Hindawi
Security and Communication Networks
Volume 2021, Article ID 5448370, 11 pages
https://doi.org/10.1155/2021/5448370

Research Article

An Improved Coercion-Resistant E-Voting Scheme

Yuanjing Hao, Zhixin Zeng, and Liang Chang

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

Correspondence should be addressed to Liang Chang; changl@guet.edu.cn

Received 16 August 2021; Revised 20 September 2021; Accepted 22 September 2021; Published 18 October 2021

Academic Editor: Chunhua Su

E-voting has gradually replaced the traditional voting methods to make it easier for people to conduct an election. Recently, Liu et al. propose an unconditional secure e-voting scheme using secret sharing and k-anonymity. Their scheme achieves correct tallying results without revealing raw voting information. However, in this paper, we observe that Liu et al.'s scheme cannot achieve coercion resistance in e-voting since the voter can prove the content of his ballot to the colluded candidates. Then, we propose an improved e-voting scheme to cover up the ballot of the voter with masked values. In this way, even if the voter colludes with corresponding candidates, he cannot prove which candidate he has voted for. Moreover, comparing with Liu et al.'s scheme, the security analysis shows that our proposed e-voting scheme achieves these security requirements like the coercion resistance, integrity of ballots, privacy of ballots, multiple-voting detection, and fairness. Through performance analysis, the experimental results show that our proposed e-voting scheme has higher time efficiency. Compared with other schemes, our scheme achieves a complete voting process and obtains the correct tallying result without complex computation and intricate communication process.

1. Introduction

At present, election is regarded as an indispensable democratic activity in real life. Over time, it has been divided into two categories: traditional election and electronic election. The traditional election consumes a lot of time and resources and has low tallying efficiency. Thus, Chaum [1] first proposed the electronic voting scheme in 1981, which eliminates these disadvantages. Subsequently, various e-voting schemes continue to spring up. Recently, cloud technology and blockchain technology are widely used in e-voting to achieve secure electronic election. For the cloud technology, Shankar et al. [2] proposed a secure e-voting protocol, which realizes secure data transfer with cloud effectively. Anjima and Hari [3] proposed a secure cloud e-voting system using fully homomorphic elliptical curve cryptography, which greatly ensures the privacy of ballots and minimizes the risk of the vote being tampered or leaked. Although the cloud technology presents advantages in the application of e-voting, it is less used than blockchain technology. Currently, some e-voting researches related to blockchain have a tendency to increase gradually, such as reducing voter fraud [4], preventing ballot content attacks [5], and achieving the universal verification of ballot [6]. However, the previously mentioned description mainly illustrates the recent development of e-voting, rather than the scope of our study.

In a real election, due to multiparty participation, the voter may sell the content of his ballot to others to obtain profit. Out of curiosity, candidates may collude with other participants to infer the content of the original ballot. Therefore, in practical application, the secure e-voting scheme needs to satisfy some necessary security requirements to protect the privacy of ballot, such as freedom (no one can be forced to cast a certain vote); fairness (no one can use more than his own votes to influence the tallying result); confidentiality (no one can know other voter's content except himself); coercion resistance [7–10] (the voter proves nothing about the content of his ballot to others); verifiability [11, 12] (every voter can verify if his ballot is correctly tallied, and any participant can verify the correctness of tallying result).

For meeting the previously mentioned security requirements, some encryption techniques have been popularly applied to e-voting to achieve secure election, such as mix-net [13–16], blind signature [17–23], homomorphic encryption [24–28], and secret sharing [29–31]. Meanwhile,

due to the high overhead, mix-net is hard to be applied for the actual election. Although blind signature has better practicality in e-voting, it does not satisfy the security requirement of receipt-freeness and verifiability to some extent. At present, in order to achieve secure and feasible e-voting, homomorphic encryption is popular in conjunction with other encryption techniques, such as zero-knowledge proof [32] and partial knowledge proof [33]. However, the computation burden becomes a problem that needs to be solved. Thus, avoiding these disadvantages of above encryption techniques, secret sharing is applied to e-voting because of its better completeness and feasibility and also achieves running time in linear [34]. Based on such advantages, Liu and Zhao [35] recently proposed an e-voting scheme using secret sharing and k-anonymity, which achieves the correct tallying result and satisfies the necessary security requirements. Concretely, the content of one ballot is used to sever as the coefficients of the shared polynomial. The calculated shares are regarded as the encrypted form of one ballot, respectively held by voter, voting system, and all candidates. Then, according to the additive homomorphism of secret sharing, the total number of ballots can be correctly obtained for each candidate. Liu and Zhao [35] declare their e-voting scheme achieves the security requirement of coercion resistance, which means the voter cannot prove the content of his ballot to others.

However, in this paper, we observe that Liu et al.'s scheme cannot achieve the security requirement of coercion resistance. The voter can collude with candidates to prove the content of his ballot. Thus, we propose an improved coercion-resistant e-voting scheme to cover up the content of ballot with masked values, which achieves the security requirement of coercion resistance. Meantime, we also solve the abstention from voting. Additionally, through theoretical analysis and data simulation, we indicate that our proposed e-voting scheme can solve the shortcoming in [35] and has higher time efficiency compared with [32, 33]. Our contributions are shown in details as follows:

(1) In Liu et al.'s scheme [35], all voters and candidates hold shares. The shared polynomial constructed from the original ballot information can be recovered if the voter colludes with corresponding candidates. The voter can prove which candidate he has voted for. Liu et al.'s scheme does not satisfy the coercion-resistant security requirement. Thus, we propose an improved e-voting scheme, which replaces the content of the original ballot with masked values to achieve the construction of the share polynomial. In this way, even if the voter colludes with corresponding candidates to recover the shared polynomial, he cannot prove the content of his ballot to others. The improved e-voting scheme achieves coercion-resistant security requirement.

(2) The improved e-voting scheme considers abstention which Liu et al.'s scheme [35] does not accomplish. In the improved e-voting scheme, voting system constructs the shared polynomial of abstainer only using masked values, and then performs subsequent voting process. Finally, all participants can obtain the correct tallying result.

(3) The security analysis shows that the improved e-voting scheme not only inherits some security requirements in Liu et al.'s scheme [35] but also achieves coercion-resistant security requirement which Liu et al.'s scheme does not satisfy. Moreover, the scheme also achieves additional security properties which consist of the integrity of ballots, the privacy of ballots, multiple-voting detection, and fairness. The performance analysis shows that the proposed e-voting scheme has higher time efficiency when candidates and voters are, respectively, specific number.

The rest of this paper is organized as follows. In Section 2, the steps of Liu et al.'s e-voting scheme are reviewed. The system model and threat model are presented in Section 3. Section 4 proposes our improved e-voting scheme in detail. In Section 5, we state the differences between Liu et al.'s scheme and the improved e-voting scheme. Finally, the system analysis and conclusion are, respectively, presented in Section 6 and Section 7.

2. Review

In this section, Liu et al.'s scheme [35] is reviewed. It mainly consists of three phases: prevoting phase, voting phase, and postvoting phase. And the process of communication is shown in Figure 1.

2.1. Prevoting Phase. Assume that there are n voters and m candidates, respectively. The voters are divided into several sets, and each set contains k voters.

2.2. Voting Phase

Step 1. Each voter $V_i\,(i = 1, \ldots, n)$ registers to a trusted authority centre (AC). Then, the voting system (VS) issues a temporary identity ID_i for each voter, and no one knows the relationship between voter and his temporary identity ID_i.

Step 2. If the candidate $C_j\,(j = 1, \ldots, m)$ is selected by the voter V_i, $a_{i,j} = 1$; otherwise, $a_{i,j} = 0$. Then, VS generates the shared polynomial $f_i(x) = a_{i,0} + a_{i,1}x + a_{i,2}x^2 + \cdots + a_{i,m}x^m \bmod p$ and computes $m + 2$ shares $(x_j, y_{i,j}),\ \ (j = 1, 2, \ldots, m + 2)$ by using the IDs of voter V_i, candidate $C_j\ \ (j = 1, \ldots, m)$ and VS.

Step 3. VS stores the share $(x_{m+1}, y_{i,m+1})$, and then sends shares $(x_j, y_{i,j}),\ \ (j = 1, 2, \ldots, m)$ to corresponding candidate C_j and credential $CR_i = \{a_{i,0}, x_{m+2}, y_{i,m+2}\}$ to the voter V_i.

2.3. Postvoting Phase. In this phase, first, voters are randomly divided into some sets, and each set contains k voters. The process can be briefly described in the following steps:

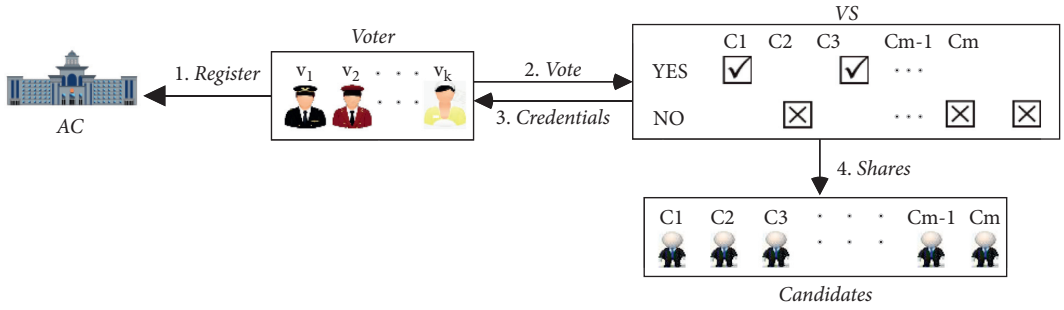

Figure 1: The process of communication.

Step 1. The voters who are located in a set publish their $a_{i,0}$, $(i = 1, \ldots, k)$ on the bulletin board.

Step 2. VS and C_j compute $y_j = \sum_{i=1}^{k} y_{i,j}$ and publish the points (x_j, y_j), $(j = 1, 2, \ldots, m+1)$ on the bulletin board. According to these points, each participant can recover the polynomial $F(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m \bmod p$, where $a_j = \sum_{i=1}^{k} a_{i,j}$, $(j = 0, 1, \ldots, m)$.

Step 3. VS publishes the aggregated ballots $\{a_0, a_1, a_2, \ldots, a_m\}$ of k voters on the bulletin board.

Step 4. The participant verifies the correctness of the aggregated ballots by the equation $a_0 = \sum_{i=1}^{k} a_{i,0}$. If the verification is true, everyone can compute the result of C_j, $\text{vote}_j = \sum a_j$, $(j = 1, 2, \ldots, m)$. Otherwise, all candidates and VS are asked to check their publishing information and reconstruct the polynomial again.

3. The System Model and Threat Model

In this section, the system model, threat model, and design goals are introduced, respectively.

3.1. The System Model. In e-voting system, the participants involved are, respectively, a voter (V), candidate (C), trusted authority centre (AC), voting system (VS), and bulletin board, which is used to publish information in voting process. These participants mainly achieve the following functions:

V: the voter votes for his favourite candidate and obtains the credential from VS

C: the candidate and VS collaborate to get the tallying result together

AC: AC authorizes the legal voter to cast the ballot and takes charge of arbitrating the disputes and granting the digital certificate for each participant

VS: VS generates shares for candidate and credential for voter, respectively; moreover, VS leaks nothing about the intention of the voter

In this paper, the communication model is the same as Liu et al.'s scheme and presented in Figure 1. In the communication model, a legal voter casts his favourite candidate using VS. VS generates corresponding credential for this voter and divides the masked voting intention of this voter into m shares. Then, VS sends credential to this voter and m shares to each candidate C_j $(j = 1, \ldots, m)$.

3.2. The Threat Model. In this section, the threat model is described, mainly embodied in the security issue of Liu et al.'s scheme. Many secure e-voting schemes can ensure the correctness of the tallying result. Meanwhile, Liu et al.'s scheme uses the homomorphic additivity of polynomial to get the correct tallying result. However, in this scheme, the voter can prove the content of his ballot to others. Their scheme cannot resist coercive attack from the internal voter, which cannot achieve coercion-resistant security requirement in e-voting. For the shortcoming in Liu et al.'s scheme, we give a brief example to describe the attack model. Assume that there are four candidates, and their IDs are separately 2, 3, 4, and 5.

3.2.1. Adversary. Assume that V_1 is an internal attacker who launches the coercive attack to prove the content of his ballot to others. Meantime, assume that V_i's ID is 1 and he casts candidates C_1, C_3, C_4, $a_{1,1} = 1, a_{1,2} = 0, a_{1,3} = 1, a_{1,4} = 1$.

3.2.2. Attack Process

(1) First, for simplifying computation, we choose $p = 29$. In voting phase, according to the selection of the voter V_1, VS generates the shared polynomial $f_1(x) = 3 + x + x^3 + x^4 \bmod p$. Then, VS computes four shares (2,0), (3,27), (4,8), and (5,4), which are separately sent to C_1, C_2, C_3, C_4 and one credential $\{3, 1, 6\}$, which is sent to V_1.

(2) After receiving the credential, V_1 colludes with the candidates C_1, C_3, C_4 since he casts the supporting ballot for them. In this way, V_1 can recover the shared polynomial $f_1(x)$ by owned random number 3 and known three shares of candidates C_1, C_3, C_4.

(3) In order to prove the correctness of the recovered polynomial $f_1(x)$, V_1 verifies the recovered polynomial $f_1(x)$ using his share (1,6) and published random number $a_{1,0} = 3$. If the verification is true, the candidates C_1, C_3, C_4 believe that the recovered polynomial $f_1(x)$ is true. In fact, the verification is usually true as long as the calculation is correct.

3.2.3. Attack Result. Through construction of the shared polynomial in Liu et al.'s scheme, we know that the coefficient of the shared polynomial can show whether corresponding candidate obtains the ballot or not. If the coefficient is 1, it shows that the voter casts the candidate whose identity is the same as power of the shared polynomial. Thus, according to the description in attack process, the candidates C_1, C_3, C_4 believe the correctness of the recovered polynomial $f_1(x)$. Naturally, V_1 can prove he cast the supporting ballot for the candidates C_1, C_3, C_4. Liu et al.'s scheme cannot achieve the security requirement of coercion resistance in e-voting.

Therefore, to solve the shortcoming of Liu et al.'s scheme, we propose the improved coercion-resistant e-voting scheme. The scheme not only satisfies the coercion-resistant security requirement but also solves the issue of abstainers. The specific process is presented in section 4.

3.3. Design Goals. For the design goals, we mainly introduce some necessary security requirements, which needs to be satisfied in next proposed e-voting scheme. These security requirements include coercion resistance, which Liu et al.'s scheme does not achieve and other additional security requirements, which are integrity of ballots, privacy of ballots, multiple-voting detection, and fairness.

(i) Coercion resistance: no one voter can prove to others which candidate he has voted for.

(ii) Integrity of ballots: in order to obtain correct tallying result, the ballots of all voters involved in the voting process should be counted validly.

(iii) Privacy of ballots: no one participant can leak any voting information.

(iv) Multiple-voting detection: a legal voter only can cast ballot once. If a voter votes for more than once, the superfluous ballots should be detected.

(v) Fairness: no one candidate can know his own ballot in advance.

4. The Improved Voting Scheme

In this section, we present the improved e-voting scheme in detail. We first suppose that the trust assumptions are the same as [35]. The improved e-voting scheme consists of four phases: prevoting phase, voting phase, postvoting phase, and abstention from voting. Meanwhile, all computations are over a finite field F_p, where p is a secure prime, which is published by AC before the prevoting phase. The list of symbols used in the improved e-voting scheme is shown in Table 1, and Figure 2 shows the specific voting process in voting phase, postvoting phase, and abstention from voting.

4.1. Prevoting Phase. Assume that there are n voters $V_1, \ldots, V_n$ and m candidates $C_1, \ldots, C_m$.

4.2. Voting Phase. In this phase, the session keys are negotiated freely among voters, and VS computes the masked values. Then, each voter casts his favourite candidates and gets the credential in a face-to-face way. The process is described as follows:

Step 1. Every voter V_i, $(i = 1, 2, \ldots, n)$ registers to AC. VS generates a temporary identity ID_i, $(i = 1, 2, \ldots, n)$ for V_i, and no one knows the relationship between V_i and ID_i.

Step 2. V_i negotiates session key k_{ij}, $(i, j \in \{i = 1, 2, \ldots, n\}, i \neq j)$ with other $\beta_i \in \{i = 1, 2, \ldots, n-1\}$ voters in a set and then obtains his session key list $\{k_{i1}, k_{i2}, \ldots, k_{i\beta_i}\}$. For example, there are three voters $\{V_1, V_2, V_3\}$ in a set, V_1 and V_2 share the session key k_{12}, and V_1 and V_3 share the session key k_{13}. Then, V_1, V_2, and V_3 can, respectively, obtain their session key lists $\{k_{12}, k_{13}\}$, $\{k_{21}\}$, and $\{k_{31}\}$, where $k_{12} = k_{21}$, $k_{13} = k_{31}$.

Step 3. V_i sends his session key list to VS via a secure channel. VS computes $\lambda_{i,l} = \sum_{j=1, j\neq i}^{\beta_i} (ID_i - ID_j) H(k_{ij} | l)$, $(i \in \{i = 1, 2, \ldots, n\}, l \in \{i = 1, 2, \ldots, m\})$ and then divides $\lambda_{i,l} = \sum_{j=1}^{n} b_{l,j}$, where H: $Z_p^* \longrightarrow Z_p^*$ is a secure cryptographic hash function, which is published and $b_{l,1}, b_{l,2}, \ldots, b_{l,n}$ are n random numbers. Afterwards, VS computes masked values $\sum_{j=1}^{n} b_{1,i} = B_{1,i}, \sum_{j=1}^{n} b_{2,i} = B_{2,i}, \ldots, \sum_{j=1}^{n} b_{m,} \; i = B_{m,i}$, $(i = 1, 2, \ldots, n)$. Meanwhile, the masked values of the voter V_i can be represented as the list $\{B_{1,i}, B_{2,i}, \ldots, B_{m,i}\}$.

Step 4. V_i casts his favourite candidates. If the candidate C_j $(j = 1, \ldots, m)$ is selected, $a_{i,j} = 1$; otherwise, $a_{i,j} = 0$. According to the computation of masked values for the voter V_i, VS constructs the shared polynomial $f_i(x) = a_{i,0} + (B_{1,i} + a_{i,1})x + (B_{2,i} + a_{i,2})\, x^2 + \cdots + (B_{m,i} + a_{i,m})\, x^m \bmod p$, where $a_{i,0} \neq 0$ is a random number.

Step 5. Assume that the IDs of candidates C_j $(j = 1, \ldots, m)$, the voter V_i, and VS are, respectively, x_j, x_{m+1} and x_{m+2}. VS computes $m + 2$ shares $(x_j, y_{i,j})$, $(j = 1, 2, \ldots, m + 2)$ by the polynomial in Step 4. Then, VS stores the share $(x_{m+1}, y_{i,m+1})$ and sends shares $(x_j, y_{i,j})$, $(j = 1, 2, \ldots, m)$ to corresponding candidates C_j $(j = 1, \ldots, m)$ and credential $CR_i = \{a_{i,0}, x_{m+2}, y_{i,m+2}\}$ to the voter V_i.

4.3. Postvoting Phase. In this phase, VS and all candidates reconstruct polynomial together by the sum of shares, and each participant can obtain the correct tallying result by verifying the constant coefficient of the reconstructed polynomial. The steps are given as follows:

Step 1. All voters are published, and each voter V_i, $(i = 1, 2, \ldots, n)$ publishes their $a_{i,0}$, $(i = 1, 2, \ldots, n)$ on the bulletin board.

Step 2. VS and C_j compute $y_j = \sum_{i=1}^{n} y_{i,j}$and publish the points (x_j, y_j), $(j = 1, 2, \ldots, m + 1)$. Then, each participant can recover the polynomial $F(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m \bmod p$, where $a_j = \sum_{i=1}^{n} a_{i,j}$, $(j = 0, 1, \ldots, m)$. Finally, VS publishes the aggregated ballots $\{a_1, a_2, \ldots, a_m\}$ of n voters on the bulletin board.

Table 1: List of notations.

Symbol	Significance
n	The number of voters
m	The number of candidates
V_i	i-th voter
C_j	j-th candidate
ID_i	Temporary identification of V_i, $(i \in \{1, 2, \ldots, n\})$
k_{ij}	Session key of V_i, $(i \in \{1, 2, \ldots, n\})$
β_i	The number of session keys negotiated with V_i, $(i \in \{1, 2, \ldots, n\})$
$\lambda_{i,l}$	A value can be used to compute masked values
$B_{j,i}$	j-th masked value of the i-th shared polynomial
$a_{i,j}$	A ballot from V_i, $(i \in \{1, 2, \ldots, n\})$ for C_j, $(j \in \{1, 2, \ldots, m\})$
$(x_j, y_{i,j})$	The shares computed by the i-th shared polynomial
CR_i	The credential of V_i, $(i \in \{1, 2, \ldots, n\})$
y_j	The sum of shares computed by C_j, $(j \in \{1, 2, \ldots, m\})$
a_j	The total number of ballots for C_j, $(j \in \{1, 2, \ldots, m\})$

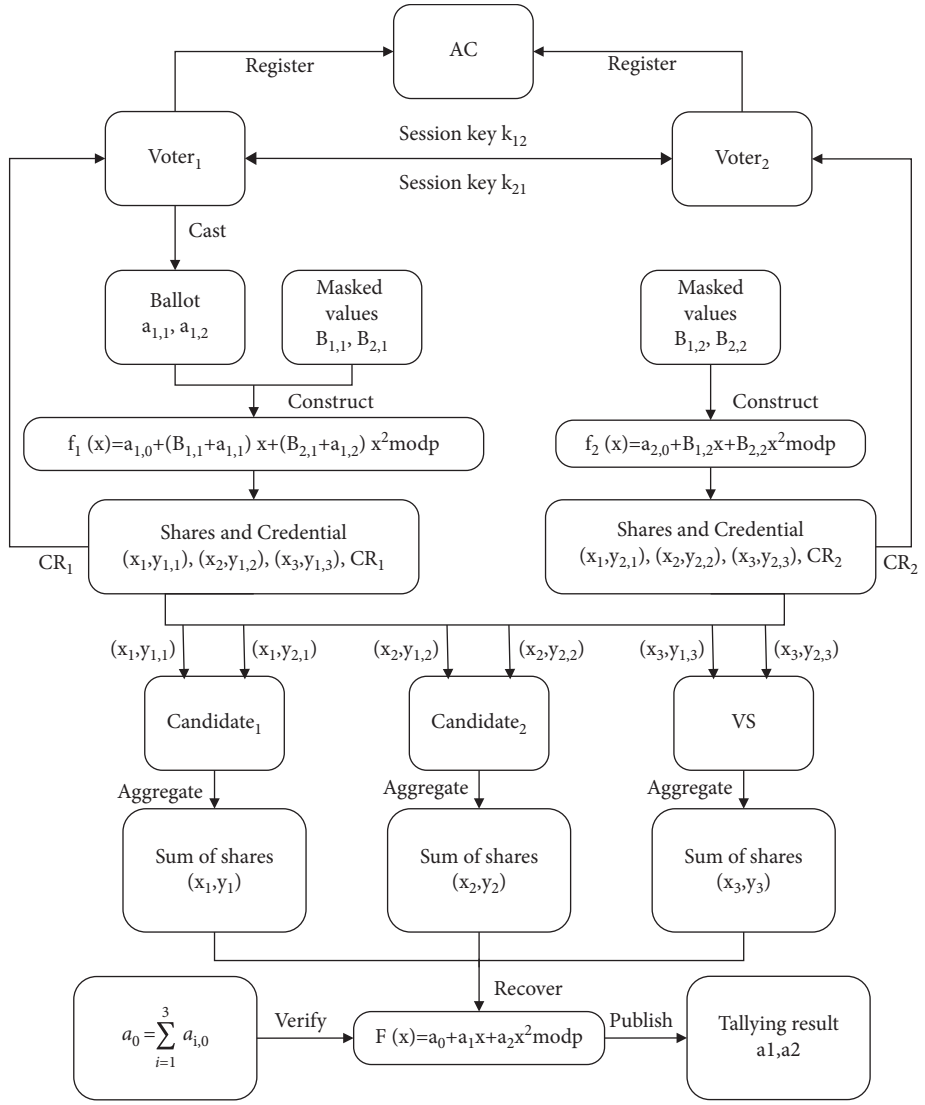

Figure 2: The voting phase, postvoting phase, and abstention from voting of two voters and two candidates in the improved e-voting system. Assume the Voter_2 abstains from voting.

Step 3. Each participant verifies the correctness of the aggregated ballots by the equation $a_0 = \sum_{i=1}^{n} a_{i,0}$. If the verification is not true, VS and all candidates are asked to check their publishing information and reconstruct the polynomial again.

4.4. Abstention from Voting. In the real-life case, abstention from voting is widespread. For obtaining the correct tallying result, when there are abstainers in voting phase, VS sets their ballots as 0 and then constructs the shared polynomials only using the masked values. In proposed e-voting scheme, if the candidate C_j, $(j \in \{1, \ldots, m\})$ obtains the supporting ballot of the voter V_i, $(i \in \{1, 2, \ldots, n\})$, $a_{i,j} = 1$. For one abstainer, it can consider that all candidates do not get the supporting ballot from the abstainer. VS sets $a_{i,j} = 0$, $(i \in \{1, 2, \ldots, n\}, j = 1, \ldots, m)$. In this way, the voting system not only ensures the normal voting process but also does not make a difference for the voting result. Therefore, the improved e-voting scheme solves the issue of abstainers and guarantees the correctness of the tallying result.

5. Differences of Two Schemes

In this section, the differences are expounded between Liu et al.'s scheme [35] and the improved e-voting scheme. We describe these differences in terms of the following five security requirements:

Coercion resistance: coercion resistance means that no one voter can prove the content of his ballot to others. The requirement is described from the aspect of the voter. When the voter acts as an internal attacker, he cannot disclose the content of the original ballot. In Liu et al.'s scheme, VS constructs the shared polynomial with the ballot of one voter. However, if this voter colludes with at most m candidates, he can recover the shared polynomial to disclose the content of the original ballot and prove which candidate he has voted for. Therefore, Liu et al.'s scheme cannot resist the coercive attack from the internal voter. In the improved e-voting scheme, the masked values are computed and added to the coefficients of the original shared polynomial. In this way, even if the voter recovers the shared polynomial, he also cannot prove the content of his ballot to others. The improved e-voting scheme achieves the security requirement of coercion resistance.

Abstention from voting: in a real election, there are voters who may abstain from voting. In Liu et al.'s scheme, all voters take part in the election. Liu et al.'s scheme does not consider the issue of the abstainer. However, in the improved e-voting scheme, for an abstainer, we set his ballot as 0. In this way, all candidates cannot obtain the supporting ballot from the abstainer, which ensures the correctness of tallying result. Therefore, comparing Liu et al.'s scheme, the improved e-voting scheme considers the issue of abstainer and can obtain the correct tallying result.

Privacy: in Liu et al.'s scheme, the voter can reveal the content of his ballot by colluding with some candidates. The scheme does not meet the privacy requirement in e-voting. However, in the improved e-voting scheme, the computation of the masked values prevents the voter from revealing the content of his ballot. Moreover, the participant can only obtain the tallying result by recovering the polynomial in postvoting phase. Thus, the improved e-voting scheme satisfies the privacy requirement of ballot.

Security: security means that the voting scheme does not rely on the hard problem, such as discrete logarithm and integer factorization, and still can achieve the confidentiality of the voting process. This requirement is described from the aspect of the voting scheme. Without additionally complex conditions, the voting scheme can resist attacks from external and internal adversaries, respectively, and achieve the confidentiality of the original ballot. In Liu et al.'s scheme, it shows that the malicious adversary cannot obtain any voting information from some shares. In fact, according to the executive process of secret sharing, Liu et al.'s scheme does not achieve the confidentiality of the original ballot. First, as described in the security requirement of the coercion resistance, Liu et al.'s scheme cannot resist the coercive attack from an internal adversary. Second, since the number of shareholders exceeds the threshold m of secret sharing in Liu et al.'s scheme. Likewise, Liu et al.'s scheme is also hard to prevent external adversary from obtaining the content of the original ballot. Thus, Liu et al.'s scheme cannot guarantee the requirement of security. However, in the improved e-voting scheme, the shares cannot be served as an advantage for adversary to reveal the content of the original ballot. The improved e-voting scheme guarantees the confidentiality of original ballot forever, which achieves the requirement of security.

Fairness: fairness means that no one can know the ballot information in advance. In Liu et al.'s scheme, the voter can prove the content of his ballot to corresponding some candidates. In this way, these candidates can know partial ballots in advance. Liu et al.'s scheme does not satisfy the fairness requirement in e-voting. However, in the improved e-voting scheme, no one can know any ballot information in advance, and the correct tallying result can be obtained simultaneously by each participant. The improved e-voting scheme achieves the fairness requirement.

6. System Analysis

The system analysis includes the security analysis and the performance analysis.

6.1. Security Analysis. The improved e-voting scheme inherits these security requirements, which are correctness, anonymity, confidentiality, efficiency, noncheating, and

universal verifiability in Liu et al.'s scheme [35]. Moreover, the improved e-voting scheme also achieves coercion-resistant security requirement, which Liu et al.'s scheme does not accomplish by adding masked values to the coefficients of the original shared polynomial. In this way, the content of one ballot can be protected, and corresponding privacy requirement can also be satisfied. Meantime, the improved e-voting scheme considers the abstention from voting, which not only ensures the correct tallying result but also achieves integrity of ballots.

In the following part of this section, we give theoretical analysis and proof of the integrity of ballots, privacy of ballots, multiple-voting detection, fairness, and coercion resistance of the improved e-voting scheme.

6.1.1. Integrity of Ballots

Theorem 1. *For voters who submit the session key list, VS should hold their voting information to ensure the integrity of ballots and then achieve the correct tallying result.*

Proof. In a real election, the registered voter may give up casting his ballot. In the proposed e-voting system, assume that a voter V_t, $(t \in \{1, 2, \ldots, n\})$ gives up voting for a ballot after submitting the session key list to VS.

For simplifying analysis, assume that separately negotiates the session key with the remaining voters in voting phase. First, VS computes and divides λ as follows:

$$\begin{cases} \lambda_{1,1} = \left(-H\left(k_{12}|1\right)\right) + \cdots + (1-t)H\left(k_{1t}|1\right) + \cdots + (1-n)H\left(k_{1n}|1\right) = b_{1,1} + \cdots + b_{1,t} + \cdots + b_{1,n}, \\ \cdots, \\ \lambda_{1,m} = \left(-H\left(k_{12}|m\right)\right) + \cdots + (1-t)H\left(k_{1t}|m\right) + \cdots + (1-n)H\left(k_{1n}|m\right) = b_{m,1} + \cdots + b_{m,t} + \cdots + b_{m,n}, \\ \vdots, \\ \vdots, \\ \lambda_{n,1} = (n-1)H\left(k_{n1}|1\right) = b_{1,1} + \cdots + b_{1,t} + \cdots + b_{1,n}, \\ \cdots, \\ \lambda_{n,m} = (n-1)H\left(k_{n1}|1\right) = b_{m,1} + \cdots + b_{m,t} + \cdots + b_{m,n}. \end{cases} \tag{1}$$

Equation (1) shows $\sum_{i=1}^{n} \lambda_{i,l} = 0$, $(l \in \{1, 2, \ldots, m\})$. Then, VS computes the masked values $B_{1,i} = \sum_{j=1}^{n} b_{1,i}, \ldots, B_{m,i} = \sum_{j=1}^{n} b_{m,i}$, $(i = 1, 2, \ldots, n)$.

For the abstainer V_t, $(t \in \{1, 2, \ldots, n\})$, if VS does not construct his shared polynomial, and the sum of shares can be computed as

$$\begin{aligned} &\left\{ \sum_{i=1, i\neq t}^{n} f_i(x) = \sum_{i=1, i\neq t}^{n} a_{0,i} + \left(\sum_{i=1}^{n} \lambda_{i,1} - \sum_{j=1}^{n} b_{1,t} + \sum_{j=1}^{n} a_{i,1} \right) x + \cdots + \left(\sum_{i=1}^{n} \lambda_{i,m} - \sum_{i=1}^{n} b_{m,t} + \sum_{i=1, i\neq t}^{n} a_{i,m} \right) x^m \bmod p \right. \\ &\quad = \sum_{i=1, i\neq t}^{n} a_{0,i} + \left(\sum_{j=1}^{n} b_{1,t} + \sum_{i=1, i\neq t}^{n} a_{i,1} \right) x + \cdots + \left(-\sum_{j=1}^{n} b_{m,t} + \sum_{i=1, i\neq t}^{n} a_{i,m} \right) x^m \bmod p. \end{aligned} \tag{2}$$

According to secret sharing homomorphism, the tallying result is $-\sum_{j=1}^{n} b_{1,t} + \sum_{i=1, i\neq t}^{n} a_{i,1}, \ldots, -\sum_{j=1}^{n} b_{m,t} + \sum_{i=1, i\neq t}^{n} a_{i,m}$, instead of $\sum_{i=1, i\neq t}^{n} a_{i,1}, \ldots, \sum_{i=1, i\neq t}^{n} a_{i,m}$.

Thus, in order to obtain the correct tallying result, VS should ensure the integrity of ballots. In our voting system, VS sets the ballot of abstainer V_t as 0 and constructs the shared polynomial $f_t(x) = a_{t,0} + \sum_{j=1}^{n} b_{1,t} x + \cdots + \sum_{j=1}^{n} b_{m,t} x^m \bmod p$. In this way, the sum of shares is $\sum_{i=1}^{n} f_i(x) = \sum_{i=1}^{n} a_{0,i} + \sum_{i=1}^{n} a_{i,1} x + \cdots + \sum_{i=1}^{n} a_{i,m} x^m \bmod p$. The ballot of V_t is 0. Therefore, the tallying result is $\sum_{i=1}^{n} a_{i,1} = \sum_{i=1, i\neq t}^{n} a_{i,1}, \ldots, \sum_{i=1}^{n} a_{i,m} = \sum_{i=1, i\neq t}^{n} a_{i,m}$.

To sum up, in a real election, abstention from voting needs to be considered to ensure the integrity of ballots and obtain the correct tallying result. □

6.1.2. Privacy of Ballots

Theorem 2. *No one voter or candidate can reveal any voting information.*

Proof. In proposed voting scheme, assume the voter V_k, $(k \in \{1, 2, \ldots, n\})$ colludes with m candidates after receiving credential and then recovers the shared polynomial $f_k(x) = a_{k,0} + (\sum_{j=1}^{n} b_{1,k} + a_{k,1})x + \cdots + (\sum_{j=1}^{n} b_{m,k} + a_{k,m})x^m \bmod p$. However, the voting information $a_{k,1}, \ldots, a_{k,m}$ cannot be revealed because of the masked values $\sum_{j=1}^{n} b_{1,k}, \ldots, \sum_{j=1}^{n} b_{m,k}$. Therefore, in the proposed e-voting scheme, even if a voter or candidate has enough computing power, he also cannot reveal any voting

information. The scheme achieves the privacy requirement of ballots. □

6.1.3. Multiple-Voting Detection

Theorem 3. *A legal voter only can submit ballot to VS once.*

Proof. In the proposed e-voting system, assume the legal voter V_h, ($h \in \{1, 2, \ldots, n\}$) submits ballot to VS twice. In this way, VS can construct two shared polynomials $f_{h1}(x)$ and $f_{h2}(x)$ for V_h according to twice different submissions. Then, the voter V_h can receive two credentials, and each candidate can receive $n+1$ shares. However, according to the computation of the sum of shares in postvoting phase, each candidate only can hold n shares. Moreover, when all voters are published, each candidate can discover that the number of received shares is not equal to n. Thus, the multiple-voting is detected for the voter V_h. The improved e-voting scheme satisfies the requirement that a legal voter casts a ballot once. □

6.1.4. Fairness

Theorem 4. *No one candidate can know his own ballot in advance.*

Proof. For knowing the voting information about himself, the candidate is willing to collude with one voter to reveal the content of one ballot after receiving shares. However, in the proof of Theorem 2, it shows that no one voter can leak any privacy of ballots. Thus, it is impossible for one candidate to know the content of the single ballot in advance. Moreover, in postvoting phase, the sums of shares are published on the bulletin board, and any participant can obtain the tallying result. Therefore, the improved e-voting scheme achieves the requirement of fairness in e-voting. □

6.1.5. Coercion Resistance

Theorem 5. *No one voter can prove the content of his ballot to others.*

Proof. In voting phase, assume that VS constructs the shared polynomial $f_e(x) = a_{e,0} + (B_{1,e} + a_{e,1})x + (B_{2,e} + a_{e,2})x^2 + \cdots + (B_{m,e} + a_{e,m})x^m \bmod p$ for the voter V_e, ($e \in \{1, 2, \ldots, n\}$), and computes shares $(ID_{C_1}, f_e(ID_{C_1})), \ldots, (ID_{C_m}, f_e(ID_{C_m}))$, $(ID_{VS}, f_e(ID_{VS}))$ and credential $\{a_{e,0}, ID_e, f_e(ID_e)\}$. The shares $(ID_{C_1}, f_e(ID_{C_1})), \ldots, (ID_{C_m}, f_e(ID_{C_m}))$ are sent to corresponding candidates $C_1, \ldots, C_m$, and the credential $\{a_{e,0}, ID_e, f_e(ID_e)\}$ is sent to the voter V_e. For proving the content of the ballot, it is most likely for V_e to recover the shared polynomial $f_e(x)$ by colluding with m candidates. However, different from the Liu et al.'s scheme [35], the improved e-voting scheme masks the relationship between coefficient of shared polynomial and voting information. Even if the voter V_e recovers the shared polynomial $f_e(x)$, he cannot prove his voting intention $a_{e,1}, \ldots, a_{e,m}$ to others. Thus, the scheme achieves the security requirement of coercion resistance. □

6.2. Performance Analysis. In this section, the performance of our proposed e-voting system is analysed. The prevoting phase has no computation, which only distributes the numbers of the voters and candidates. Thus, we mainly analyse the computation cost of the voting phase and postvoting phase. In addition, we compare our scheme with [32, 33, 35] for partial security requirement and computation complexity, which is shown in Table 2. Moreover, we also, respectively, test the total time cost for the different numbers of voters and candidates by using the 1024-bit session key and the 512-bit shared secret on a laptop with Intel i5 3.1 GHz CPU and 8.00 GB memory, and the result is shown in Figures 3 and 4.

6.2.1. Performance Analysis of the Voting Phase. In the voting phase, the five steps are as follows: registering identification for voters, negotiating session keys among voters, generating masked values, constructing shared polynomials, and computing shares. Meanwhile, the computation cost mainly concentrates upon generating masked values and computing shares. Assume that the computation costs of one masked value and one share are separately expressed as $\text{cost}_{\text{mask}}$ and $\text{cost}_{\text{share}}$. The total computation cost in this phase can be expressed as $\text{cost}_{\text{voting\_phase}} = n \cdot m \cdot \text{cost}_{\text{mask}} + n \cdot (m+2) \cdot \text{cost}_{\text{share}}$.

6.2.2. Performance Analysis of the Postvoting Phase. In postvoting phase, VS and candidates are responsible for computing the sum of shares and then publish. Each participant reconstructs a polynomial to obtain the tallying result and then verifies it. Meanwhile, computing the sum of shares, recovering polynomial, and verifying the tallying result are the main computation cost in this phase. Assume that they are separately expressed as $\text{cost}_{\text{share\_sum}}$, $\text{cost}_{\text{recover}}$, and $\text{cost}_{\text{verify}}$. The total computation cost in this phase is $\text{cost}_{\text{post\_voting}} = (m+1) \cdot \text{cost}_{\text{share\_sum}} + \text{cost}_{\text{recover}} + \text{cost}_{\text{verify}}$.

From the previously mentioned analysis of two phases, the total computation cost is $\text{cost}_{\text{total}} = \text{cost}_{\text{voting\_phase}} + \text{cost}_{\text{post\_voting}}$ in the improved e-voting scheme and increases with the numbers of voters and candidates. Thus, the computation complexity is $O(nm)$ in the improved e-voting scheme. In Table 2, it shows that our e-voting scheme simultaneously achieves privacy, verifiability, and coercion resistance, and the computation complexity is less than that mentioned in [32] due to $m \ll n$.

In Figure 3, we select $m = 5$ candidates to test the total time cost with different numbers of voters. As shown in Figure 3, the total time cost of the improved e-voting scheme is slightly higher than the scheme [35]. Liu et al.'s scheme [35] is unaffected by the numbers of voters. Therefore, it has an advantage in total time cost. However, it cannot achieve the security requirement of coercion resistance in e-voting. Although the improved e-voting scheme increases the total

Table 2: Comparison of partial security requirement and computation complexity.

Performance	[35]	[32]	[33]	Our scheme
Privacy	No	Yes	Yes	Yes
Coercion resistance	No	No	No	Yes
Verifiability	Yes	Yes	Yes	Yes
Computation complexity	$O(nm)$	$O(\text{nlogn})$	$O(nm)$	$O(nm)$

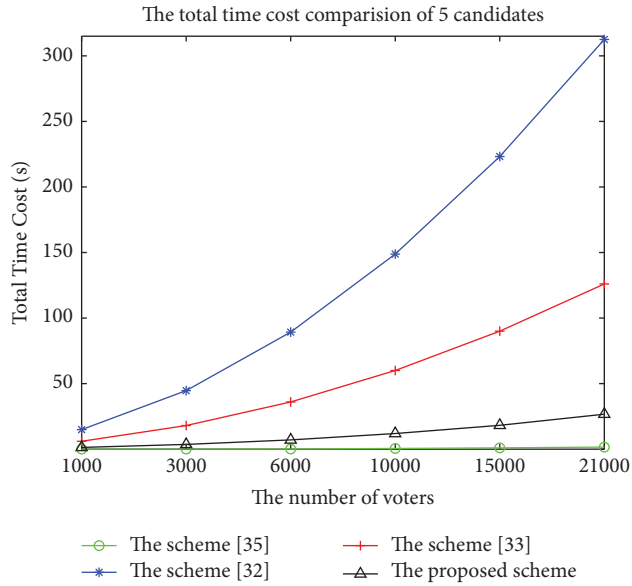

Figure 3: The total time cost comparison for four schemes in the case of five candidates: the number of voters is, respectively, 1000, 3000, 6000, 10000, 15000, and 21000.

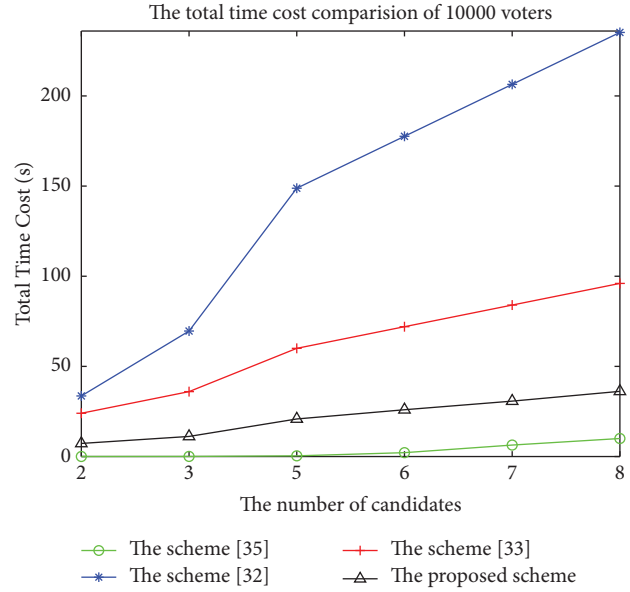

Figure 4: The total time cost comparison for four schemes in the case of 10000 voters: the number of candidates is, respectively, 2, 3, 5, 6, 7, and 8.

time cost, it achieves the coercion-resistant security requirement. Moreover, comparing [32, 33], the improved e-voting scheme takes less time overall.

In Figure 4, we select $n = 10000$ voters to test the total time cost with different numbers of candidates. As shown in Figure 4, both the improved e-voting scheme and the scheme [35] increase with the numbers of candidates in the total time cost. Similarly, the total time cost of the improved e-voting scheme is slightly higher than the scheme [35]. In order to achieve the security requirement of coercion resistance, the improved e-voting scheme adds masked values on the basis of the scheme [35]. Thus, the computation cost is higher than Liu et al.'s scheme [35]. However, the total time consumption is still smaller than those in [32, 33].

7. Conclusions

In this paper, we first show that the e-voting scheme recently proposed by Liu et al. in [35] suffers from the coercive attack by internal voter. Then, we proposed an improved e-voting scheme to achieve coercion resistance and solve abstention from voting. Different from the scheme proposed by Liu et al., the improved e-voting scheme uses the sum of the masked value and the value of the original ballot to achieve the construction of shared polynomial. The scheme prevents malicious voter proving the content of his ballot to others, which achieves the security requirement of coercion resistance. Besides, VS sets the ballot of the abstainer as 0, and correct tallying result can be obtained in subsequent voting process. Moreover, theoretical analysis shows that our proposed scheme not only inherits all security requirements of Liu et al.'s scheme but also achieves the integrity of ballots, privacy of ballots, multiple-voting detection, and fairness. The performance evaluation results also indicate our scheme can achieve higher efficiency than other e-voting schemes in terms of total time consumption. In future, with the increasing application of blockchain, we are going to combine blockchain technology to propose novel and secure e-voting scheme.

Data Availability

All data generated or analysed during this study are included in this published article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this study.

Acknowledgments

This work was supported by the Natural Science Foundation of China (grant nos. 61966009, U1811264, U1711263, and 62072133) and Natural Science Foundation of Guangxi Province (grant nos. 2018GXNSFDA281045 and 2018GXNSFD A281040). The authors would like to thank everyone for the guidance of paper writing.

References

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

[2] A. Shankar, P. Pandiaraja, K. Sumathi, T. Stephan, and P. Sharma, "Privacy preserving E-voting cloud system based on ID based encryption," *Peer-to-Peer Networking and Applications*, vol. 14, no. 4, pp. 2399–2409, 2021.

[3] V. S. Anjima and N. N. Hari, "Secure cloud e-voting system using fully homomorphic elliptical curve cryptography," in *Proceedings of the 2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, pp. 858–864, Secunderabad, India, June 2019.

[4] N. Kshetri and J. Voas, "Blockchain-Enabled E-voting," *IEEE Software*, vol. 35, no. 4, pp. 95–99, 2018.

[5] S. Panja and B. Roy, "A secure end-to-end verifiable e-voting system using blockchain and cloud server," *Journal of Information Security and Applications*, vol. 59, Article ID 102815, 2021.

[6] S. Zhang, L. Wang, and H. Xiong, "Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability," *International Journal of Information Security*, vol. 19, no. 3, pp. 323–341, 2020.

[7] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in *Towards Trustworthy Elections: New Directions in Electronic Voting*, D. Chaum, M. Jakobsson, R. L. Rivest et al., Eds., Springer Berlin Heidelberg, Berlin, Germany, 2010.

[8] O. Spycher, R. Koenig, R. Haenni, and M. Schläpfer, "A new approach towards coercion-resistant remote E-voting in linear time," in *Financial Cryptography and Data Security*, G. Danezis, Ed., pp. 182–189, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[9] P. Grontas, A. Pagourtzis, A. Zacharakis, and B. Zhang, "Towards everlasting privacy and efficient coercion resistance in remote electronic voting," in *Financial Cryptography and Data Security*, A. Zohar, I. Eyal, V. Teague et al., Eds., pp. 210–231, Springer Berlin Heidelberg, Berlin, Germany, 2019.

[10] P. Grontas, A. Pagourtzis, and A. Zacharakis, "Coercion resistance in a practical secret voting scheme for large scale elections," in *Proceedings of the 2017 14th International Symposium on Pervasive Systems, Algorithms and Networks & 2017 11th International Conference on Frontier of Computer Science and Technology & 2017 Third International Symposium of Creative Computing (ISPAN-FCST-ISCC)*, pp. 514–519, Exeter, United Kingdom, June 2017.

[11] A. Kiayias, T. Zacharias, and B. Zhang, "An efficient E2E verifiable E-voting system without setup assumptions," *IEEE Security & Privacy*, vol. 15, no. 3, pp. 14–23, 2017.

[12] R. Küsters, J. Liedtke, J. Müller, D. Rausch, and A. Vogt, "Ordinos: a verifiable tally-hiding E-voting system," in *Proceedings of the 2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 216–235, Genoa, Italy, September 2020.

[13] C. A. Neff, "A verifiable secret shuffle and its application to E-voting," in *Proceedings of the 8th ACM Conference on Computer and Communications Security*, pp. 116–125, Association for Computing Machinery, Philadelphia, PA, USA, November 2001.

[14] X. Boyen, T. Haines, and J. Müller, "A verifiable and practical lattice-based decryption mix net with external auditing," in *Computer Security – ESORICS 2020*, L. Chen, N. Li, K. Liang,

and S. Schneider, Eds., Springer International Publishing, New York, NY, USA, pp. 336–356, 2020.

[15] N. Islam, K. M. R. Alam, S. Tamura, and Y. Morimoto, "A new e-voting scheme based on revised simplified verifiable re-encryption mixnet," in *Proceedings of the 2017 International Conference on Networking, Systems and Security (NSysS)*, pp. 12–20, Dhaka, Bangladesh, December 2017.

[16] C. Culnane, A. Essex, S. J. Lewis, O. Pereira, and V. Teague, "Knights and knaves run elections: internet voting and undetectable electoral fraud," *IEEE Security & Privacy*, vol. 17, no. 4, pp. 62–70, 2019.

[17] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds., pp. 199–203, Springer, Boston, MA, USA, 1983.

[18] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale elections," in *Advances in Cryptology — AUSCRYPT '92*, J. Seberry and Y. Zheng, Eds., Springer Berlin Heidelberg, Berlin, Germany, pp. 244–251, 1993.

[19] X. Chen, Q. Wu, F. Zhang et al., "New receipt-free voting scheme using double-trapdoor commitment☆," *Information Sciences*, vol. 181, no. 8, pp. 1493–1502, 2011.

[20] M. Kumar, S. Chand, and C. P. Katti, "A secure end-to-end verifiable internet-voting system using identity-based blind signature," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2032–2041, 2020.

[21] M. Kumar, C. P. Katti, and P. C. Saxena, "A secure anonymous E-voting system using identity-based blind signature scheme," in *Information Systems Security*, R. K. Shyamasundar, V. Singh, and J. Vaidya, Eds., Springer International Publishing, New York, NY, USA, pp. 29–49, 2017.

[22] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-based reliable and efficient certificateless signature for IIoT devices," *IEEE Transactions on Industrial Informatics*, vol. 14, p. 1, 2021.

[23] W. Wang, H. Huang, L. Zhang, Z. Han, C. Qiu, and C. Su, "BlockSLAP: blockchain-based secure and lightweight Authentication protocol for smart grid," in *Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1332–1338, Guangzhou, China, December 2021.

[24] R. L. Rivest, L. M. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Found. Secure Compuation.*vol. 4, pp. 169–180, 1978.

[25] K. Peng, R. Aditya, C. Boyd, E. Dawson, and B. Lee, "Multiplicative homomorphic E-voting," in *Progress in Cryptology - INDOCRYPT 2004*, A. Canteaut and K. Viswanathan, Eds., pp. 61–72, Springer Berlin Heidelberg, Berlin, Germany, 2005.

[26] J. Dossogne and F. Lafitte, "Blinded additively homomorphic encryption schemes for self-tallying voting," *Journal of Information Security and Applications*, vol. 22, pp. 40–53, 2015.

[27] S. M. Toapanta Toapanta, L. J. Chávez Chalén, J. G. Ortiz Rojas, and L. E. Mafla Gallegos, "A homomorphic encryption approach in a voting system in a distributed architecture," in *Proceedings of the 2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS)*, pp. 206–210, Shenyang, China, July 2020.

[28] X. Fan, T. Wu, Q. Zheng, Y. Chen, and X. Xiao, "DHS-voting: a distributed homomorphic signcryption E-voting," in *Dependability in Sensor, Cloud, and Big Data Systems and Applications*, G. Wang, M. Z. A. Bhuiyan, S. De Capitani di Vimercati, and Y. Ren, Eds., pp. 40–53, Springer Singapore, Singapore, Asia, 2019.

[29] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting," in *Advances in Cryptology — CRYPTO' 99*, M. Wiener, Ed., Springer Berlin Heidelberg, Berlin, Germany, pp. 148–164, 1999.

[30] L. Yuan, M. Li, C. Guo, W. Hu, and X. Tan, "A verifiable E-voting scheme with secret sharing," in *Proceedings of the 2015 IEEE 16th International Conference on Communication Technology (ICCT)*, pp. 304–308, Hangzhou, China, October 2015.

[31] R. Tso, Z.-Y. Liu, and J.-H. Hsiao, "Distributed E-voting and E-bidding systems based on smart contract," *Electronics*, vol. 8, no. 4, p. 422, 2019.

[32] X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han, "A secure verifiable ranked choice online voting system based on homomorphic encryption," *IEEE Access*, vol. 6, pp. 20506–20519, 2018.

[33] X. Fan, T. Wu, Q. Zheng, Y. Chen, M. Alam, and X. Xiao, "HSE-Voting: a secure high-efficiency electronic voting scheme based on homomorphic signcryption," *Future Generation Computer Systems*, vol. 111, pp. 754–762, 2020.

[34] J. Li, X. Wang, Z. Huang, L. Wang, and Y. Xiang, "Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing," *Journal of Parallel and Distributed Computing*, vol. 130, pp. 91–97, 2019.

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