IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 21, 2019, accepted August 3, 2019, date of publication August 16, 2019, date of current version August 30, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2935895

An Anti-Quantum E-Voting Protocol in Blockchain With Audit Function

SHIYAO GAO, DONG ZHENG, RUI GUO, CHUNMING JING, AND CHENCHENG HU
National Engineering Laboratory for Wireless Security, School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

Corresponding author: Shiyao Gao (gaoshiyao719@163.com)

This work was supported in part by the Natural Science Foundation of China under Grant 61802303 and Grant 61772418, in part by the Innovation Ability Support Program in Shaanxi Province of China under Grant 2017KJXX-47, and in part by the Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2016JM6033 and Grant 2018JZ6001.

ABSTRACT As an important method of making democratic decisions, voting has always been a topic of social concern. Compared with the traditional, e-voting is widely used in various decision scenarios because of the convenience, easy to participate and low cost. However, the proposed e-voting protocols are at the risk of excessive authority and tampered information, which makes it impossible to achieve true fairness and transparency in e-voting. By combining the blockchain technology, it enables to solve these problems with the decentralization and tamper-resistant features. Moreover, the misoperations of the voters will also affect this fairness, such as voting for non-candidates, abstention or repeated voting. Therefore, to ensure the efficiency of the voting process and maintain the fairness of the voting environment, it is important to append the function of audit in e-voting protocol. This paper proposes an e-voting protocol based on blockchain, which provides transparency in the process of voting. At the same time, this scheme has the ability to audit voters operating incorrectly and resist quantum attacks by adopting the certificateless and code-based cryptography. After performance analysis, our scheme is suitable for the small-scale election and has some advantages in security and efficiency when the number of voters is small.

INDEX TERMS Anti-quantum, audit, blockchain, certificateless, e-voting.

I. INTRODUCTION

Voting as a way of making decisions symbolizes national and organizational democracy. With the development of network technology, e-voting has been applied to various decision scenarios due to its convenience, rapidity, easy participation and low cost. In 1981, Chaum [1] proposed the first e-voting protocol with the features of legality, anonymity, non-repeatable, tamper-resistant and so on [2]–[4], which realized the purpose of election online. However, there is a unified manager who supervises the whole voting process of the existed e-voting protocols. This mode will lead to unfair elections caused by the dishonesty of the manager, and the existed techniques are difficult to solve it. To avoid the central authority, the blockchain with decentralization can be employed as a new carrier of e-voting.

The blockchain [5] is a decentralized distributed ledger system, which is constructed in a distributed network consisting of several interconnected nodes. And all the nodes in the network have a distributed ledger respectively, which contains the transaction records that have been recognized in the blockchain. It is able to read the contents of this ledger for anyone that has access to the network. In the blockchain system, all nodes manage and maintain this chain together. When the most nodes achieve consensus, the transaction is recognized and recorded in the distributed ledger of each node, which means that the recorded transactions cannot be modified. The voting process and results are recorded in the blockchain, and all the authorized nodes have the ability to check the recorded data on the chain. Therefore, all participants supervise the e-voting system together to make the voting fairer and more transparent. Blockchains include public chains, alliance chains, and private chains. Because our scheme applies to small-scale election scenarios, it is intended to be built on the private chain. Each transact is a voting process, and a new block is generated for each transaction. This approach not only ensures fairness and transparency in the election process, but also provides fairness in the election result. Besides, the blockchain technology also provides the anonymity of nodes, which be used in e-voting to achieve anonymous voting.

There are two methods of realizing anonymous in the blockchain. The first is to generate wallet address through public key as pseudonym [6] of node and hide its identity

The associate editor coordinating the review of this article and approving it for publication was Abdullah Iliyasu.

by pseudonym. Nevertheless, this method achieves no real anonymity since the real identity of the node can be determined by address clustering and other methods. The other method is to adopt the ring signature scheme for signing transaction data. In 2001, Rivest *et al.* [7] first presented the concept of the ring signature. Different from the group signature, there is no manager in the ring signature, the members in the ring need not be predefined and randomly composed. And the verifier knows the group of the signer but cannot determine who is the concrete signer. By employing the above two methods, even if the data on the chain is completely open, the identity of both parties in the transaction fails to be revealed. This paper implements anonymity of voter by using of the certificateless ring signature scheme for the blockchain.

Although completely anonymous voting environment protects voters' privacy, it is impossible to find malicious voters. This will not only reduce voting efficiency, but also be detrimental to the maintenance of the electronic voting system, and the audit function will be the focus on research consequently. In the traditional public key cryptosystem, there is a problem of user's public key certificate verification. Therefore, Shamir [8] proposed identity-based cryptosystem in 1984. At the same time, the problem of key escrow arises. To this end, in 2003, Al-Riyami and Paterson [9] first put forward certificateless public key cryptography (CLPKC) to solve the key escrow problem. In CLPKC, KGC is a key generation center to generate the partial private keys of users. The user combines it with the secret value of his choice to generate a complete public-private key pair, thereby reducing the dependence on the trusted center. In this scenario, we use the KGC in the certificateless ring signature algorithm as a regulator, allowing it to generate partial private keys of voters and implement the audit function of e-voting.

Most of the existed e-voting is built up the classical public key cryptography, whose security is based on the difficulty of number theory. Because the classical computer cannot solve the difficult problem of number theory effectively in the polynomial time range, the security of the scheme is guaranteed. With the recent research on quantum computing [10]–[13], the quantum attack [14] has also become a new threat to the security of cryptographic algorithms. And code-based cryptosystem is one of the effective ways to resist the quantum attack. Different from the traditional public key cryptosystem based on the difficulty of number theory, the security of the code-based be reduced to the mathematical difficulty problem in coding theory [15]. In this paper, our scheme combines a certificateless traceable ring signature in [16] with the code-based algorithm, which can audit while resisting quantum attacks.

A. RELATED WORK

We researched some of the past articles and found that in traditional e-voting protocols, cryptographic tools are often used to ensure the security of voting, such as homomorphic encryption, zero-knowledge proof, ring signature, secret sharing, and so on. Martin Hirt proposed efficient receipt-free voting based on homomorphic encryption in [17] to prevent the purchase and coercion of votes. At the same time, Lee and Kim [18] also realized the receipt-free voting by applying zero-knowledge proof. Subsequently, Chow *et al.* [19] improved this scheme by adopting escrowed linkable ring signature and realized the receipt-free voting while achieved universal verifiability. However, none of the above schemes are able to guarantee the anonymity of voters, nor can they provide the security features of auditing and anti-quantum. Hsiao *et al.* [20] offered an e-voting system based on the ring anonymous signcryption, which realized the anonymity and fairness. Huian Li provided a viewable e-voting scheme in [21], which realized the visualization of elections by using verifiable secret sharing. However, [20] and [21] are also unable to audit and resist quantum attacks.

In recent years, with the popularity of blockchain, the combination of e-voting and blockchain has become a research hotspot. Shahzad B *et al.* presented a trustworthy e-voting system in [22] to adjust the block creates and seals by changing the hash function in the blockchain to achieve the credibility and fairness of the election. In the DATE proposed by Lai *et al.* [23], the fairness of the e-voting and the privacy protection for voters were realized by employing the blockchain and ring signature technology. At the same time, it also had self-tallying feature. Unfortunately, because there is no third-party authority on the scheme, it cannot be audited. In an e-voting system based on blockchain and ring signature put forward by Wu [24], transparency and privacy were solved. Lai and Wu [25] suggested an efficient decentralized anonymous voting system. The system was based on the Ethernet and used the ring signature scheme to ensure the transparency and privacy of the system. It achieved the goal of high efficiency and speed through parallel operation in the counting stage. Subsequently, McCorry *et al.* [4] offered a blockchain e-voting protocol, which not only achieved anonymity and transparency but also increased the modifiability of the ballot by utilizing blind signature and commitment technology in the blockchain. This has also become a new direction in the study of e-voting systems. McCorry Pd *et al.* proposed a blockchain smart contract for board elections in [26], which is the first scheme that does not rely on any trusted authority to count and guarantee voter privacy. After that, Adiputra [27] proposed "A Proposal of Blockchain-Based Electronic Voting System" in 2018, which solved the general verifiability problem of the blockchain electronic voting schemes, although it did not discuss the privacy problem of e-voting. In a recent study, Li *et al. et al.* [28] proposed a blockchain-based e-voting scheme in distributed IoT. In this scheme, the blockchain is similar to the bulletin board, and achieved the fairness, maximal ballot secrecy, and self-tallying of e-voting. However, other security requirements such as anonymity been ignored. The above schemes achieved the basic requirements of the e-voting system but

cannot resist quantum attacks. At present, there is no scheme has the ability to meet these requirements at the same time. To solve the above problems, this paper provides a blockchain e-voting protocol with audit and anti-quantum functions.

B. OUR CONTRIBUTION

Currently, most e-voting protocols use public key cryptosystems based on numerical theory difficulties. The research shows that these schemes have problems of verifying the public key certificates, besides cannot resist quantum attacks. In addition, these schemes focus on the privacy protection for voters, while ignoring the accountability of violators. Since the imperfections in security and function, we construct an e-voting protocol in blockchain by combining the code-based public key cryptography with the certificateless cryptography, which can resist the quantum attacks and audit the violators. Our scheme has the following advantages.

(1) Our scheme solves the problem of verifying public key certificates in traditional public key cryptosystem by introducing certificateless traceable ring signature algorithm, besides realizes the audit function in the e-voting.

(2) In this paper, we adopt the code-based public key cryptographic algorithm, which makes the e-voting protocol can resist the quantum attacks.

(3) The presented e-voting protocol is supported by the blockchain technology, which guarantees the fairness and transparency of the voting process and results.

C. ORGANIZATION

The remaining of the article is structured in the following manner. Section 2 gives the related technologies involved in our e-voting protocol. Section 3 and 4 introduce the anti-quantum e-voting protocol in blockchain with the audit function proposed in this paper particularly. Section 5 analyses the security and efficiency of this scheme, and the last section summarizes the whole paper.

II. PRELIMINARIES

This section describes the cryptographic tools involved in our scheme and some hard problems.

A. CODE-BASED CRYPTOGRAPHIC ALGORITHM

In 1978, Robert McEliece [29] first suggested a public key cryptographic algorithm based on coding theory, which has not been broken up so far. Then the Niederreiter [30] algorithm is advanced, which security was reduced to the syndrome decoding (SD) problem of coding theory and is equivalent to McEliece algorithm [31]. SD problem is an NP-complete problem [32], which proves that it can resist quantum attacks.

Definition 1 (Binary Syndrome Decoding (SD) problem): Let n, k, and l be positive integers with $n > k > l$. Given a binary $(n-k) \times n$ matrix H, a binary vector $s \in F_2^{n-k}$, and an integer $l > 0$, find a word $x \in F_2^n$ of weight $w(x) \leq l$, such that $Hx^T = s$.

B. CERTIFICATELESS TRACEABLE RING SIGNATURE ALGORITHM

In this paper, the bilinear pairings and the computational Diffie-Hellman problem on elliptic curves are involved in the digital signature algorithm. Their definitions are as follows.

Definition 2 (Bilinear Pairings): Suppose $G1$ is a cyclic additive group generated by P, whose order is a large prime q. And $G2$ is a cyclic multiplicative group of the same order, let random numbers $a, b, c \in Z_q$. A map $e: G1 \times G1 \rightarrow G2$ is called a bilinear mapping if it satisfies the following properties:

(1) Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G1$ and $a, b \in Z_q$.

(2) Non-degenerate: there exist $P, Q \in G1$ such that $e(P, Q) \neq 1$.

(3) Computable: there is an efficient algorithm to compute eP, Q for all $P, Q \in G1$.

Definition 3 (Computational Diffie-Hellman Problem (CDHP)): Given a cyclic additive group G generated by g, two known elements $g_1 = ag$, $g_2 = bg$ and a, b are unknown. It is difficult to calculate $g_3 = abg$.

III. SYSTEM MODEL AND SECURITY MODEL

In this section, we propose the system model of the e-voting protocol with audit function based on blockchain which can resist quantum attacks, as shown in Figure 1. And then list the symbols involved in the scheme. Finally, we provide the security model of our e-voting protocol.

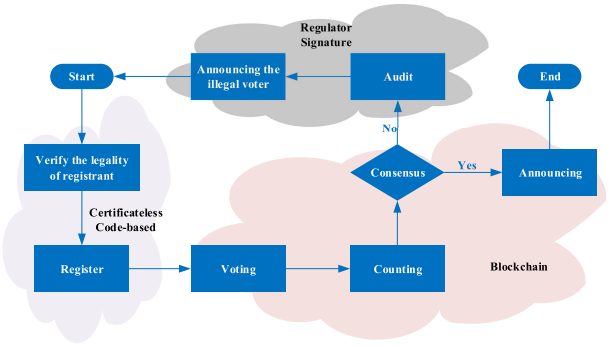

FIGURE 1. The process of our protocol.

A. SYSTEM MODEL

There are four roles in the system, namely, regulator, voting initiator, voter and candidate. The following are descriptions of these four roles, voting and ballots. To ensure the security of our e-voting protocol, we make the following assumptions:

(1) Assume that the regulator is trustworthy, and it only goes online when he generates and distributes the Partial Private Keys (PSK) for voters and recovers the identities of voters during the audit phase. In the process of voting, the regulator cannot intervene.

(2) Voters and candidates are extensible. During initialization and preparation, they join the blockchain system.

Voters remain online during the implementation of the protocol and voluntarily cooperate with the regulator to recover their identity, when the regulator audits the voter identity corresponding to the ballot. Candidates are only online when verifying the signed ballot.

- **Regulator:** The regulator in our e-voting system is the KGC in the certificateless cryptosystem, which is responsible for verifying whether the registrant is up to the voting standard. Also, the regulator generates and distributes the PSK for registered legitimate voters in the system. The PSK of every voter is generated by the Master Key (MK) in the initialization phase and its identity information ID_i. At the same time, the identity of the voter and the PSK are established the corresponding relationship and archived as an important tool for audit. When the voting result is in dispute, the regulator revokes the anonymity of voters in the voting process through the correspondence $ID - PSK$, finding out the voters who misoperate and prosecute them. The regulator does not participate in the voting process.
- **Voting Initiator:** The voting initiator publishes the voting content and the Candidate List in the blockchain smart contract, in detail, the corresponding relationship between the name and the public key address (Name-Address) of a candidate.
- **Voter:** Staffs register with the regulator and become voters spontaneously. Since our scheme is suitable for the small-scale voting, the regulator has a list of company personnel beforehand and verifies whether they are eligible to vote when they register. After successful registration, the PSK generated and distributed by the regulator for voters. And voters compute the complete private key $SK2$ and the public key address $PK2$ according to the random secret value selected by them, and anonymous voting will be conducted through the $SK2$ and $PK2$. The voters should toe the mark of the e-voting system, namely, cannot abstain, cannot vote for non-candidates, one man one vote. When the nodes cannot reach a consensus on the counting results, the malicious voters will be restored by the regulator and take responsibility.
- **Candidate:** Candidates are announced by the voting initiator, which is essentially a node in the blockchain.
- **Voting:** The voting process is a transaction from voter to a candidate on the blockchain. The voter signs the ballot firstly, then broadcasts the signed ballot and its hash value to all nodes in the blockchain network. The node searches for the hash value collision according to the computing power or other consensus methods. After the verification is successful, the hash value is combined with the previous to form the Merkel tree recorded in the new block, so each block contains all the ballot information. In addition, the regulator does not interfere with the election, and our scheme provides the voter's anonymity by using the ring signature algorithm when voters sign the ballots.
- **Ballot:** A ballot is a transaction form on the blockchain that records the name and the public key address of the candidate.

The formal definition of our e-voting protocol is presented below.

Definition 4 (Anti-Quantum E-voting Protocol in Blockchain With Audit Function): An anti-quantum e-voting protocol in blockchain with audit function is a collection of four algorithms: setup, voting, counting and announcing, auditing. The details are as follows.

(1) Setup: On input the security parameter, it outputs the system parameters. This algorithms contains two stages. In initialization, it outputs the MK, also outputs the public and private key pairs used by the company members to securely transmit PSK. In preparation, it outputs the PSK of the registered voter and their complete key pairs.

(2) Voting: On input the election content, the voter chooses some parameters, the public key of other voters and his or her private key. Finally, the algorithm is performed by a voter to output the signed ballot.

(3) Counting and announcing: On input all the signed ballot, any node in the blockchain can view the contents of the ballot. The statistical results of all nodes reach a consensus and output the final election result. Otherwise, the system executes the auditing algorithm.

(4) Auditing: On input the signed ballot, and the regulator interacts with the voter by performing the algorithm to output the voter corresponding to the signed ballot.

In order to describe our scheme conveniently, some symbols and parameters will be used as an auxiliary. Table 1 gives a list of symbols and parameters used in this paper.

B. SECURITY MODEL

In the practical environment, an e-voting protocol must satisfy the following security requirements.

(1) **Conditional anonymity of voters.** Our e-voting scheme ensures that no one can identify the real voter from the ballots during the voting process. At the same time, when the final election result does not reach a consensus, the regulator can restore the real identity of the voter corresponding to the ballot.

(2) **Uniqueness.** The uniqueness of the ballot requires that the ballots are non-repeatable and unforgeable. No voter can produce two identical ballots. At the same time, anyone cannot pretend to be a real voter to vote and cannot fake the real voter's signed ballot.

(3) **Fairness.** Fairness means that in the process of voting and counting, there will be no third-party authority to intervene in the choice of voters or influence the final election results.

(4) **Verifiability.** The verifiability of ballots includes personal verifiability and universal verifiability. Individual verifiability means that each voter participating in the election has the ability to view if his or her ballot is recorded on the blockchain or not. And universal verifiability means that

TABLE 1. List of the symbols used in our scheme.

Notation	Meaning
i	The voter i
s	The master key of the system
ID_i	The identity information of Voter i
x_i	The secret value is chosen randomly by voter i
C_i	The binary irreducible (n, k) Goppa code chosen by voter i
H_i^0	The parity-check matrix of C_i
DHC_{H_i}	The corresponding syndrome decoding algorithm of C_i
M_i	The binary $(n-k)\times(n-k)$ invertible matrix is chosen by voter i
B_i	The binary $n \times n$ permutation matrix chosen by voter i
$PK1_i, SK1_i$	The key pair generated by the voter for secret transmit the Partial Private Key of voter i
D	A $n \times 1$ matrix of Partial Private Keys generated by the regulator for all voters
d_i	The elements in D
Q	A $n \times 1$ matrix of the hash values of all voters' identity ID_i
q_i	The elements in Q
$PK2_i, SK2_i$	The public key address and complete private key used in the voting phase generated by voter i
PK_i, SK_i	All key pairs generated by voter i
k	The signer
$Ballot$	The ballot generated by the voter
r_i	The values are chosen randomly by the signer for voters including themselves
$a_j, j \neq k$	The values are chosen randomly by the signer for each voter except himself
a_k	The values are chosen randomly by the signer

anyone can verify the validity of the ballot and count the election results.

(5) **Auditability.** The auditability of the ballots means that when the election results fail to reach a consensus, the regulator can revoke the anonymity of the signed ballots and restore the real identity of the voters, thereby audits the voters that violated the rules.

(6) **Anti-Quantum.** Our scheme is anti-quantum, and the advantage is that it can resist the attack of quantum computers.

Based on the above security requirements, we consider the following oracles, which together simulated the adversary's ability to attack the security of the schemes:

- The Joining Oracle is defined as $\mathcal{JO}$, it is executed when a new user joins the system, and the user's public key $PK_i \in \mathcal{PK}$ is returned.
- The Corruption Oracle is defined as $\mathcal{CO}$, on input a public key $PK_i \in \mathcal{PK}$ and it outputs the corresponding private key $SK_i \in \mathcal{SK}$ by querying the $\mathcal{CO}$.
- The Signing Oracle is defined as $\mathcal{SO}$, on input a ballot, a set $\mathcal{U}$ of all the voters' public keys and the signature voter's public key, it outputs a valid signed ballot σ.

Our scheme is simulated by a random oracle if its security can be proved in the random oracle model.

The unforgeability of the e-voting scheme is defined in the following game, which is played between the Simulator $\mathcal{S}$ and the Adversary $\mathcal{A}$, where $\mathcal{A}$ is allowed to query oracles $\mathcal{JO}$, $\mathcal{CO}$, $\mathcal{SO}$ and the random oracle.

a. $\mathcal{S}$ generates and gives $\mathcal{A}$ the system parameters param.
b. $\mathcal{A}$ may query the oracles according to any adaptive strategy.
c. $\mathcal{A}$ gives $\mathcal{S}$ a set $\mathcal{U}$ of all the voters' public keys in $\mathcal{PK}$, a ballot, and a signed ballot σ.

$\mathcal{A}$ wins the game if the signed ballot σ generated by $\mathcal{A}$ can be recorded on the blockchain at the end of the voting algorithm and be verified at the counting and announcing. At the same time, all the public keys in $\mathcal{U}$ are query outputs of $\mathcal{JO}$, no public keys in $\mathcal{U}$ have been input to $\mathcal{CO}$ and σ is not a query output of $\mathcal{SO}$.

We denote by

$$Adv_A^{unf}(\lambda) = Pr[\mathcal{A}\text{winsthegame}].$$

Definition 5 (Unforgeability): Our e-voting scheme is unforgeable if for any probabilistic polynomial time (PPT) adversary $\mathcal{A}$, $Adv_A^{unf}(\lambda)$ is negligible.

The conditional anonymity of the e-voting scheme is defined as the following game, which is performed between the Simulator $\mathcal{S}$ and the Adversary $\mathcal{A}$, and $\mathcal{A}$ can query the $\mathcal{JO}$.

a. $\mathcal{S}$ generates and gives $\mathcal{A}$ the system parameters *param*.
b. $\mathcal{A}$ query the $\mathcal{JO}$ adaptively.
c. $\mathcal{A}$ gives $\mathcal{S}$ a set $\mathcal{U}$ of all the voters' public keys in $\mathcal{PK}$ and a ballot. $\mathcal{S}$ randomly chooses an index $k \in \{1, 2, \ldots, n\}$ and computes the signed ballot σ_k with the private key $SK_k \in \mathcal{SK}$ the voter k.
d. $\mathcal{A}$ outputs an index $k' \in \{1, 2, \ldots, n\}$ corresponding to the voter he or she guessed.

We denote by

$$Adv_A^{con-anon}(\lambda) = \left| Pr\left[k' = k\right] - \frac{1}{|\mathcal{U}|} \right|.$$

Definition 6 (Conditional Anonymity): Our e-voting scheme is conditional anonymity, when the vote goes smoothly, and the regulator does not require interaction with the voters to restore their identities. For any unbounded Adversary $\mathcal{A}$, $Adv_A^{con-anon}(\lambda) = 0$.

IV. CONCRETE SCHEME

The e-voting protocol in this paper consists of five phases. The schematic diagram of protocol timing is shown in Figure 2. Following is a detailed description of the voting process in our scheme according to the steps in Figure 2.

A. INITIALIZATION

In the initialization phase, the voting rules that voters are not allowed to abstain, vote for non-candidates, and one man one vote are determined. And the system initializes the regulator, KGC, to generate the MK. After that, generating the key

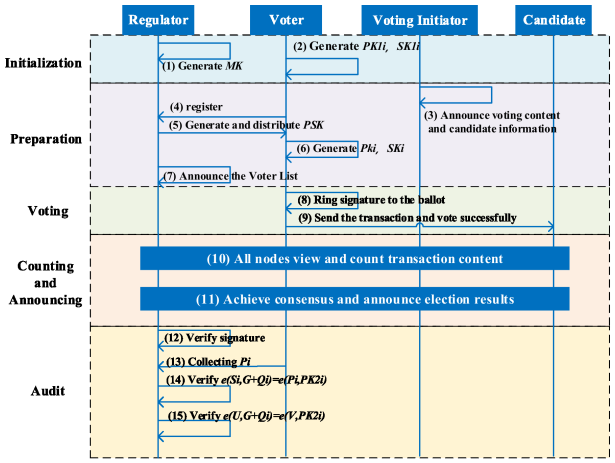

FIGURE 2. The schematic diagram of protocol timing.

pairs $PK1_i, SK1_i$ for potential voters to encrypt and decrypt the PSK. In addition, all other protocols and algorithms in systems such as initialization blockchains are implemented.

Step 1 (Generate MK): (1) The system chooses a cyclic additive group G_1 of order q whose generator is a point G on an elliptic curve. And G_2 is a cyclic multiplicative group of the same order. A bilinear mapping $e : G_1 \times G_1 \rightarrow G_2$. Select secure hash functions $H_1 : \{0, 1\}^* \rightarrow G_1$,$H_2 : \{0, 1\}^* \rightarrow Z_q$, where q is a large prime. Define a function $f : G_1 \rightarrow F_2^n$.

(2) The system randomly generates a secret parameter $s \in Z_q^*$ for the regulator as the MK.

(3) Compute $P_{pub} = sG$ to generate the PSK for legitimate voters.

Step 2 (Generate $PK1_i, SK1_i$): (1) The identity information $ID_i \in F_2^n,\ i = 1, 2, \ldots, n$ of every potential voter is first selected.

(2) A binary irreducible (n, k) Goppa code C_i is chosen that can correct t errors. A parity-check matrix H_i^0 of C_i, and a corresponding syndrome decoding algorithm DHC_{H_i} of C_i. A binary $(n-k) \times (n-k)$ invertible matrix M_i and a binary $n \times n$ permutation matrix B_i.

(3) Compute $PK1_i = M_i H_i^0 B_i$, and the voter obtains the public key $PK1_i$ and the private key $SK1_i =< M_i, H_i^0, DHC_{H_i} >$, which used to transmit the PSK securely in the voting phase.

(4) The public parameters of the system are generated, that is, $param = \{G_1, G_2, G, C_i, PK1_i, H_1, H_2, P_{pub}, g, e, f\}$.

Simultaneously, the blockchain is initialized with the initialization block, which will serve as the starting block. And this block does not contain any ballots, in other words, no transactions are recorded, whereas it contains all the data about the voting, including the election time, participant information, the expected total number of ballots N_{prior} and other public parameters. In this way, the blockchain is associated with a specific election, at the same time, the value of N_{prior} also corresponds to different elections. And whole public data is recorded in the chain to prevent tampering, thus avoiding possible controversy. In addition, it should be noted that since the Goppa code is a linear code and an algebraic geometric code, there are many ways to decode it, and it is not unique. It is not the focus on research in this paper. The method described in [33] is selected.

B. PREPARATION

In this phase, the preparatory work before voting is completed through the following four steps. Owing to the code-based encryption and decryption algorithms are used to transmit the PSK, the security of the system is improved, and the quantum attack is resisted.

Step 3 (Announce Voting Content and Candidate information): The voting initiator publishes the voting content and announces the Candidate List in the blockchain smart contract, namely the corresponding relationship Name-Address.

Step 4 (Register): (1) The member who wishes to participate in the election sends his or her ID_i and $PK1_i$ to the regulator.

(2) The regulator verifies the ID_i with the latest list of company personnel and knows which employees had the ability of voting during the initialization.

(3) When the ID_i of the registrant is in the list, its identity will be registered.

Step 5 (Generate and Distribute PSK): (1) The regulator composes the identity information ID_i of all voters into matrix $A = \begin{pmatrix} ID_1 \\ \cdots \\ ID_n \end{pmatrix}$.

(2) Compute $Q = H_1(A) = (H_1(ID_i))_{n\times 1}$ and $D = sQ$. D is a matrix of all voters' PSK, q_i is an element in Q, satisfying the relationship $q_i = H_1(ID_i)$.

(3) Map D to a $n \times n$ matrix by function f, d_i is an element in D, satisfying the relationship $d_i = H_1(f(d_i))$.

(4) Encrypt the matrix by row through the $PK1_i$, $c = E_{PK1_i}(f(d_i))$, and send it to the voters.

Step 6 (Generate PK_i, SK_i): (1) The voters decrypt c with their private key $SK1_i$, $PSK = d_i = H_1(D_{SK1_i}(c))$.

(2) The voters randomly choose the secret value $x_i \in Z_q^*$.

(3) The voters compute the public key address $PK2_i$ and the complete private key $SK2_i$. $PK2_i = x_i(G + q_i)$, $SK2_i = x_i d_i$.

(4) Every voter gets his or her whole key pairs, which are $PK_i = \{PK1_i, PK2_i\}$, $SK_i = \{SK1_i, SK2_i\}$.

Step 7 (Announce the Voter List): The regulator collects and publishes the voters' public key addresses $PK2_i$ as the Voters List that represents the legitimacy of their identities. And the authenticated voters can execute subsequent operations.

C. VOTING

In the voting stage, the public key address of voter is hidden with ring signature technology, which realizes anonymous voting. The information about a candidate in the ballot will not be hidden to achieve real-time attention to the election results.

Step 8 (Generate the Signed Ballot): (1) Every voter chooses one of the candidates as the recipient of the

transaction, then records his or her name and public key address in the transaction form. Such a transaction form is the $Ballot =< Name_i - Address_i >, i \in \{Candidate\}$.

(2) The voter signs this ballot. Our scheme provides the anonymous of a voter during the voting with the traceable ring signature technology. The specific signature process is as follows:

Suppose the signer is k. $Ballot \in F_2^n$. And the matrix A is the identities of n voters in the system.

a. The signer k randomly chooses different $r_i \in Z_q^*, i = 1, 2, \ldots, n, a_j \in Z_q^*, j = 1, 2, \ldots, n, j \neq k$.
Compute $T_j = a_j G, P_i = r_i (G + q_i), S_i = r_i PK2_i, U = x_k \sum_{i=1}^{n} P_i$.
Compute the determinant of matrix A, $det(A)$.
Map T_j, P_i, S_i, U through function f.
Compute $h_j = H_2 \left(Ballot || f\left(T_j\right) || f(U) || det(A)\right)$.

b. The signer k randomly chooses $a_k \in Z_q^*$.
Compute $T_k = a_k Q_k - \sum_j^n \left(T_j + h_j PK2_j\right)$, and $T_k \neq T_j$, otherwise, the singer k chooses $a_k \in Z_q^*$ again.
Map T_k through function f.
Compute $h_k = H_2 (Ballot || f(T_k) || f(U) || det(A))$.
Compute $Z = h_k x_k P_{pub} + h_k SK2_k + a_k d_k$.

c. The signature of the ballot is $\sigma = (Ballot, T_1, T_2, \ldots, T_n, S_1, S_2, \ldots, S_n, U, Z, A)$.

d. Then the signed ballot is $(Ballot)_{Sig_k} = \sigma$.

Step 9 (Send the Vote Successfully): (1) Compute the hash value of signed ballot $h = H_2(\sigma)$.

(2) The voter broadcasts the signed ballot $(Ballot)_{Sig_k}$ and its hash value h to the blockchain network.

(3) Other nodes in this network verify the signed ballot when they receive the broadcast message.

The process of verifying the signature is as follows:

a. Compute $h_i = H_2 (Ballot || f(T_i) || f(U) || det(A))$.

b. Verify the validity of the equation $e\left(P_{pub}, \sum_{i=1}^{n} T_i + h_i PK2_i\right) = e(G, Z)$, if the equation is validated, the node finds the collision of the hash value h according to the computing power or other consensus methods.

(4) The first node that completes the above steps records the ballot in the newly generated block, that is, *Ballot* takes effect, and also records the Merkel tree composed of the hash values of all the ballots, the $N_{current}$ updated to the current total number of ballots.

D. COUNTING AND ANNOUNCING

At this stage, the ballots will be counted, and the results of the elections will be announced according to the structure of the blocks in our scheme.

Step 10 (All the Nodes View and Count the Vote Content): The verifiers who interested in the election result to count the ballots by accessing the data on the block. According to the block structure shown in Figure 3, there are the number and the content of the transaction in the body, and when entering the counting phase, the $N_{current}$ updates the total number of ballots for this election. The number of the transaction is the current total number of ballots $N_{current}$. The content

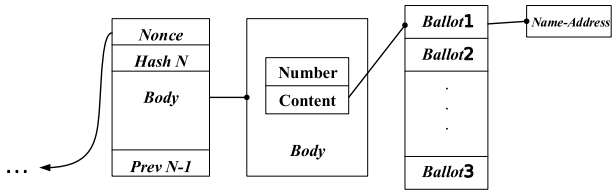

FIGURE 3. The block structures.

of the transaction is composed of all the current signed ballots. When counting, firstly verify the validity of the signed ballot $(Ballot)_{Sig_k} = (Ballot, T_1, T_2, \ldots, T_n, S_1, S_2, \ldots, S_n, U, Z, A)$. Compute $h_i = H_2 (Ballot || f(T_i) || f(U) || det(A))$ and verify the validity of the equation $e\left(P_{pub}, \sum_{i=1}^{n} T_i + h_i PK2_i\right) = e(G, Z)$, if the equation holds, the signature is correct and the original ballot is obtained. After that, the verifier continues to check $Ballot =< Name_i - Address_i >, i \in \{Candidate\}$. Voting in the expected time range T, at the end of T, the polls are obtained by counting the information of a candidate in every ballot. Finally compared with the $N_{current}$ and the election requirements N_{prior} recorded in the initialization block.

Step 11 (Achieve Consensus and Announce Election Results): The counting result was published by every node and the final election result was generated through blockchain consensus algorithms, such as Practical Byzantine Fault Tolerance (PBFT), if $N_{prior} = N_{current}$. When the consensus was reached on the elections result within the limits of allowable errors, it will be published and recorded in the blocks, and then the election is going to be close. Otherwise, it shows that there are voters' misoperations in voting. The regulator audits the voters who violate the rules and revokes their anonymity with traceable ring signature algorithm afterward.

It should be noted that the consensus mechanism of this scheme, such as PBFT, ensures the consistency of results. In this paper, the choice of consensus algorithm is not the focus on research.

E. AUDIT

In the audit phase, the regulator will revoke the anonymity of voters through the following four steps, find the violators and hold them accountable.

Step 12 (Verify Signature): When $N_{prior} \neq N_{current}$ or voters fail to reach a consensus on the counting result or still vote after the counting, and the regulator revokes the anonymity of voters who misoperate with the signature σ. Firstly, compute $h_i = H_2 (Ballot || f(T_i) || f(U) || det(A))$. Secondly, verify the validity of the equation $e\left(P_{pub}, \sum_{i=1}^{n} T_i + h_i PK2_i\right) = e(G, Z)$, if the equation is validated, the signature σ is correct.

Step 13 (Collecting P_i): The regulator collects $P_i = S_i {x_i}^{-1}$ from the corresponding voters according to the S_i and the matrix A of voters' identities in the signature σ.

Step 14 (Verify $e(S_i, G + q_i) = e(P_i, PK2_i)$): The regulator decides whether the bilinear pairing $e(S_i, G + q_i) = e(P_i, PK2_i)$ is valid or not, and P_i is validated when the equation holds.

Step 15 (Verify $e(U, G+q_i) = e(V, PK2_i)$): Compute $V = \sum_{i=1}^{n} P_i$, and revoke the anonymity of voters with $e(U, G+q_i) = e(V, PK2_i)$.

In our protocol, it should be noted that we suppose the regulator is reliable. After generating and distributing the *PSK* for every legitimate voter, the regulator will not participate in the whole process of voting, counting and will not cheat in the audit process.

V. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

This section will discuss the security performance of our protocol and evaluate efficiency. Finally, some related e-voting protocols are compared.

A. SECURITY ANALYSIS OF OUR SCHEME

Theorem 1 (Unforgeability): Based on the hard of CDHP, our e-voting scheme is unforgeable in the random oracle model.

Proof: Setup: The Adversary $\mathcal{A}$ is given the system parameters $param = \{G_1, G_2, G, C_i, PK1_i, H_1, H_2, P_{pub}, g, e, f\}$ generated by the Simulator $\mathcal{S}$.

Random Oracle: The Simulator $\mathcal{S}$ receives the hash request from the Adversary $\mathcal{A}$, then $\mathcal{S}$ queries the hash function H_2 and returns the hash value to $\mathcal{A}$ as a response.

Joining Oracle $\mathcal{JO}$: The Adversary $\mathcal{A}$ gets a set $\mathcal{U} = \{PK_1, PK_2, \ldots, PK_n\}$ of all the voters' public keys through n queries.

Corruption Oracle $\mathcal{CO}$: On input a public key $PK_i \in \mathcal{PK}$ that is output from $\mathcal{JO}$, and the Simulator $\mathcal{S}$ checks whether it corresponds to the set $\mathcal{U}$. If it is, $\mathcal{S}$ stops immediately, otherwise, $\mathcal{S}$ outputs the corresponding private key.

Signing Oracle $\mathcal{SO}$: On input a ballot, a set $\mathcal{U}$ and the signature voter's public key, then $\mathcal{S}$ simulates the following process:

(1) Choose a random index $k \in \{1, 2, \ldots, n\}$.

(2) The Simulator $\mathcal{S}$ selects random numbers $r_i \in Z_q^*, i = 1, 2, \ldots, n$, $a_j \in Z_q^*, j = 1, 2, \ldots, n, j \neq k$ and computes $T_j = a_j G, P_i = r_i(G+q_i), S_i = r_i PK2_i, U = x_k \sum_{i=1}^{n} P_i$. Then $\mathcal{S}$ computes the hash value $h_j = H_2\left(Ballot||f\left(T_j\right)||f(U)||det(A)\right)$ by using Random Oracle.

(3) $\mathcal{S}$ selects the random number $a_k \in Z_q^*$ and computes $T_k = a_k Q_k - \sum_j^n \left(T_j + h_j PK2_j\right)$. Then $\mathcal{S}$ computes the hash value $h_k = H_2(Ballot||f(T_k)||f(U)||det(A))$ by Random Oracle.

(4) Compute $Z = h_k x_k P_{pub} + h_k SK2_k + a_k d_k$ and get the final signed ballot

$$\sigma = (Ballot, T_1, T_2, \ldots, T_n, S_1, S_2, \ldots, S_n, U, Z, A).$$

(5) Adversary $\mathcal{A}$ can adaptively query the $\mathcal{SO}$.

We prove the unforgeability of our scheme through contradiction. Assume that the Adversary $\mathcal{A}$ can forge a valid signed ballot

$$\sigma = (Ballot', T_1', T_2', \ldots, T_n', S_1', S_2', \ldots, S_n', U', Z', A')$$

that was not obtained through the $\mathcal{SO}$. According to the forking lemma for ring signature [34], the Adversary $\mathcal{A}$ can forge another valid signed ballot

$$\sigma = (Ballot', T_1', T_2', \ldots, T_n', S_1', S_2', \ldots, S_n', U', Z'', A')$$

with non-negligible probability. The two forged signed ballots have the same randomness for the same content of ballot and the ring user group $\mathcal{U}$ formed by the voters.

$$e\left(P_{pub}, \sum_{i=1}^{n} T_i + h_i' PK2_i'\right) = e\left(G, Z'\right)$$
$$e\left(P_{pub}, \sum_{i=1}^{n} T_i + h_i'' PK2_i'\right) = e\left(G, Z''\right)$$

According to the above formulas, we get

$$e\left(G, Z' - Z''\right) = e\left(P_{pub}, \sum_{i=1}^{n} (h_i' - h_i'') PK2_i'\right)$$

By using the forking lemma for ring signature, there are indexes i and j, which satisfy $h_i' - h_i'' = 0$ and $h_j' - h_j'' \neq 0$, $i \neq j$.

Thus

$$e\left(G, Z' - Z''\right) = e\left(P_{pub}, (h_j' - h_j'') PK2_j'\right)$$

The probability of $PK2_j' = PK2_k$ is $\frac{1}{|\mathcal{U}|}$, so there is

$$\begin{aligned} e\left(G, Z' - Z''\right) &= e\left(P_{pub}, (h_j' - h_j'') a(G+q)\right) \\ &= e\left(G, sa(h_j' - h_j'')(G+q)\right) \end{aligned} \quad (1)$$

Thus

$$\begin{aligned} Z' - Z'' &= sa(h_j' - h_j'')(G+q) \\ &= saG(h_j' - h_j'') + saq(h_j' - h_j'') \\ saG &= (Z' - Z'' - saq(h_j' - h_j''))(h_j' - h_j'')^{-1} \end{aligned} \quad (2)$$

Based on the computational difficulty of CDHP, the probability that the Adversary $\mathcal{A}$ wins the game is negligible.

Theorem 2 (Conditional Anonymity): Our e-voting scheme is conditional anonymity.

Proof: We prove the conditional anonymity of our scheme from the following two points.

(1) In this e-voting system, the anonymous is realized by using the ring signature technology to hide the identities of voters. When voters sign the *Ballot*, they first compute $S_i = r_i PK2_i$ through the public key addresses of all voters.

(2) Secondly, when computing $T_k = a_k Q_k - \sum_j^n \left(T_j + h_j PK2_j\right)$, their public key addresses are also required. S_i and T_k will be the part of the signed ballot $(Ballot)_{Sig_k}$. Therefore, the signer's public key address can be hidden in all of the authenticated voters, and anyone, including the regulator, cannot judge the determined signer from signature σ. Only when the audit is required, the regulator revokes their anonymity through cooperating with every voter.

Theorem 3 (Verifiability): Our e-voting scheme is verifiability.

Proof: Verifiability includes personal verifiability and universal verifiability. In terms of personal verifiability,

according to the nature of the blockchain, all of the voters can check and count the transaction data on the chain to verify whether their ballots are counted. In terms of universal verifiability, because the distributed ledgers in the blockchain are public, anyone interested in the election results is able to get a copy of the ledgers, verifying whether the digital signature is correct, count the election results, and compare with the official results to ensure the verifiability of the electronic voting scheme.

The correctness of the digital signature is verified as follows:

Verifier Knows $(Ballot)_{Sig_k} = (Ballot, T_1, T_2, \ldots, T_n, S_1, S_2, \ldots, S_n, U, Z, A)$, then computes $h_i = H_2\,(Ballot||f\,(T_i)\,||\,f\,(U)\,||det\,(A))$ and verifies the validity of bilinear pairings

$$\begin{aligned} & e\left(P_{pub}, \sum_{i=1}^{n} T_i + h_i PK2_i\right) \\ &= e\,(G, Z)\cdot \quad e\left(P_{pub}, \sum_{i=1}^{n}\left(T_i + h_i PK2_i\right)\right) \\ &= e\left(sG, T_k + h_k PK2_k + \sum_{j=1}^{n}\left(T_j + h_j PK2_j\right)\right) \\ &= e\left(sG, a_k Q_k - \sum_{j}^{n}\left(T_j + h_j PK2_j\right)\right. \\ &\quad \left. + h_k PK2_k + \sum_{j=1}^{n}\left(T_j + h_j PK2_j\right)\right) \\ &= e\,(G, s(a_k Q_k + h_k PK2_k)) \\ &= e\left(G, a_k d_k + h_k x_k\left(P_{pub} + d_k\right)\right) \\ &= e\,(G, Z) \end{aligned} \tag{3}$$

Theorem 4 (Auditable): Our e-voting scheme is auditable.

Proof: Since the traceable ring signature technology is employed in our e-voting scheme, and the KGC in certificateless cryptosystem is introduced as the regulator who distributes the *PSK* used in signature to voters without participating in the voting process. When the consensus of voting cannot be reached, the anonymity of voter is revoked through a round of interaction with them and find the signer corresponding to the ballot.

The correctness of the anonymity revocation of the voter is verified as follows:

a. The regulator verifies the validity of bilinear pairings $e\,(S_i, G + Q_i) = e\,(P_i, PK2_i)$.

$$\begin{aligned} & e\,(S_i, G + Q_i) \\ &= e\,(r_i PK2_i, G + Q_i) \\ &= e\,(r_i x_i\,(G + Q_i)\,, G + Q_i) \\ &= e\,(r_i\,(G + Q_i)\,, x_i\,(G + Q_i)) \\ &= e\,(P_i, PK2_i) \end{aligned} \tag{4}$$

b. The regulator verifies the validity of bilinear pairings $e\,(U, G + Q_i) = e\,(V, PK2_i)$.

$$\begin{aligned} & e\,(U, G + Q_i) \\ &= e\left(x_k \sum_{i=1}^{n} P_i, G + Q_i\right) \\ &= e\left(\sum_{i=1}^{n} P_i, x_k\,(G + Q_i)\right) \\ &= e\,(V, PK2_i) \end{aligned} \tag{5}$$

Theorem 5 (Resistance to Attacks): Our e-voting protocol is able to defend against the replay attack, the man-in-the-middle attack, the counterfeiting attack, the modification attack and quantum attack.

Proof: The details of the defense against the above attacks are as follows.

(1) **Replay attack:** In the process of generating signed ballots, the voters are required to choose random numbers $r_i \in Z_q^*, i = 1, 2, \ldots, n$, $a_j \in Z_q^*, j = 1, 2, \ldots, n, j \neq k$, $a_k \in Z_q^*$. Therefore, it is possible to detect the replay of the signed ballot and conclude that our scheme can resist the replay attack.

(2) **Man-in-the-middle attack:** In the preparation phase, the generation of the key pair $PK2_i$, $SK2_i$ that the voter uses to sign the ballot is based on CDHP. Any adversary cannot get the private key through the public values or parameters.

(3) **Counterfeiting attack:** Based on the proof of Theorem 1, any adversary is not capable of forging a signed ballot $(Ballot)_{Sig_k} = (Ballot, T_1, T_2, \ldots, T_n, S_1, S_2, \ldots, S_n, U, Z, A)$ without the voter's private key.

(4) **Modification attack:** In our scheme, the voters sign the ballot and record the signed ballot on the blockchain. If the adversary tampers with the ballot, it can be found by verifying its digital signature. Secondly, based on the advantage of blockchain technology in tamper-resistance, it is impossible for an attacker to tamper with the recorded transaction, since every block of the chain contains the hash values of all transactions. The modification attack is successful if the attacker can modify the recorded ballots in each block. However, this probability is negligible due to the anti-collision of the hash function. Therefore, it is impossible for anyone to modify the ballots and election results in the blockchain.

(5) **Quantum attack:** In our protocol, the regulator generates and distributes the *PSK* for each voter by using the Niederreiter algorithm. The algorithm is a cryptographic algorithm based on the code, and its security is reduced to the syndrome decoding (SD) problem of coding theory. This is an NP-complete problem, which is difficult to solve even in front of quantum computers with powerful computing power. So, our e-voting scheme is able to resist the quantum attack.

B. PERFORMANCE ASSESSMENT AND COMPARISONS

In our scheme, the scalar multiplication, the point addition and the bilinear pairing on an elliptic curve, the point multiplication of matrix and determinant operation will be involved.

TABLE 2. The operation involved in this scheme.

T_e	The time of a bilinear pair operation is executed.
T_{mul}	The time of a scalar multiplication operation.
T_{add}	The time of a point addition operation.
T_{H_1}	The time of a hash function mapped to a point on an elliptic curve.
T_{H_2}	General hash function execution time.
T_{mat}	The time of a matrix point multiplication operation.
T_{det}	The time of a matrix determinant execution.
$\|p\|$	The size of an element in G_1.
$\|r\|$	The size of an element in Z_q^*.

TABLE 3. The computation overhead and communication overhead in different phase.

Phase	Computation overhead	Communication overhead
Initialization	$T_{mul} + 2T_{mat}$	$\|r\|+nw(PK1_i)$
Preparation	$nT_{H_1} + (n+2)T_{mul} + T_{add}$	$n(w(ID_i) + w(c) + \|p\|)$
Voting	$(5n+1)T_{add} + (5n+3)T_{mul} + 2nT_{H_2} + T_{det} + 2T_e$	$(2n+2)\|p\|+w(A) + w(Ballot)$
Achieve consensus and announce election results	0	0
Audit	$4nT_e + nT_{add} + nT_{mul}$	$2n\|p\|$

For ease of description, the following definitions will be made in Table 2. And Table 3 shows the computation overhead and communication overhead in different phase.

(1) Initialization

- The computation overhead: In the initialization phase, the computation overhead includes $T_{mul} + 2T_{mat}$.
- The communication overhead: In the initialization phase, the communication overhead between the system and the regulator is $|r|$ bits. And because of the $PK1_i$ is a binary $(n-k)n$ matrix, the communication overhead between the voters and the system is $nw(PK1_i)$ bits, where $w(PK1_i)$ represents its Hamming weight. The total communication overhead in initialization is $|r| + nw(PK1_i)$ bits.

(2) Preparation

- The computation overhead: In the preparation phase, the regulator performs $nT_{H_1} + nT_{mul}$ and $n - times$ Niederreiter encryption algorithm, voters perform one Niederreiter decryption algorithm, $T_{add} + 2T_{mul}$. The total computation overhead in preparation is $n - times$ Niederreiter encryption algorithm, one Niederreiter decryption algorithm and $nT_{H_1} + (n+2)T_{mul} + T_{add}$.
- The communication overhead: In the preparation phase, the communication overhead between the voters and the regulator is $n(w(ID_i) + w(c) + |p|)$ bits.

(3) Voting

- The computation overhead: In the voting stage, the signer needs $(4n+3)T_{mul}$, $(3n+1)T_{add}$, nT_{H_2} and a T_{det}. And the other nodes need nT_{H_2}, $2T_e$, nT_{mul} and $2nT_{add}$ when they verify the signed ballot. The total computation overhead needs $(5n+1)T_{add} + (5n+3)T_{mul} + 2nT_{H_2} + T_{det} + 2T_e$.
- The communication overhead: In the voting phase, the signer broadcasts the signed ballot to the blockchain network, which creates communication overhead $(2n+2)|p| + w(A) + w(Ballot)$.

(4) Achieve consensus and announce election results

- The computation overhead: The process of counting is the same as the ballot generation. After verifying the authenticity of all the signed ballots, the election result is obtained. Therefore, the computation overhead at this phase has been completed in the voting stage.
- The communication overhead: In the counting phase, each node generates statistical results and generates the final election result from a consensus algorithm. This process is completed by the blockchain network, and there is no process of interaction between the nodes, so the communication overhead is not generated.

(5) Audit

- The computation overhead: In the audit phase, if the worst case is considered, the regulator needs $4nT_e + nT_{add} + nT_{mul}$.
- The communication overhead: In the audit phase, the regulator sends S_i to the corresponding voter. Then the voter computes the P_i with the corresponding private key x_i and returns it to the regulator. Therefore, considering the worst case, the communication overhead needs $2n|p|$.

The performance of Niederreiter algorithm is related to its error correction ability t and length n. On the premise of guaranteeing the security of Niederreiter algorithm, such that $t \in [19, 65]$. The number of public keys increases with the increase of error correction ability t, while the information rate decreases with the increase of t [35]. The value of t should be determined according to the requirement of the number of public keys and the information rate.

In DELL Intel (R) Core (TM) i5 = 8250U CPU @ 1.60GHz 1.80GHz, we use JPBC and JAMA get the operation time involved in our scheme, as shown in Table 4. And we are drawing through python matplotlib.

TABLE 4. The number of operations and running time in our scheme.

T_e	T_{mul}	T_{add}	T_{H_1}	T_{H_2}	T_{mat}	T_{det}
5.72ms	9.15ms	0.04ms	0.59ms	<0.01ms	<0.01ms	<0.01ms

The computation overhead of the initialization phase is fixed, it takes 9.15ms. And the computation overhead of the preparation, voting, and audit increases with the number of voters. Figure 4 to Figure 6 show the relationship of computation overhead with the number of voters in different phases.

In [20], the e-voting system based on ring anonymous signcryption uses $7n+4$ T_{mul}, $3n-1$ T_{add}, $2n$ T_{H_2} and one modular operation. The computational cost of [24] depends

TABLE 5. Comparison of E-voting in requirement.

Scheme	Hard Problem	Security Requirement						
		Anonymity	Fairness	Uniqueness	Verifiability	Audit	Anti-Quantum	Tamper-Resistant
[20]	ECDLP	✓	✓	✓	✓			
[24]	RSA	✓	✓	✓	✓			✓
[25]	ECC	✓		✓	✓			✓
Our scheme	SD, ECC	✓	✓	✓	✓	✓	✓	✓

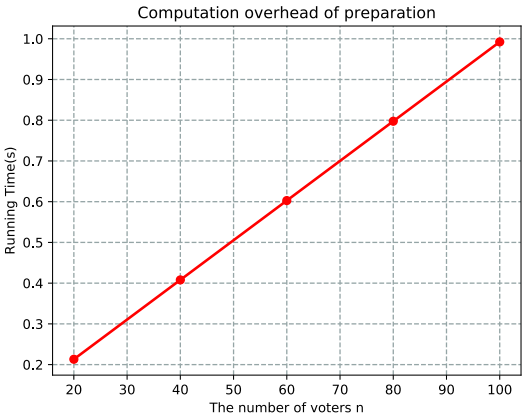

FIGURE 4. Computation overhead of preparation.

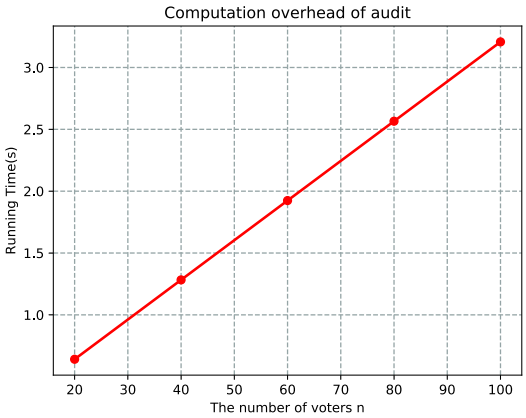

FIGURE 6. Computation overhead of audit.

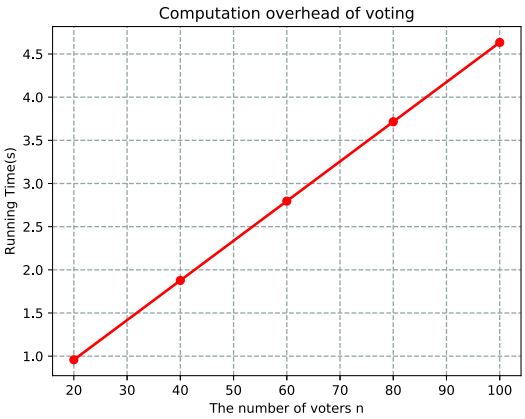

FIGURE 5. Computation overhead of voting.

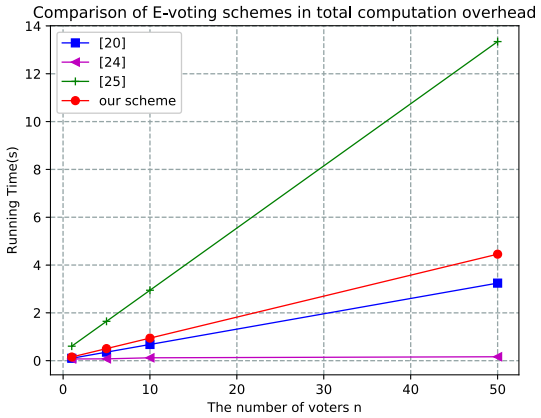

FIGURE 7. Comparison of E-voting schemes in total computation overhead.

on the time of signature and verification of ring signatures and block generation in bitcoins. And the efficient decentralized anonymous voting described in [25], 5 T_{mul}, one T_{H_1} and one T_{add} are involved in generating the key pairs and ballots. The time of generating signature ballots and verifying ballots is linearly related to the number of ring members.

Figure 7 compares the running time of our scheme with [20], [24], [25] under different values of n. Our protocol has some efficiency advantages when the number of voters is small, and it is suitable for the election activities within the company.

Table 4 gives a comparison of the security requirement of our scheme and [20], [24], [25]. Our scheme has more advantages in security requirement than them.

VI. CONCLUSION

In this paper, a blockchain e-voting protocol with audit function is introduced. We adopt the code-based Niederreiter algorithm to resist the quantum attacks. In our scheme, the KGC in certificateless cryptosystem is introduced as a regulator. It not only realized the anonymous of voters but also provided the feature of the audit by combining with the traceable ring signature algorithm, to maintain the fairness and correctness of the election. Through the analysis of our scheme, we get the conclusion that when the number of voters is small, it has some advantages in security and efficiency, which is suitable for small-scale election; when the number is large, it achieves higher security by reducing part of efficiency.

REFERENCES

[1] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, pp. 84–90, Feb. 1981.

[2] K.-H. Wang, S. K. Mondal, K. Chan, and X. Xie, "A review of contemporary E-voting: Requirements, technology, systems and usability," *Data Sci. Pattern Recognit.*, vol. 1, no. 1, pp. 31–47, 2017.

[3] R. Anane, R. Freeland, and G. Theodoropoulos, "E-voting requirements and implementation," in *Proc. 9th IEEE Int. Conf. E-Commerce Technol., 4th IEEE Int. Conf. Enterprise Comput., E-Commerce E-Services (CEC-EEE)*, Jul. 2007, pp. 382–392.

[4] F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, "E-voting with blockchain: An E-voting protocol with decentralisation and voter privacy," 2018, *arXiv:1805.10258*. [Online]. Available: https://arxiv.org/abs/1805.10258

[5] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015.

[6] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 839–858.

[7] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2001, pp. 552–565.

[8] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1984, pp. 47–53.

[9] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Berlin, Germany: Springer, 2003, pp. 452–473.

[10] T.-Y. Wang, J.-F. Ma, and X.-Q. Cai, "The postprocessing of quantum digital signatures," *Quantum Inf. Process.*, vol. 16, no. 1, p. 19, 2017.

[11] T.-Y. Wang, X.-Q. Cai, and R.-L. Zhang, "Security of a sessional blind signature based on quantum cryptograph," *Quantum Inf. Process.*, vol. 13, no. 8, pp. 1677–1685, 2014.

[12] T.-Y. Wang and Z.-L. Wei, "One-time proxy signature based on quantum cryptography," *Quantum Inf. Process.*, vol. 11, no. 2, pp. 455–463, 2012.

[13] T.-Y. Wang, X.-Q. Cai, Y.-L. Ren, and R.-L. Zhang, "Security of quantum digital signatures for classical messages," *Sci. Rep.*, vol. 5, Mar. 2015, Art. no. 9231.

[14] T.-Y. Wang and Z.-L. Wei, "Analysis of forgery attack on one-time proxy signature and the improvement," *Int. J. Theor. Phys.*, vol. 55, no. 2, pp. 743–745, 2016.

[15] F. Ren, D. Zheng, and J.-L. Fan, "Survey of digital signature technology based on error correcting codes," *Chin. J. Netword Inf. Secur.*, vol. 2, no. 11, pp. 1–10, 2016.

[16] H.-J. Yang, X.-H. Miao, H.-T. Zhu, and Y.-R. Li, "Efficient certificateless ring signature scheme with identity tracing," *Inf. Secur. Technol.*, vol. 5, no. 7, pp. 32–35, 2014.

[17] M. Hirt and K. Sako, "Efficient receipt-free voting based on homomorphic encryption," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 2000, pp. 539–556.

[18] B. Lee and K. Kim, "Receipt-free electronic voting scheme with a tamper-resistant randomizer," in *Proc. Int. Conf. Inf. Secur. Cryptol.* Berlin, Germany: Springer, 2002, pp. 389–406.

[19] S. S. M. Chow, J. K. Liu, and D. S. Wong, "Robust receipt-free election system with ballot secrecy and verifiability," in *Proc. NDSS*, vol. 8, 2008, pp. 81–94.

[20] T.-C. Hsiao, Z.-Y. Wu, C.-H. Liu, and Y.-F. Chung, "Electronic voting systems for defending free will and resisting bribery and coercion based on ring anonymous signcryption scheme," *Adv. Mech. Eng.*, vol. 9, no. 1, pp. 1–9, 2017.

[21] H. Li, Y. Sui, W. Peng, X. Zou, and F. Li, "A viewable E-voting scheme for environments with conflict of interest," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2013, pp. 251–259.

[22] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019.

[23] W.-J. Lai, Y.-C. Hsieh, C.-W. Hsueh, and J.-L. Wu, "DATE: A decentralized, anonymous, and transparent E-voting system," in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Aug. 2018, pp. 24–29.

[24] Y. Wu, "An E-voting system based on blockchain and ring signature," M.S. thesis, Dept. Comput. Sci., Univ. Birmingham, Birmingham, U.K., 2017.

[25] W.-J. Lai and J.-L. Wu, "An efficient and effective decentralized anonymous voting system," 2018, *arXiv:1804.06674*. [Online]. Available: https://arxiv.org/abs/1804.06674

[26] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Cham, Switzerland: Springer, 2017, pp. 357–375.

[27] C. K. Adiputra, R. Hjort, and H. Sato, "A proposal of blockchain-based electronic voting system," in *Proc. 2nd World Conf. Smart Trends Syst., Secur. Sustainability (WorldS)*, Oct. 2018, pp. 22–27.

[28] Y. Li, W. Susilo, G. Yang, Y. Yu, D. Liu, and M. Guizani, "A blockchain-based self-tallying voting scheme in decentralized IoT," 2019, *arXiv:1902.03710*. [Online]. Available: https://arxiv.org/abs/1902.03710

[29] R. J. McEliece, "A public-key cryptosystem based on algebraic," *Coding Thv*, vol. 4244, pp. 114–116, Apr. 1978.

[30] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory," *Problems Control Inf. Theory*, vol. 15, no. 2, pp. 159–166, 1986.

[31] Y. X. Li, R. H. Deng, and X. M. Wang, "On the equivalence of McEliece's and Niederreiter's public-key cryptosystems," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 271–273, Jan. 1994.

[32] E. Berlekamp, R. J. McEliece, and H. C. A. Van Tilborg, "On the inherent intractability of certain coding problems (Corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 384–386, May 1978.

[33] B. Li, D.-G. Feng, and S.-H. Qing, "A survey on decoding algorithms of algebraic-geometric codes," *Acta Electron. Sinica*, vol. 29, no. 1, pp. 110–117, 2001.

[34] J. Herranz and G. Sáez, "Forking lemmas for ring signature schemes," in *Proc. Int. Conf. Cryptol. India*. Berlin, Germany: Springer, 2003, pp. 266–279.

[35] L. Yuanxing and W. Xinmei, "On the security of the Niederreiter's publickey algebraic-code cryptosystem and the optimization of parameters," *Acta Electron. Sinica*, vol. 1, no. 7, pp. 33–36, 1993.

SHIYAO GAO received the B.S. degree from the Xi'an University of Posts and Telecommunications, in 2017. She is currently pursuing the M.S. degree with the Xi'an University of Posts and Telecommunications, China. She is doing research at the National Engineering Laboratory for Wireless Security. Her research interests include blockchain technology, electronic voting, and information security.

DONG ZHENG received the Ph.D. degree from Xidian University, in 1999. He joined the School of Information Security Engineering, Shanghai Jiao Tong University. He is currently a Professor with the Xi'an University of Posts and Telecommunications, China. His research interests include information theory, cryptography, and information security. He is also a Senior Member of the Chinese Association for Cryptologic Research and a member of the Chinese Communication Society.

RUI GUO received the Ph.D. degree from the State Key Laboratory of Networking and Switch Technology, Beijing University of Posts and Telecommunications, China, in 2014. He is currently a Lecturer with the National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications. His current research interests include attribute-based cryptograph, cloud computing, and blockchain technology.

CHUNMING JING received the bachelor's degree from the Xi'an University of Posts and Telecommunications, in 2017, where he is currently pursuing the master's degree with the National Engineering Laboratory for Wireless Security. His research interests include security and privacy in the Internet of Things, and blockchain technology.

CHENCHENG HU received the B.Eng. degree from the Xi'an University of Posts and Telecommunications, in 2016, where he is currently pursuing the M.S. degree. He is doing research at the National Engineering Laboratory for Wireless Security. His current research interests include blockchain technology, user authentication, and information security.