# BFV-Blockchainvoting：支持 BFV 全同态加密的区块链电子投票系统

杨亚涛[1,2]，刘德莉[1]，刘培鹤[2]，曾萍[1,2]，肖嵩[1,2]

（1. 西安电子科技大学通信工程学院，陕西 西安 710071；2. 北京电子科技学院电子与通信工程系，北京 100070）

**摘 要：**当前的电子投票系统大多依赖于中心服务器和可信第三方，这种系统架构增加了投票的安全隐患，甚至使投票可能失败。为了解决这一问题，将区块链技术应用于电子投票系统，使区块链代替可信第三方，提出了一种支持 BFV 全同态加密的区块链电子投票系统 BFV-Blockchainvoting。首先，用一个公开透明的公告板记录选票信息，同时设计了智能合约来实现验证、自计票功能；其次，为进一步提高投票过程的安全可靠性，使用 SM2 签名算法对投票者的注册信息进行签名处理，再选择能够互相监督的双方共同监管选票，并使用 BFV 同态加密算法来隐藏计票数据。经过测试与分析，所提系统单张选票的计票时间平均为 1.69 ms。所提方案可以为投票过程中的不可操纵性、匿名性、可验证性、不可重用性、不可胁迫性和抗量子攻击等安全属性提供保障，适用于多种投票场合，并且可以满足大型投票场景下的高效率需求。

**关键词：**电子投票；区块链；全同态加密；BFV 同态加密；智能合约

**中图分类号：**TP309

**文献标志码：**A

**DOI:** 10.11959/j.issn.1000−436x.2022172

# BFV-Blockchainvoting: blockchain-based electronic voting systems with BFV full homomorphic encryption

YANG Yatao[1,2], LIU Deli[1], LIU Peihe[2], ZENG Ping[1,2], XIAO Song[1,2]

1. School of Telecommunication Engineering, Xidian University, Xi'an 710071, China

2. Department of Electronic and Communication Engineering, Beijing Electronics Science and Technology Institute, Beijing 100070, China

**Abstract:** Current electronic voting systems mostly relied on central server and the trusted third party, this kind system architecture increases the security risks of voting, and even makes voting fail. In order to solve this issue, an electronic voting system BFV-blockchainvoting that supported BFV homomorphic encryption was proposed, and this system applied the blockchain technology to the electronic voting system to replace the trusted third party. Firstly, an open and transparent bulletin board was used to record the vote information, and an intelligent contract was used to realize the functions of verification and self counting. Secondly, in order to further improve the security and reliability of the voting process, the voter's registration information was signed by SM2 signature algorithm, the ballot was managed by both parties that can supervise each other, and the counting data was encrypted by the BFV full homomorphic encryption algorithm. Finally, the evaluation of performance shows that it only costs 1.69 ms to complete one ballot in the proposed electronic voting system. This electronic voting scheme based on the BFV full homomorphic encryption and blockchain has better security attributes such as manipulation-resistance, anonymity, verifiability, double-voting resistance, coercion-resistance and resistance to quantum attacks. The scheme is suitable for a variety of voting scenarios and can meet the efficiency requirements in large voting scenarios.

**Keywords:** electronic voting, blockchain, full homomorphic encryption, BFV homomorphic encryption, smart contract

**收稿日期：**2022−04−02；**修回日期：**2022−06−06

**基金项目：**北京高校高精尖学科建设基金资助项目（No.3201023）；“通信工程”“电子信息工程”国家级一流本科专业建设点基金资助项目；国家密码科学基金资助项目

**Foundation Items:** Advanced and High Level Discipline Construction Fund of Universities in Beijing (No.3201023), The National First-class Under Graduate Dicipline Construction of “Communication Engineering” and “Electronic Information Engineering”, The National Cryptography Science Foundation of China

## 0　引言

电子投票为目前的纸质投票提供了一种方便且成本效益高的替代方案。早在 1981 年 Chaum[1]就首次提出了电子投票技术，电子投票的安全保障也被认为是最难被解决的问题之一[2]。当前的电子投票系统大多以密码学为基础保障，根据所依据的密码学工具不同主要分为三类：基于混合网络的电子投票方案[3-5]、基于盲签名的电子投票方案[6-8]以及基于同态加密的电子投票方案[9-11]。其中，同态加密技术逐渐被越来越多的电子投票方案所采用，其构造过程更加清晰简单，且加密过程具有同态性，可以较好地解决远程电子投票中的隐私保护和数据安全问题。

目前，大多数电子投票系统都依赖第三方机构的管理和计票，选票面临被黑客攻击或被第三方机构篡改的风险，这也给投票系统带来较大的安全隐患，甚至使投票失败。区块链中的存储信息去中心化、不可篡改性和公开透明等特点，非常适合安全电子投票系统中公开不可篡改的公告板的要求，因此将区块链技术应用于电子投票领域具有非常广阔的应用前景。

## 1　相关工作

同态加密技术应用于电子投票系统中，允许在不解密的情况下计算选票。目前，由于 ElGamal 和 Paillier 加密算法具有加法同态特性，因此在电子投票中的应用较多。其中，ElGamal 加密算法在 Helios[12]系统中得到了较好实践。文献[13]提出了具有乘法同态性质的 ElGamal 加密方案的增强形式，乘法群生成器的使用保证了投票方案的安全性。文献[14]提出了一种分布式同态签密的电子投票方案，该方案可以快速完成签名验证，同时提高选举的可信度。文献[15]利用同态加密对选民信息进行加密来保证选民信息的隐私安全，但这种加密方式没有发挥同态加密的最大优势，造成算力资源的浪费。文献[16]分别将 ElGamal 算法和 Paillier 算法应用于电子投票系统，并对 2 种算法的性能进行对比。文献[17]将 Ducas 等[18]设计的自举全同态加密方案应用于电子投票系统，将全域密文转换成具有特定语义的密文，避开了零知识证明架构的烦琐交互。文献[19]提出的 Schulze 投票方案使用 BGV（Brakerski-Gentry- Vaikuntanathan）全同态加密算法来加密选票，实现计票过程中的隐私保护。文献[11]提出一种基于 SEAL 库的同态加权电子投票系统，使用 BFV（Brakerski-Fan-Vercauteren）全同态加密方案保证系统的抗量子攻击特性和安全性，同时对电子投票方案性能也进行了分析。

区块链技术替代可信第三方应用于电子投票系统中，可以避免投票系统出现单点故障，增强系统的安全性。文献[20]展示了一个基于区块链投票系统的概念框架，提出的方案可以解决拒绝服务攻击问题，但不具备抗胁迫性等安全属性。文献[21]提出了一种基于以太坊的轻量级远程区块链电子投票系统，并采用变化的哈希值来增加系统的抗胁迫性。文献[22]使用 Hyperledger Fabric 来部署投票系统，使用 Paillier 加密算法、零知识证明和可链接环签名等密码技术来提供独立于区块链平台的安全和隐私保护功能。文献[23]将区块链与 ElGamal 算法相结合，利用 ElGamal 加法同态性质来保证选票安全。区块链应用于电子投票解决了系统依赖第三方机构的弊端，而同态加密算法的引入又能保证投票过程的不可操纵性。目前，应用在电子投票领域的同态加密算法多为部分同态加密算法，不满足同时进行加法和乘法操作的客观需要，在安全性和运算效率上也有所不足。

本文设计的投票系统使用了由我国国家密码管理局发布的商用密码标准算法 SM2、SM4 和文献[24]提出的 BFV 全同态加密算法，并选择基于 SEAL 库的 BFV 同态加密方案。SEAL 库是微软公司基于 C++开发的开源全同态加密软件库。

本文的主要贡献如下。

1) 提出了一个基于 BFV 全同态加密和区块链相结合的电子投票系统方案 BFV-Blockchainvoting。该方案使用 SM2 算法对投票者的注册信息进行签名处理，使用 SM4 算法加密选票，结合可以互相监督的两方共同监管完成选票的获取，可以保证投票过程具有不可操纵性、匿名性、可验证性、不可重用性、不可胁迫性和抗量子攻击等安全属性。使用 BFV 全同态加密算法对选票加密，利用同态加密密文可计算的性质，实现计票过程的隐私保护。使用区块链替代第三方机构，利用智能合约实现安全性验证和自计票功能，有效避免了因过分依赖第三方机构而产生的安全隐患。

2) 对方案进行了初步构建和性能测试。基于

Golang 编写的公链系统作为底层架构，通过测试分析，本文系统单张选票的计票时间平均为 1.69 ms。相比于 Pandey 等[20]提出的 VoteChain 投票系统的计票时间减少了 98.87%；相比于杨亚涛等[11]提出的基于 SEAL 库的同态加权电子投票系统的计票时间减少了 9.62%；相比于 Panja 等[25]提出的基于区块链的端到端的电子投票系统的计票时间减少了 32.4%。该方案适用于多种投票场景，可以满足大型投票场景的效率要求。

## 2 BFV-Blockchainvoting 电子投票系统设计

### 2.1 系统组成

本文系统由 5 个主要实体组成，具体说明如下。

投票者 $V_i$：具有投票权的投票者集合，其中 $i \in [1,n]$。

管理员 $A$：负责生成一组唯一且随机的电子选票，并以匿名的方式将选票与投票者共享。

主持人 $M$：负责保护投票者的隐私，将选票匿名后分发给投票者。

候选人 $C_k$：合格的选举对象集合，其中 $k \in [1,m]$。

区块链网络：一个基于国密算法的公链系统，是一个公开、可访问、不可篡改的公告板，通过智能合约实现票据合法性检验、自计票。

系统关键参数及含义如表 1 所示。

**表 1 系统关键参数及含义**

| 参数 | 含义 |
|---|---|
| $V_i, i \in [1,n]$ | 投票者 |
| $A$ | 管理员 |
| $M$ | 主持人 |
| $C_k, k \in [1,m]$ | 候选人 |
| $b_i, i \in [1,n]$ | 选票 |
| $x_a$ | 管理员的私钥 |
| $P_A$ | 管理员的公钥 |
| $x_v$ | 投票者的私钥 |
| $P_V$ | 投票者的公钥 |
| $(r,s)$ | SM2 签名值 |
| $k_i$ | SM4 加密密钥 |
| sk | BFV 私钥 |
| pk | BFV 公钥 |
| rlk | BFV 计算密钥 |

### 2.2 系统架构与智能合约设计

#### 2.2.1 系统架构

通过分析电子投票系统的基本流程，可以得到该系统网络架构，如图 1 所示。

传统的电子投票系统需要依赖第三方机构与中心服务器进行数据管理，这种结构容易造成第三方机构篡改选票或中心服务器被攻击瘫痪的潜在风险。本文系统采用区块链的 P2P 网络结构，不需要第三方机构进行计票，通过调用智能合约实现票据合法性检验与自计票功能，可以提升系统的安全性与稳健性。

在本文系统中，根据权限不同，区块链节点分为普通节点和特殊节点，普通节点是具有投票资格的投票者，而特殊节点包括管理员和主持人。各节点通过区块链网络连接，共同访问链上数据，并通过浏览器访问 Web 前端的可视化投票界面。

#### 2.2.2 智能合约设计

基于同态加密的智能合约架构主要分为上下两层：网络层和智能合约层。网络层是整个系统的核心，采用基于国密算法的公链系统，链上的节点根据权限不同分为普通节点和特殊节点，其中，普通节点是具有投票资格的投票者，而特殊节点包括管理员和主持人。智能合约层主要负责整个投票系统的运转，包括生成 BFV 同态加密算法的密钥对、广播 BFV 算法公私钥、收集选票、验证选票是否合法、计票和广播选票结果等环节。智能合约执行生成创世区块、设置节点以及监听端口等工作，然后被部署在链上，时刻监听链上信息。一旦投票者点击提交选票，区块链中便会新增一个区块，智能合约通过区块获取投票信息，收集选票进行验证和计票，在计票时间结束后，解密选票信息同时广播结果。

本文设计的投票系统 BFV-Blockchainvoting 的区块链底层架构为自建的基于国密算法的公链系统，该系统是基于 REST/JSON API、TCP 服务器、国密算法和工作量证明（PoW, proof of work）共识算法的区块链系统。相比于 Hyperledger Fabric 和以太坊等架构，本文系统使用的架构更为安全可靠，减少了由于频繁更新应用系统经常面临崩溃等问题。Blockchain.go 为支撑底层架构的主要代码，其数据结构如表 2 所示。

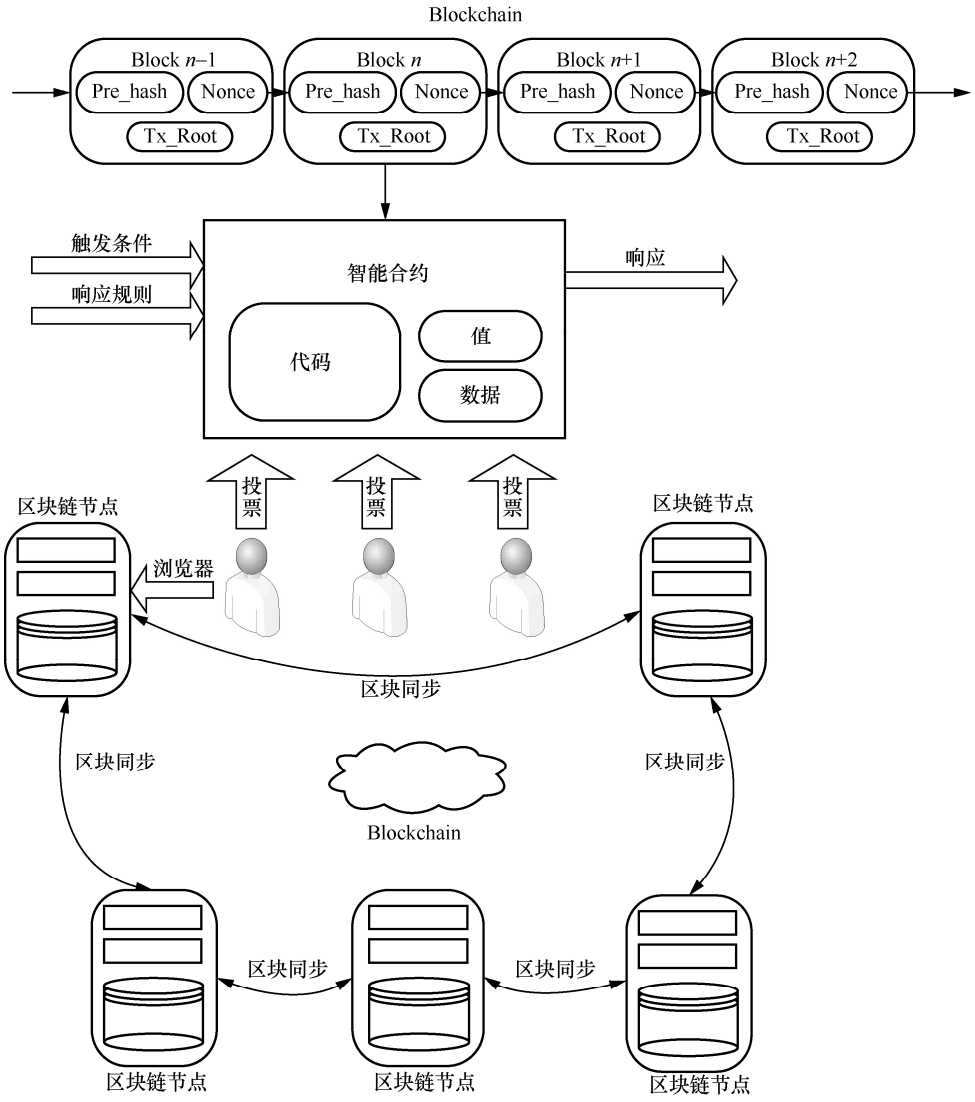



图 1　电子投票系统网络架构

**表 2　Blockchain.go 数据结构**

| 结构名称 | 结构类型 | 存储数据 |
|---|---|---|
| BlockID | int64 | `json:"blockID"` |
| Timestamp | int64 | `json:"timestamp"` |
| Transactions | string | `json:"transactions"` |
| Hash | []transactionStruct | `json:"hash"` |
| PrevHash | string | `json:"prevhash"` |
| Difficulty | string | `json:"difficulty"` |
| Nonce | int | `json:"nonce"` |

Voting.go 为本文系统的底层智能合约，智能合约中涉及的主要方法及功能如表 3 所示。

**表 3　智能合约方法及功能**

| 方法 | 功能 |
|---|---|
| TimeSetup() | 设置各阶段时间 |
| KeyGenerator() | 生成 BFV 算法公私钥 |
| VaildID() | 验证投票者身份是否合法 |
| isVoted() | 判断投票者是否重复投票 |
| TallyElection() | 计票 |
| DecryptVote() | 广播选票结果 |

基于 BFV 全同态加密算法的智能合约主要算法如算法 1 所示。首先，获得选票 $b_i$ 后，初始化检查 $b_i$ 是否属于选票名单 $\gamma$，如果属于，智能合约则通过检查投票者是否被标记来确认投票者是否已经投过票，如果 voters[$i$] = false，说明投票者为首

次进行投票，符合计票要求，再通过调用 SEAL 库的全同态加法运算进行计票。其次，该选票计票结束后，对选票进行标记，设置 voters[$i$] = true，避免双重投票。最后，对全部选票计票结束后，调用 SEAL 库全同态加法的解密算法，将计票结果解密，恢复最终计票结果。

**算法 1** 基于 BFV 全同态加密算法的智能合约主要算法

**输入** 选票 $b_i$

**输出** 候选人的最终计票结果 resultVotes[$k$]

**初始化** 获得选票后，检查选票 $b_i$ 是否属于选票名单 $\gamma$

if $b_i$ 属于 $\gamma$

检查该投票者是否为第一次提交选票

if voters[$i$] = false，then

连接 SEAL 库，进行 BFV 加法运算

Candidate[$k$]= evaluator.add_inplace(encrypted1, encrypted2)

voters[$i$] =true

else if 该投票者已经提交过选票

Continue，跳过该选票

end if

else if $b_i$ 不属于选票名单 $\gamma$

Continue，跳过该选票

end if

if 计票阶段时间结束

连接 SEAL 库，进行 BFV 解密运算

decryptor.decrypt(encrypted1, plain_result)

int result-Votes[$k$]=encoder.decode_int32(plain_result)

end if

return resultVotes[$k$]

在统计选票时，通过执行智能合约，使用 BFV 全同态加密算法进行密文计票，最终在计票时间结束后，自动解密选票并公布结果。智能合约主要通过全同态加密机制及其密码协议来保障其安全性，每张选票都以密文形式计入智能合约并参与计算，在整个计票过程中选票信息始终保密，保证了计票过程的安全性。

### 2.3 方案设计

本文提出的 BFV-Blockchainvoting 方案主要包括 4 个连续的阶段，每个阶段都发生在投票组织者预先确定的特定时间范围内。设 $G$ 是椭圆曲线上的

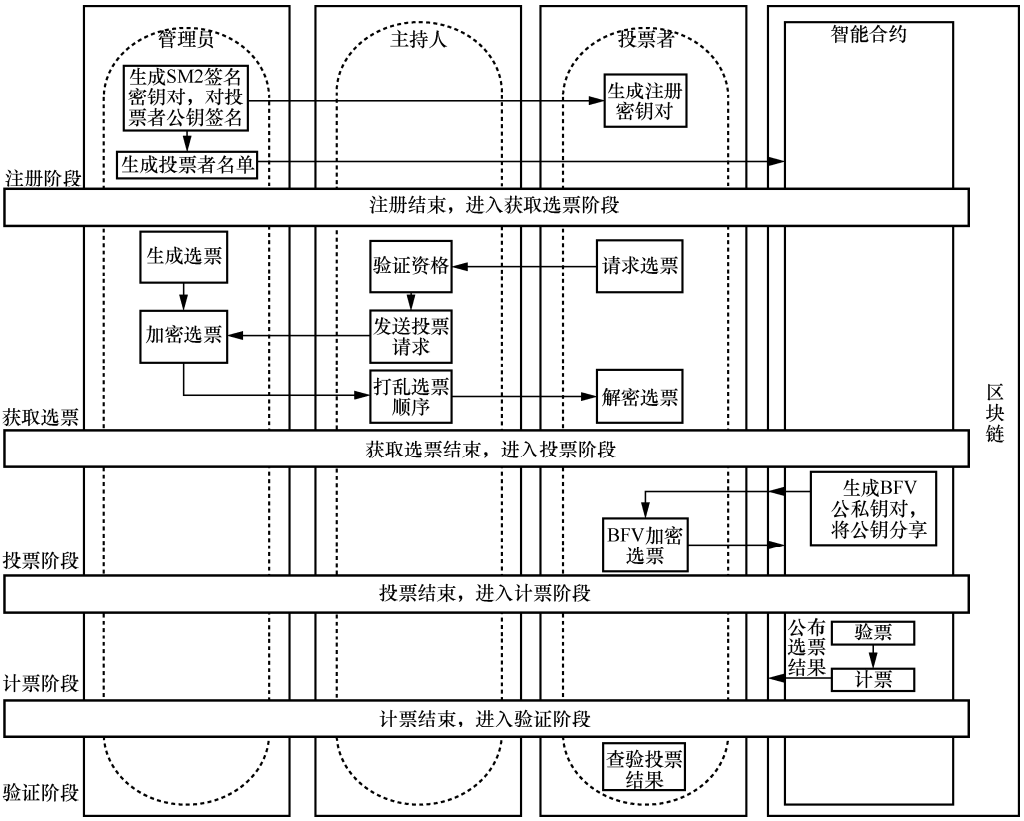



图 2 电子投票系统流程

一个点，其阶为素数 $q$，$G$ 的坐标为 $(x_G, y_G)$；$a_1$ 和 $a_2$ 是有限域上定义一条椭圆曲线的元素；$H_v()$ 是消息摘要为 $v$ bit 的密码杂凑函数。图 2 为电子投票系统流程。

**2.3.1** 注册阶段

在注册阶段，管理员 $A$ 使用由国家密码管理局发布的 SM2 签名算法对投票者的公钥进行签名。具体签名过程如下。

1) 管理员签名密钥生成。管理员 $A$ 需要一组签名密钥对，以便将合格的投票者添加到投票者名册时对其进行签名。注册器随机选取密钥 $x_a \in Z_q^*$，根据此密钥计算出与之对应的公钥为 $P_A = x_a G$。

2) 投票者密钥生成和注册。投票者 $V_i$ 必须拥有与其身份对应的选举密钥对，$V_i$ 选择一个密钥 $x_v \in Z_q^*$，与之对应的公钥为 $P_V = x_v G$。在注册阶段，投票者 $V_i$ 和管理员 $A$ 共享其公钥。

3) 管理员对投票者的公钥签名。为了授予 $V_i$ 投票权，管理员 $A$ 事先要验证投票者的资格，对于符合资格的投票者，对其公钥进行 SM2 签名后再添加到投票者名册中。签名的生成过程为

$$Z_A = \mathrm{H}_{256}\left(\mathrm{ENTL}_A \| \mathrm{ID}_A \| a_1 \| a_2 \| x_G \| y_G \| P_A\right) \quad (1)$$

其中，$\mathrm{ID}_A$ 是管理员 $A$ 的可辨别标识，本文选用管理员的地址值作为标识，$\mathrm{ID}_A$ 的长度为 $\mathrm{entl}_A$ bit；$\mathrm{ENTL}_A$ 是由整数 $\mathrm{entl}_A$ 转换而成的 2 个字节。式(1)将椭圆曲线中各种参数的数据类型转换为比特串，然后对投票者 $V_i$ 的公钥 $P_V$ 进行签名，计算

$$M = \mathrm{Hash}(P_V) \quad (2)$$

$$\bar{M} = Z \| M \quad (3)$$

$$e' = H_v(\bar{M}) \quad (4)$$

选择随机数 $k \in [1, q-1]$，计算椭圆曲线上的点 $(x_1, y_1) = kG$，然后计算

$$r = x_1 + e' (\mathrm{mod}\, q) \quad (5)$$

$$s = (1 + x_a)^{-1}(k - r x_a) (\mathrm{mod}\, q) \quad (6)$$

其中，$(r, s)$ 是签名值。

在注册阶段结束时，管理员 $A$ 公布投票者名册。

**2.3.2** 获取选票

1) 选票生成。管理员 $A$ 生成 $n$ 个唯一且随机的数字选票 $b_i, i \in [1, n]$。

2) 请求投票。投票者 $V_i$ 的公钥对主持人 $M$ 公开，$V_i$ 向 $M$ 请求投票后，$M$ 通过验证 $V_i$ 的签名确认他们是否符合投票资格。

3) 验证投票者身份。主持人 $M$ 收到投票者 $V_i$ 的公钥 $P_V$ 后，通过 SM2 验签算法进行验证，检查 $V_i$ 是否存在于投票者名册中并且验证签名 $(r, s)$ 是否有效。

首先，检查 $r, s \in [1, q-1]$ 是否成立，如果成立，设 $\bar{M} = Z \| M$，计算 $e' = H_v(\bar{M})$，$t = r + s$，如果 $t = 0$，则验证不通过；否则，计算椭圆曲线上的点

$$(x_2, y_2) = sG + tP_V \quad (7)$$

然后，验证 $r \equiv e' + x_2 (\mathrm{mod}\, q)$ 是否成立，如果成立则验证通过，投票者 $V_i$ 合法。

4) 主持人请求选票。如果验证通过，主持人 $M$ 将投票者的公钥 $P_V$ 发送给管理员 $A$，请求获得选票。

5) 选票分配和加密。管理员 $A$ 收到主持人 $M$ 的投票请求后，将选票按照特定的置换顺序随机分配给投票者 $V_i$。

在将选票分配给主持人 $M$ 以发送给 $V_i$ 之前，$A$ 与 $V_i$ 利用 SM2 的密钥交换协议协商出 SM4 的加密密钥 $k_i$，$k_i$ 为 128 bit。然后利用 SM4 算法对选票进行加密。

使用 $k_i$ 生成轮密钥后对选票进行如下加密

$$\mathrm{enb}_i = \mathrm{SM4\text{-}Enc}_{k_i}(b_i) \quad (8)$$

其中，SM4-Enc 是 SM4 加密函数，$\mathrm{enb}_i$ 是加密后的选票。对选票进行加密的目的是向主持人 $M$ 隐藏选票，$V_i$ 拿到的选票是匿名的。管理员 $A$ 将 $\mathrm{enb}_i$ 发送给 $M$。

6) 加密选票传输。主持人 $M$ 将加密后的选票 $\mathrm{enb}_i$ 打乱顺序，然后发送给投票者 $V_i$。

7) 解密选票。$V_i$ 收到 $\mathrm{enb}_i$ 后，将其解密

$$b_i = \mathrm{SM4\text{-}Dec}_{k_i}(\mathrm{enb}_i) \quad (9)$$

其中，SM4-Dec 是 SM4 的解密函数。

**2.3.3** 投票阶段

持有选票的已经登记的投票者 $V_i$ 可以对候选人 $C_k$ 进行投票。

1) 智能合约生成 BFV 公私钥对

私钥 sk 是随机生成的一个系数为−1、0 或 1 的多项式，公钥 $\mathrm{pk} = ([-a\mathrm{sk} + e]_p, a)$。其中，$a$ 为在密文空间中随机生成的一个多项式，其系数模为 $p$；$e$ 为噪声多项式，是在离散高斯分布中随机选取的一组小系数，$e$ 在此处只用一次，用完后丢弃。

生成 BFV 公私钥对后，私钥由本地数据库保留，公钥 pk 通过区块链分享给所有投票者 $V_i$。

2) 双重加密

$$B=(b_i \| \text{vote}) \tag{10}$$

其中，$\text{vote}=(c_1,c_2,\cdots,c_m)$ 表示候选人 $C_k$ 的序列。$c_m=\text{BFV-Enc}(\text{cand}_m)$ 表示加密后的选票，BFV-Enc 表示 BFV 同态加密函数。

$$\text{cand}_k=\begin{cases}1, \text{投票支持第}k\text{个候选人}\\ 0, \text{投票反对第}k\text{个候选人}\end{cases} \tag{11}$$

BFV 全同态加密是建立在环上的同态加密方案，密文由 2 个多项式组成，加密过程为

$$\text{rlk}=\left(\left[-(a_i\text{sk}+e_i)+T^i\text{sk}^2\right]_p,a_i\right), i\in[0,1,\cdots,l] \tag{12}$$

$$c_m=\left(\left[\text{pk}_0u+e_1+\frac{qm}{t}\right]_p,[\text{pk}_1u+e_2]_p\right) \tag{13}$$

其中，rlk 为计算密钥，用于 BFV 中的密文计算；$m$ 为明文，本文方案中投票者的选票 $b_i$ 中对某个候选人的 $\text{cand}_k$ 即需要加密的明文；$T$ 为分解模数，$l=\lfloor \log_T(p) \rfloor$；$u$ 为系数为−1、0 或 1 的多项式；$t$ 为远小于系数模 $p$ 的整数；$e_1$、$e_2$ 取自相同的高斯离散分布，这些多项式只在加密过程中使用，使用完后丢弃；pk 为 BFV 的公钥，$\text{pk}_0=\text{pk}[0]$，$\text{pk}_1=\text{pk}[1]$。

3) 提交选票

投票者 $V_i$ 提交选票触发智能合约，一旦智能合约的结果被附加到区块链，投票将被永久保存。

#### 2.3.4 计票阶段

投票阶段结束后，智能合约将收集此阶段内出现在区块链上的选票，以进行验证和计数。为了验证，管理员 $A$ 公开分配给投票者 $V_i$ 所有选票 $\gamma$。智能合约收到 $T=(b_i \| \text{vote})$ 后进行验证，如果 $b_i\in\gamma$，将检查所附的投票顺序，依次将选票密文计入候选人 $C_k$ 的票数。

$$\text{Add}(c_{im},c_{jm},\text{rlk})=(\text{ct}_i[0]+\text{ct}_j[0],\text{ct}_i[1]+\text{ct}_j[1]) \tag{14}$$

其中，$\text{Add}(c_{im},c_{jm},\text{rlk})$ 表示将投票者 $v_i$ 和 $v_j$ 对候选人 $\text{cand}_m$ 的投票情况密文相加的结果，利用全同态加密密文可计算的性质，即可计算出所有候选人的密文票数总和；$\text{ct}_i[0]$ 和 $\text{ct}_i[1]$ 分别表示明文 $m_i$ 加密后得到的两位密文；$\text{ct}_j[0]$ 和 $\text{ct}_j[1]$ 分别表示明文 $m_j$ 加密后得到的两位密文。

计票阶段结束后，智能合约用生成的 BFV 私钥 sk 解密选票结果，并将选票结果在区块链上发布。

$$m'=\left\lfloor \frac{t[c_0+c_1s]_p}{p} \right\rfloor_t \tag{15}$$

其中，$m'$ 为 BFV 解密后的计票结果，$c_0=c_m[0]$，$c_1=c_m[1]$。

表 4 总结了 BFV 同态加密算法在本文方案中各个阶段的具体应用。

### 2.4 密钥管理

2.3 节详细介绍了电子投票系统 BFV-Block

**表 4　BFV 同态加密算法在本文方案中各个阶段的具体应用**

| BFV 流程 | 具体应用 |
|---|---|
| 私钥 sk 生成 | 随机生成的一个系数为−1、0 或 1 的多项式 |
| 公钥 pk 生成 | $\text{pk}=([-a\text{sk}+e]_p,a)$，其中，$a$ 为在密文空间中随机生成的一个多项式，其系数模为 $p$；$e$ 为噪声多项式，是在离散高斯分布中随机选取的一组小系数，$e$ 在此处只用一次，用完后丢弃 |
| 计算密钥 rlk 生成 | $\text{rlk}=\left[\left(\left[-(a_i\text{sk}+e_i)+T^i\text{sk}^2\right]_p,a_i\right)\right], i\in[0,1,\cdots,l]$，其中，$T$ 为分解模数，$l=\lfloor \log_T(p) \rfloor$，$a_i$、$e_i$ 的生成方式与公钥生成阶段该多项式的生成方式相同 |
| 选票加密(密文为 $c_m$) | $c_m=\left(\left[\text{pk}_0u+e_1+\frac{qm}{t}\right]_p,[\text{pk}_1u+e_2]_p\right)$，其中，$m$ 为明文，本文方案中投票者的选票 $b_i$ 中对某个候选人的 $\text{cand}_k$ 即需要加密的明文；$u$ 为系数为−1、0 或 1 的多项式；$t$ 为远小于系数模 $p$ 的整数；$e_1$、$e_2$ 取自相同的高斯离散分布；$u$、$e_1$、$e_2$ 只在加密过程中使用，使用完后丢弃；pk 为 BFV 的公钥，$\text{pk}_0=\text{pk}[0]$，$\text{pk}_1=\text{pk}[1]$ |
| 计票(BFV 密文相加运算) | $\text{Add}(c_{im},c_{jm},\text{rlk})=(\text{ct}_i[0]+\text{ct}_j[0],\text{ct}_i[1]+\text{ct}_j[1])$，其中，$\text{Add}(c_{im},c_{jm},\text{rlk})$ 表示将投票者 $v_i$ 和 $v_j$ 对候选人 $\text{cand}_m$ 的投票情况密文相加的结果，$\text{ct}_i[0]$ 和 $\text{ct}_i[1]$ 分别表示明文 $m_i$ 加密后得到的两位密文，$\text{ct}_j[0]$ 和 $\text{ct}_j[1]$ 分别表示明文 $m_j$ 加密后得到的两位密文 |
| BFV 解密 | $m'=\left\lfloor \frac{t[c_0+c_1s]_p}{p} \right\rfloor_t$，其中，$c_0=c_m[0]$，$c_1=c_m[1]$，$m'$ 为 BFV 解密后的计票结果 |

chainvoting 的方案设计，方案中涉及的加密算法有 SM2、SM4 和 BFV 全同态加密算法，接下来，分别对这几种算法在方案中的密钥管理过程和必要性进行解释。

1) 密钥生成

SM2 算法的私钥 $x_a \in Z_q^*$ 由注册器随机选取产生，根据此私钥计算出与之对应的公钥为 $P_A = x_a G$ 。

SM4 的密钥 $k_i$ 由管理员 $A$ 和投票者 $V_i$ 通过 SM2 的密钥交换协议协商得到，$k_i$ 为 128 bit。

BFV 算法的密钥由智能合约调用 SEAL 库生成，其中安全参数设置为 $\lambda = 2\,048$ 。

2) 密钥分发与更新

SM2 的私钥 $x_a$ 由管理员 $A$ 保存，公钥 $P_A$ 公开。

SM4 算法的密钥 $k_i$ 由投票者 $V_i$ 和管理员 $A$ 各自保存，分别用来加密和解密。

BFV 算法的私钥 sk 由本地数据库保存，公钥 pk 由智能合约广播，投票者 $V_i$ 保存。

每次启动 BFV-Blockchainvoting 系统组织一次投票时，都将进行密钥更新，SM2、SM4、BFV 的密钥全部重新生成。

3) 密钥销毁

本文提出的 BFV-Blockchainvoting 方案主要包括 4 个连续的阶段，每个阶段都发生在投票组织者预先确定的特定时间范围内。时间段由智能合约通过方法 TimeSetup()设置，在选票公布结束后，SM2、SM4、BFV 的密钥全部回归初始化配置。

SM2 算法应用在投票者注册阶段，在此阶段管理员对投票者的公钥进行签名，标记合法的投票者，形成投票者名册，以便主持人在分发选票时识别合法的投票者。SM4 算法应用在获取选票阶段，为了保证传输过程中选票信息的机密性，管理员将选票使用 SM4 加密后分发给主持人，主持人再将加密后的选票分发给投票者，投票者解密选票信息后进行投票，通过上述流程保证了投票过程的不可操纵性。相比于国外的 RSA、ECC、AES 等算法，我国的 SM2 和 SM4 算法自主可控、安全可靠、处理速度快、使用方便快捷。

## 3　安全性证明与分析

本文提出的电子投票系统 BFV-Block chainvoting 是以区块链为底层框架的投票系统，该系统基于未花费交易输出（UTXO, unspent transaction output）[26]安全模型进行选票的分发与投出。UTXO 模型的概念来源于比特币，用来处理关联在某个比特币地址上的比特币交易金额，是一个包含了数据与可执行代码的数据结构。UTXO 模型中的每一笔输入都来自上一笔 UTXO 的输出，直到交易结束。本文方案中每张选票的分发或投出都依据 UTXO 模型的输入输出原理进行。UTXO 模型的使用可以减轻链上计算负担、抵御重放攻击、增强投票的隐私性。

### 3.1　安全性证明

本文提出的电子投票方案主要分为 4 个阶段：注册、获取选票、投票和计票。在投票者注册阶段，使用 SM2 签名算法对投票者的注册信息进行签名处理，标记投票者信息。在获取选票阶段，使用 SM4 算法加密选票，选择互相监督的机构（管理员和主持人）执行安全的多方监管，而互相监督的双方不会出现串通行为，从而保证选票在由主持人转交给投票者的过程中，主持人不知道选票信息。因此本文方案在注册阶段和获取选票阶段是安全的。

计票阶段由区块链的智能合约进行自动计票，智能合约的计票功能由底层代码设计，同时在计票过程中没有任何一方的参与，所以计票阶段也是安全的。

因此，证明本文提出的电子投票方案的安全性可以归约为证明方案中投票阶段的安全性。本文参考文献[27]，选用 Game Model 来证明投票阶段的安全性，在该模型中，允许对手通过预言机查询加密后的选票信息。

BS 安全性：如果在下面的博弈中，没有多项式有界对手 $\mathbb{A}$ 对挑战者 $\mathbb{C}$ 具有不可忽略的优势，那么称该投票方案是 BS[27]安全的。

1) $\mathbb{C}$ 运行公钥生成算法 PublicKey(sk)生成公钥，并将公钥 pk 交给 $\mathbb{A}$ 。

2) $\mathbb{A}$ 通过预言机选择明文 $m_i, i \in [1,\cdots,n]$，并查询不同明文的密文 $c_i, i \in [1,\cdots,n]$ 。

3) $\mathbb{A}$ 发送相同长度的明文 $m_0$ 、$m_1$ 给 $\mathbb{C}$，$\mathbb{C}$ 随机的选择 $b \in \{0,1\}$，加密 $m_b$ 发送给 $\mathbb{A}$ 。

4) $\mathbb{A}$ 输出猜测 $b' \in \{0,1\}$，如果 $b = b'$ 则攻击成功。但在投票阶段，本文方案选用 BFV 全同态加密算法对选票进行加密，BFV 算法是基于环上错误学习（RLWE, learning with error over ring）问题的算法，所以 $\mathbb{A}$ 的优势可以规约为解决 RLWE 问题的优势，因此

$$\mathrm{Adv}_{\mathrm{BFV},\mathbb{A}}(\lambda) = \left|\Pr[b = b'] - \frac{1}{2}\right| = \mathrm{RLWE}(\mathbb{A}) \quad (16)$$

其中，$\mathbb{A}$ 的优势可以忽略不计。对于任意多项式时间 $\mathbb{A}$ 获胜的概率定义为

$$\mathrm{Adv}(\mathbb{A})=\left|\mathrm{P}[b=b']-\frac{1}{2}\right|=\mathrm{negl}(\lambda) \tag{17}$$

综上所述，本文方案在投票阶段是 BS 安全的，同时本文提出的电子投票方案是安全的。

### 3.2 安全性分析

1) 不可重用性（防止双重投票）

不同场景下投票政策不同，有些政策允许投票者使用同一张选票进行多次投票，只计算他们的第一张选票。但是有些政策只允许投票者提交一次选票，取消多次提交选票的投票者的投票资格。

在这 2 种情况下，本文方案都是抵制双重选票的，因为本文方案选用区块链系统作为公告板。对于前者，智能合约扫描区块链，所有多次出现的选票，只计算第一次出现的选票。对于后者，智能合约取消多次出现选票的投票者的投票资格。

2) 不可胁迫性

投票者收到有效的选票 $b_i$ 才可以进行投票，在本文提出的方案中，投票者并没有直接获得选票，投票者收到的是经过密钥 $k_i$ 加密后的选票 $\mathrm{enb}_i$。这意味着威胁者要求投票者解密选票后，才可以拿到投票者的投票凭证。投票者可以用 $k_i'$ 解密 $\mathrm{enb}_i$，然后将假选票 $b_i'$ 分享给威胁者。根据 DDH（decisional diffie-hellman）假设，不可能在一个概率多项式时间内通过暴力破解区分出 $(g,g^a,g^b,g^c,k_i=g^{abc})$ 和 $(g,g^a,g^b,g^c,k_i'=R)$，其中 $R\in\mathbb{Z}_P^*$，DDH 假设为

$$\left|\Pr\left[\mathcal{A}(g,g^a,g^b,g^c,k_i=g^{abc})\right]-\Pr\left[\mathcal{A}(g,g^a,g^b,g^c,k_i'=R)\right]\right|\geqslant\varepsilon \tag{18}$$

对于随机选择 $a,b,c\in Z_p^*$，如果没有多项式时间算法在解决 DDH 问题上具有不可忽略的优势，那么 DDH 假设成立。所以本文方案具有不可胁迫性。

3) 不可操纵性

投票者投出的选票在区块链上公开永久地存储，本文方案使用 BFV 同态加密算法加密选票，因此投票在整个过程中都是被隐藏的。投票者无法在势均力敌的竞选中通过投票来支持某位候选人从而操纵选举结果。

4) 匿名性

本文方案利用互相监督的机构来保护选民的隐私，使各方无法同时拥有选民和选票的信息，避免通过某张选票的信息而关联到投票者投票的内容，使投票者的匿名性得到保证。

5) 可验证性

计票阶段结束时，智能合约会在区块链上发布投票结果，投票者可以验证他们的选票是否被正确清点。

6) 抗量子攻击安全性

BFV 全同态加密运算的安全性基于 RLWE 上的格困难问题，可以抵抗量子计算攻击，保证了系统的抗量子攻击安全性。

## 4 测试与分析

本文测试的实际测试环境为 Intel 酷睿 i5 处理器、8 GB 内存、2.3 GHz、Windows 10 64 位操作系统的笔记本电脑。

### 4.1 投票系统性能测试

本文提出的电子投票系统使用区块链替代可信第三方，其中区块链的底层架构为自建的基于国密算法的公链系统，相比于 Hyperledger Fabric 和以太坊区块链的频繁更新或升级而造成的系统不稳定，本文系统不仅能够可靠运行，还可以满足投票系统的性能要求。下面，对本文系统的通信开销和存储开销进行分析和测试。

本文系统的底层区块链框架采用 PoW 共识算法，本节选用生成一个有效区块所需要的平均通信次数来衡量其通信开销，文献[28]中给出了区块链通信开销的计算方法，如式(19)所示。

$$C_{\mathrm{PoW}}=\alpha T_1(N-1)\left(2-P_s^{N-1}\right)+\frac{(N-1)^2}{N}(1-P_s)+N-1 \tag{19}$$

其中，$C_{\mathrm{PoW}}$ 表示基于 PoW 共识算法的区块链通信开销，$\alpha$ 表示全网节点的交易到达率，$T_1\approx\dfrac{D}{Nr_1}$ 表示正常生成一个区块所需要的平均时间，$N$ 表示节点个数，$r_1$ 表示节点算力，$D$ 表示目标难度值。

为评估本文系统的通信开销，根据式(19)，本节测试了系统中的关键参数。全网节点的交易到达率 $\alpha$=5 TPS（transaction per second），节点算力 $r_1$=7.5 MH/s（每秒 $10^6$ 次 Hash 运算），PoW 的难度值 $D$=2.0。图 3 为节点传输成功概率 $P_s$ 为 0 和 0.85 这 2 种情况下的通信开销。从图 3 可以看出，通信次数（通信开销）与节点个数成正比，当节点个数

为 150 时，通信次数（通信开销）为 174。本文系统的节点传输成功率较高，所产生的通信开销对系统正常运行产生的影响很小。

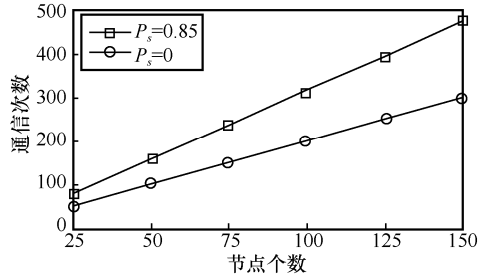



图 3　不同节点个数下的通信开销

每名投票者的存储开销包括个人公/私钥、地址、未花费证明数据和区块链上投票数据等。每名投票者由于存储个人公/私钥以及地址值约带来 3 KB 的存储开销。每名投票者只有一张选票，所以其未花费证明数据所占的存储开销也较小。随着投票人数的增加，影响存储开销的主要因素为区块链上的投票数据。

为评估本文系统的存储开销，本节在 1 名候选人的情况下，分别设置了 1 次投票、25 次投票和 50 次投票的投票环境，得到不同投票次数下的存储开销，如图4所示，并依此评估了5 000次投票时的存储开销。根据评估可知，每次投票链上数据约增长 2 KB，进行 5 000 次投票所产生的存储开销约为 9.8 MB，该存储开销满足投票系统的性能需求。

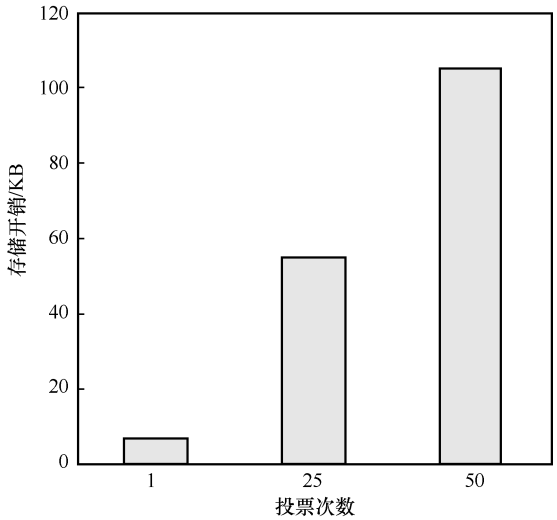



图 4　不同投票次数下的存储开销

本文提出的 BFV-Blockchainvoting 方案主要包括 4 个连续的阶段，每个阶段都发生在投票组织者预先确定的特定时间范围内。投票者注册、选票分发以及投票者投出选票的过程为并发进行，其效率对系统的运行影响不大，而计票效率是决定系统能否在规定时间内完成计票的关键。为测试计票效率，本节设置了 50 名投票者、1 名候选人的投票环境。图 5 展示了 50 次计票的测试结果。经过测试，本文系统单张选票的计票时间平均为 1.69 ms。通过对 10 组密文状态的计票结果进行解密测试，进而得到明文状态的计票结果，平均每次解密时间为 163.70 ms。

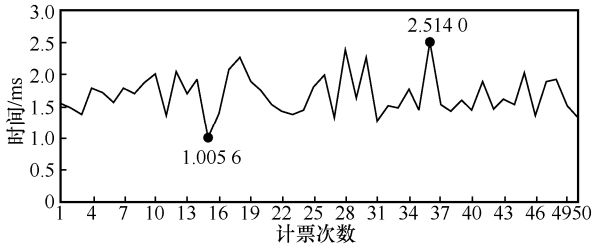



图 5　单张选票的计票时间测试

### 4.2　相似类型的电子投票系统对比分析

将本文方案与其他基于区块链或同态加密技术的电子投票系统进行对比，结果如表 5 所示。目前，国内外大多数学者没有将区块链与全同态加密算法相融合的技术引入电子投票系统的设计中，并很少进行实际环境下的效率测试。表 5 中，文献[22]和文献[29]都采用了区块链与同态加密算法相结合的方案，但其采用 Pallier 部分同态加密算法，其同态性计算通过幂运算实现，相比于本文提出的投票系统 BFV-Blockchainvoting 所采用的 BFV 全同态加密算法来说效率较低。文献[30]也采用 Pallier 部分同态加密算法，但没有依托区块链环境，投票效率较低。相比于采用以太坊架构且包含 6 个节点的文献[29]，本文方案的计票时间减少了 99.79%。相比于文献[30]，本文方案的计票时间减少了 95.77%。文献[31]和文献[11]也选用了具有抗量子计算攻击特性的全同态加密算法，但同样也没有依托区块链环境。相比于文献[11]中借助第三方机构与 BFV 全同态加密算法相结合的投票方案，本文方案的计票时间减少了 9.63%。文献[20]和文献[25]使用了区块链架构，但其没有使用同态加密算法。相比于文献[20]，本文方案的计票时间减少了 98.87%。文献[25]使用投票者的指纹作为登记认证信息，系统为降低指纹识别的错误拒绝率需要消耗较长时间，相比于采用以太坊架构且包含 50 个节点的文献[25]，本文方案的计票时间减少了 32.4%。

表 5 本文方案与其他方案的性能比较

| 方案 | 区块链技术 | 同态加密算法 | 多方安全监管 | 抗量子攻击 | 抗胁迫性 | 不可操纵性 | 匿名性 | 可验证性 | 计票时间/ms |
|---|---|---|---|---|---|---|---|---|---|
| 文献[22] | √ | Pallier | × | × | √ | √ | √ | √ | — |
| 文献[29] | √ | Pallier | × | × | × | √ | √ | √ | 813 |
| 文献[30] | × | Pallier | × | × | × | × | √ | √ | 39.94 |
| 文献[31] | × | GSW | × | √ | × | √ | √ | √ | — |
| 文献[11] | × | BFV | × | √ | × | √ | √ | √ | 1.87 |
| 文献[20] | √ | — | × | × | × | √ | √ | √ | 150 |
| 文献[25] | √ | — | × | × | × | √ | √ | √ | 2.5 |
| 本文方案 | √ | BFV | √ | √ | √ | √ | √ | √ | 1.69 |

## 5 结束语

本文提出的电子投票系统将区块链和 BFV 全同态加密算法相结合，利用全同态加密算法加密选票信息，使选票可以在密文情况下被统计，候选人的获票情况直到解密最终计票结果后才会公布，保证了投票过程的抗操纵性。在注册与获取选票阶段，使用 SM2 数字签名算法对投票者的注册信息进行签名，使用 SM4 算法来加密选票，选择具有能够互相监督的双方共同监管选票，确保投票者与选票信息分离。投票者提交选票后，利用区块链上的智能合约实现对投票者的合法性验证和自计票功能。使用区块链替代可信第三方，避免第三方虚假计票或服务器被攻击后的信息泄露风险，计票效率也得到提升。通过测试，本文系统单张选票的计票时间平均为 1.69 ms，相比于文献[29]中使用区块链和 Pallier 部分同态加密算法相结合的投票方案的计票时间减少了 99.79%；相比于文献[11]中借助第三方机构与 BFV 全同态加密算法相结合的投票方案的计票时间减少了 9.62%；相比于文献[25]未使用同态加密算法，只使用区块链架构的投票方案的计票时间减少了 32.4%。本文方案总体计算开销合理，计票效率较高，可以为大规模电子投票场景提供借鉴。下一步的研究思路是探讨全同态签密技术在区块链电子投票中的应用，并进行智能合约的安全性测试与分析。

## 参考文献：


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

[2] WANG K H, MONDAL S K, CHAN K, et al. A review of contemporary E-voting: requirements, technology, systems and usability[J]. Data Science and Pattern Recognition, 2017, 1(1): 31-47.

[3] ALAM K M R, TAMURA S, RAHMAN S M S, et al. An electronic voting scheme based on revised-SVRM and confirmation numbers[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(1): 400-410.

[4] ARANHA D F, BAUM C, GJØSTEEN K, et al. Lattice-based proof of shuffle and applications to electronic voting[C]//Cryptographers' Track at the RSA Conference (CT-RSA). Berlin: Springer, 2021: 227-251.

[5] HAINES T, GORÉ R, SHARMA B. Did you mix me? Formally verifying verifiable mix nets in electronic voting[C]//Proceedings of 2021 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2021: 1748-1765.

[6] KUMAR M, CHAND S, KATTI C P. A secure end-to-end verifiable Internet-voting system using identity-based blind signature[J]. IEEE Systems Journal, 2020, 14(2): 2032-2041.

[7] KUMAR M, KATTI C P, SAXENA P C. A secure anonymous e-voting system using identity-based blind signature scheme[C]//International Conference on Information Systems Security (ICISS). Berlin: Springer, 2017: 29-49.

[8] ZHANG X, ZHANG J Z, XIE S C. A secure quantum voting scheme based on quantum group blind signature[J]. International Journal of Theoretical Physics, 2020, 59(3): 719-729.

[9] FAN X Y, WU T, ZHENG Q H, et al. HSE-Voting: a secure high-efficiency electronic voting scheme based on homomorphic signcryption[J]. Future Generation Computer Systems, 2020, 111: 754-762.

[10] FAN X Y, WU T, ZHENG Q H, et al. DHS-voting: a distributed homomorphic signcryption E-voting[C]//International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications (DepenSys). Berlin: Springer, 2019: 40-53.

[11] 杨亚涛, 赵阳, 张奇林, 等. 基于 SEAL 库的同态加权电子投票系统[J]. 计算机学报, 2020, 43(4): 711-723.
YANG Y T, ZHAO Y, ZHANG Q L, et al. Weighted electronic voting system with homomorphic encryption based on SEAL[J]. Chinese Journal of Computers, 2020, 43(4): 711-723.

[12] ADIDA B. Helios: Web-based open-audit voting[C]//USENIX Security Symposium (USS). Berkeley: USENIX Association, 2008: 335-348.

[13] ARA A, AL-RODHAAN M, TIAN Y, et al. A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems[J]. IEEE Access, 2017, 5: 12601-12617.

[14] ANJIMA V S, HARI N N. Secure cloud e-voting system using fully homomorphic elliptical curve cryptography[C]//Proceedings of 2019 International Conference on Intelligent Computing and Control

Systems (ICCS). Piscataway: IEEE Press, 2019: 858-864.

[15] KIM H, KIM K E, PARK S, et al. E-voting system using homomorphic encryption and blockchain technology to encrypt voter data[J]. arXiv Preprint, arXiv: 2111.05096, 2021.

[16] PATEL B, TANDEL P, SANGHVI S. Efficient ballot casting in ranked based voting system using homomorphic encryption[C]//International Conference on Advances in Computing and Data Sciences (ICACD). Berlin: Springer, 2019: 565-576.

[17] CHILLOTTI I, GAMA N, GEORGIEVA M, et al. A homomorphic LWE based E-voting scheme[C]//Post-Quantum Cryptography (PQC). Berlin: Springer, 2016: 245-265.

[18] DUCAS L, DURMUS A, LEPOINT T, et al. Lattice signatures and bimodal Gaussians[C]//33rd Annual Cryptology Conference on Advances in Cryptology (CRYPTO). Berlin: Springer, 2013: 40-56.

[19] YADAV V K, ANAND A, VERMA S, et al. Private computation of the Schulze voting method over the cloud[J]. Cluster Computing, 2020, 23(4): 2517-2531.

[20] PANDEY A, BHASI M, CHANDRASEKARAN K. VoteChain: a blockchain based E-voting system[C]//Proceedings of 2019 Global Conference for Advancement in Technology (GCAT). Piscataway: IEEE Press, 2019: 1-4.

[21] ALAM A, RASHID S M Z U, ABDUS SALAM M, et al. Towards blockchain-based E-voting system[C]//Proceedings of 2018 International Conference on Innovations in Science, Engineering and Technology (ICISET). Piscataway: IEEE Press, 2018: 351-354.

[22] YU B, LIU J K, SAKZAD A, et al. Platform-independent secure blockchain-based voting system[C]//International Conference on Information Security (ICIS). Berlin: Springer, 2018: 369-386.

[23] PRIYA J C, BHAMA P R S, SWARNALAXMI S, et al. Blockchain centered homomorphic encryption: a secure solution for E-balloting [C]//International Conference on Computer Networks, Big Data and IoT. Berlin: Springer, 2018: 811-819.

[24] FAN J, VERCAUTEREN F. Somewhat practical fully homomorphic encryption [J]. IACR Cryptology Eprint Archive, 2012, 1(1): 144-156.

[25] PANJA S, ROY B. A secure end-to-end verifiable E-voting system using blockchain and cloud server[J]. Journal of Information Security and Applications, 2021, 59: 102815.

[26] 杨亚涛, 蔡居良, 张筱薇, 等. 基于 SM9 算法可证明安全的区块链隐私保护方案[J]. 软件学报, 2019, 30(6): 1692-1704.
YANG Y T, CAI J L, ZHANG X W, et al. Privacy preserving scheme in block chain with provably secure based on SM9 algorithm[J]. Journal of Software, 2019, 30(6): 1692-1704.

[27] KHADER D, SMYTH B, RYAN P Y A, et al. A fair and robust voting system by broadcast[J]. Lecture Notes in Informatics, 2012, 23(2): 285-299.

[28] 曹宾, 聂凯君, 彭木根, 等. 无线网络中区块链共识算法的开销分析[J]. 北京邮电大学学报, 2020, 43(6): 140-146.
CAO B, NIE K J, PENG M G, et al. Overhead analysis of blockchain consensus algorithm in wireless networks[J]. Journal of Beijing University of Posts and Telecommunications, 2020, 43(6): 140-146.

[29] DAGHER G G, MARELLA P B, MILOJKOVIC M, et al. Broncovote: secure voting system using ethereum's blockchain[J]. Computer Science, 2018, 48(4): 96-107.

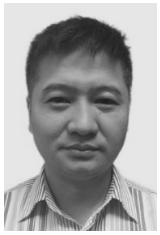
[30] SAADEH I A, ABANDAH G A. Investigating parallel implementations of electronic voting verification and tallying processes[C]//Proceedings of 2017 European Conference on Electrical Engineering and Computer Science (EECS). Piscataway: IEEE Press, 2017: 70-75.

[31] 何倩. 基于全同态加密的电子投票方案研究[D]. 杭州: 浙江理工大学, 2019.
HE Q. Research on electronic voting scheme based on fully homomorphic encryption[D]. Hangzhou: Zhejiang Sci-Tech University, 2019.

[作者简介]

**杨亚涛**（1978− ），男，河南平顶山人，博士，北京电子科技学院教授、博士生导师，西安电子科技大学硕士生导师，主要研究方向为密码学与通信安全、全同态加密、密码协议和算法等。

**刘德莉**（1998− ），女，山东德州人，西安电子科技大学硕士生，主要研究方向为区块链安全、安全协议与算法。



**刘培鹤**（1972− ），男，黑龙江鹤岗人，北京电子科技学院工程师，主要研究方向为网络与通信安全、区块链安全。

**曾萍**（1969− ），女，河南焦作人，博士，北京电子科技学院教授，主要研究方向为通信与网络安全、车联网安全、区块链安全等。

**肖嵩**（1977− ），女，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为多媒体通信安全、通信与信息安全等。