World Wide Web (2019) 22:1657–1667
https://doi.org/10.1007/s11280-018-0575-0

E-voting scheme using secret sharing and K-anonymity

Yining Liu [1,2] · **Quanyu Zhao** [1]

Received: 7 August 2017 / Revised: 9 January 2018 / Accepted: 17 April 2018 /
Published online: 25 April 2018

Abstract E-voting maybe replaces the traditional voting scheme in the future, however, the security threat must be paid enough attention. In this paper, a novel e-voting scheme is proposed using secret sharing and k-anonymity, which not only satisfies the basic security goals such as the non-cheating, the universal verifiability, the confidentiality, and the anonymity, but also achieves the addition properties including coercion-resistance and unconditional security since the security of the proposed scheme does not rely on any computational hard problem.

Keywords E-voting · Secret sharing · K-anonymity · Coercion-resistance · Unconditional security

1 Introduction

The election scheme should be secure and robust enough to resist a variety of malicious attacks to protect the sensitive information. Moreover, the transparency and comprehensibility are also vital, otherwise, the election result is not easily accepted by the public, and some literatures have tried to address these issues [1, 2]. Usually, they are divided into the traditional election and electronic election. The former needs a trusted election device, an authorized organizer, and the complicated mechanisms. In detail, the paper ballot, the handling of the ballot boxes and counting process in paper-based voting scheme must be trusted by all participators. Next, the process of the traditional election needs the time and resource, such as, (1) the cost is high since the paper ballots spend much money and a lot of workers must be hired; (2) inconvenient since it requires the voter casts his ballot in the voting booth [3, 4]. In addition, it is possible that the boxes are lost, manipulated or destructed.

To overcome these difficulties, the electronic election is researched in recent years, which is different from the traditional election in many ways. In fact, the cryptographic technique is the

✉ Yining Liu
ynliu@guet.edu.cn

[1] Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China

[2] Guizhou Provincial Key Laboratory of Public Big data, Guizhou University, Guiyang 550025, China

important tool in designing the e-voting scheme. The first e-voting scheme is proposed by Chaum [5], then, many researchers focus this area [6–12]. The necessary security properties include: (1) confidentiality, nobody can know other voter's content except himself, (2) non-cheating, no one can cheat others in the process of voting, (3) anonymity, a voter's ballot should not be linked with his identity, (4) verifiability, every voter can verify if his ballot is correctly tallied, (5) coercion-resistance, the voter proves nothing of his ballot to others to prevent from selling the vote, (6) authentication, each voter must be identified as a legal participator, and only casts once.

The development of the e-voting can be divided into two stages: 1) the security requirements are guaranteed using the complicated encryption technique such as mix-nets, homomorphic encryption and blind signatures, etc. The related protocols are listed in the Table 1 to achieve the security requirements using different methods. These protocols are computationally secure under the assumption that the adversary has the bounded computing power. 2) the protocols are unconditional security, i.e., it is still secure even if the adversary owns the unbounded computing power [34–36].

In this paper, an unconditional secure e-voting scheme is proposed based on secret sharing and *k*-anonymity, which not only ensures the ballot to be correctly tallied, but also guarantees each voter to verify the correctness of the result without knowing others' information. Moreover, the proposed protocol is efficient.

Note that the original idea has been presented in the conference [37], in the current version, more detailed description is added to make it more easily understandable, for example, the security assumption, the design goals. Especially, an example is used to illustrate the proposed scheme, and the analysis proves that the claimed goals are really achieved.

The rest of this paper is organized as follows. In Section 2, some preliminaries are introduced, and the system model is presented in Section 3. In Section 4, the proposed voting protocol is presented with an example to make it more easily readable. Finally, the analysis and the conclusion are respectively presented in Section 5 and Section 6.

2 Preliminaries

The following cryptographic concepts are necessary for understanding the proposed scheme.

2.1 Shamir's (*t*,*n*) secret sharing scheme

In 1979, secret sharing schemes were introduced in [38, 39]. Primarily, a mutually trusted dealer *D* divides a secret *s* into *n* shares that are securely shared among *n* shareholders. Then,

Table 1 Related works

Cryptographic Tools	Protocols
Mix-nets	Abe M [13], Jakobsson [14], Park [15], Kazue [16]
Homomorphic encryption	Benaloh [17, 18], Cramery [19], Cohen [20], Martin [21], Byoungcheon [22], Dahlia [23], C Andrew [24], Peng [25], Sako [26]
Blind signatures	Camenisch [27], Chaum [28], Fujioka [29], Ibrahim [30], Okamoto [31], Rivest [32], Atreya [33]

no fewer than t shares can recover the secret data s easily, and fewer than t shares gain nothing about s. There are vast research papers on secret sharing schemes [40–43].

Shamir's (t,n) secret sharing scheme is an unconditionally secure scheme without relying on any computational hard problem, which consists of n shareholders $\{P_1, P_2, \cdots, P_n\}$ and D, and includes two algorithms over a finite field F_p, where p is a secure prime.

Algorithm 1 Shares generation

Input:

n shareholders $\{P_1, P_2 \cdots P_n\}$, D, and the secret s.

Output:

1: D picks $f(x) = s + a_1x + a_2x^2 + \cdots a_{t-1}x^{t-1}$, $a_i \in F_p (i = 1, \cdots, t-1)$;
2: D computes $y_i = f(x_i)$, $(i = 1, 2, \cdots, n)$, where x_i is the identification of P_i;
3: D sends y_i to P_i via a secure channel, $(i = 1, 2, \cdots, n)$.

Algorithm 2 Secret reconstruction

No fewer than t shareholders can recover the secret s.

s is recovered by computing $s = f(0) = \sum_{i=1}^{t} f(x_i) \prod_{v=1, v\neq 1}^{t} \frac{-x_v}{x_i - x_v} \bmod p$.

2.2 Secret sharing homomorphism

Secret sharing homomorphism was introduced by Benaloh [44]. Assuming there are two secrets s_1, s_2, they are shared by two polynomials $f(x)$ and $g(x)$ respectively. $f(i) + g(i)$, $(1 \le i \le n)$ can be regarded as the shares corresponding to $s_1 + s_2$, which are distributed to n shareholders, and any t of them can recover the result.

2.3 *k*-anonymity

k-anonymity means that any element included in a set appears with the probability no greater than $1/k$, i.e., for any element, there are at least other k–1 indistinguishable elements in this set [45]. For example, $T(A_1, A_2, \cdots, A_n)$ is a table with n attributes $(A_1, A_2, \cdots, A_n)$. If each sequence of values in a set of attributes appears with at least k occurrences [46], T is k-anonymous.

In this voting scheme, any random k voters' receipts are generated and published, nobody can distinguish the individual one [47] to guarantee the k-anonymity.

3 The system model

In this section, the system model, the security requirements, and the design goals are introduced.

3.1 System model

The main participants include a trusted authority center (*AC*), voting system (*VS*), voter (*V*), candidate (*C*), and bulletin board that is the information publishing platform. Their functions are described as follows:

> ***AC*:** *AC* authorizes the legal voter to cast the ballot no more than once, and *AC* is responsible for arbitrating the disputes and issuing the digital certificate to each participant.
> ***VS*:** *VS* generates the credential for *V*, and leaks nothing about the voters' intention.
> ***V*:** *V* selects the favorite candidate and gets the credential using *VS*.
> ***C*:** *C* collaborates to tally the ballots to obtain the result with the help of *VS*.

The communication model is shown in Figure 1. An authorized voter *V* casts his ballot using the voting system (*VS*), and *VS* generates the corresponding credential for *V*, divides the voter's masked intention data into *m* pieces $d_1, \cdots, d_m$, and sends d_j to C_j, ($j = 1, \cdots, m$).

3.2 Trust assumption

In order to ensure the practicability, the following trust assumptions are necessary:

- *VS* is assumed to execute functionally without being infected by the computer virus.
- *V* is not assumed to be honest, he may sell his vote by proving the ballot's content.
- C is not assumed to be honest.
- Adversary can obtain the data transmitted between *VS* and candidate through the communication channel, and launch the attack to destroy the data integrity.

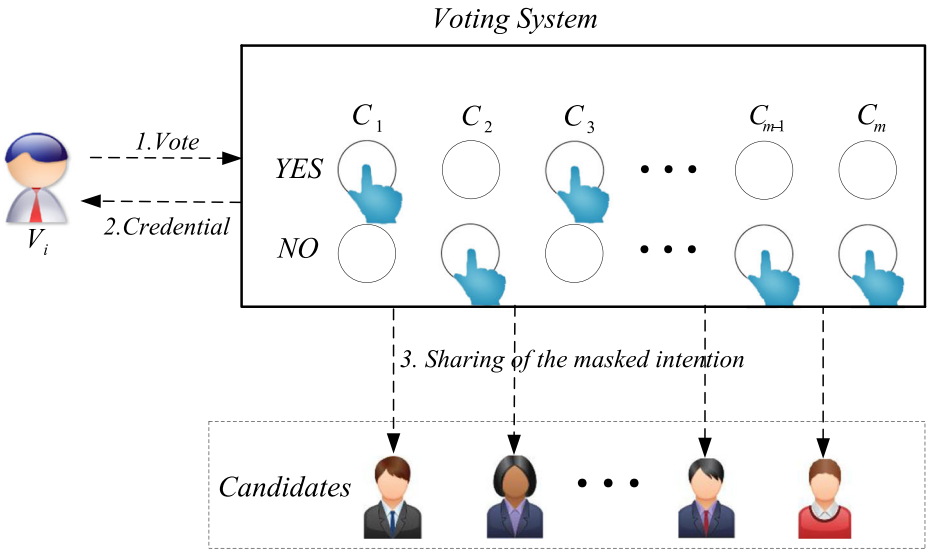

Figure 1 The communication model

3.3 Design goal

The necessary properties should be achieved, including the efficiency, the unconditional security, the universal verifiability and the coercion-resistance.

- *Unconditional security:* Even though the adversary has enough computing power, he can't infer any information about voter's ballot.
- *Universal verifiability:* Each voter can verify that his ballot is counted, and each candidate can verify if the result is correct.
- *Coercion-resistance:* Each voter cannot prove to others which candidate he has casted.
- *Efficiency:* The efficiency including the communication overhead and the computation cost should be lightweight.

When tallying the result, inside adversaries (also called "cheaters") can deceive the honest shareholders by altering the shares. Many research papers [48–50] have been proposed to address the problems of cheater detection and identification. For instance, Xu et al. [48] assumes the cheat is less than one third, then, increasing the number of shares can address the problem of cheater detection and identification. In this paper, the situation that the malicious shareholder changes the share is not considered, which will be researched in the future.

4 The proposed e-voting scheme

The proposed voting protocol consists of *Pre-voting Phase, Voting Phase* and *Post-voting Phase*, and all computations are over F_p, where p is a secure prime. Before the Pre-voting phase, AC publishes p and the anonymity measurement k.

4.1 Pre-voting phase

Assume that there are n voters $V_1, \cdots, V_n$, m candidates $C_1, \cdots, C_m$, and n voters are divided into several sets, each set consists of k voters.

4.2 Voting phase

Voter casts his favorite candidates and gets the credential via a secure manner such as face to face, and it can be used to verify whether the ballot is counted or not. The voting phase is listed as follows.

Step1. When V_i, $(i = 1, \cdots, n)$ registers to AC, VS issues a temporary ID to V_i, nobody knows the relationship between V_i and the temporary ID;
Step2. When the candidate C_j, $(j = 1, \cdots, m)$ is selected, $a_{i,j} = 1$, otherwise $a_{i,j} = 0$. Then, VS generates a polynomial $f_i(x) = a_{i,0} + a_{i,1}x + a_{i,2}x^2 + \cdots + a_{i,m}x^m \bmod p$, where $a_{i,0}$ is a non-zero random number;
Step3. VS computes $m + 2$ shares $(x_j, y_{i,j})$, $(j = 1, \cdots, m + 2)$, where x_j, $(j = 1, \cdots, m)$ is the identification of C_j, $(j = 1, 2, \cdots, m)$, x_{m+1}, x_{m+2} are the identifications of VS, V_i respectively, and $y_{i,j} = f_i(x_j)$. Then VS distributes $(x_j, y_{i,j})$ to C_j, $(j = 1, \cdots, m)$, $(x_{m+1}, y_{i,m+1})$ is stored in VS, and V_i gets the credential $CR_i = \{a_{i,0}, x_{m+2}, y_{i,m+2}\}$.

4.3 Post-voting phase

In Post-voting Phase, *VS* and all candidates reconstruct the polynomial and tally the result.

Step1. *VS* divides the voters randomly into some sets with k voters.
Step2. The temporary IDs of k voters in a set, for example, V_i, (i=2,⋯,k) is published, and these voters publish their $a_{i,0}$, (i=2,⋯,k) on the bulletin board;
Step3. C_j and *VS* compute $y_j = \sum_{i=1}^{k} y_{i,j}$, publish the points (x_j, y_j), $(j = 1, 2, \cdots, m+1)$, and each participant recovers $F(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m \bmod p$, where $a_j = \sum_{i=1}^{k} a_{i,j}, j = 0, 1, \cdots, m$. Then, *VS* publishes the aggregated ballots $\{a_0, a_1, a_2, \cdots, a_m\}$ of k voters on the bulletin board;
Step4. If the sum of the published $a_{i,0}$, $(i = 1, 2, \cdots k)$ does not to equal to a_0, *VS* and all candidates are asked to check their publishing information, and reconstruct the polynomial again;
Step5. Everyone computes the result of C_j, $vote_j = \sum a_j$, $(j = 1, 2, \cdots, m)$.

Voting phase and the post-voting phase is shown in Figure 2.

For more easily understand the proposed scheme, we assume that there are 20 voters V_i, $(i = 1, 2, \cdots, 20)$ and 4 candidates C_j, $(j = 1, 2, 3, 4)$, and $p = 29$, $k = 10$. Voters' intention, the random number and the interpolation polynomial is showed in Table 2.

VS generates the shares. The shares and voters' credential are showed in Table 3

Assume that *VS* selects a set with 10 members including V_1,V_3,V_4,V_8,V_9,V_{13},V_{16},V_{18},V_{19}, V_{20}, and they publish their random numbers 3,5,3,5,3,8,12,1,8,9 on the bulletin board.

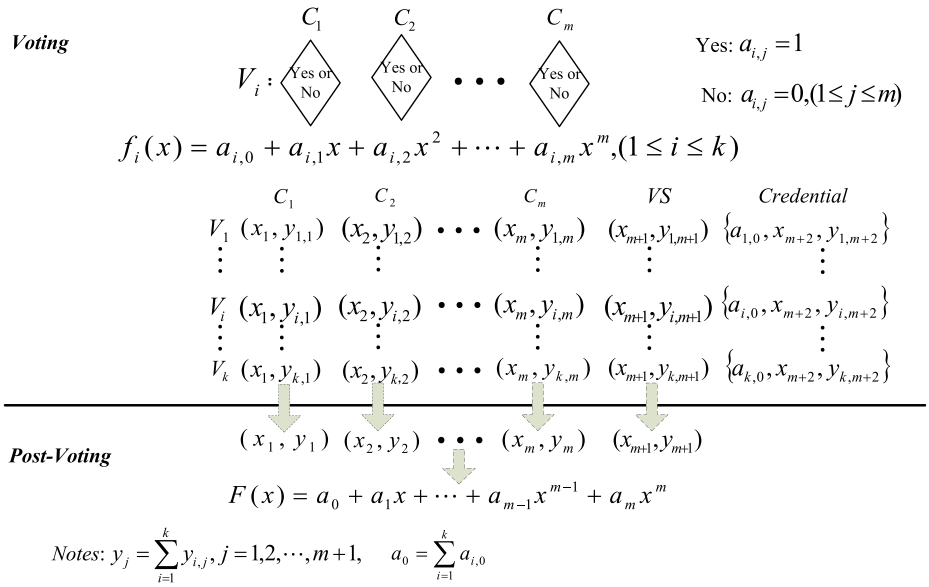

Figure 2 The proposed e-voting scheme

Table 2 Voters' intention, the random number and polynomial

	C_1	C_2	C_3	C_4	*Random number*	*Polynomial*
	$a_{i,1}$	$a_{i,2}$	$a_{i,3}$	$a_{i,4}$	$a_{i,0}$	$f(x)$
V_1	1	0	1	1	3	$f_1(x)=3+x+x^3+x^4$
V_2	0	0	1	0	4	$f_2(x)=4+x^3$
V_3	1	1	0	0	5	$f_3(x)=5+x+x^2$
V_4	0	0	1	0	3	$f_4(x)=3+x^3$
V_5	0	1	0	1	6	$f_5(x)=6+x^2+x^4$
V_6	1	0	1	1	5	$f_6(x)=5+x+x^3+x^4$
V_7	1	0	0	1	2	$f_7(x)=2+x+x^4$
V_8	0	1	0	1	5	$f_8(x)=5+x^2+x^4$
V_9	0	1	1	1	3	$f_9(x)=3+x^2+x^3+x^4$
V_{10}	1	1	0	1	4	$f_{10}(x)=4+x+x^2+x^4$
V_{11}	1	0	0	1	10	$f_{11}(x)=10+x+x^4$
V_{12}	1	0	0	0	9	$f_{12}(x)=9+x$
V_{13}	1	1	1	1	8	$f_{13}(x)=8+x+x^2+x^3+x^4$
V_{14}	0	1	0	1	5	$f_{14}(x)=5+x^2+x^4$
V_{15}	0	0	0	1	6	$f_{15}(x)=6+x^4$
V_{16}	0	1	1	0	12	$f_{16}(x)=12+x^2+x^3$
V_{17}	0	0	0	1	13	$f_{17}(x)=13+x^4$
V_{18}	1	1	0	1	1	$f_{18}(x)=1+x+x^2+x^4$
V_{19}	1	1	0	1	8	$f_{19}(x)=8+x+x^2+x^4$
V_{20}	1	0	0	1	9	$f_{20}(x)=9+x+x^4$

Moreover, the sum of the shares from the V_1,V_3,V_4,V_8,V_9,V_{13},V_{16},V_{18},V_{19},V_{20} is computed by all candidates and *VS*. The sum of the shares is showed in Table 4

After the sum is published, everyone generates a polynomial of degree 4 passing through five points (2,17), (5,13), (8,1), (9,22) and (11,28). Everyone computes the corresponding linear equations:

Table 3 The shares and voters' credential

	C_1	C_2	C_3	C_4	*VS*	*Credential*
$f_1(x)$	(2,0)	(5,4)	(8,8)	(9,23)	(11,7)	{3,1,6}
$f_2(x)$	(2,12)	(5,13)	(8,23)	(9,8)	(11,1)	{4,1,5}
$f_3(x)$	(2,11)	(5,6)	(8,19)	(9,8)	(11,21)	{5,1,7}
$f_4(x)$	(2,11)	(5,12)	(8,22)	(9,7)	(11,0)	{3,1,4}
$f_5(x)$	(2,26)	(5,18)	(8,19)	(9,7)	(11,7)	{6,1,8}
$f_6(x)$	(2,2)	(5,6)	(8,10)	(9,25)	(11,9)	{5,1,8}
$f_7(x)$	(2,20)	(5,23)	(8,17)	(9,18)	(11,9)	{2,1,4}
$f_8(x)$	(2,25)	(5,17)	(8,18)	(9,6)	(11,6)	{5,1,7}
$f_9(x)$	(2,2)	(5,24)	(8,6)	(9,8)	(11,1)	{3,1,6}
$f_{10}(x)$	(2,26)	(5,21)	(8,25)	(9,14)	(11,16)	{4,1,7}
$f_{11}(x)$	(2,28)	(5,2)	(8,25)	(9,26)	(11,17)	{10,1,12}
$f_{12}(x)$	(2,11)	(5,14)	(8,17)	(9,18)	(11,20)	{9,1,10}
$f_{13}(x)$	(2,9)	(5,5)	(8,19)	(9,22)	(11,17)	{8,1,12}
$f_{14}(x)$	(2,25)	(5,17)	(8,18)	(9,6)	(11,6)	{5,1,7}
$f_{15}(x)$	(2,22)	(5,22)	(8,13)	(9,13)	(11,2)	{6,1,7}
$f_{16}(x)$	(2,24)	(5,17)	(8,8)	(9,10)	(11,14)	{12,1,14}
$f_{17}(x)$	(2,0)	(5,0)	(8,20)	(9,20)	(11,9)	{13,1,14}
$f_{18}(x)$	(2,23)	(5,18)	(8,22)	(9,11)	(11,13)	{1,1,4}
$f_{19}(x)$	(2,1)	(5,25)	(8,0)	(9,18)	(11,20)	{8,1,11}
$f_{20}(x)$	(2,27)	(5,1)	(8,24)	(9,25)	(11,16)	{9,1,11}

Table 4 The sum of shares

C_1	C_2	C_3	C_4	VS
(2,17)	(5,13)	(8,1)	(9,22)	(11,28)

$$\begin{cases} a_0 + 2a_1 + 4a_2 + 8a_3 + 16a_4 = 17 \\ a_0 + 5a_1 + 25a_2 + 9a_3 + 16a_4 = 13 \\ a_0 + 8a_1 + 6a_2 + 19a_3 + 7a_4 = 1 \\ a_0 + 9a_1 + 23a_2 + 4a_3 + 7a_4 = 22 \\ a_0 + 11a_1 + 5a_2 + 26a_3 + 25a_4 = 28 \end{cases} \quad (1)$$

Then, they recover the aggregated polynomials $F(x) = 28 + 6x + 7x^2 + 5x^3 + 7x^4$, and VS publishes {28, 6, 7, 5, 7} on the bulletin board. Thereafter, V_1, V_3, V_4, V_8V_9, V_{13}, V_{16}, V_{18}, V_{19}, V_{20} verify if their ballots are counted correctly by checking the eq. $3 + 5 + 3 + 5 + 3 + 8 + 12 + 1 + 8 + 9 = 28$ mod 29. In fact, all participants know that the results of C_1,C_2,C_3,C_4 are respectively 6, 7, 5, 7. After the sum share of another group is posted on the bulletin board, every participant knows that the results of C_1,C_2,C_3,C_4 are respectively 5, 3, 2, 8. Then, every participant computes the sum of each candidate to obtain the votes of C_1,C_2,C_3,C_4, they are respectively 11, 10, 7, 15.

5 Security analysis

The proposed scheme not only satisfies the correctness, unconditional security, anonymity, confidentiality, efficient, and non-cheating, but also achieves the universal verifiability and the coercion-resistance.

5.1 Correctness

V_i recovers the polynomial $f_i(x)$ using the random number on his credential and his intention, verifies if his ballot is correctly counted by checking the equation $y_{i,\ m+2} = f_i(x_{m+2})$, $(i = 1, 2, \cdots, k)$.

In the post-voting phase, k voters publish $a_{1,\ 0}$, $a_{2,\ 0}$, $\cdots$, $a_{k,\ 0}$ on the bulletin board. After recovering the aggregated polynomial $F(x)$, voters verify $a_0 = \sum_{i=1}^{k} a_{i,0}$. If it holds, the result is correct. Therefore, the correctness is achieved.

Scenario1. Nobody knows the voting result before the voting result is published.

Proof Using secret sharing method, no information about the result can be obtained since the polynomial cannot be recovered with fewer than m candidates or VS. Therefore, nobody including candidates and VS can infer any information from his share. The result cannot be known until the polynomials are reconstructed and the coefficients of them are published.

5.2 Anonymity

Anonymity means that nothing about the voter's information is leaked. Actually, *AC* does not know any information about the voter since voter uses a temporary ID in the proposed scheme. Some ballots are aggregated and posted in the post-voting phase, which masks the voter's intention. Hence, the anonymity is achieved.

5.3 Confidentiality

According to V_i 's intention, *VS* generates a polynomial and divides it among m candidates and *VS*, thereafter, *VS* destroys the polynomial. Only m candidates and *VS* can recover the polynomial and get the aggregated ballots together, the content of voters' ballot is confidential before it is published. The single ballot is still confidential after it is published since the aggregated ballots are posted on the bulletin board together, which guarantees the confidentiality.

5.4 Efficiency

The computation in the proposed scheme includes modular, addition and subtraction operation. Without using any complicated cryptography method, the proposed scheme achieves the efficiency requirement.

5.5 Unconditional security

Unconditional security means the security does not rely on the hard problem such as discrete logarithm and integer factorization. In fact, the unconditional security is especially vital for the voting scheme since the voting result should be confidential forever. In the proposed scheme, the shares are divided among the candidates and *VS*. Even if the malicious adversary has enough computing power, he can't infer any information about the vote from some shares. Then, our scheme is unconditional secure.

5.6 Non-cheating

In the post-voting phase, the coefficient of aggregation polynomial will be published on the bulletin board. A dishonest candidate in the set will be detected when $a_0 \neq \sum_{i=1}^{k} a_{i,0}$, then, the shares will be published and reconstructed again.

5.7 Universal verifiability

A polynomial can be recovered by using the random number on voter's credential and his intention. If the polynomial passes through the share $(x_{m+2}, y_{1,\ m+2})$ on his credential, voter believes the credential to reflect his intention. C_j, $(j = 1, 2, \cdots, m)$ verifies if his result is correct by checking $y_j = F(x_j)$, $(j = 1, \cdots, m)$. Everyone verifies that the result is correct by checking $a_0 = \sum_{i=1}^{k} a_{i,0}$. Therefore, the scheme satisfies the universal verifiability.

5.8 Coercion-resistance

Scenario 2. The voter can't prove the content of his ballot to others.

Proof The credential CR_i contains nothing about the intention of the voter. Even if the voter wants to prove his intention to others, he has nothing evidence. For example, V_{17} shows his credential to C_4, and C_4 obtains four polynomials $f_{17}(x) = 13 + x$, $f_{17}(x) = 13 + x^2$, $f_{17}(x) = 13 + x^3$ or $f_{17}(x) = 13 + x^4$, from V_{17} 's credential. Therefore, C_4 does not know whether V_{17} casts him or not. Then, the proposed voting scheme can resist coercion attack.

6 Conclusion

An unconditional secure e-voting scheme is proposed based on Shamir's secret sharing and *k*-anonymity, in which the voting system generates a polynomial according to the intention of the voters, computes and divides the shares among candidates and *VS*. Candidates and *VS* reconstruct the polynomial and aggregate the ballot together. Moreover, the proposed scheme satisfies the correctness, efficiency, unconditional security, non-cheating, universal verifiability, confidentiality, anonymity, coercion-resistance.

Acknowledgments This work was partly supported by National Natural Science Foundation of China under grant No. 61662016, 61363069, Guangxi Key Laboratory of Trusted Software (kx201717), and Foundation of Guizhou Provincial Key Laboratory of Public Big Data.

References

1. Fujiwara, T.: Voting technology, political responsiveness, and infant health: evidence from Brazil. Econometrica. **83**(2), 423–464 (2015)
2. Aggarwal, R., Saffi, P., Sturgess, J.: The role of institutional investors in voting: Evidence from the securities lending market. J. Financ. **70**(5), 2309–2346 (2015)
3. Liaw, H.: A secure electronic voting protocol for general elections. Comput. Secur. **23**(2), 107–119 (2004)
4. Chang, C., Lee, J.: An anonymous voting mechanism based on the key exchange protocol. Comput. Secur. **25**(4), 307–314 (2006)
5. Chaum, D.: Untraceable electronic mail, return addresses and digital pseudonyms. Commun. ACM. **24**(2), 84–90 (1981)
6. Cortier, V., Eigner, F., Kremer, S., et al.: Type-based verification of electronic voting protocols. POST2015. LNCS. **9036**, 303–323 (2015)
7. Grewal, G., Ryan, M., Chen, L., et al.: Du-vote: remote electronic voting with untrusted computers. 2015 I.E. 28th Comput. Secur. Found. Symp. 155–169 (2015)
8. Ryan, P., Schneider, S., Teague, V.: End-to-end verifiability in voting systems, from theory to practice. IEEE Secur. Priv. **13**(3), 59–62 (2015)
9. Cubric, M., Jefferies, A.: The benefits and challenges of large-scale deployment of electronic voting systems: university student views from across different subject groups. Comp. Educ. **87**, 98–111 (2015)
10. Chun, T., Min, S., Chi, Y.: An electronic voting protocol with deniable authentication for mobile ad hoc networks. Comput. Commun. **31**(10), 2534–2540 (2008)
11. Fan, C., Sun, W.: An efficient multi-receipt mechanism for uncoercible anonymous electronic voting. Math. Comput. Model. **48**(9), 1661–1627 (2008)
12. Francesc, S., Josep, M., Miret, J., Jordi, P.: Simple and efficient hash-based verifiable mixing for remote electronic voting. Comput. Commun. **33**(6), 667–675 (2010)
13. Abe, M.: Mix-networks on permutation networks. AsiaCrypt'99. LNCS. **1716**, 258–273 (1999)
14. Jakobsson, M.: A practical mix. International Conference on the Theory and Applications of Cryptographic Techniques. EuroCrypt'98. LNCS. **1403**, 448–461 (1998)
15. Park, C., Itoh, K., Kurosawa, K.: Efficient anonymous channel and all nothing election scheme. Workshop on the Theory and Application of Cryptographic Techniques. EuroCrypt'93. LNCS. **765**, 248–259 (1993)

16. Sako, K., Kilian, J.: Receipt-free mix-type voting scheme. EuroCrypt'95. LNCS. **921**, 393–403 (1995)
17. Benaloh J.: Verifiable secret-ballot elections. Yale University, Department of Computer Science, (1987)
18. Benaloh, J., Tuinstra, D.: Receipt-free secret-ballot elections. Proc. Twenty-Sixth Annu. ACM Symp. Theor. Comput. 544–553 (1994)
19. Cramer, R., Gennaro, R., Schoenmakers, B.: A secure and optimally efficient multi-authority election scheme. Eur. Trans. Telecommun. **8**(5), 481–490 (1997)
20. Cohen J, Fischer M. A robust and verifiable cryptographically secure election scheme. Yale University. Department of Computer Science, (1985)
21. Hirt, M., Sako, K.: Efficient receipt-free voting based on homomorphic encryption. EuroCrypt'2000. LNCS. **1807**, 539–556 (2000)
22. Lee, B., Kim, K.: Receipt-free electronic voting through collaboration of voter and honest verifier. Proc. JW-ISC2000. 101–108 (2000)
23. Malkhi, D., Margo, O., Pavlov, E.: E-voting without cryptography. FC'2002. LNCS. **2357**, 1–15 (2002)
24. Neff, C.: A verifiable secret shuffle and its application to e-voting. CCS'01, ACM. 116–125 (2001)
25. Peng, K., Aditya, R., Boyd, C., et al.: Multiplicative homomorphic e-voting. IndroCrypt'2004. LNCS. **3348**, 61–72 (2004)
26. Sako, K., Kilian, J.: Secure voting using partially compatible homomorphisms. Crypto'94. LNCS. **839**, 411–424 (1994)
27. Camenisch, J., Piveteau, J., Stadler, M., et al.: Blind signatures based on the discrete logarithm problem. EuroCrypt'94. LNCS. **950**, 428–432 (1994)
28. Chaum, D.: Blind signatures for untraceable payments. Crypto'82. 199–203 (1983)
29. Fujioka, A., Okamoto, T., Ohta, K.: A practical secret voting scheme for large scale elections. AusCrypt'92. LNCS. **718**, 244–251 (1992)
30. Ibrahim, S., Kamat, M., Salleh, M., et al.: Secure e-voting with blind signature. NCTT. **2003**, 193–197 (2003)
31. Okamoto, T.: Receipt-free electronic voting schemes for large scale elections. Security Protocols 1997. LNCS. **1361**, 25–35 (1997)
32. Rivest, R.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM. **21**(2), 120–126 (1978)
33. Atreya, M., Paine, S., Hammond, B., et al.: Digital signatures. Osborne/McGraw-Hill, Berkeley (2002)
34. Chaum, D.: Secret-ballot receipts: true voter-verifiable elections. IEEE Secur. Priv. **2**(1), 38–47 (2004)
35. Liu, J., Au, H., Susilo, W., et al.: Linkable ring signature with unconditional anonymity. IEEE Trans. Knowl. Data Eng. **26**(1), 157–165 (2014)
36. Bohli, J., Müller-Quade, J., Röhrich, S.: Bingo voting: secure and coercion-free voting using a trusted random number generator. Vote-ID 2007. LNCS. **4896**, 111–124 (2007)
37. Zhao, Q., Liu, Y.: E-voting scheme using secret sharing and K-anonymity. BWCCA. **2016**, 893–900 (2016). https://doi.org/10.1007/978-3-319-49106-6_91
38. Shamir, A.: How to share a secret. Commun. ACM. **22**(11), 612–613 (1979)
39. Blakley, G.: Safeguarding cryptographic keys. Proc. AFIPS'79 Nat. Comput. Conf. **48**, 313–317 (1979)
40. Mashhadi, S., Dehkordi, M.: Two verifiable multi-secret sharing schemes based on non-homogeneous linear recursion and LFSR public-key cryptosystem. Inf. Sci. **294**, 31–40 (2015)
41. Hadavi, M., Jalili, R., Damian, E., et al.: Security and search ability in secret sharing based data outsourcing. Int. J. Inf. Secur. **14**(6), 513–529 (2015)
42. Harn, L., Lin, C., Li, Y.: Fair secret reconstruction in (t, n) secret sharing. J. Inf. Secur. Appl. **23**, 1–7 (2015)
43. Song, Y., Li, Z., Li, Y., et al.: A new multi-use multi-secret sharing scheme based on the duals of minimal linear codes. Secur Commun. Netw. **8**(2), 202–211 (2015)
44. Benelux, J.: Secret sharing homomorphism: keeping shares of a secret secret. Crypt'86. LNCS. **263**, 251–260 (1986)
45. Kabir, M.E., Wang, H., Bertino, E.: Efficient systematic clustering method for *k*-anonymization. Acta Informatica. **48**(1), 51–66 (2011)
46. Ciriani, V., Vimercati, S., Foresti, S., Samarati, P.: K-anonymity. Secure data management in decentralized systems. Springer US. **33**, 323–353 (2007)
47. Zhang, Y., Chen, Q., Zhong, S.: Privacy-preserving data aggregation in mobile phone sensing. IEEE Trans. Inform. Forensics Secur. **11**(5), 980–992 (2016)
48. Xu, R., Morozov, K., Takagi, T.: On cheater identifiable secret sharing schemes secure against rushing adversary. IWSEC'2013. LNCS. **8231**, 258–271 (2013)
49. Lin, P.: Distributed secret sharing approach with cheater prevention based on QR code. IEEE Trans. Ind. Inform. **12**(1), 384–392 (2016)
50. Chen, Z., Li, S., Zhu, Y., et al.: A cheater identifiable multi-secret sharing scheme based on the Chinese remainder theorem. Secur. Commun. Netw. **8**(18), 3592–3601 (2015)