electronic Voting Form

There are usually three forms of electronic voting [17]:

1) Voters choose yes or no, which is only suitable for the case of 2 choosing 1;

2) Voters choose one candidate from multiple candidates, and the number of candidates should be greater than 2;

3) Voters choose multiple candidates from multiple candidates.

3.3 Composition of Electronic Voting

A complete electronic voting system consists of four parts [3,6,13,17,20,25]: voters, registration agencies, vote issuing agencies and vote counting agencies.

- Voters: Actual Participants in Voting Activities
- Registration agency: To verify the identity of voters, only when the conditions for verification specified by the Registrar are met, can the voter be eligible for voting.
- Ballot issuing agency: Issuing blank votes to legitimate voters.
- Vote counting institution: Statistics of the total number of votes and verification of the legitimacy of votes.

In the actual electronic voting activities, registration agency, vote issuing agency and vote count agency can merge, but also can be decomposed into multiple institutions.

Generally, a complete voting process is as follows: Voters apply to the registration agency for authentication. After the registration agency receives the application, it examines the voting qualifications of the voter. If satisfied, it will be validated successfully and become a valid voter. Otherwise, the application is rejected. Then the vote issuing agency will send the blank vote to the voter who is a valid voter. The voter fills in the blank vote after received, and then send the filled vote to the vote-counting institution, which counts the vote and publishes the final results.

4 Electronic Voting Scheme Based on LUC Secret System and Secret Sharing

The scheme consists of five agencies: Voters $V_1, V_2, ..., V_m$, regulatory agency abbreviated as RA, secret distribution agency abbreviated as DA, vote counting agency abbreviated as CA, including n vote counters $C_1, C_2, ..., C_n$, verification agency recorded as PA, all of the above agencies and entities are credible, p,q are two large enough prime numbers, let $N = pq$, the LUC public key and private key of voter $V_i (i = 1, 2, ...m)$ are $\{N, e_i\}$ and d_i (i = 1, 2,...,m), the LUC public key and private key of RA are $\{N, d_{RA}\}$ and e_{RA}, Q is a randomly selected prime greater than N, ID number is the random identifier of V_i.

4.1 Initial Phase

At this phase, voter identification is verified and voters get blank votes.

Step 1: If voter P_i (i=1,2,...,m) authentication is required. P_i firstly forms his or her own private key e_i and public key $\{N, d_i\}$, where e_i is also P_i's identity information and meets the voting requirements. Then, it sends the authentication request Request to RA through anonymous channel.

Step 2: After receiving P_i's Request, RA randomly selects an integer g from $(\sqrt{N}, N - 1)$ and sends g to P_i via anonymous channel.

Step 3: After receiving g, P_i uses his or her own private key e_i to sign g, which is calculated by LUC encryption method, and sends the result of signature to RA through the anonymous channel.

Step 4: After receiving P_i's signature, RA uses $\{N, d_i\}$ to verify the validity of $V_{d_i}(g, 1)$ *mod* N, that is, is $g = V_{d_i}(V_{e_i}(g, 1), 1)$ *mod* N valid. If it is valid, it randomly selects a unique ID from $(\sqrt{N}, N-1)$. Then it sends the ID number to P_i through anonymous channel, and at the same time, it sends the ID number to each vote counter $C_1, C_2, ..., C_n$, and RA encrypts the blank vote s' with its own private key using the LUC encryption method, as $V_{d_{RA}}(s', 1)$ *mod* N and sends the encrypted blank vote to P_i through anonymous channel. If not, RA sends a Rejection message to P_i, P_i can re-sign and verify, If P_i authentication fails more than three times, RA refuses to accept P_i's authentication.

4.2 Secret Sharing Phase

This phase includes participants vote and send votes to secret distribution agency (DA), which uses Shamir's (t, n) to decompose votes into multiple secret sharings, and then sends them to n vote counters.

Step 1: After receiving the ID number and the encrypted blank vote, the voter P_i decrypts blank vote as $V_{e_{RA}}(V_{d_{RA}}(s', 1), 1)\ mod\ N$, The voter P_i fills in the blank vote s' and gets the vote s_i. After encrypting the s_i and ID number ID with P_i's LUC private key, P_i sends them to the secret distribution agency (DA) through the anonymous channel.

Step 2: After DA receives P_i's vote, it decrypts the vote s_i and the corresponding ID with P_i's public key. DA randomly selects n different non-zero elements $x_1, x_2, ..., x_n$ from $GF(q)$ (q is a large prime and $q > n$), DA exposes $x_i (i = 1, 2, ..., n)$ and assigns to $C_j (j = 1, 2, ..., n)$.

Step 3: DA randomly chooses $t-1$ elements a_{i1}, a_{i2}, $\cdots$, a_{in} from $GF(q)$. The $t-1$ polynomial is constructed as follows:

$$f_{(P_i)}(x) = s_i + a_{i1}x + a_{i2}x^2 + ... + a_{i(t-1)}x^{t-1}.$$

DA calculates $y_j = f_{(P_i)}(x_j)$, $1 \le j \le n$, $1 \le i \le m$.

Step 4: DA encrypts y_j and ID number of P_i and PI by LUC and sends them to the corresponding vote counter $C_j (j = 1, 2, ..., n)$.

4.3 Counting Phase

After each vote counter receives the secret sharing and ID number, it decrypts by LUC. Then, it checks whether it has received the secret sharing of the same ID number, discards it if it has received it, and saves it if it has not received it. Because the Shamir's (t, n) method is (+, +) homomorphic, the addition operation is performed after all secret sharings received by each vote counter. The final voting result can be restored directly, which is proved as follows. Let

$$F(C_j) = \sum_{i=1}^{m} f_{(P_i)}(x_j).$$

It can be written as:

$$\begin{aligned} F(C_j) &= \sum_{i=1}^{m} f_{(P_i)}(x_j) \\ &= (s_1 + s_2 + ... + s_m) + (a_{11} + a_{21} + ... + a_{m1})x_j \\ &\quad +(a_{12} + a_{22} + ... + a_{m2})x_j^2 + ... + (a_{1(t-1)} \\ &\quad +a_{2(t-1)} + ... + a_{m(t-1)})x_j^{t-1} \quad (j = 1, 2, ..., n). \end{aligned}$$

According to the following formula, the final result of voting can be obtained:

$$s_1 + s_2 + ... + s_m = \sum_{j=1}^{t} F(C_j) \prod_{i=1, j\neq i}^{t} \frac{x_i}{x_i - x_j}.$$

4.4 Verification Phase

After obtaining the final result of the voting activity directly through the homomorphic nature of secret sharing, if there are voters who doubt whether their voting information is accurately recorded, they can submit their ID number to CA for application verification, and CA can recover the votes through the t in n vote counters according to the ID number by the following formula, where $r = 1, 2, ..., m$.

$$s_r = \sum_{i=1}^{t} f_{(P_r)}(x_i) \prod_{j=1, j\neq i}^{t} \frac{x_j}{x_j - x_i} \tag{1}$$

If existing voters or any third party organizations question the overall results of the voting, CA can recover all the information of the votes through t in n vote counters, and then calculate the final results by the following formula.

$$\begin{aligned} s_1 + s_2 + ... + s_m &= \sum_{i=1}^{t} f_{(P_1)}(x_i) \prod_{j=1, j\neq i}^{t} \frac{x_j}{x_j - x_i} \\ &+ \sum_{i=1}^{t} f_{(P_2)}(x_i) \prod_{j=1, j\neq i}^{t} \frac{x_j}{x_j - x_i} + ...+ \\ &\sum_{i=1}^{t} f_{(P_m)}(x_i) \prod_{j=1, j\neq i}^{t} \frac{x_j}{x_j - x_i} \end{aligned} \tag{2}$$

5 Security Analysis

We provide a security analysis of the proposed scheme from the following ten aspects.

- Completeness: In the verification phase, whether the number of ID numbers of the vote counter is equal to the number of successful voters can ensure that all legitimate and valid votes are counted correctly. At the same time, the number of ID numbers received by DA can also ensure the consistency of the number of votes, thus ensuring the integrity of the number of votes in the whole voting process.
- Soundness: This scheme is based on LUC cryptosystem. It combines the introduction of ID number and the use of Shamir'(t, n) secret sharing to ensure the security of voting activities, and to ensure that illegal or malicious voters can not affect and destroy the voting process.
- Privacy: In this scheme, the identity information of voters is used and verified as the LUC private key. Malicious voters and third parties can not obtain the

identity information of legitimate voters through illegal channels. Also, the unique *ID* number generated by *RA* for voters randomly is also sent to voters through LUC encryption, which ensures that *ID* number is not leaked, that is, the *ID* number is not disclosed. Even if the *ID* number is leaked, it can not bind the *ID* number to the voter's identity information. At the same time, it can not obtain the correct blank votes, which ensures the privacy of the voter's identity. The voting process uses the LUC encryption and decryption. Although the secret sharing process does not encrypt the secret sharings, the leakage of a certain number of secret sharings will not cause leakage of the vote.

- Unreusability: Voters need to send their *ID* number when voting. When voting is restored and counted, if the counters receive the secret sharings of the same *ID* number, they will be discarded and can not be counted normally, which ensures that voters can only vote once legally and effectively.

- Eligibility: In this scheme, voters need to authenticate to *RA* for obtaining blank votes and their unique *ID* number before voting, and don't allow voters who have not been authenticated to vote.

- Fairness: In this scheme, *RA, DA, CA, PA* and n counters are credible, which can guarantee the objectivity and fairness of the whole voting process. As long as the successful voters are verified by *RA*, they will get the only *ID* number and blank votes which can ensure that voters' votes do not tamper.

- Verifiability: If there are voters who doubt whether their voting information is accurately recorded, they can submit their *ID* number to *CA* for application verification, and *CA* can recover the votes through the t in n vote counters according to the *ID* number by Formula (1).

- Receipt-Freeness: In the process of identification, voting and counting, voters can not prove their votes. Even if there are Bribery electors at all phases, voters can not prove their votes to bribery electors. In the later phase of voting verification, voters can only check whether their votes are counted, but can not show their contents of votes to *CA*.

- Universal Verifiability: If existing voters or any third party organizations question the overall results of the voting, *CA* can recover all the information of the votes through t in n vote counters, and then calculate the final results by Formula (2).

- Coercion-Resistance: If voters are coerced to disclose their voting content after voting, because the scheme has receipt-freeness, voters can not prove that their open voting content is the real content of the original voting, and the content obtained by the coerced person may not have any relevance to the actual situation of voting.

The security of electronic voting of our method is compared with the methods in [13, 27, 38, 40]. As shown in Table 1.

Our scheme meets ten security requirements of electronic voting. Scheme [13] does not satisfy receipt-freeness and universal verifiability; scheme [38] does not satisfy Privacy, Receipt-Freeness, universal verifiability and Coercion-Resistance; scheme [27] does not satisfy Privacy, Verifiability, Receipt-Freeness, and Universal Verifiability; Scheme [40] does not satisfy Privacy, Receipt-Freeness and Universal Verifiability. Based on the comparison, we can see that our proposed scheme is better than its peer methods.

6 Conclusions

The first part of this paper introduces the current research situation of electronic voting. The second part introduces Shamir's (t, n) secret sharing, the LUC cryptosystem and the homomorphism of secret sharing. The third part illustrates the security requirements and the form and composition of the electronic voting system. The fourth part presents our proposed electronic voting scheme in this paper. The fifth part analyses the security of our scheme and compares it with other similar ones.

This scheme uses the LUC cryptosystem to verify voters' identities. With the voter's identity information as the private key, *RA* cannot obtain the identity information, and the *ID* number generated cannot bind to the voter's identity. It achieves the privacy of voter's identity and guarantees the receipt-free voting process. After voter votes, *SD* uses Shamir's (t, n) secret sharing method to divide vote into several secret shares and send them to n vote counters. Each vote counter adds the secret shares received homomorphically. The vote counter does not need to restore each vote to obtain the final result of the voting. In the verification phase, if someone doubts the voting process or results, the voters'votes need to be restored for verification. This process reachs the security requirements of electronic voting and has high efficiency. Since the number of voters can find the best value according to the scale of voting activities, the scheme in this paper is suitable for electronic voting activities of different scales.

Our scheme does not encrypt the secret sharings, because considering that if an attacker can not get the vote information if he or she obtains a single secret sharing, but if the scale of the voting and the number of vote counters are small, it will inevitably affect the security of voting process, but at the same time it will affect the efficiency of the vote decomposition and counting process, which need to be considered in future research activities. Besides, the scheme can achieve overall verifiability, but all votes must be restored. For large-scale voting activities,

Table 1: Security comparison of electronic voting

Security	**Our Scheme**	**FOO. [13]**	**Shilbayeh *et al.* [38]**	**Luo *et al.* [27]**	**Yuan *et al.* [40]**
Completeness	Y	Y	Y	Y	Y
Soundness	Y	Y	Y	Y	Y
Privacy	Y	Y	N	Y	N
Unreusability	Y	Y	Y	N	Y
Eligibility	Y	Y	Y	Y	Y
Fairness	Y	Y	Y	Y	Y
Verifiability	Y	Y	Y	N	Y
Receipt-Freeness	Y	N	N	N	N
Universal Verifiability	Y	N	N	N	N
Coercion-Resistance	Y	Y	N	Y	Y

the efficiency is low. Whether there are better methods is worthy of attention in future research.

Acknowledgments

This study was supported by the National Natural Science Foundation of China (61501064), Sichuan Technology Support Program (2015GZ0088), the Guangxi Key Laboratory of Hybrid Computation and IC Design Analysis (HCIC201502, HCIC201701). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] J. C. Benaloh, "Secret sharing homomorphisms: Keeping shares of a secret secret," in *Conference on the Theory and Application of Cryptographic Techniques (CRYPTO'86)*, pp. 251–260, Aug. 1986.

[2] J. Benaloh, M. J. Fischer, "A robust and verifiable cryptographically secure election scheme," in *Proceedings of the 26th IEEE Symposium on Foundations of Computer Science (FOCS'85)*, pp. 372–382, Oct. 1985.

[3] J. Benaloh, D. Tuinstra, "Receipt-free secret-ballot elections," in *Proceedings of 26th Annual ACM Symposium on Theory of Computing (STOC'94)*, May 1994.

[4] J. C. Benaloh, M. 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'86)*, pp. 52–62, Aug. 1986.

[5] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.

[6] X. F. Chen, J. L. Wang, Y. M. Wang, "Receipt-free electronic voting based on semi-trusted model," *Chinese Journal of Computers*, vol. 26, no. 5, pp. 557–562, 2003.

[7] J. D. Cohen, M. J. Fischer, "A robust and verifiable cryptographically secure election scheme," in *Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science (SFCS'85)*, pp. 372–382, Oct. 1985.

[8] R. Cramer, R. Gennaro, B. Schoenmakers, "A secure and optimally efficient multi-authority election scheme," in *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'97)*, pp. 103–118, May 1997.

[9] L. F. Cranor, R. K. Cytron, "Sensus: A security-conscious electronic polling system for the Internet," in *Proceedings of the 30th Hawaii International Conference on System Sciences*, pp. 561–570, Feb. 1997.

[10] I. Damgard, J. Groth, G. Salomonsen, "The theory and implementation of an electronic voting system," *Secure Electronic Voting*, vol. 7, pp. 77–99, 2003.

[11] I. Damgard, M. Jurik, "A generalisation, a simplification and some applications of paillier's probabilistic public-key system," in *International Workshop on Public Key Cryptography (PKC'01)*, pp. 119–136, Feb. 2001.

[12] B. W. DuRette, "Multiple administrators for electronic voting," *Bachelor's Thesis Mit*, 1999. (`https://pdfs.semanticscholar.org/e6e7/b4c046eb657d6497467083d1c6b0d4e2a545.pdf`)

[13] A. Fujioka, T. Okamoto, K. Ohta, "A practical secret voting scheme for large scale elections," in *International Workshop on the Theory and Application of Cryptographic Techniques (AUSCRYPT'92)*, pp, 244–251, 1992.

[14] J. Groth, "A verifiable secret shuffle of homomorphic encryptions," in *The 6th International Workshop on Practice and Theory in Public Key Cryptography*, pp. 145–160, Jan. 2003.

[15] J. Groth, "Efficient maximal privacy in boardroom voting and anonymous broadcast," in *International Conference on Financial Cryptography (FC'04)*, pp. 90–104, Feb. 2004.

[16] J. He, E. Dawson, "Multistage secret sharing based on one-way functions," *Electronics Letters*, vol. 30, no. 19, pp. 1591–1592, 1995.

[17] Z. Hong, L. S. Huang, Y. L. Luo, "A multi-candidate electronic voting scheme based on secure sum protocol," *Journal of Computer Research and Development*, vol. 43, no. 8, pp. 1405–1410, 2006.

[18] S. Iftene, "General secret sharing based on the Chinese Remainder Theorem with applications in E-voting," *Electronic Notes in Theoretical Computer Science*, vol. 186, no. 1, pp. 67–84, 2007.

[19] R. Joaquim, A. Zuquete, P. Ferreira, "REVS V A roubst electronic voting system", *IADIS International Journal on WWW/Internet*, vol. 1, no. 2, pp. 47-63, 2004.

[20] A. E. Latif, X. Yan, L. Li, *et al.*, "A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption," *Optics & Laser Technology*, vol. 54, pp. 389–400, 2013.

[21] C. T. Li, M. S. Hwang, Y. C. Lai, "A verifiable electronic voting scheme over the internet," in *Sixth International Conference on Information Technology: New Generations*, pp. 449-454, 2009.

[22] H. X. Li, C. T. Cheng, L. J. Pang, "An improved multi-stage(t, n) threshold secret sharing scheme," in *Advances in Web-Age Information Management (WAIM'05)*, pp. 267–274, Oct. 2005.

[23] H. X. Li, C. T. Cheng, L. J. Pang, "A new (t, n)-threshold multi-secret sharing scheme," in *International Conference on Computational and Information Science (CIS'05)*, pp. 421–426, Dec. 2005.

[24] H. X. Li, C. T. Chen, L. J. Pang, "LUC-based secret sharing scheme with access structures," *Journal of Southeast University (English Edition)*, vol. 36, no. 1, pp. 43–46, 2006.

[25] I. C. Lin, M. S. Hwang, C. C. Chang, "Security enhancement for anonymous secure E-voting over a network," *Computer Standards & Interfaces*, vol. 25, no. 2, pp. 131–139, 2003.

[26] Y. N. Liu, Q. Y. Zhao, "E-voting scheme using secret sharing and K-anonymit," *World Wide Web*, vol. 22, no. 4, pp. 1657–1667, 2019.

[27] F. Luo, C. L. Lin, S. Zhang, Y. Liu, "Receipt-freeness electronic voting scheme based on voting protocol," *Computer Science (in Chinese)*, vol. 42, no. 8, pp. 180–184, 2015.

[28] D. G. Nair, V. P. Binu, G. S. Kumar, "An improved E-voting scheme using secret sharing based secure multi-party computation," in *Cryptography and Security*, pp. 130–137, 2015.

[29] A. C. Neff, "A verifiable secret shuffle and its application to E-voting," in *Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS'01)*, pp. 116–125, Nov. 2001.

[30] P. Paillier, "Public-key cryptosystem based on composite degree residuosity class," in *International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt'99)*, pp. 223–238, May 1999.

[31] L. J. Pang, Y. M. Wang, "A new (t, n) multi-secret sharing scheme based on Shamir's secret sharing," *Apllied Mathematics and Computation*, vol. 167, no. 2, pp. 840–848, 2005.

[32] L. J. Pang, Y. M. Wang, "A (t, n) secret sharing scheme based on the LUC cryptosystem," *Journal of Xidian University*, vol. 32, no. 6, pp. 927–930, 2005.

[33] H. G. Rong, J. X. Mo, B. G. Chang, G. Sun, F. Long, "Key distribution and recovery algorithm based on Shamir's secret sharing," *Journal on Communications (in Chinese)*, vol. 36, no. 3, pp. 64–73, 2015.

[34] K. Sako, J. Killian, "Receipt-free mix type voting scheme a practical solution to the implementation of a voting booth," in *International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'95)*, pp. 393–403, May 1995.

[35] R. A. Saidi, N. Shilbayeh, E. Elnahri, and K. Alhawiti, "E-voting authentication preparation scheme (EV-APS) based on Evox-MA and REVS E-voting blind signature protocols," *International Journal of Engineering Innovations and Research*, vol. 5, no. 3, pp. 590–596, 2014.

[36] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting," in *Advances in Cryptology (CRYPTO'99)*, pp. 148–164, Aug. 1999.

[37] A. Shamir, "How to share a secret," *Commmunications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[38] N. F. Shilbayeh, R. A. Saidi, S. T. Khuffash, E. Elnahri, "Efficient and secure operations of the new secure E-voting authentication preparation scheme (EV-APS)," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS'16)*, vol. 5, no. 1, pp. 35–41, 2016.

[39] P. Smith, "LUC public-key encryption: A secure alternative to RSA," *Dobb's Journal*, vol. 18, no. 1, pp. 44–49, 1993.

[40] L. F. Yuan, M. C. Li, C. Guo, W. T, Hu, Z. Z. Wang, "A veriable E-voting scheme with secret sharing," *International Journal of Network Security*, vol. 19, no. 2, pp. 260–271, 2017.

Biography

Hongquan Pu received the M.S. degree in computer application technology from University of Chinese Academy of Sciences in 2014. He is currently a Ph.D. candiadate in University of Chinese Academy of Sciences. His current research interests include Electronic voting, Secret Sharing, LUC Secret System, Secure Multi-Party Computation(SMPC).

Zhe Cui received the degree of Bachelor in Electronic Precision Machinery from University of Electronic Science and Technology of China in 1992. He received the M.S. degree in Computer Application Technology from Chengdu Institute of Computer Applications, Chinese Academy of Sciences in 1995. He received the Ph.D. degree in Computer Software and Theory from Chengdu Institute of Computer Applications, Chinese Academy of

Sciences in 2011. He is currently a Ph.D. supervisor at the University of Chinese Academy of Sciences. The main research fields include pattern recognition and information security.

Ting Liu received the M.S. degree in Computer Software and Theory from Xi'an Technological University in 2011. He is currently a Ph.D. candiadate in University of Chinese Academy of Sciences. His research interests include Electronic voting, Blockchain and Secret Sharing.

Zhihan Wu received the degree of Bachelor of Engineering in Information Scecurity from Sichuan University in 2017. She is currently a M.D. candiadate in University of Chinese Academy of Sciences. Her current research interests include Electronic voting, Blockchain, Cryptography.

Hongjiang Du received the degree of Bachelor of Engineering in Computer Science and Technology from Sichuan University in 2002. He received the degree of Master of Engineering in Computer Science and Technology from Sichuan University in 2006. He is currently a Ph.D. candidate in University of Chinese Academy of Sciences. His current research interests include Electronic voting, coding theory, information security.