Journal of Computer Applications
计算机应用, 2020, 40(7): 1989 - 1995
ISSN 1001-9081
CODEN JYIIDU
2020-07-10
http://www.joca.cn

文章编号:1001-9081(2020)07-1989-07
DOI:10.11772/j.issn.1001-9081.2019122171

# 基于区块链的安全电子选举方案

吴芷菡[1,2],崔　喆[1,2*],刘　霆[1,2],蒲泓全[1,2]
(1. 中国科学院 成都计算机应用研究所,成都 610041; 2. 中国科学院大学,北京 100049)
(*通信作者电子邮箱 cuizhe@casit.com.cn)

**摘　要**:当前电子选举方案主要存在两个矛盾点:一是既要保证选举行为的合法合规性,又要保证选举过程的匿名性;二是既要保证选票信息的隐私保密要求,又要保证选举结果的公众可验证性。针对这些矛盾,提出一种基于以太坊区块链和零知识证明的去中心化的安全电子选举方案。在该方案中,利用非交互式零知识证明算法和区块链去中心化架构设计了选民身份合法性零知识证明和选票合法性零知识证明;利用智能合约和Paillier密码体制实现无需可信第三方计票机构的自动计票。理论分析和模拟实验结果表明,在没有中心信任机构的条件下,该方案满足电子选举安全性要求,可应用于小型社区选举。

**关键词**:电子选举;非交互式零知识证明;区块链;智能合约;去中心化
**中图分类号**:TP311.1　　**文献标志码**:A

## Secure electronic voting scheme based on blockchain

WU Zhihan[1,2], CUI Zhe[1,2*], LIU Ting[1,2], PU Hongquan[1,2]
(1. *Chengdu Institute of Computer Application, Chinese Academy of Sciences, Chengdu Sichuan* 610041, *China*;
2. *University of Chinese Academy of Sciences, Beijing* 100049, *China*)

**Abstract:** There are two main contradictions in the existing electronic voting schemes, one is to ensure the legality and compliance of election behavior while ensuring the anonymity of election process, and the other is to ensure the privacy security of ballot information while ensuring the public verifiability of election results. Focusing on these contradictions, a decentralized electronic voting scheme based on Ethereum blockchain and zero-knowledge proof was proposed. In the proposed scheme, the non-interactive zero-knowledge proof algorithm and decentralized blockchain architecture were fused to build zero knowledge proof of voter identity and zero knowledge proof of ballot legality. And smart contract and Paillier algorithm were used to realize self-counting without trusted third-party counting mechanism. The theoretical analysis and simulation results show that the scheme can achieve security requirements of electronic voting and can be applied to small-scale community election.

**Key words:** electronic voting; non-interactive zero-knowledge proof; blockchain; smart contract; decentralization



## 0　引言

随着现代信息技术的发展,社会对电子选举技术以及社会民主进步的关注日益增加。近年来,电子选举已经成为国际信息技术界一个特殊重要的领域。如今国际电子选举系统研究主要分为两个方向:一是基于远程网络通信的电子选举(Remote e-Voting),主要是基于数论的密码学工具和应用技巧,主要有基于同态加密的电子选举方案、基于秘密共享的电子选举方案、基于盲签名的电子选举方案和基于混合网络的电子选举方案;二是基于抵近物理站站点投票的电子选举(Site-Polling e-Voting),主要凭借物理设备和先进的信息技术手段实现高可信、高可靠的选举系统,例如应用于我国人民代表大会的选举系统。本文的研究方向是基于远程网络通信的电子选举。

基于同态加密的方案通过同态加密算法:ElGamal密码体制[1]、LWE(Learning With Errors)密码体制[2]和Paillier[3]密码体制对选票进行加密,然后由可信第三方计票机构接收和计算加密选票,文献[1-2]采用乘法同态、全同态运算,计算效率低,复杂度高,实用性较低。基于秘密共享[4-5]的方案通过将拆分后的选票发送至多个机构存储,由部分或全部机构恢复选票并统计结果,虽然多个可信任计票机构中心降低了单一权威计票机构内部欺诈的风险,但超过一定门限数量的机构串通仍可进行共谋攻击,控制选举。基于盲签名的方案有FOO(FUJIOKA-OKAMOTO-OHTA)[6]、基于ElGamal签名体制[7]等协议,通过盲签名技术对选民选票签名,存在依赖选举管理机构的公正性、选票碰撞、选举过程操作繁琐、协议效率低等问题。基于混合网络的方案算法复杂,实现困难[8]。针对现有方案存在的投票效率低、可能存在内部欺诈、依赖可信

**收稿日期**:2019-12-26;**修回日期**:2020-02-16;**录用日期**:2020-03-03。
**基金项目**:四川省重点研发项目(2018GZ0545);四川省重大科技专项(2019ZDZX0005)。
**作者简介**:吴芷菡(1994—),女,四川成都人,硕士研究生,主要研究方向:信息安全、可信计算、区块链; 崔喆(1970—),男,四川巴中人,研究员,博士,主要研究方向:可信计算、信息安全; 刘霆(1978—),男,天津人,博士研究生,主要研究方向:信息安全、区块链; 蒲泓全(1990—),男,四川巴中人,博士研究生,主要研究方向:信息安全、电子投票。

第三方等问题和电子选举主要的两个矛盾点,结合区块链公开透明、不可篡改、集体维护等特性,本文提出了基于区块链的去中心化电子选举方案。选民身份管理设计基于非交互式零知识证明算法 zk-SNARKs (zero-knowledge Succinct Non-interactive ARgument of Knowledges)[9]和区块链架构,既保证了选举的匿名性又保证了公开可验证性;选票隐私保护设计基于Paillier公钥密码体制;通过以太坊智能合约实现选举投票和计票流程自动化,去中心化。

## 1 预备知识

### 1.1 以太坊与智能合约

以太坊(Ethereum)是一个基于区块链技术的,可创建、使用智能合约(Smart Contract)和去中心化应用(Decentralized Application, DApp)的开源平台[10]。智能合约是以太坊网络上运行的程序,是一种由事件驱动的,具有具体状态的代码合约和算法合约。智能合约的代码编译后生成的字节码可以在以太坊客户端和节点运行。以太坊平台对底层区块链技术进行了封装,让区块链应用开发者可以直接基于以太坊平台进行开发,只专注于开发应用本身逻辑的智能合约,这样可以大幅度降低开发难度和成本。智能合约适用于对信任、安全和持久性要求较高的应用场景,例如数字货币、数字资产、投票、保险、金融应用、预测市场、产权所有权管理、物联网、点对点交易等。

### 1.2 零知识证明

零知识证明(Zero-Knowledge Proof)由 Goldwasser 等[11]在20世纪80年代初提出,证明者能够在不向验证者提供任何有用的信息的情况下,使验证者相信某个论断是正确的。Goldwasser 等[11]提出的是交互式零知识证明,需要证明者和验证者进行多轮通信证明,对于复杂问题证明效率较低。De Santis 等[12]首次提出了非交互零知识证明的概念,证明者只需要按照协议向验证者发送一次消息就可以让验证者以高概率确信一个论断是正确的。最初的非交互式零知识证明系统的效率是非常低,难以应用于实际问题。后续研究证明对于所有的NP语言都存在对应的非交互式零知识证明[13],研究者们通常将非交互式零知识问题规约到NP问题上。非交互式零知识证明已被广泛应用于当今的密码体制中。

区块链中每一笔交易的共识验证过程都涉及区块链网络的每一个节点,采用交互式零知识证明开销过大,所以在区块链系统中更适合采用非交互式零知识证明。zk-SNARKs是典型的非交互式零知识证明协议,通过同态隐藏、多项式盲估、匹诺曹协议、椭圆曲线配对等技术,实现了证明者只需要提供的短小的零知识证明字符串 proof 就可以完成简洁、高效的证明过程。目前匿名性较好的密码学货币 Zerocash[9]就是利用 zk-SNARKs 实现交易信息隐私保护。Zerocash 中隐私交易信息可以在区块链上完全加密,在加密的情况下仍然可以通过 zk-SNARKs 证明在该交易在共识规则下的有效性。

### 1.3 Pailier公钥密码体制

Paillier算法是一种具有语义安全性,是基于复合剩余类的困难问题的公钥密码体制,该加密算法满足加法同态性和混合乘法同态性,其中加法同态性适用于电子选举系统的选票加密[14]。加法同态指的是通过密文 $E(X)$ 和 $E(Y)$ 可计算获得 $E(X+Y)$,解密后可得到 $X+Y$。

Paillier 密钥生成　随机且彼此独立地选择两个大质数 $p$ 和 $q$,且满足 $\gcd(p\times q,(p-1)\times(q-1))=1$,gcd 表示最大公约数,计算 $n=p\times q$ 和 $\lambda=\mathrm{lcm}(p-1,q-1)$,lcm 表示最小公倍数。选择随机整数 $g\in G$,$G$ 为模 $n^2$ 的乘法群,并且满足 $\mu=\left(L\left(g^{\lambda} \bmod n^2\right)\right)^{-1} \bmod n$,其中定义函数 $L(x)=(x-1)/n$。Paillier算法公钥为 $(n,g)$,私钥为 $(\lambda,\mu)$。

Paillier 加密　设 $m(0\leqslant m<n)$ 为需要加密的信息,选择加密随机数 $r$,$r$ 需满足 $0<r<n$ 和 $r\in G$,确保 $\gcd(r,n)=1$。加密算法 $E_p(m)=g^m\times r^n \bmod n^2$,分别对明文 $m1$ 和 $m2$ 进行加密,得到对应密文为 $c1=g^{m1}\times r^n \bmod n^2$ 和 $c2=g^{m2}\times r^n \bmod n^2$。密文性质有 $c1\times c2=g^{(m1+m2)}\times r^{2n} \bmod n^2=E_p(m1+m2)$,所以Paillier算法具有加法同态性[14]。

Paillier 解密　$m=D_p(c)=L(c^{\lambda} \bmod n^2)\times\mu \bmod n$

## 2 去中心化电子选举方案

### 2.1 方案设计

在本电子选举方案中,参与者如下:

选举发起方　发起选举,初始化选举信息。

线下认证中心(由选举发起方指定)　选举方在注册阶段设置线下验证点,对选民的身份进行验证。

选民　用 $V_1,V_2,\cdots,V_n$ 表示。

候选人　一场选举中有多个候选人,对应的候选人用 $C_1,C_2,\cdots,C_m$ 表示。

选举初始化阶段,选举发起方初始化选举信息,部署选举智能合约至区块链;选举注册阶段,选民在线下认证中心认证、注册获得投票资格;选举投票阶段,选民通过 zk-SNARKs 零知识证明算法生成身份证明 *proofV* 和选票合法性证明 *proofB*,通过 Paillier 算法加密选票,将零知识证明和加密选票发送至区块链;选举计票阶段,智能合约自动调用计票算法,获取区块链上的加密选票,利用 Paillier 算法加法同态实现加密计票。整个选举过程数据经国密算法 SM2 椭圆曲线公钥密码算法[15]、SM3 密码杂凑算法[16]处理后公开写入区块链,任何参与者都可以验证投票数据和选举结果。

### 2.2 基于 zk-SNARKs 算法选民身份隐藏方案

选民身份管理是电子选举的一大难题,在选举过程中为保证选民身份合法性,需要对选民身份进行有效的认证,但在选举过程中又要需要保证匿名性。针对这个问题,通过区块链架构和 zk-SNARKs 非交互式零知识证明实现选举匿名性和选民身份合法性验证。投票阶段,通过 zk-SNARKs 生成选民身份证明 *proofV*,将 *proofV* 和加密选票一同写入区块链;计票阶段,智能合约通过调用验证算法验证 *proofV* 间接验证选民身份的合法性。区块链的数据是公开透明的,任何人都可以对区块链上的 *proofV* 进行验证;区块链具有一定的匿名性,在区块链实现一次身份隐藏的基础上再通过 zk-SNARKs 实现二

次身份隐藏;基于zk-SNARKs非交互式特性,一次生成证明*proofV*,无需多次交互,保证选举效率。

由于zk-SNARKs不能直接应用于任意问题,必须有可量化的输入,因此需要将实际问题转换成zk-SNARKs可处理的数学描述模型:首先将需要证明的问题约化为指定的NP问题,实现基于算术电路的NP问题的证明和验证;然后再通过多项式盲验证、同态隐藏、匹诺曹协议等技术生成零知识证明字符串*proof*;最终生成的*proof*基于多项式等式的抽样验证只需要$O(1)$的验证代价,验证更为高效、简洁。

zk-SNARKs身份证明算法生成*proofV*过程如下[9,17]:

1)算术逻辑方程验证转化为算术电路验证。

选民需要在不暴露$i$的具体数值情况下证明自己是合法选民$V_1,V_2,\cdots,V_n$中的一员$V_i$,算术逻辑方程可表示为:

$$(V_1 - V_i)(V_2 - V_i)\cdots(V_n - V_i) = 0 \tag{1}$$

式(1)的门电路可表示为方程组(2):

$$\begin{cases} sys_1 = (V_1 - V_i) \\ sys_2 = (V_2 - V_i) \\ sys_3 = sys_1 * sys_2 \\ \vdots \\ sys_m = (V_n - V_i) \\ out = (sys_m) * (sys_{m-1}) \end{cases} \tag{2}$$

将算术方程转化为算术电路,首先将方程分解为加法、乘法组成的最小操作,然后增加中间变量,把复杂的计算方程转化为简单的门电路表示,最终门电路的输出结果与原表达式等价。

其中$sys_1,sys_2,\cdots,sys_m$是算术电路设计新增的中间变量,*out*是整个电路的输出,等价于方程的计算结果。该方程的电路表示如图1所示。

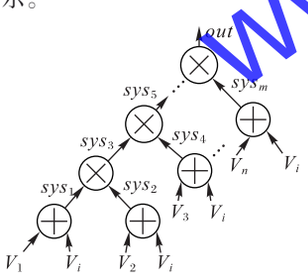


图1　选民身份证明算术电路

Fig. 1　Arithmetic circuit of voter identification

2)算术电路验证转化为向量验证R1CS(Rank-1 Constraint System)[18]。

将每一个门电路表示为等价的向量点积形式,这个过程称为R1CS,就是将门电路转化成向量的表达方式。首先用一组向量定义算术电路中的所有的变量。上述电路可表示为:*one*代表常量变量1,$V_1,V_2,\cdots,V_n$,$V_i$代表输入,$sys_1,sys_2,\cdots,sys_m$代表中间门电路的输出,*out*代表整体电路输出。则定义$\boldsymbol{s}$如下:

$$\boldsymbol{s} = [one, V_1, V_2, \cdots, V_n, V_i, sys_1, sys_2, \cdots, sys_m, out]$$

然后对于每个门电路,存在一组向量$(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c})$,使得$\boldsymbol{s}\cdot\boldsymbol{a} * \boldsymbol{s}\cdot\boldsymbol{b} - \boldsymbol{s}\cdot\boldsymbol{c} = 0$成立。例如门电路$sys_1 = (V_1 - V_i)$,存在向量组:

$\boldsymbol{a} = [1,0,\cdots,0,0,0,\cdots,0]$,$\boldsymbol{s}\cdot\boldsymbol{a}$结果为*one*;

$\boldsymbol{b} = [0,1,\cdots,0,-1,0,\cdots,0]$,$\boldsymbol{s}\cdot\boldsymbol{b}$结果为$V_1 - V_i$;

$\boldsymbol{c} = [0,0,\cdots,0,0,1,\cdots,0]$,$\boldsymbol{s}\cdot\boldsymbol{c}$结果为$sys_1$;

代入$\boldsymbol{s}\cdot\boldsymbol{a} * \boldsymbol{s}\cdot\boldsymbol{b} - \boldsymbol{s}\cdot\boldsymbol{c} = 0$,可计算得到:$one * (V_1 - V_i) - sys_1 = 0$,等价于$sys_1 = (V_1 - V_i)$。以此类推,可将所有门电路转化成向量表达式$\boldsymbol{s}\cdot\boldsymbol{a} * \boldsymbol{s}\cdot\boldsymbol{b} - \boldsymbol{s}\cdot\boldsymbol{c} = 0$,获得每个门电路对应的向量组$(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c})$。

3)向量验证R1CS转化为QAP(Quadratic Assignment Problems)[19]多项式验证。

本文方案选择将选民身份验证问题归约的NP问题为二次算数问题QAP,证明QAP多项式成立就是证明选民身份合法性。QAP指的是有一系列多项式和一个目标多项式,存在多项式的组合能整除目标多项式。

已知$w$个门电路都对应存在向量组$(\boldsymbol{a},\boldsymbol{b},\boldsymbol{c})$,将$\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}$中每个系数看成一个多项式的结果,例如每个门电路对应的向量$\boldsymbol{a}$的系数作为一个多项式的解,可以反推出多项式$a(x) = [f_0(x),f_1(x),\cdots,f_k(x)]$:对于门电路1,已知解$f_0(1)$,以此类推$f_0(2),f_0(3),\cdots,f_0(w)$都是已知值,可以通过拉格朗日插值法反推出多项式$f_0(x)$,当向量比较大时,可以通过快速傅里叶变化进行优化。同理可以算出$f_1(x),f_2(x),\cdots,f_k(x)$。最终,转化完成后可获得三个多项式数组$a(x),b(x),c(x)$。

定义多项式$P(x) = \boldsymbol{s}\cdot a(x) * \boldsymbol{s}\cdot b(x) - \boldsymbol{s}\cdot c(x)$,$x \in (1,2,\cdots,w)$,$w$是门的数量。已知每个门电路对应的向量组都满足$\boldsymbol{s}\cdot\boldsymbol{a} * \boldsymbol{s}\cdot\boldsymbol{b} - \boldsymbol{s}\cdot\boldsymbol{c} = 0$,则当$x$取1至$w$任意值,都有$P(x) = 0$。根据多项式特性,若$P(a) = 0$,则$(x - a)$可以整除$P(x)$,以此类推,$P(x)$可以被$(x-1)(x-2)\cdots(x-w)$整除,即满足QAP定义,存在$H(x) = 0$使得$T(x) = (x-1)(x-2)\cdots(x-w)$目标多项式可以整除多项式组合$P(x)$,生成QAP方程:

$$\boldsymbol{s}\cdot a(x) * \boldsymbol{s}\cdot b(x) - \boldsymbol{s}\cdot c(x) = T(x) * H(x) \tag{3}$$

将验证计算方程式(1)转化为验证QAP方程式(3)过程中的向量$\boldsymbol{s}$是证明者独有,也只有正确的$\boldsymbol{s}$才能使方程成立,且在转化过程中插入的混淆值与计算方程的逻辑没有任何关系,QAP多项式的验证不等于原方程的验证,而是原方程的验证包含在QAP方程的验证里,那么验证QAP方程等于验证原方程。zk-SNARKs算法通过抽样实现简洁验证,并不需要验证所有的$x$,$x \in (1,2,\cdots,w)$,只需要随机抽查任意一个点验证即可,所以算法验证速度快。

4)zk-SNARKs零知识证明。

验证方程为式(3),为了方便表示,定义$A(x) = \boldsymbol{s}\cdot a(x)$,$B(x) = \boldsymbol{s}\cdot b(x)$,$C(x) = \boldsymbol{s}\cdot c(x)$,则方程表示可为$A(x) * B(x) - C(x) = T(x) * H(x)$。

椭圆曲线配对[20]　证明过程采用椭圆曲线加密算法$E(x) = g^x$,$g$为生成元。已知椭圆曲线满足加法同态,在验证方程$A(x) * B(x) - C(x) = T(x) * H(x)$时涉及乘法,可以通过椭圆曲线配对实现计算层面的乘法同态。已知配对函数定义

如下：$e(g^x,g^y)=e(g,g)^{xy}$，对于明文 $m1$ 和 $m2$，对应密文为 $E(m1),(m2)$，存在等式：

$$e\left(g^{E(m1)},g^{E(m2)}\right)=e(g,g)^{E(m1)E(m2)} \tag{4}$$

**椭圆曲线 $\alpha$ 对**[20] zk-SNARKs 零知识证明利用了 $\alpha$ 对的性质实现多项式盲验证。椭圆曲线的 $\alpha$ 对指的是椭圆曲线上满足 $y=\alpha*x$ 的一对值 $(x,y)$，利用 $\alpha$ 对的性质，可设计如下证明过程以满足在不暴露隐私信息的情况下让验证相信证明者拥有某个信息：

验证者生成 $\alpha$ 参数，根据参数生成 $\alpha$ 对 $(x,y)$，验证者保存参数 $\alpha$，将 $\alpha$ 对 $(x,y)$ 发送给证明者。

证明者持有信息 $\beta$，与验证生成的 $\alpha$ 对进行计算可获得 $(x',y')=(\beta*x,\beta*y)$。已知 $y=\alpha*x$，利用交换律，则 $y'=\beta*y=\beta*\alpha*x=\alpha*(\beta*x)=\alpha*x'$，根据定义 $(x',y')$ 也是一个 $\alpha$ 对。证明者将 $(x',y')$ 发送给验证者。

验证者验证 $(x',y')$ 是否是 $\alpha$ 对，就可以知道证明者是否持有信息 $\beta$，且验证过程不会暴露证明者拥有的信息 $\beta$。

**公共参考串（Common Reference String，CRS）模型**[21] zk-SNARKs 为了实现非交互式零知识证明，采用了公共参考串模型 CRS，将验证参数进行处理后公示。若 $k,\alpha,\beta_a,\beta_b,\beta_c$ 随机参数被泄露，则证明的安全前提将不复存在，所以 ZeroCash 选择了世界各地 6 个可信任机构分别生成密钥的一部分，6 份密钥拼接在一起生成随机参数 $k,\alpha,\beta_a,\beta_b,\beta_c$ 和随机参数的公示数据 CRS 后便被分别销毁，随机参数 $k,\alpha,\beta_a,\beta_b,\beta_c$ 也被销毁，由此来保证 CRS 的安全性。生成 *proof* 阶段：

步骤一　验证者确定生成元为 $g$、阶为 $n$ 的有限群，已知 $A(x),B(x),C(x)$ 多项式的最高阶为 $d$，随机选择有限群中的元素 $k$，和随机参数 $\alpha,\beta_a,\beta_b,\beta_c$ 计算生成 CRS，式(5)写入区块链并公布。

$$\begin{cases}E(k^0),E(k^1),\cdots,E(k^d);\\ E(\alpha k^0),E(\alpha k^1),\cdots,E(\alpha k^d);\\ E(T(k)),E(\alpha T(k));\\ E(a(k)),E(\alpha a(k));\\ E(b(k)),E(\alpha b(k));\\ E(c(k)),E(\alpha c(k));\\ E(\alpha),E(\beta_a\alpha),E(\beta_b\alpha),E(\beta_c\alpha);\\ E(\beta_a a(k)),E(\beta_b b(k)),E(\beta_c c(k));\\ E(\beta_a t(k)),E(\beta_b t(k)),E(\beta_c t(k));\end{cases} \tag{5}$$

步骤二　证明者利用椭圆曲线的同态性质，读取验证者公布在区块链上的参数 CRS 可计算生成 $proofV_i$ 如式(6)：

$$\begin{cases}E(A(k)),E(\alpha A(k));\\ E(B(k)),E(\alpha B(k));\\ E(C(k)),E(\alpha C(k));\\ E(H(k)),E(\alpha H(k));\\ E\left(\beta_a A(k)+\beta_b B(k)+\beta_c C(k)\right);\end{cases} \tag{6}$$

验证 *proof* 阶段：

步骤一　验证者仅根据 $E(A(k)),E(B(k)),E(C(k))$ 是无法确认是由多项式 $A(x),B(x),C(x)$ 的计算生成，利用 $\alpha$ 对的特性，进行多项式盲验证，验证选民的 $proofV_i$ 是由多项式计算生成。以 $A(x)$ 为例，验证式(7)和式(8)运算结果相等，则证明 $E(A(k))$ 和 $E(\alpha A(k))$ 是 $\alpha$ 对，以此类推 $E(B(k))$ 和 $E(\alpha B(k)),E(C(k))$ 和 $E(\alpha C(k)),E(H(k))$ 和 $E(\alpha H(k))$ 是 $\alpha$ 对，由此证明 $A(x),B(x),C(x),H(x)$ 都是多项式形式。

$$e\left(E(A(k)),g^{\alpha}\right)=e\left(g^{A(k)},g^{\alpha}\right)=e(g,g)^{\alpha A(k)} \tag{7}$$

$$e\left(E(\alpha A(k)),g\right)=e\left(g^{\alpha A(k)},g\right)=e(g,g)^{\alpha A(k)} \tag{8}$$

步骤二　整个验证过程中，验证方只随机抽查任意一点 $k$，若验证者无法确认方程(3)是否由 $\boldsymbol{s}$ 生成，同时证明者知道验证者选择的验证点 $k$，那么证明者就可以任意构造满足验证点的方程，而这个方程可以不由向量 $\boldsymbol{s}$ 生成。所以验证过程还需要验证 $A(x),B(x),C(x)$ 是由同一个向量 $\boldsymbol{s}$ 生成，利用多项式特性，只要证明者给出 $A(x),B(x),C(x)$ 的线性组合，则能证明 $A(x),B(x),C(x)$ 从同一组参数 $\boldsymbol{s}$ 生成，验证式(9)和式(10)相等，则证明 $\beta_a A(k)+\beta_b B(k)+\beta_c C(k)$ 为线性组合。

$$\begin{aligned}&e\left(E(\alpha),E\left(\beta_a A(k)+\beta_b B(k)+\beta_c C(k)\right)\right)=\\ &\quad e\left(g^{\alpha},g^{\beta_a A(k)+\beta_b B(k)+\beta_c C(k)}\right)=\\ &\quad e(g,g)^{\alpha\left(\beta_a A(k)+\beta_b B(k)+\beta_c C(k)\right)}\end{aligned} \tag{9}$$

$$\begin{aligned}&e\left(E(\beta_a\alpha),E(A(k))\right)*\\ &\quad e\left(E(\beta_b\alpha),E(B(k))\right)*e\left(E(\beta_c\alpha),E(C(k))\right)=\\ &\quad e\left(g^{\beta_a\alpha},g^{A(k)}\right)*e\left(g^{\beta_b\alpha},g^{B(k)}\right)*e\left(g^{\beta_c\alpha},g^{C(k)}\right)=\\ &\quad e(g,g)^{\beta_a\alpha A(k)}*e(g,g)^{\beta_b\alpha B(k)}*e(g,g)^{\beta_c\alpha C(k)}=\\ &\quad e(g,g)^{\alpha\left(\beta_a A(k)+\beta_b B(k)+\beta_c C(k)\right)}\end{aligned} \tag{10}$$

步骤三　通过步骤一和步骤二保证验证数据的合法性，然后验证式(11)和式(12)若相等，则证明 $A(x)*B(x)=T(x)*H(x)+C(x)$，即证明方程 $A(x)*B(x)-C(x)=T(x)*H(x)$ 成立。

$$e\left(E(A(k)),E(B(k))\right)=e\left(g^{A(k)},g^{B(k)}\right)=e(g,g)^{A(k)B(k)} \tag{11}$$

$$\begin{aligned}&e\left(E(H(k)),E(T(k))\right)*e\left(E(C(k)),g\right)=\\ &\quad e\left(g^{H(k)},g^{T(k)}\right)*e\left(g^{C(k)},g\right)=\\ &\quad e(g,g)^{H(k)T(k)}*e(g,g)^{C(k)}=e(g,g)^{H(k)T(k)+C(k)}\end{aligned} \tag{12}$$

### 2.3　基于 Paillier 算法的选票加密方案

针对既要保证选票信息的隐私保密要求，又要保证选举结果的公众可验证性，通过区块链架构、zk-SNARKs 算法、Paillier 密码体制选票实现选票加密方案。投票阶段，将 Paillier 算法加密的选票和 zk-SNARKs 算法生成选票合法性证明 *proofB* 写入区块链；计票阶段，通过以太坊智能合约实现自动计票，利用 Paillier 算法加法同态性质计算选举结果。算法实行多次加密选票，一次解密选举结果，既提高了计票效率又实现选票隐私保密；利用加法同态比乘法同态和全同态计算效率更高；选举数据写入区块链，任何人都进行验证，满足公众可验证性。

选票表示为$(V_iC_1, V_iC_2, \cdots, V_iC_m)$,$V_iC_j$指的是第$i$位选民投给第$j$位候选人的票数,$V_iC_j \in (0,1)$,$i \in (1,2,\cdots,n)$,$j \in (1,2,\cdots,m)$。初始化选票阶段,数组每一位为0,投票阶段,选择哪位候选者就将对应的那一位置为1。用于选票加密的Paillier算法的公钥为$(g', n')$,私钥为$(\lambda, \mu)$。对选票进行加密,加密后公开发布至区块链,选民选票加密情况如表1所示。

**表1　加密选票**

Tab. 1　Encrypted ballots

| 选民 | 候选人 | | | |
|---|---|---|---|---|
| | $C_1$ | $C_2$ | … | $C_m$ |
| $V_1$ | $E_P(V_1C_1)$ | $E_P(V_1C_2)$ | … | $E_P(V_1C_m)$ |
| $V_2$ | $E_P(V_2C_1)$ | $E_P(V_2C_2)$ | … | $E_P(V_2C_m)$ |
| ⋮ | ⋮ | ⋮ | | ⋮ |
| $V_n$ | $E_P(V_nC_1)$ | $E_P(V_nC_2)$ | … | $E_P(V_nC_m)$ |

则候选人$C_j$的加密票数由Paillier算法加法同态计算得到:

$$E_p(C_j) = E_p(V_1C_j) \times E_p(V_2C_j) \times \cdots \times E_p(V_nC_j) = g^{(V_1C_j + V_2C_j + \cdots + V_nC_j)} \times r^{n*n'} \bmod n'^2 = E_p(V_1C_j + V_2C_j + \cdots + V_nC_j) \tag{13}$$

使用私钥$(\lambda, \mu)$进行解密即可获得候选人$C_j$的总票数:

$$t_j = D_p(E_p(C_j)) = V_1C_j + V_2C_j + \cdots + V_nC_j \tag{14}$$

以此类推可计算出所有候选者的票数$(t_1, t_2, \cdots, t_m)$。

由于选票加密后无法验证选票具体数值,也就无法直接验证选票是否合法(最多只能有一位置为1,其余位全为0),将选票合法性验证问题归约为zk-SNARKs证明。选民需要在不暴露选票$(V_iC_1, V_iC_2, \cdots, V_iC_m)$的情况下证明选票合法,则逻辑算术表达式为$V_iC_1 + V_iC_2 + \cdots + V_iC_m = 0$或$V_iC_1 + V_iC_2 + \cdots + V_iC_m = 1$,转化为算术电路如图2。

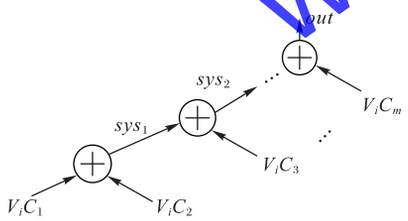


图2　选票合法性证明算术电路

Fig. 2　Arithmetic circuit of proof of ballot legality

若选民没有选择候选人,则电路$out = 0$,否则$out = 1$。两种不同情况对应不同的$out$,该电路可表示为:$one$代表常量变量1,$(V_iC_1, V_iC_2, \cdots, V_iC_m)$代表输入,$sys_1, sys_2, \cdots, sys_v$代表中间门电路的输出,$out$代表整体电路输出。则定义$\boldsymbol{s}$如下:

$$\boldsymbol{s} = [one, V_iC_1, V_iC_2, \cdots, V_iC_m, sys_1, sys_2, \cdots, sys_v, out]$$

后续根据$\boldsymbol{s}$计算每个门电路对应的向量组$(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c})$,转化为向量验证和再转化为QAP多项验证与选民身份证明$\boldsymbol{s}$生成过程相同,最终可生成选票合法性证明。

### 2.4　去中心化电子选举方案流程

整体选举流程如图3所示。

1)选举系统初始化阶段。

选举发起方登录以太坊账号:

初始化选举基础信息:选举名称、选举起止时间等;

初始化用于选票加密的Paillier公私钥:公钥为$(g', n')$,私钥为$(\lambda, \mu)$;

初始化用于选票序列号加密的SM2公私钥:公钥为$P_0$,私钥为$d_0$;

初始化投票智能合约:候选人名单,$C(C_1, C_2, \cdots, C_m)$部署投票智能合约至区块链。

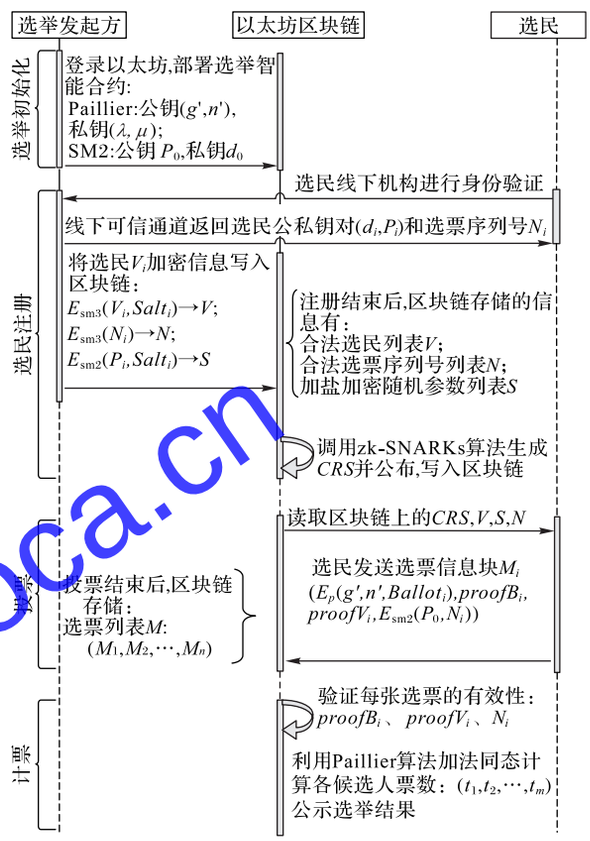


图3　选举流程

Fig. 3　Election flow

2)选民注册阶段。

选民需要在线下官方机构认证是否是此次选举的合法选民。认证通过后,利用物理可信通道为选民进行注册;

生成选民的SM2公私钥对$(d_i, P_i)$,随机生成唯一选票序列号$N_i$;

调用SM3算法,对选民身份信息进行加盐哈希处理,生成$E_{sm3}(V_i, Salt_i)$,调用智能合约存储至区块链合法选民名单$V = (E_{sm3}(V_1, Salt_1), E_{sm3}(V_2, Salt_2), \cdots, E_{sm3}(V_i, Salt_i))$;

调用SM3算法,对选票序列号进行哈希处理$E_{sm3}(N_i)$,调用智能合约存储至区块链合法选票列表$N = (E_{sm3}(N_1), E_{sm3}(N_2), \cdots, E_{sm3}(N_i))$;

调用SM2加密算法对$Salt_i$进行加密处理$E_{sm2}(P_i, Salt_i)$,调用智能合约存储至区块链加盐加密随机参数列表$S = (E_{sm2}(P_1, Salt_1), E_{sm2}(P_2, Salt_2), \cdots, E_{sm2}(P_i, Salt_i))$;

选民自行保管身份信息$V_i$,私钥$d_i$和选票序列号$N_i$。

注册完毕后,区块链上存储的信息为:

$V=(E_{sm3}(V_1,Salt_1),E_{sm3}(V_2,Salt_2),\cdots,E_{sm3}(V_n,Salt_n))$

$N=(E_{sm3}(N_1),E_{sm3}(N_2),\cdots,E_{sm3}(N_n))$

$S=(E_{sm2}(P_1,Salt_1),E_{sm2}(P_2,Salt_2),\cdots,E_{sm2}(P_n,Salt_n))$

调用zk-SNARKs算法生成后续零知识证明需要的公示参数*CRS*,写入区块链公示。

3) 投票阶段。

选民在终端使用以太坊账号登录。

选民读取存储在区块链上的$S$,获取对应的$E_{sm2}(P_i,Salt_i)$,通过SM2解密算法获得处理身份信息的$Salt_i$:$D_{sm2}(d_i,E_{sm2}(P_i,Salt_i))$。

选民调用SM3哈希算法计算得到$E_{sm3}(V_i,Salt_i)$,读取存储在区块链上的选民身份信息集合$V$,调用基于zk-SNARKs选民身份证明算法生成证明字符串$proofV_i$:证明$E_{sm3}(V_i,Salt_i)$属于选民集合$V$。

选民选择对应的候选人$C_j$,然后生成选票$Ballot_i=(V_iC_1,\cdots,V_iC_j,\cdots,V_iC_m)$,如:$(0,\cdots,1,\cdots,0)$;调用基于zk-SNARKs选票合法性证明算法生成$proofB_i$,证明选票合法;调用基于Paillier加密体制的选票加密算法对选票进行加密获得$E_P(g',n',Ballot_i)$;调用SM2加密算法对选票序列号进行加密获得$E_{sm2}(P_0,N_i)$。

选民将选票信息块$M_i$发布至区块链即完成投票环节:$M_i=(E_p(g',n',Ballot_i),proofB_i,proofV_i,E_{sm2}(P_0,N_i))$。

投票结束,所有选票信息块为$M=(M_1,M_2,\cdots,M_n)$。

4) 计票阶段。

整个计票流程写入智能合约,当计票环节开始时,自动调用智能合约进行以下流程:获取区块链上所有选票信息块列表$M$,通过zk-SNARKs验证算法验证每张选票对应证明信息$proofB_i$、$proofV_i$是否合法;通过SM2算法解密$D_{sm2}(d_0,E_{sm2}(P_0,N_i))$获得$N_i$,验证$E_{sm3}(N_i)$是否属于$N$;若两项验证都通过即证明该张选票合法,$N_i$只能使用一次,证明该张选票合法后,对应的$E_{sm3}(N_i)$失效。

利用Paillier算法加法同态性质计算获得候选人$(C_1,C_2,\cdots,C_m)$的票数$(t_1,t_2,\cdots,t_m)$,公布选举结果。

选举结束。

## 3 实验与结果分析

本文采用以太坊Rinkeby测试链作为去中心化数据库,Web端通过Web3j接口与链上智能合约进行交互。实验条件为:64位操作系统Windows10,内存为16 GB,CPU为Intel Core i5-7300HQ 2.5 GHz。实验目的:1)验证该去中心化电子选举方案的可行性;2)测试在不同选举规模下选民身份证明算法效率以及计票效率。实验设定选举参数为5位候选人,分别测试不同选民数量零知识证明*proofV*生成和验证平均耗时,以及选举结果计算耗时(每张选票平均耗时)。实验过程中,选举执行流程按照智能合约的设定执行,实现无需可信第三方计票机构完成计票流程。实验结果表明,随着选举规模的扩大,选民身份证明的生成与验证耗时、选举结果计算耗时增加,该方案适用于小规模选举应用场景。测试结果如图4所示。

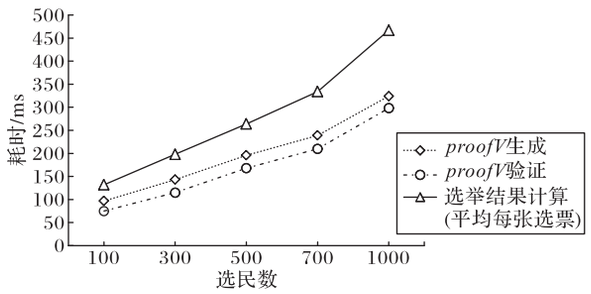


图4 不同选民数量各环节耗时比较

Fig. 4 Time comparison of different stages with differentnumber of voters

匿名性 区块链具有一定匿名性,所有用户都通过以太坊账户地址进行交易,对选民身份进行了第一次隐藏;基于zk-SNARKs实现的身份隐藏算法生成*proofV*对身份信息$V_i$进行二次隐藏。攻击者无法通过写入区块链的身份证明*proofV*追踪具体的选民。选民在不暴露身份信息的情况下实现合法性证明,实现了选举的匿名性。

选票的隐私性 该选举方案中通过Paillier密码体制加密选票,通过zk-SNARKs算法生成选票合法性零知识证明*proofB*,攻击者无法通过*proofB*获取任何信息。且相较于基于乘法同态、全同态选举方案,Paillier算法加法同态计算效率更高。

健壮性 非法选民不能破坏系统的正常运行。测试环节中,针对投票、计票阶段进行攻击测试。构造非法选民$V_h\left(h\notin(1,2,\cdots,n)\right)$写入非法投票信息块$M_h$,计票环节验证非法身份证明$proofV_h$无法通过,非法选票被丢弃。只有合法有效的投票才能被正确地统计。选举数据存储在区块链分布式数据库中,单一节点损坏不影响系统正常运行。

可验证性 整个选举过程的数据都公开写入区块链,任何投票者都可以检验自己的选票是否已经被正确计入,也可以验证区块链上任意一张选票的投票信息块$M_i$的*proofV*、*proofB*的合法性,实现了公开可验证。

## 4 结语

本文针对电子选举主要的两个矛盾点,设计了基于区块链的去中心化安全电子选举方案。通过零知识证明算法zk-SNARKs实现了选民身份隐藏,通过Paillier算法实现了选票信息隐藏,切断了公布的选票信息与每张选票具体持有选民这二者之间的直接联系;通过智能合约实现自动计票,无需可信第三方计票机构。但是实验表明由于零知识证明算法和同态加密算法限制,随着选民规模的扩大,验证与计算的速度降低,仅适用于小规模选举。如何实现去中心化、高效率的大规模选举是今后的研究方向,可以对零知识身份证明算法和同态计算进行进一步研究。

**参考文献** (References)

[1] CERVERÓ M À, MATEU V, MIRET J M, et al. An efficient homomorphic e-voting system over elliptic curves[C]// Proceedings of the 3rd International Conference on Electronic Government and the In-

formation Systems Perspective, LNCS 8650. Cham: Springer, 2014: 41-53.

[2] CHILLOTTI I, GAMA N, GEORGIEVA M, et al. A homomorphic LWE based e-voting scheme[C]// Proceedings of the 7th International Workshop on Post-Quantum Cryptography, LNCS 9606. Cham: Springer, 2016: 245-265.

[3] WILL M A, NICHOLSON B, TIEHUIS M, et al. Secure voting in the cloud using homomorphic encryption and mobile agents [C]// Proceedings of the 2015 International Conference on Cloud Computing Research and Innovation. Piscataway: IEEE, 2015: 173-184.

[4] SCHOENMAKERS B. A simple publicly verifiable secret sharing scheme and its application to electronic voting[C]// Proceedings of the 19th Annual International Cryptology Conference, LNCS 1666. Berlin: Springer, 1999: 148-164.

[5] LIU Y, ZHAO Q. E-voting scheme using secret sharing and *K*-anonymity[J]. World Wide Web, 2019, 22(4): 1657-1667.

[6] FUJIOKA A, OKAMOTO T, OHTA K. A practical secret voting scheme for large scale elections[C]// Proceedings of the 1992 International Workshop on the Theory and Application of Cryptographic Techniques, LNCS 718. Berlin: Springer, 1992: 244-251.

[7] 刘雯,张建中. 一种基于ElGamal签名体制的代理多重盲签名方案[J]. 计算机工程与应用, 2012, 48(10):95-97. (LIU W, ZHANG J Z. Proxy blind multi-signature scheme based on ElGamal signature [J]. Computer Engineering and Applications, 2012, 48(10):95-97.)

[8] LEE B, BOYD C, DAWSON E, et al. Providing receipt-freeness in mixnet-based voting protocols[C]// Proceedings of the 6th International Conference on Information Security and Cryptology, LNCS 2971. Berlin: Springer, 2003: 245-258.

[9] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from bitcoin[C]// Proceedings of the 2014 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2014: 459-474.

[10] 贺海武,延安,陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与发展, 2018, 55(11): 2452-2466. (HE H W, YAN A, CHEN Z H. Survey of smart contract technology and application based on blockchain [J]. Journal of Computer Research and Development, 2018, 55(11): 2452-2466.)

[11] GOLDWASSER S, MICALI S, RACKOFF C. The knowledge complexity of interactive proof systems[J]. SIAM Journal on Computing, 1989, 18(1): 186-208.

[12] DE SANTIS A, PERSIANO G. Zero-knowledge proofs of knowledge without interaction[C]// Proceedings of the 33rd Annual Symposium on Foundations of Computer Science. Piscataway: IEEE, 1992: 427-436.

[13] DE SANTIS A, DI CRESCENZO G, PERSIANO G. Randomness-optimal characterization of two NP proof systems[C]// Proceedings of the 6th International Workshop on Randomization and Approximation Techniques in Computer Science, LNCS 2483. Berlin: Springer, 2002: 179-193.

[14] GALBRAITH S D. Elliptic curve Paillier schemes[J]. Journal of Cryptology, 2002, 15(2): 129-138.

[15] 国家密码管理局. SM2 椭圆曲线公钥密码算法[EB/OL]. [2019-05-22]. http://www.oscca.gov.cn/sca/xxgk/2010-12/17/1002386/files/b791a9f908bb4803875ab6aeeb7b4e03.pdf. (State Cryptography Administration. Public key cryptographic algorithm SM2 based on elliptic curve[EB/OL]. [2019-05-22]. http://www.oscca.gov.cn/sca/xxgk/2010-12/17/1002386/files/b791a9f908bb4803875ab6aeeb7b4e03.pdf.)

[16] 国家密码管理局. SM3 密码杂凑算法[EB/OL]. [2019-05-22]. http://www.oscca.gov.cn/sca/xxgk/2010-12/17/1002389/files/302a3ada057c4a73830536d03e683110.pdf. (State Cryptography Administration. SM3 cryptographic hash algorithm [EB/OL]. [2019-05-22]. http://www.oscca.gov.cn/sca/xxgk/2010-12/17/1002389/files/302a3ada057c4a73830536d03e683110.pdf.)

[17] FUCHSBAUER G. Subversion-zero-knowledge SNARKs[C]// Proceedings of the 21st IACR International Workshop on Public Key Cryptography, LNCS 10769. Cham: Springer, 2018: 315-347.

[18] BEN-SASSON E, CHIESA A, RIABZEV M, et al. Aurora: transparent succinct arguments for R1CS[C]// Proceedings of the 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 11476. Cham: Springer, 2019: 103-128.

[19] ANSTREICHER K, BRIXIUS N, GOUX J P, et al. Solving large quadratic assignment problems on computational grids[J]. Mathematical Programming, 2002, 91(3): 563-588.

[20] BARRETO P S L M, KIM H Y, LYNN B, et al. Efficient algorithm for pairing-based cryptosystems [C]// Proceedings of the 22nd Annual International Cryptology Conference, LNCS 2442. Berlin: Springer, 2002: 354-369.

[21] YAO A C C, YAO F F, ZHAO Y. A note on universal composable zero-knowledge in the common reference string model[J]. Theoretical Computer Science, 2009, 410(11): 1099-1108.

This work is partially supported by the Key Research and Development Program of Sichuan Province (2018GZ0545), the Major Science and Technology Program of Sichuan Province (2019ZDZX0005).

**WU Zhihan**, born in 1994, M. S. candidate. Her research interests include information security, trusted computing, blockchain.

**CUI Zhe**, born in 1970, Ph. D., research fellow. His research interests include trusted computing, information security.

**LIU Ting**, born in 1978, Ph. D. candidate. His research interests include information security, blockchain.

**PU Hongquan**, born in 1990, Ph. D. candidate. His research interests include information security, electronic voting.