Quantum-Resistant Zero-Knowledge Proof Blockchain Electronic Voting System

Pengsen Yu[1]*

1. College of Information Technology, Shanghai Ocean University, Shanghai 201306, China
Corresponding Author's Email: ypengsen@163.com

Abstract: Following the emergence of the COVID-19 pandemic, electronic voting has gradually become an inseparable part of people's lives. However, it has also raised a series of severe privacy and trust challenges. The immutable and publicly transparent characteristics of blockchain are a perfect fit for the development of electronic voting systems, effectively eliminating voters' concerns about ballot tampering.At the same time, zero-knowledge proofs enable the prover to show they possess certain information to the verifier, without disclosing the actual details. It is important to note that with the rapid development of quantum technology, traditional cryptographic schemes face unprecedented security threats. To address this challenge, We present a quantum-resistant blockchain solution for electronic voting, incorporating zero-knowledge proofs. Compared to conventional elliptic curve-based zero-knowledge proof schemes, our proposed solution is based on RLWE, ensuring voter privacy, and uses BFV fully homomorphic encryption technology to implement a blockchain-based electronic voting protocol, ensuring the system's high availability, security, and anonymous voting. Security analysis and performance testing, along with comparisons to existing similar solutions, show that our scheme has advantages in terms of security and robustness, making it highly practical.

Keywords: Quantum-resistant; Blockchain; Zero-Knowledge Proofs; Homomorphic Encryption; Electronic Voting

Introduction

Due to the rapid advancements in information technology and the fast-paced digitalization, traditional voting methods are gradually transitioning to electronic voting. As early as 1981, Chaum [1] first introduced the concept of electronic voting technology. Its purpose is to utilize electronic technology for elections or voting, aiming to improve the productiveness, accuracy, and accessibility of voting. Compared to traditional voting methods, electronic voting offers a fast, reliable, and secure voting platform, which can significantly increase voter participation and satisfaction. At the same time, it supports remote voting, allowing voters with physical limitations or those in remote geographic locations to easily participate, enhancing the inclusivity of elections. Additionally, by implementing electronic voting, human errors are significantly reduced, leading to improved accuracy and faster vote counting. The application of electronic technology inevitably brings a series of security and privacy protection challenges [2].

In recent years, to protect voter privacy and ensure vote confidentiality and the verifiability of election results, online voting systems utilize cryptographic schemes like hybrid network encryption, blind signatures, ring signatures, and homomorphic encryption. Despite these premunitions, the security of online election systems remains a significant concern. In 2018, on the eve of Mexico's elections, a database without password protection was exposed online, containing the registration information of 93 million Mexican voters. These data breaches have sparked widespread public concern and alarm, serving as a wake-up call for researchers in various related fields.

Security challenges in online election systems not only include data security and system tamper-resistance but also extend to protecting voter privacy and preventing potential cyberattacks. Therefore, it is essential to develop one not only secure but also reliable electronic voting system, which must integrate effective security protocols and privacy protection technologies within its design.

Among the new security measures and privacy protection technologies, blockchain technology stands out as a distributed ledger system [4]. It allows data to be recorded in a decentralized and immutable database, where the data structure consists of a series of blocks arranged in chronological order. Each block will be linked to its predecessor, forming chains of blocks. This structure ensures data permanence and transparency, while protecting it from tampering or forgery. Since each block is validated through a consensus algorithm of network nodes before being added to the chain, once data is written to the blockchain, it is almost impossible to alter. This makes it nearly impossible to alter ballots.

While blockchain greatly improves the safety and transparency of electronic voting scheme, traditional techniques like RSA or ECC still depend on mathematical problems. The emergence of quantum computational capabilities poses significant threats to conventional cryptographic frameworks, particularly in their vulnerability to quantum-based cryptanalytic approaches [5]. The advancement of quantum computational capabilities renders conventional cryptographic schemes increasingly vulnerable to quantum cryptanalysis. Notably, Shor's algorithm [6], offering polynomial-time solutions to foundational mathematical problems, jeopardizes the security of cryptographic infrastructures dependent on these computational assumptions. In light of this, adopting quantum-resistant encryption technology has become essential to safeguarding the long-term security of electronic voting systems. Quantum-resistant cryptographic techniques, such as lattice-based encryption, hash-based encryption, and multivariate polynomial encryption, offer viable solutions, not only resist quantum computing attacks but also retain the high efficiency and relatively low computational complexity of traditional cryptography. These technologies provide a solid security foundation for electronic voting systems without compromising system performance, ensuring that even in the face of potential threats from quantum computers, voter data and vote results remain immutable and fully private, thereby strongly safeguarding the fairness and reliability of the electronic voting system.

Therefore, our research will focus on how to effectively integrate quantum-resistant encryption technologies into existing electronic voting systems to address the security challenges posed by future technological developments. By comparing and analyzing the performance and security of existing cryptographic schemes and quantum-resistant encryption schemes in the application of electronic voting, the goal is to propose a practical and efficient solution to enhance the resilience of electronic voting systems in the face of quantum computing threats.

Contribution: This research makes three key contributions:

(1) Architectural Innovation: We design a RLWE-based quantum-resistant voting system utilizing blockchain smart contracts, guaranteeing post-quantum security through lattice cryptography primitives;

(2) Privacy Preservation: A non-interactive zero-knowledge proof (NIZK) authentication protocol achieves single-round identity verification without exposure, while BFV fully homomorphic encryption ensures end-to-end confidentiality of voting data;

(3) Protocol Optimization: By developing modulus alignment techniques and error control strategies, we reconcile algebraic structures between RLWE authentication and BFV encryption. Experimental evaluations validate the high practicability of our solution.

2. Related Work

This section will review the existing research focused on developing a secure electronic voting system. Table

Table 1 provides an overview of the latest electronic voting protocols.

Table 1 The summary of the recent e-voting protocols.

Article	Year	Implementation	Advantages	Disadvantages
A Blockchain-based, Anonymous, Robust,and Scalable Ranked-choice Voting Protocol[7]	2023	Use a ZKP to authenticate that the submitted score is within a range publicly defined in advance	Support rating voting	Can only be applied to small and medium-sized voting
Privacy-Preserving E-Voting System Supporting Score Voting Using Blockchain [12]	2022	Developed libraries for several RS voting algorithms, integrated Merkle trees for voter registration, and used semaphores for zkSNARK implementation	Support multiple types of ranking selection(RS) through e-voting	The Ranked selection and Merkle tree structure algorithms are inefficient.
Tornado Vote: Anonymous Blockchain-based Voting[9]	2023	Anonymous provider, Merkle tree structure, ERC-20 token, ZKP verification	Adjusted the comprehensive mixed protocol tornado cash to	The remaining capacity model ignores transaction costs, leading to a

			separate voters' wallets from their votes	surge in transaction costs
An effcient and versatile e-voting scheme on blockchain[10]	2024	Blind signature aggregation, zero-knowledge proofs, and threshold encryption techniques for enhancing smart contracts	Once voters obtain one-time identity authentication from the smart contract, they can vote multiple times until their identity is revoked	The verification cost is variable and may not be ideal for large-scale voting scenarios
Post-quantum Online Voting Scheme[11]	2021	Lattice-based, Threshold Version of Blind Signature	Support multi-candidates and complex ballots structure	Unable to achieve Correctness, Verifiability, Anonymity as using Mix-net

Blockchain Based e-voting. Since the seminal publication of Bitcoin's whitepaper by the pseudonymous Satoshi Nakamoto in 2008[4], distributed ledger technology has emerged as a transformative paradigm in secure decentralized systems. It is a decentralized distributed ledger system that ensures data immutability, traceability, and programmability by chaining blocks of data in chronological order, utilizing cryptographic methods, consensus protocols, and smart contracts. This technology enables information verification and transmission between mutually distrustful parties without the need for a centralized authorization authority. The distributed and public nature of blockchain not only guarantees transparent recording of all voting activities and results but also allows all authorized participants to review and verify the voting process and outcomes, thereby increasing system transparency and enhancing voter trust in the election process. Moreover, blockchain uses advanced techniques to hold back unauthorized access to data and can be designed to support anonymous voting, protecting voter privacy while ensuring the immutability of vote records.

Although blockchain technology was initially used primarily for cryptocurrencies, the widespread application of smart contracts has driven its expansion into various use cases. These blockchain-based applications are referred to as decentralized applications (DApps). Each blockchain node runs a smart contract, which contains business rules and logic, to maintain and update its local copy depending on the results.Since smart contracts are stored on the blockchain, blockchain eliminates the reliance on trusted third parties, thus strengthening its decentralized nature.

In 2015, Chan et al. [9] first proposed a blockchain-based electronic voting solution that utilized Bitcoin's reward and penalty mechanisms to achieve voting transparency and openness. However, due to the reliance on Bitcoin’s implementation and the limitations of its consensus mechanism, this solution has not been widely adopted in practical applications, and it suffers from low vote counting efficiency and high complexity. Additionally, the solution has shortcomings in ensuring the security of voting results.Lee et al. [12] enhanced

Chan's solution by introducing a trusted third party, aiming to guarantee the security of the voting process. McCorry [13] proposed an automated voting solution based on Ethereum, which implements automatic vote counting on the blockchain through smart contracts and protects voter privacy using ring signatures. However, this solution is limited to scenarios where voters choose between two candidates.The scheme in [8] enables ranked-choice voting on the blockchain network, ensuring security and privacy in a way similar to other current research, utilizing a signal tool for Zk-SNARKS implementation, and employing Merkle trees for voter registration. Scheme [7] builds on these foundations and proposes an electronic voting solution that supports score voting.

Zk Based e-voting. In addition, to prevent invalid ballots from disrupting the voting system, implementing vote validity verification becomes necessary, and zero-knowledge proof technology provides effective technical support for this. Unlike traditional digital signatures that rely on non-repudiation, zero-knowledge proofs do not directly depend on non-repudiation, but they provide a higher level of privacy protection.A zero-knowledge proof is a cryptographic method that confirms the validity of a statement while keeping any specific details about it confidential. Zero-knowledge proof protocols enable the verification of ballot correctness in e-voting systems while maintaining strict voter anonymity and ensuring the secrecy of electoral selections.In 2008, Camenisch et al. [14] introduced the set membership determination problem and constructed the first Zero-Knowledge Set Membership Proof (ZSMPP) protocol under the Strong Diffie-Hellman (SDH) assumption in a bilinear group. Subsequently, Morais et al. [15] optimized the proof stage of [14]'s protocol using a digital signature scheme [16], significantly reducing the computational overhead to a constant level. Recently, Yin et al. [17] constructed a zero-knowledge proof protocol based on an aggregation function that supports both "belonging to" and "not belonging to" relationships, with its security also relying on the SDH assumption. Robert[18] combined Tornado Cash with non-interactive succinct zero-knowledge proofs (zk-SNARKs) to verify the hash values of voters. Meanwhile, Wang et al. [10] integrated Bulletproof technology with threshold encryption, significantly enhancing the fairness of voting.

Lattices Based e-voting. Quantum computing advancements expose vulnerabilities in classical security schemes when facing quantum threats [5]. Post-quantum cryptography's integration into electronic voting systems is a growing research focus, but its application remains in the early stages.Lattice-based fully homomorphic encryption is a key technology for constructing post-quantum systems.Kim [11] combines lattice cryptography and blind signature technology to achieve a voting system supporting multiple candidates, but its voting structure is too complex to lead to poor practicability. Ronne[19] proposes a homomorphic encryption scheme that can be executed in linear time to enhance the ability to counter quantum attacks, but the scheme lacks formal security proof against conventional attacks. Naidu et al.[20] have developed a new electronic voting system that combines blockchain technology with homomorphic encryption, focusing primarily on the encryption of voter information rather than the ballot information. The benefit of this system is its ability to perform statistical analysis of the voting results while maintaining voter privacy. However, This method can not achieve the whole process of quantum resistance, does not make full use of the potential of homomorphic encryption, our scheme protects both voter information and ballot information.

3. Preliminaries

In this section,we provides an overview of the relevant techniques and cryptographic primitives employed in this paper. The main symbols of our scheme in this scheme are shown in Table

Table 2.

Table 2 Notation

Notation	Definition
n	security parameter, it’s a power of 2

q	a positive integer
$C_i, i \in [1, n]$	candidate
EI	Electoral institutions
Sk_A	Secret information
(Pk_B, Sk_B)	Public and private key pairs of EI
(Pk_C, Sk_C)	Public and private key pairs of Voters
π	Proof
(Pk_D, Sk_D)	Public and private key pairs of BFV
ω	Signal function
χ, χ_a	Discrete Gaussian distribution
H_1, H_2	Hash function
ct	Encrypted voting
$\mathrm{mod2}()$	mod2 denoising function

3.1 Non-interactive zero-knowledge proof

Definition 1. A non-interactive zero-knowledge proof (NIZKP) is a variant of zero-knowledge proof where the proof process does not require multiple interactions with the verifier. Instead, the prover generates a proof certificate and sends it to the verifier, who can verify its validity. This non-interactive feature makes NIZKP more efficient and convenient in practical applications, especially for scenarios where public certification is required, such as transaction verification in the blockchain. To function properly, the non-interactive zero-knowledge proof protocol requires three essential properties: Completeness, Soundness, and Zero-Knowledge.

Completeness. If the statement holds true, the honest verifier will trust the fact based on the honest prover's claim. Integrity ensures that the verifier can correctly verify and accept the certificate when the witness does have the declared knowledge (such as the secret key in cryptography) and follows the protocol steps. This feature ensures that the system does not incorrectly reject legitimate proofs under normal circumstances.This means that for $\forall x \in L$,the fruit proof has a secret value s ,so there is：

$$\Pr[\pi \leftarrow P(x,s) : V(x,\pi) = 1] \geq 1 - negl(\lambda) \tag{1}$$

Soundness. If the statement holds true, no one of the provers as an adversary can convince the honest verifier that it is true, unless the probability is negligible. This means that ideally only true statements can pass verification, while forged statements are almost impossible to pass, for $\forall x \notin L$,If the witness has no secret value s ,then：

$$\Pr[\pi \leftarrow P(x) : V(x,\pi) = 1] \leq negl(\lambda) \tag{2}$$

Zero-knowledge. If this assertion holds, the verifier remains unaware of the secret, yet the assertion itself is valid. In other words, there exists a simulator operating in polynomial time such that, for $\forall x \in L$ and the corresponding secret value s , the following two distributions cannot be distinguished computationally:

$$|\Pr[Exp_{ZK-real}]-\Pr[Exp_{ZK-sim}]|\le negl(\lambda) \quad (3)$$

Non-interactive. The provfier only conducts one round of communication with the verifier in the proof stage, and in our scheme represents the voters only one round of communication with the blockchain.

3.2 Ring learning with error

The RLWE assumption used in this paper is based on the classical hard problem on lattices defined by Regev [21].

Definition 2. Discrete Gaussian distribution: the central point of the distribution for $\forall\sigma>0, x\in Z^n$ is specified by c . Furthermore, the n-dimensional discrete Gaussian distribution is characterized by $\rho_{\sigma,c}(x)=(\frac{1}{\sigma})^n e^{\frac{-\pi||x-c||^2}{\sigma^2}}$. Mathematically, the discrete Gaussian distribution can be formally defined as: $D_{L,\sigma,c}=\frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(L)}$.

Lemma 1. Set $R=Z[x]/(x^n+1)$,for any $a,b\in R$,we have $||a\cdot b||\le\sqrt{n}\,||a||\cdot||b||$ and $\|a\cdot b\|_\infty\le\|a\|_\infty\cdot\|b\|_\infty$.

Lemma 2. For any $\sigma\ge\omega(\sqrt{\log(n)})$,then we have $\Pr_{x\leftarrow D_{L,\sigma,c}}[\|x\|>\sigma\sqrt{n}]\le 2^{-n}$

Definition 3. RLWE difficult problem[22]:set $n\in Z$ is of a power of 2, q is a positive integer,The discrete Gaussian distribution on the R_q is given by χ_α .For polynomial rings,a uniformly selected element s in the R_q, $a\leftarrow R_q$ .Set A_{s,χ_α} is the distribution of the pair $(a, as+2e)\in R_q\times R_q$,and $e\leftarrow\chi_\alpha$ is independent of a .In the distribution $R_q\times R_q$, A_{s,χ_α} is indistinguishable in polynomial algorithm time.

Assumption 1.[22]The safety of our protocol relies on the RLWE assumption that,which is defined as $(a_i, a_i s+e_i)$, inside a_i is random number on R_q, s, e_i are small, indistinguishable polynomials.

3.3 BFV full homomorphic encryption

In 2012, Brakerski and colleagues adapted the fully homomorphic encryption scheme originally based on the LWE problem to one based on the RLWE problem, thereby yielding the BFV fully homomorphic encryption algorithm. This algorithm is constructed over a polynomial ring $R=Z[x]/(x^N)+1$. In our proposed system, the BFV algorithm is utilized for ballot addition, encryption, and counting. The scheme comprises six core algorithms: private key generation, public key generation, re-linearization key generation, encryption, decryption, and homomorphic addition.

Private key generation:random selection s , s is a polynomial with a coefficient of-1,0,1, outputting the private key $sk = s$.

Public key generation:input private key sk ,Select a as a random polynomial,its coefficient mode is q , e is a sufficiently small enough noise polynomial to output the public key $pk = ([-as + e]_q, a)$.

Re-linearized key generation:input private key sk ,random selection a_i and e_i , $i \in \{0,1,\ldots,l\}$, $l = \lfloor \log_w(q) \rfloor$, w is the base of the log,output $rk = ([-(a_i s + e_i) + w^i s^2]_q, a_i)$.

Encryption algorithm:input the plain text m ,public key pk ,three random polynomials were randomly generated simultaneously e_1, e_2, u ,the first two are noise, u is a polynomial with a coefficient of-1,0, and 1, which is calculated $ct = ([\lfloor q/t \rfloor [m]_t + pk_0 u + e_1]_q, [pk_1 u + e_2]_q)$.

Decrypt algorithm: input the private key sk , $c = (c_0, c_1)$, output $m' = \llbracket t/q[c_0 + c_1 s]_q \rrbracket$.

Homomorphic addition operations: input ciphertext ct and ct', output $(ct[0] + ct'[0], ct[1] + ct'[1])$.

3.4 Signal function

Given $Z_q \in \{-\frac{q-1}{2}, \ldots, \frac{q-1}{2}\}$,we use the signal function[23] to eliminate error caused by the function $\bmod_2$ on R_q.

Definition 4. Signal function:let $E_1 = [-\left\lfloor \frac{q}{4} \right\rfloor, \left\lceil \frac{q}{4} \right\rceil]$, $E_2 = [-\left\lfloor \frac{q}{4} \right\rfloor + 1, \left\lceil \frac{q}{4} \right\rceil + 1]$,there is a signal function $Sig() : Z_q \to \{0,1\}$ as follows:

$$Sig(x) = \begin{cases} 0 & , x \in E_1 \ or \ x \in E_2 \\ 1 & , otherwise \end{cases} \tag{4}$$

Definition 5. $\bmod_2$ function: $Z_q \times \{0,1\} \to \{0,1\}$ is defined as:

$$\bmod_2(x, a) = (x + a \cdot \frac{q-1}{2}) \bmod q \bmod 2$$

Lemma 3. Let q be an odd number, $x, y \in Z_q$ and $\| x-y \|_\infty < \frac{q}{4}$, $a = char(x)$,we have

$$\mathrm{mod}_2(x,a) = \mathrm{mod}_2(y,a) \tag{5}$$

Proof. known $\| x-y \|_\infty < \frac{q}{4}$,let $x = y + 2\varepsilon$, $|2\varepsilon| \le \frac{q}{4} - 2$,notice $(x + a \cdot \frac{q-1}{2}) \mathrm{mod}_q = (y + a \cdot \frac{q-1}{2} + 2\varepsilon) \mathrm{mod}_q$,from the functions $Sig()$ we define, we know that: $|x + a \cdot \frac{q-1}{2}| < \frac{4}{q} + 1$,because $|y + a \cdot \frac{q-1}{2} + 2\varepsilon| \le |y + a \cdot \frac{q-1}{2}| + |2\varepsilon| \le \frac{q}{2} - 1$, $(y + a \cdot \frac{q-1}{2} + 2\varepsilon) \mathrm{mod}_q = (y + a \cdot \frac{q-1}{2}) \mathrm{mod}_q + 2\varepsilon$,after the mod_2 operation on both sides of the equation, we get:

$$\mathrm{mod}_2(x,a) = (x + a \cdot \frac{q-1}{2}) \mathrm{mod}_q \, \mathrm{mod}_2 = (y + a \cdot \frac{q-1}{2}) \mathrm{mod}_q \, \mathrm{mod}_2 = \mathrm{mod}_2(y,a)$$

□

Then, the signal function mod_2 and the mod_q function are extended to polynomial rings by each coefficient that $x_i \in Z_q$ .Theorem 3 after extending to the polynomial ring still holds.So we can extend the signal functions and functions mod_2 to polynomial rings $R_q^{n \times n}$ in our scheme.

Current research on RLWE key security reveals critical insights: Ding et al. [22][23] identified potential key leakage vulnerabilities in signal function implementation during long-term public key reuse, while simultaneously acknowledging its cryptographic significance. Subsequently, Gao et al. [24] proposed an enhanced key reuse paradigm incorporating user-specific identifiers and modified error parameters to mitigate these security concerns.

3.5 BlockChain

Blockchain is a data structure[25], which is open and transparent. The blockchain infrastructure maintains an immutable distributed ledger composed of sequentially linked transaction blocks. This architecture enforces strict append-only operations through decentralized consensus mechanisms, ensuring data integrity by preventing modification or deletion of recorded transactions. Another key feature of blockchain is that it is open and transparent. Blockchain technology has some of its following important features:/

1) Decentralized:a blockchain network is composed of many independently running nodes, each with a

complete copy of the data.

2) Invariance:The blockchain's immutability property ensures permanent data preservation through cryptographic chaining mechanisms. Each block's integrity is maintained by its cryptographic linkage (typically via hash functions) to its predecessor, creating an unalterable chain of records resistant to modification or deletion.

3) Non-repudiation :transactions and data records on the blockchain cannot be denied by the sender. Typically, these transactions include digital signatures, ensuring that only those with the corresponding private key can generate valid transactions.

4) Transparency:the openness of the blockchain allows anyone to view all the transactions and records on the chain. While personal identities can remain anonymous or fake names, details of the transaction are made public.

5) Traceability:every transaction made on the blockchain can be traced and validated. Each block contains timestamps and transaction data, forming an immutable history.

4. System and Security Models

The body and safety model of the proposed scheme are discussed in this section.

4.1 Election Subject Model

The voting body consists of three parts, namely blockchain, voter and electoral body, as shown in Figure 1.

Blockchain: Responsible for verifying all voting requests and automatically counting votes. All of the relevant business logic is stored in the smart contract;

Electoral institution: An electoral institution may be any entity that conducts elections or decision voting; this entity need not have a political objective. Electoral agencies should be responsible for issuing election announcements to the blockchain and deploying smart contracts. They are also responsible for generating a list of candidates and qualified voters;

Voter: Within the electoral framework, voters represent authenticated entities authorized to participate in the voting process. The system enforces strict identity verification protocols, ensuring that only properly authenticated votes are included in the final tally, while rejecting submissions lacking valid authorization credentials.

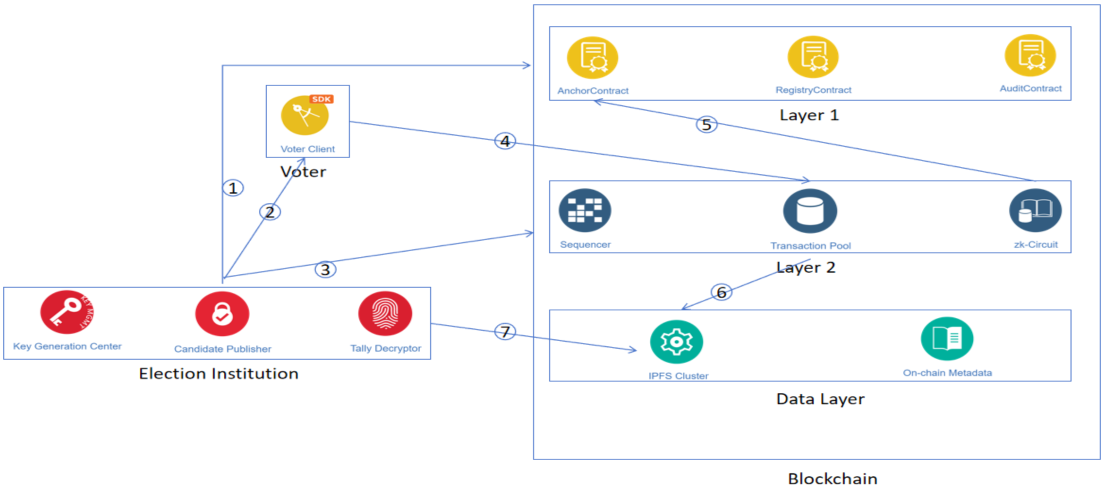

Figure 1. System architecture: 1) Upload system parameters; 2) Send registration information; 3) Sync initial identity data; 4) Submit encrypted votes and proof ; 5) Commit proof and stateroot; 6) Store the encrypted ballots; 7) Aggregate and homomorphic decrypt.

4.2 Security Model

This section formalizes a security framework for publicly verifiable non-interactive zero-knowledge proofs (NIZK) under a semi-honest adversarial model. Building upon the standard NIZK definition **Error! Reference source not found.**, we incorporate a curious-but-honest third party that strictly adheres to protocol specifications while attempting to extract maximal information from legitimately obtained data. Our security model operates in the random oracle paradigm and considers two distinct adversarial categories:

1.External adversaries limited to public information access, attempting to generate valid proofs prior to semi-trusted party intervention.

2.Internal adversaries (the semi-trusted party) with access to registration and certification phase data.

5. The Voting Scheme

This chapter presents a self-tallying electoral system that integrates zero-knowledge protocols and quantum-resistant techniques. The cryptographic underpinnings of the system merge a non-interactive zero-knowledge (NIZK) authentication protocol for secure key exchange with the Brakerski-Fan-Vercauteren (BFV) fully homomorphic encryption scheme to enable privacy-preserving vote tabulation. In the following discussion, we will elaborate on the pertinent aspects.

5.1 Setup Phase

Before the election begins, the electoral body publishes a list of candidates $\{C_1,..., C_k\}$ .Select a random matrix $a_i \leftarrow R_q$ for each voter and obtain the secret vector satisfying the discrete Gaussian distribution

Sk_A ,The electoral body issues both secret vectors and a random matrix to the voters, who generate Pk_A based on both terms. The specific operations are described as follows:

1. Set $H_1:\{0,1\}^{n\times n}\rightarrow\{0,1\}^n$ $H_2:\{0,1\}^{n\times n}\rightarrow\{0,1\}^n$,both hashing algorithms are SHA-3, $Sk_A, e_A \leftarrow \chi_\alpha$ .Voter calculation: $Pk_A = a_i \cdot Sk_A + 2e_A \mod q$, Sk_A is secret information.

2. Voters need to prove that they have secret information to authenticate, and then they calculate their public and private keys $Pk_C = a_i \cdot Sk_C + 2e_C \mod q$, $Sk_C, e_C \leftarrow \chi_\alpha$, the voter's private key is Sk_C .

3. The same goes for the electoral body SI ,it's private key is Sk_B ,public key $Pk_B = a_i \cdot Sk_B + 2e_B \mod q$. $Pk_A, Sk_A, Pk_B, Sk_B, Pk_C, Sk_C$ will be used by voters and electoral institution to construct zero knowledge proof π 。

The BFV algorithm used in this scheme was implemented by invoking the Tenseal library. Smart contracts generate public and private key pairs used for BFV homomorphism encryption and decryption,private key Sk_D is a randomly generated polynomial with a coefficient of-1,0 or 1,public key $Pk_D = ([-a_i Sk_D + e_D], a_i)$, a_i is a polynomial randomly generated in the ciphertext space,the coefficients are modulo p , e_D is a small coefficient noise polynomial randomly selected in a discrete Gaussian distribution, which is discarded after use. The public key is shared with all voters by the blockchain.

5.2 Register Phase

$Register(a_i, Pk_A, Pk_B, Pk_C) \rightarrow (P)$ the registration algorithm is executed by the electoral institution,using random matrices $a_i \leftarrow R_q$, Pk_A .Public key for the election institution Pk_B and vote's public key Pk_C as input.Using signal function ω to eliminate noise,output P ,EI save P_A and public Pk_A, P to the blockchain.The specific implementation is provided as follows:

1. Votes compute $X = Sk_A \cdot Pk_B \cdot Pk_C, x = Sk_A \cdot Pk_B$, $\omega = Sig(x)$, ω will be used to generate hashes that test the voters' legitimacy.Send Pk_A, Pk_C, ω to EI.

2. After receiving Pk_A, Pk_C, ω ,the electoral institution conducts the following operations:

First,check Pk_A ,if Pk_A is in the list,reject (prevent revoting) and add it to the list if not.

Set $Y = Pk_A \cdot Sk_B \cdot Pk_C, y = Pk_A \cdot Sk_B$,EI compute:

$$P = H_2(H_1(\mathrm{mod}_2(Y,\omega))) \tag{6}$$

3. EI open (Pk_A, Pk_B, P) to blockchain, P is the hash used by the blockchain to verify the identity of the voters.

5.3 Voting Phase

$Voting(X,\omega,m) \to (\pi,ct)$, at this stage, voters are required to submit authentication information and ballot information (π,ct) .Smart contracts will first authenticate and then count the votes. When verified, the voters will prove that they are a legal voter. After the ballot information is submitted to the blockchain, the blockchain will be verified through the following process:

1. Proof $\pi = H_1(\mathrm{mod}_2(X,\omega)), \omega = Sig(x)$,this certificate is generated by the voters, who then submit the certificate to the blockchain.After the smart contract receiving (π, P) ,Smart contracts are verified according to the equation $H_2(\pi) \overset{?}{=} P$,if $H_2(\pi) = P$ verification passes,otherwise, it does not pass.

2. When counting, this scheme is based on BFV homorphism encryption scheme, through the direct operation to vote to ensure that ballot information will not leak, each voter will generate his encryption vote sent to block chain, voters from the block chain for candidate information generated votes and vote, vote after encryption votes sent to block chain. Voters elect their supporters and generate votes,using the homomorphic encrypted public key Pk_D to encrypt the vote and get the ciphertext vote. The process is as follows:

Encrypting votes with smart contract $Pk_D = (pk_0, pk_1) = ([a_i \cdot Sk_D + 2e_D]_q, a_i)$ shared to voters:

$$ct = (c_0, c_1) = ([\left\lfloor \frac{q}{t} m \right\rfloor + pk_0 u + e_1]_q, [pk_1 u + e_2]_q) \tag{7}$$

m is plaintext,Represents voters on the list of candidates $\{C_1,..., C_n\}$, u is a polynomial with a coefficient of-1,0 or 1,and t is an integer much smaller than the coefficient module p e_1, e_2 are taken from the same discrete Gaussian distribution,These polynomials are only used during the encryption process, which voters discard them.Voters send ct to the blockchain.

5.4 Tally Phase

Following the conclusion of the voting process, the smart contracts implemented on the blockchain will aggregate and tally all the votes collected during the election. The total votes for each candidate C_k will be computed in accordance with the sequence of votes cast.

$$Add(c_{im}, c_{jm}, rk) = (ct_i[0] + ct_j[0], ct_i[1] + ct_j[1]) \tag{8}$$

1. The above formula represents the result of adding up the cipheric votes of two voters $V[i]$ and $V[j]$,By utilizing the property of fully homomorphic encryption, which allows direct computation on ciphertexts, it is possible to compute the total number of votes for all candidates. $ct_0[i]$ and $ct_0[i]$ represent the two ciphertexts obtained after encrypting the plaintext m_i . $ct_0[j]$ and $ct_1[j]$ represent the two ciphertexts obtained after encrypting the plaintext m_j .

2. After the vote tallying phase, the blockchain decrypts the votes with the BFV private key, and publishes the results on the blockchain:

$$m' = \left[\left\lfloor \frac{t}{q} [c_0 + c_1 s]_q \right\rceil \right]_t \tag{9}$$

m' is the result of BFV.

The overall voting process is shown in the Figure 2.

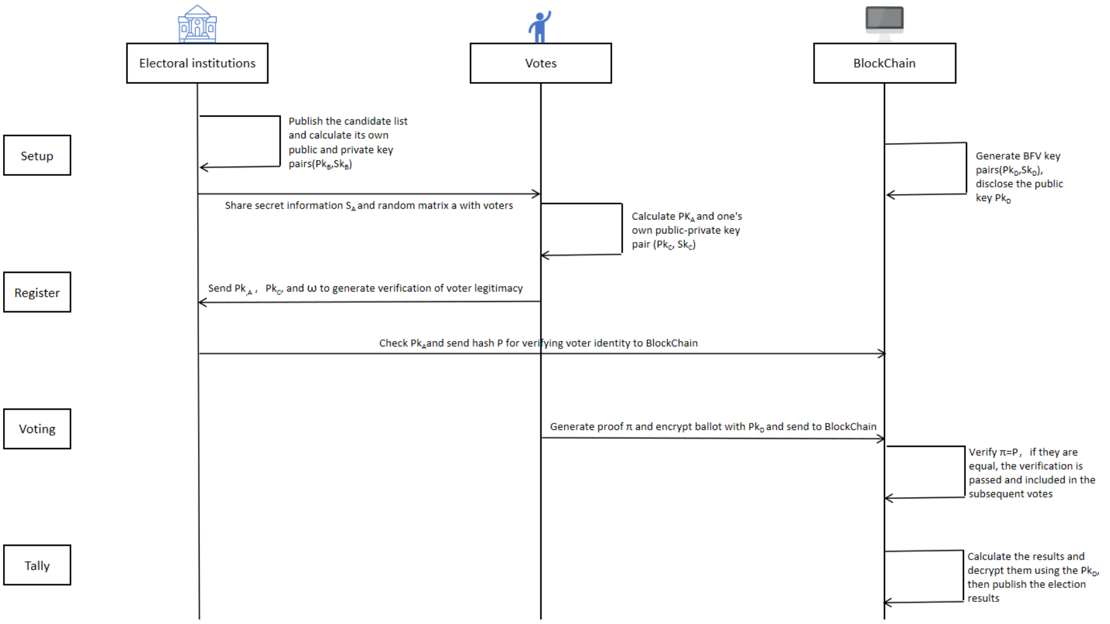
Electoral institutions
Votes
BlockChain
Setup
Register
Voting
Tally
Publish the candidate list and calculate its own public and private key pairs(Pk_B,Sk_B)
Generate BFV key pairs(Pk_D,Sk_D), disclose the public key Pk_D
Share secret information S_A and random matrix a with voters
Calculate PK_A and one's own public-private key pair (Pk_C, Sk_C)
Send Pk_A , Pk_C, and ω to generate verification of voter legitimacy
Check Pk_A and send hash P for verifying voter identity to BlockChain
Generate proof π and encrypt ballot with Pk_D and send to BlockChain
Verify π=P, if they are equal, the verification is passed and included in the subsequent votes
Calculate the results and decrypt them using the Pk_D, then publish the election results

Figure 2 The Voting Scheme

6. Security Proof and Analysis

6.1 Security Proof

This section provides a comprehensive security analysis of our RLWE-based electronic voting protocol, with particular emphasis on the zero-knowledge proof mechanisms employed throughout the voting process. The examination encompasses multiple security dimensions to establish the scheme's robustness.

Theorem 4. Let $q > 16\sigma^3 n^{\alpha 5/2}$,we have $\operatorname{mod}_2(X,\omega) = \operatorname{mod}_2(Y,\omega) = 1 - negl(\lambda)$.

Proof. Known $X = Sk_A \cdot Pk_B \cdot Pk_C, x = Sk_A \cdot Pk_B$ and $Y = Pk_A \cdot Sk_B \cdot Pk_C, y = Pk_A \cdot Sk_B$,we can launch: $X - Y = (x - y)Pk_C$, according to Lemma 3, we know $\| X_{i,j} - Y_{i,j} \|_\infty \le \frac{q}{4}$ $i, j \in \{1,\ldots,q\}$ combining lemma 3, we can introduce:

$$\| X_{i,j} - Y_{i,j} \| \le \| 2[Sk^T_{A_{i,j}} \cdot e_{B_{i,j}} - e^T_{A_{i,j}} \cdot Sk_{B_{i,j}}] \| \cdot \| P_C \| \le 4n \cdot (\sigma\sqrt{n})^3 \tag{10}$$

Combined with Lemma 3, we know $\| X_{i,j} - Y_{i,j} \|_\infty < 4\sigma^3 n^{5/2} < \frac{q}{4}$.

Therefore, when condition $q > 16\sigma^3 n^{5/2}$ is satisfied, our scheme is considered secure. □

Theorem 2. Legal voters (have the right private key Sk_A), their generated proofs always pass validation.

Proof. Voter identification $\pi = H_1(\operatorname{mod}_2(X,\omega)), \omega = Sig(x)$ is generated by the voters themselves at the registration stage,Therefore, blockchain can only see π during the verification process, and in addition, blockchain gets the verification value $P = H_2(H_1(\operatorname{mod}_2(Y,\omega)))$ from the electoral institutions.

According to Lemma 3, we know that when $q > 16\sigma^3 n^{\alpha 5/2}$,If the secret information Sk_A is true, there is:

$$\operatorname{mod}_2(X,\omega) = \operatorname{mod}_2(Y,\omega) = 1 - negl(\lambda) \tag{11}$$

We can launch the following:

$$\pi = H_1(\operatorname{mod}_2(X,\omega)) = H_1(\operatorname{mod}_2(Y,\omega)) = P \tag{12}$$

If the voter identity is true, the verification passes, meaning the voter possesses secret information Sk_A :

$$\Pr[\pi \leftarrow Voters[Sk_A^T, Pk_A, Pk_B, Pk_C] : BC(P_{Pk_A, Pk_B, Pk_C}, \ \pi)] \ge 1 - negl(\lambda)$$

□

Throrem 3. The attacker could not forge a valid proof that the π was verified.

Proof. If the adversary does not have the secret information Sk_A ,And make the blockchain believe that the adversary has secret information, with negligible probability, in other words $\exists Pk_A, Pk_B, Pk_C$,we have:

$$\Pr[\pi' \leftarrow Voters[Pk_A, Pk_B, Pk_C] : BC(P_{Pk_A, Pk_B, Pk_C}, \ \pi')] = negl(\lambda)$$

According to our setting, the electoral body is curious but honest, and so we should consider the situation that there is a malicious voter who wants to forge a legitimate ballot. If a malicious voter can successfully register $Pk_A = a \cdot Sk_A + 2e_A \mod q$ in polynomial time without the election authority revealing secret information Sk_A .Then smart contracts can also be distinguished in the same polynomial time.

In our assumptions, malicious voters are adversaries,the adversary guessed the value of Pk_A but they don't have value of Sk_A .Therefore, it cannot be calculated to generate the π used to prove their legitimacy,the adversary can also obtain the verification values P on the blockchain,then try to reverse the hash function $H_2(P)$ to try to get Sk_A ,but the hash function is hard to reverse.

So we conclude that without secret information Sk_A , the smart contract cannot be deceived to accept the verification.

$$\Pr[\pi' \leftarrow Adversary[Pk_A, Pk_B, Pk_C] : BC(P_{Pk_A, Pk_B, Pk_C}, \ \pi') = 1] = negl(\lambda)$$

□

Theorem 4. The verifier was unable to obtain any information about Sk_A from the proof π .

Proof. With Sk_A as secret information, cannot be leaked throughout the voting process,If a malicious party gets Sk_A , it can easily be verified by smart contracts. We do not need to think about blockchain, we just need to consider it from the perspective of the electoral institution.

$\pi = H_1(\mathrm{mod}_2(X, \omega))$ outputs only the hash values. While the mod_2 function maps X to a single bit or a finite value, which greatly limits information leakage, the unidirectionality of the hash function H_1 ensures that the specific value of $\mathrm{mod}_2(X, \omega)$ cannot be pushed back from π .

The simulator S can randomly generate $\pi_{sim} \leftarrow \{0,1\}^n$, and calculate $P_{sim} = H_2(\pi_{sim})$ and make public, since the hash function output is uniformly distributed under the random prediction model, true proof π is computationally indistinguishable from simulation proof π_{sim}.

$Pk_A = a \cdot Sk_A + 2e_A$ is indistinguishable from random polynomials under the RLWE assumption, ensuring that the attacker cannot be inferred by the public key Sk_A.

Therefore, the verifier can only know the validity of the proof, and cannot obtain any information of Sk_A, satisfying zero knowledge. □

In order to re-detailed prove that the encryption scheme in the electronic voting scheme meets the anti-IND-CPA (indistinguishable under plain text attack) attack, we conducted the following formal analysis based on the BFV all homomorphism encryption and RLWE hypothesis proposed in the paper, and combined with the standard security reduction method:

The security of BFV encryption is based on the difficulty of the RLWE problem. Assuming that attacker A can crack IND-CPA with a non-negligible advantage ε, we can construct algorithm B to solve the RLWE problem using A.

Initialization stage: Given the RLWE sample $(a_i, b_i) \in R_q \times R_q, b_i = a_i \cdot s + e_i$, s is secret and e_i follows the error distribution. Algorithm B sends $pk = (a_i, b_i)$ to A. Here b_i simulates the public key $pk = ([-a \cdot s + e]_q, a)$ of BFV, when A queries the encryption of plaintext m, B generates dense text according to the BFV encryption algorithm: $ct = ([\lfloor q/t \rfloor m + pk_0 \cdot u + e_1]_q, [pk_1 \cdot u + e_2]_q)$.

Challenge stage: A submit two equal length plaintext m_1 and m_2, B randomly selected $b \in \{0,1\}$ to generate challenge ciphertext c^* as follows:

If the RLWE instance is a true sample $b_i = a_i \cdot s + e_i$, then c^* is a legal BFV ciphertext.

If the RLWE instance is a random sample, then c^* is a uniform random value.

Guess stage: A output b', B judge the RLWE instance type according to b', if the advantage of A is ε, the advantage of B to solve the RLWE problem is also ε.

Game g_0: The challenger generates public and private keys and ciphertext according to the real BFV scheme, and the attacker's advantage is ε.

Game g_1: Replace the public key pk with the random polynomial pair $(a', b') \in R_q \times R_q$. Since RLWE assumes that the real public key is indistinguishable from the random value, the advantage change of the attacker can be ignored, namely: $|Adv_{g_1} - Adv_{g_0}| \leq negl(\lambda)$.

Game g_2: Replace challenge ciphertext c^* with a random value. If the RLWE problem is difficult, the attacker cannot distinguish between g_1 and g_2, namely: $|Adv_{g_2} - Adv_{g_1}| \leq negl(\lambda)$. In g_2, the attacker faces a completely random ciphertext, with an advantage of 0, so: $Adv_{g_0} \leq Adv_{g_1} + negl(\lambda) \leq Adv_{g_2} + 2 \cdot negl(\lambda) = negl(\lambda)$.

The safety of the BFV protocol depends on the following parameter selection:

(1) Polynomial ring dimension n: usually take $n \geq 1024$.

(2) Modulus q: $q > 16\sigma^3 n^{5/2}$ needs to be met to ensure that the noise item does not destroy the decryption correctness and security.

(3) Error distribution χ: The discrete Gaussian distribution parameter σ needs to be large enough, such as $\sigma = \tilde{O}(\sqrt{n})$, to ensure the difficulty of the RLWE problem.

By combining the difficulty of contracting the IND-CPA security of BFV encryption to the RLWE problem, combined with the strict conditions of parameter setting, the scheme is capable of resisting selecting plaintext attacks. Security game sequence analysis further shows that an attacker cannot distinguish the ciphertext in polynomial time to meet the requirements of the IND-CPA security.

6.2 Security Analysis

When building an efficient, safe and fair electronic voting system, it is crucial to strictly follow and meet the security protocol standard of electronic voting [27]. In order to verify the feasibility of our scheme, the following seven core security attributes are deeply analyzed to develop the proof.

(1) Privacy

Ensure privacy by maintaining the anonymity of voter and candidate identities. Provide voters with unique security proof to verify the authenticity of the ballot, and ensure that the certificate does not contain information that can identify the voter, and the ballot is also encrypted and cannot be linked to the voter identity based on the ballot information. The scheme of this paper is conducted on the local Ethereum private blockchain. Due to its huge scale and highly dispersed hash computing power, the Ethereum network makes the cost of launching 51% attacks extremely high and almost impossible to achieve, thus guaranteeing the privacy of voter identity.

(2) Confidentiality

The whole voting process is confidential, votes after BFV holhomorphism encryption encryption, until the result, votes are in ciphertext form, ballot content cannot obtain and tampered with, before the counting results, anyone cannot know the final result in advance, further strengthen the confidentiality of the voting process, to ensure the fairness and credibility of the voting system.

(3) Security

The inherent cryptographic properties of blockchain technology provide robust protection against vote tampering and unauthorized modifications. To alter any recorded data, an adversary would need to recompute the hash values for the target block and all subsequent blocks in the chain, a computational task that is computationally infeasible due to the enormous resource requirements, thereby ensuring the system's security for electoral applications.

(4) Uniqueness

The voter has a unique registration mark P_A, and the verified voter is only allowed to vote. The vote is included in the final vote, and the voter is unable to cast multiple votes, and if the voter wants to vote, he will not be entitled to continue voting.

(5) Verifiability

The inherent properties of blockchain technology provide full transaction transparency and universal verifiability across the distributed network. This enables any participant to independently validate that the officially published election outcomes precisely match the recorded results on the blockchain.

(6) Fairness

In order to ensure fairness, all votes are encrypted from the beginning to the end of voting, existing in the form of ciphertext, and the voting results will be publicly uploaded to the blockchain to ensure the authenticity and credibility of voting data. Blockchain calls the smart contracts to automatically perform the calculations and get the counting results. In this process, the voters cannot see the calculation process, which ensures the independence and confidentiality of the calculation process, and further improves the fairness of the election.

(7) Mobility

The proposed voting architecture enables universal accessibility, allowing voters to participate from any location with internet connectivity. The system's design eliminates geographical constraints and specialized infrastructure requirements, as participation only necessitates a network-enabled device and a valid blockchain address for secure network access.

In summary, the proposed scheme comprehensively addresses critical security requirements for electronic voting systems, ensuring integrity, reliability, zero-knowledge properties, privacy preservation, confidentiality maintenance, system security, vote uniqueness, result verifiability, electoral fairness, and remote accessibility. The implementation of strict voter authentication prevents unauthorized participation and potential election interference, while maintaining resistance against malicious third-party attempts to compromise the encryption scheme's semantic security.

7. Performance Analysis

The test environment runs in the Ubuntu 22.04 LTS of the Windows 11 Home native subsystem (WSL 2), and the managed device is the Redmibook16 with the Intel 12450H.

The system's smart contracts are developed in Solidity programming language, with deployment automation scripts authored in JavaScript. Utilizing the Truffle development framework, the entire solution is implemented on a localized blockchain test environment. This configuration leverages Ganache to establish a private Ethereum network, enabling comprehensive smart contract management through Truffle's toolchain capabilities - including contract compilation, network interaction, and deployment operations targeting the Ganache testnet. The integrated workflow demonstrates full compatibility with the Ethereum Virtual Machine (EVM) architecture while maintaining standalone execution efficiency.

According to the existing electronic voting scheme, we will perform a performance analysis of our scheme based on the verification time and the average running time of each phase.

Voters can generate proof locally before voting, so we do not need to consider voter generating proof time, at the same time, we designed the lattice-based non-interactive zero-knowledge proof key exchange protocol.

According to the results of our experiments, the voter proofs π are output by the hash function. Size does not change by changes in secret information Sk_A, and the validation procedure is a publicly available hash function operation. We contrast in Table 3 with [28] and [10] for the verify time and dependent hypotheses.

Table 3 Comparison of proof time

Scheme	Verify Time	Assumption
[28]	34ms	ECC
[10]	27ms	ECC
Ours	20ms	RLWE

We tested our scheme on a locally deployed private chain, in the case of four candidates, two voters from setting to vote counting, we conducted 10 tests times, the average time consuming as shown in Table 4, and the experimental results show that our scheme fully meets the voting requirements in running time.

Table 4 Average running time of each stage

Phase	Average Running Time
Setup	15ms
Register	24ms
Voting	20ms
Tally	12ms

The above tests is for the case of four candidates. We also tested the performance of our system when voting for more candidates. The test results are shown in Figure 3:

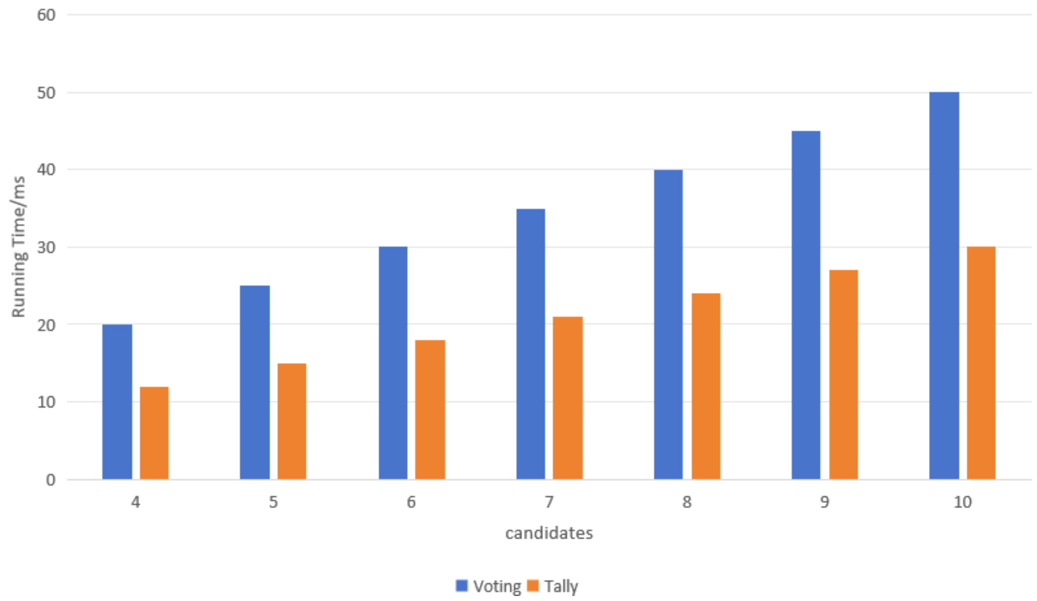

Figure 3 The performance of different candidates

In addition, to further verify that our scheme has a significant advantage in vote counting efficiency compared to other schemes, we compared it with schemes [29] and [30]. The voting scenarios we assumed consisted of 500, 1000, 1500, and 2000 voters, and we compared the vote counting times. The results are shown in Figure 4. As the number of voters increases, the time required for vote counting also increases for all schemes. Scheme [29], which uses a static Merkle tree to ensure unlimited voter additions, shows a much lower efficiency compared to the other schemes. In contrast to other schemes, our proposed scheme shows a certain improvement in vote counting efficiency, while also ensuring quantum resistance throughout the process. Scheme [30] uses the ElGamal homomorphic encryption scheme, which means it does not provide quantum resistance.

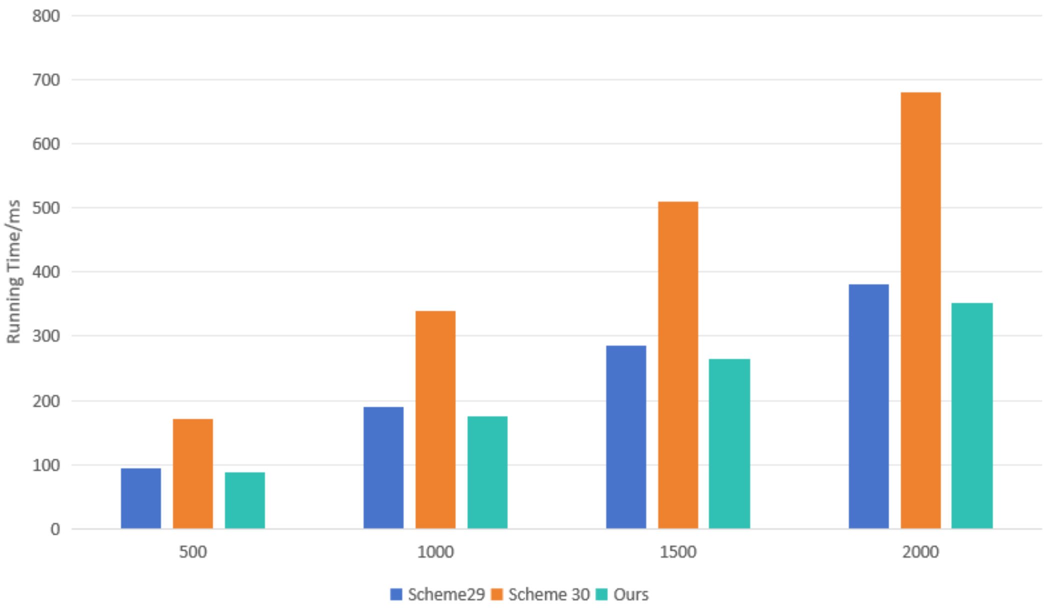

Figure 4 Efficiency comparison of similar schemes

8. Conclusion

This paper addresses the current issues in electronic voting systems, such as poor quantum resistance, lack of voter privacy, low vote counting efficiency, and fairness issues. We propose an efficient zero-knowledge proof blockchain-based electronic voting solution based on RLWE. This solution utilizes the BFV fully homomorphic encryption algorithm to achieve efficient and fair vote counting. The scheme employs a lattice-based key exchange protocol to ensure voter identity uniqueness and the security of voter information, while also using the BFV fully homomorphic encryption algorithm to encrypt votes, ensuring the security and privacy of vote content. The encrypted votes are uploaded to the blockchain by voters, ensuring transparency of information and immutability of results. Finally, smart contracts ensure the smooth execution of the entire voting process, enabling automatic vote counting and public announcement of results. The verification overhead for voters is fixed, and the overall vote counting overhead increases linearly with the number of voters. Compared to similar solutions, this scheme offers certain advantages in efficiency, ensuring that it can reduce noise and enable weighted electronic voting in large-scale elections, which is our next research direction.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, author-ship, and/or publication of this article.

Data Sharing Agreement

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Reference

[1] Chaum D L. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Communications of the ACM, 1981, 24(2): 84-90.

[2] Saltman R G. Accuracy, integrity and security in computerized vote-tallying[J]. Communications of the ACM, 1988, 31(10): 1184-1191.

[3] Alvarez R M, Hall T E. Point, click, and vote: The future of Internet voting[M]. Rowman & Littlefield, 2003.

[4] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Satoshi Nakamoto, 2008.

[5] Yan S Y. Quantum attacks on public-key cryptosystems[M]. Springer US, 2013.

[6] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings 35th annual symposium on foundations of computer science. Ieee, 1994: 124-134.

[7] Onur C, Yurdakul A. ElectAnon: A Blockchain-based, Anonymous, Robust, and Scalable Ranked-choice Voting Protocol[J]. Distributed Ledger Technologies: Research and Practice, 2023, 2(3): 1-25.

[8] Alshehri A, Baza M, Srivastava G, et al. Privacy-preserving e-voting system supporting score voting using blockchain[J]. Applied Sciences, 2023, 13(2): 1096.

[9] Zhao Z, Chan T H H. How to vote privately using bitcoin[C]//Information and Communications Security: 17th International Conference, ICICS 2015, Beijing, China, December 9–11, 2015, Revised Selected Papers 17. Springer International Publishing, 2016: 82-96.

[10] Wang B, Guo F, Liu Y, et al. An efficient and versatile e-voting scheme on blockchain[J]. Cybersecurity, 2024, 7(1): 62.

[11] Kaim G, Canard S, Roux-Langlois A, et al. Post-quantum online voting scheme[C]//Financial Cryptography and Data Security. FC 2021 International Workshops: CoDecFin, DeFi, VOTING, and WTSC, Virtual Event, March 5, 2021, Revised Selected Papers 25. Springer Berlin Heidelberg, 2021: 290-305.

[12] Lee K, James J I, Ejeta T G, et al. Electronic voting service using block-chain[J]. Journal of Digital Forensics, Security and Law, 2016, 11(2): 8.

[13] McCorry P, Shahandashti S F, Hao F. A smart contract for boardroom voting with maximum voter privacy[C]//Financial Cryptography and Data Security: 21st International Conference, FC 2017, Sliema, Malta, April 3-7, 2017, Revised Selected Papers 21. Springer International Publishing, 2017: 357-375.

[14] Camenisch J, Chaabouni R, Shelat A. Efficient protocols for set membership and range proofs[C]//Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2008 (CONF): 234-252.

[15] Morais E, Koens T, Van Wijk C, et al. A survey on zero knowledge range proofs and applications[J]. SN Applied Sciences, 2019, 1: 1-17.

[16] Boneh D, Boyen X. Short signatures without random oracles[C]//Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings 23. Springer Berlin Heidelberg, 2004: 56-73.

[17] Yin H, Chen E, Zhu Y, et al. An efficient zero-knowledge dual membership proof supporting pos-and-neg membership decision[J]. Mathematics, 2022, 10(17): 3217.

[18] Muth R, Tschorsch F. Tornado Vote: Anonymous Blockchain-Based Voting[C]//2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2023: 1-9.

[19] Rønne P B, Atashpendar A, Gjøsteen K, et al. Short Paper: Coercion-Resistant Voting in Linear Time via Fully Homomorphic Encryption: Towards a Quantum-Safe Scheme[C]//Financial Cryptography and Data Security: FC 2019 International Workshops, VOTING and WTSC, St. Kitts, St. Kitts and Nevis, February 18–22, 2019, Revised Selected Papers 23. Springer International Publishing, 2020: 289-298.

[20] Naidu P R, Bolla D R, Prateek G, et al. E-Voting system using blockchain and homomorphic encryption[C]//2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon). IEEE, 2022:

1-5.

[21] Regev O. On lattices, learning with errors, random linear codes, and cryptography[J]. Journal of the ACM (JACM), 2009, 56(6): 1-40.

[22] Ding J, Saraswathy R V, Alsayigh S, et al. How to validate the secret of a ring learning with errors (RLWE) key[J]. Cryptology ePrint Archive, 2018.

[23] Zhang J, Zhang Z, Ding J, et al. Authenticated key exchange from ideal lattices[C]//Advances in Cryptology-EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II 34. Springer Berlin Heidelberg, 2015: 719-751.

[24] Gao X, Ding J, Li L, et al. Practical randomized RLWE-based key exchange against signal leakage attack[J]. IEEE Transactions on Computers, 2018, 67(11): 1584-1593.

[25] Banafa A. Blockchain technology and applications[M]. River Publishers, 2022.

[26] Ma S, Deng Y, He D, et al. An efficient NIZK scheme for privacy-preserving transactions over account-model blockchain[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 18(2): 641-651.

[27] Fujioka A, Okamoto T, Ohta K. A practical secret voting scheme for large scale elections[C]//Advances in Cryptology—AUSCRYPT'92: Workshop on the Theory and Application of Cryptographic Techniques Gold Coast, Queensland, Australia, December 13–16, 1992 Proceedings 3. Springer Berlin Heidelberg, 1993: 244-251.

[28] Huang J, He D, Chen Y, et al. A blockchain-based self-tallying voting protocol with maximum voter privacy[J]. IEEE Transactions on Network Science and Engineering, 2022, 9(5): 3808-3820.

[29] Yuan K, Sang P, Zhang S, et al. An electronic voting scheme based on homomorphic encryption and decentralization[J]. PeerJ Computer Science, 2023, 9: e1649.

[30] El-Gburi J, Srivastava G, Mohan S. Secure voting system for elections[J]. International Journal of Computer Aided Engineering and Technology, 2022, 16(4): 497-511.