计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(2):146−151 [doi: 10.15888/j.cnki.csa.006773]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于同态加密的多候选人电子投票方案①

何　倩, 沈　炜

(浙江理工大学 信息学院, 杭州 310018)
通讯作者: 何　倩, E-mail: yolo_hq@163.com

摘　要: 电子投票因其便捷的特性, 日益受到人们的青睐. 然而电子投票中所暴露出来的安全问题成为人们所关注的重点, 如何保证电子投票中的匿名性, 公开可验证性等成为一个值得关注的问题. 针对现有电子投票中存在的各种问题, 基于数字签名算法和全同态加密提出了一种多候选人电子投票方案. 该方案采用椭圆曲线数字签名算法解决电子投票中的身份认证问题; 利用全同态加密技术实现对选票加密以及对加密选票的同态计算; 为了能够对选票进行批量处理, 采用 SIMD 技术打包选票; 针对加密选票计票中存在的编解码问题设计了一种同态计票器. 最后基于电子投票的八个安全特性对方案的安全性进行了分析, 表明该方案是安全可行的.

关键词: 电子投票; 数字签名; 全同态加密; SIMD; 同态计票器

引用格式: 何倩,沈炜.基于同态加密的多候选人电子投票方案.计算机系统应用,2019,28(2):146–151. http://www.c-s-a.org.cn/1003-3254/6773.html

Multi-Candidate Electronic Voting Scheme Based on Homomorphic Encryption

HE Qian, SHEN Wei

(School of Information Science and Technology, Zhejiang Sci-Tech University, Hangzhou 310018, China)

Abstract: Electronic voting is increasingly popular because of its convenience. However, the security problems exposed in electronic voting have become the focus of attention. How to ensure anonymity and verifiability in electronic voting has become a concern. Aiming at various problems in existing electronic voting, a multi-candidate electronic voting scheme is proposed based on digital signature algorithm and full homomorphic encryption. This scheme uses elliptic curve digital signature algorithm to solve the problem of identity authentication in electronic voting. The homomorphic encryption technology is used to realize the encryption of votes and homomorphism calculation of encrypted votes. To be able to batch votes, SIMD technology is used to packing votes. A homomorphic addition ticket counter was designed for the codec problem of encrypted votes counting. Finally, the security of the scheme is analyzed based on the eight security features of electronic voting, which shows that the scheme is safe and feasible.

Key words: electronic voting; digital signature; full homomorphic encryption; SIMD; homomorphic addition ticket counter

随着计算机和通信技术的发展, 电子投票日益成为当今时代主要的投票方式, 已经逐步取代过去的唱票表决、纸质投票, 它以其自身高效、方便的特性而为人们所普遍接受. 一般来说, 安全的电子投票必须满足以下八个特性: 合法性、匿名性、公正性、完备性、可验证性、正当性、唯一性和无争议性. 当今的电子投票大多数都是建立在密码学基础上的, 大致可以分为以下几种类型: 以 Lee[1]和 Chaum[2]等设计出的方案为代表的混合网模型、以 FOO[3]方案和 Radwin[4]的方案为代表的盲签名模型以及同态加密模型.

① 收稿时间: 2018-08-15; 修改时间: 2018-09-05; 采用时间: 2018-09-18; csa 在线出版时间: 2019-01-28

基于同态加密的方案又根据其选用算法的不同而出现了以下几种方案: 基于 ELGamal[5,6]和 Paillier[7,8]的部分同态加密方案、基于 DGHV[9]的全同态加密电子投票方案. 其中 ELGamal 方案和 Paillier 方案都可以实现多候选人投票, 但是都只能获得最终的获胜者, 不能得到具体每个人的得票数, 而且由于两种算法都是单同态加密, 计算电路深度浅, 不能大规模应用, 实用性不强; DGHV 方案支持多候选人, 其安全性是基于近似 GCD 问题, 但仍未解决无法公开验证等问题, 而且该方案效率较低.

本文基于数字签名算法和全同态加密算法提出一种电子投票方案, 数字签名算法用于保证方案各阶段的公开可验证性, 全同态加密算法用于实现对加密选票的计算, 以此来实现在选票内容保密的情况下计算选票的目的, 实现了电子投票方案的全匿名性以及公开可验证性.

1 预备知识

1.1 数字签名算法

数字签名主要是利用公钥密码学构造的密码体制, 通常包括两个部分: 签名部分和认证部分. 通常使用一对密钥中的私钥进行签名, 公钥进行验签. 本文基于 ECDSA(Elliptic Curve Digital Signature Algorithm, 椭圆曲线数字签名算法) 来实现方案的公开可验证性. ECDSA 是基于 ECC(椭圆曲线加密算法) 和 DSA(数字签名算法) 实现的一种数字签名算法 (图 1), 其安全性是基于椭圆曲线离散对数问题的不可实现性[10].

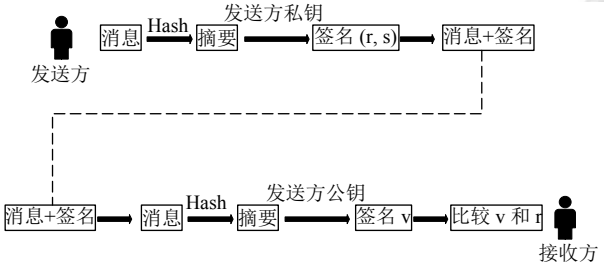

图 1 ECDSA 原理图

1.2 全同态加密算法

全同态加密是一种可以对加密数据进行任意计算的加密技术, 具体来说, 就是在无需解密密钥的情况下, 对密文进行某种操作之后进行解密, 解密结果等于对明文做相同操作的结果. 全同态加密算法的原理图如图 2 所示.

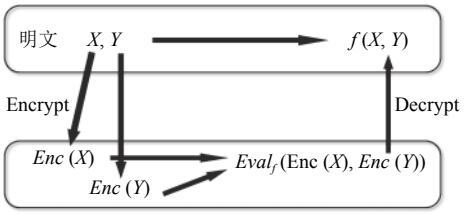

图 2 全同态加密原理图

2009 年 Gentry 构造出了第一个全同态加密方案[11], 随即掀起了全同态研究的热潮, 大量的跟进工作随即出现, 其中具有代表性的全同态加密方案有: 基于整数上的 DGHV 方案[12]、基于 RLWE 的 BGV 方案[13]以及基于近似特征向量的 GSW 方案[14].

本文基于 GSW 方案构造计票方案. GSW 方案的同态加法和同态乘法是基于矩阵上的加法和乘法. 由于原始的 GSW 方案只能对单比特进行加密, 不能很好的适用于大规模投票, 为了对选票进行打包处理, 在 GSW 方案的基础上采用 SIMD (Single-Instruction-MultiPle-Data) 打包技术[15], 通过该技术能够对选票进行打包, 从而实现多比特数据加密. 相较于传统的密文打包技术, 该打包技术可以只对投票人的选票整体进行一次加密, 保留一份私钥, 这在候选人数量较多的情况下, 能够极大地减少加密时间及节省密钥存储空间.

下面对相关知识进行介绍.

1.2.1 LWE 问题

现代密码学的基石是可证明安全, 即密码学体制本身的安全性可以规约到某个困难性假设上, 若该困难性假设是安全的, 则原密码体制安全; 反之则原密码学体制不安全. 自 2005 年, Oded Regev 基于格构造出了 LWE (Learning With Error) 困难性问题[16]以来, 对于 LWE 问题的研究一直是密码学界的一个热点. LWE 问题分为 Decision-LWE 和 Search-LWE 两个版本.

DLWE 问题定义: 安全参数 λ, 参数$n := n(\lambda) \in \mathbf{Z}$, 模$q := q(\lambda) \geqslant 2 \in \mathbf{Z}$, 错误分布$\chi := \chi(\lambda) \in \mathbf{Z}$. $DLWE_{n,q,\chi}$ 问题是区分如下两种分布: 第一种分布, LWE 样本 $(\boldsymbol{a}_i, b_i)$ 是从$\mathbf{Z}_q^n \times \mathbf{Z}_q$ 中随机取样得到; 第二种分布, $\boldsymbol{s} \xleftarrow{U} \mathbf{Z}_q^n$, 样本$(\boldsymbol{a}_i, b_i)$是通过以下方式得到: 均匀采样 $\boldsymbol{a}_i \xleftarrow{U} \mathbf{Z}_q^n, \boldsymbol{e}_i \xleftarrow{R} \chi$, 令$b_i := < \boldsymbol{a}_i, \boldsymbol{s} > + e_i \bmod q$.

1.2.2 RAO-GSW 算法

RAO-GSW 全同态加密算法[15]由五个算法组成, 分别为: Setup、KeyGen、Encrypt、Decrypt 和 Evaluate.

1) Setup(λ): 安全参数λ, 格维$n := n(\lambda) \in \mathbf{Z}$, 模

$q:=q(\lambda)\geqslant 2\in \mathbf{Z}$, 错误分布$\chi:=\chi(\lambda)\in\mathbf{Z}$, 参数$\ell=\lceil\log q\rceil$, $m:=O(n+r)\log q$, $N:=(n+r)\cdot\ell$, 其中r为要加密的比特数, 定义明文空间为$\{0,1\}^{r\times r}$, 密文空间为$\mathbf{Z}_q^{(n+r)\times N}$. $\boldsymbol{g}^{\mathrm{T}}=(1,2,\cdots,2^{\ell-1})$, $\mathbf{G}=\boldsymbol{g}^{\mathrm{T}}\otimes\boldsymbol{I}_{n+r}$, $\otimes$代表张量积.

2) KeyGen($1^\lambda,r$): 随机均匀采样矩阵$\boldsymbol{A}\xleftarrow{U}\mathbf{Z}_q^{n\times m}$, 私钥矩阵$\boldsymbol{S}'\xleftarrow{R}\chi^{r\times n}$, 噪声矩阵, 设$\boldsymbol{E}\xleftarrow{R}\chi^{r\times m}$, 设

$$\boldsymbol{S}:=[\boldsymbol{I}_r\|-\boldsymbol{S}']\in\mathbf{Z}_q^{r\times(n+r)} \tag{1}$$

其中, $\boldsymbol{I}_r$为r阶单位矩阵. 令$\boldsymbol{S}$第i行为$\boldsymbol{s}_i^{\mathrm{T}}$. 设:

$$\boldsymbol{B}:=\begin{pmatrix}\boldsymbol{s}'\boldsymbol{A}+\boldsymbol{E}\\ \boldsymbol{A}\end{pmatrix}\in\mathbf{Z}_q^{(n+r)\times m} \tag{2}$$

使$\boldsymbol{M}_{(i,j)}\in\{0,1\}^{r\times r}(i,j=1,\cdots,r)$是这样一个矩阵: 位置$(i,j)$处为 1, 其余位置全为 0. 对于所有的$i,j=1,\cdots,r$, 样本$\boldsymbol{R}_{(i,j)}\xleftarrow{U}\{0,1\}^{m\times N}$, 并且有如下集合:

$$\boldsymbol{P}_{(i,j)}:=\boldsymbol{B}\boldsymbol{R}_{(i,j)}+\begin{pmatrix}\boldsymbol{M}_{(i,j)}\boldsymbol{S}\\ 0\end{pmatrix}\boldsymbol{G}\in\mathbf{Z}_q^{(n+r)\times N} \tag{3}$$

输出密钥对: 公钥$pk:=\left(\left\{\boldsymbol{P}_{(i,j)}\right\}_{i,j\in[r]},\boldsymbol{B}\right)$, 私钥$sk:=\boldsymbol{S}$.

3) $Enc_{pk}(\boldsymbol{M}\in\{0,1\}^{r\times r})$, 随机均匀采样矩阵$\boldsymbol{R}\xleftarrow{U}\{0,1\}^{m\times N}$, 输出密文如下:

$$\boldsymbol{C}:=\left(\boldsymbol{B}\boldsymbol{R}+\sum\nolimits_{i,j\in[r];M[i,j]=1}\boldsymbol{P}_{(i,j)}\right)\in\mathbf{Z}_q^{(n+r)\times N} \tag{4}$$

4) $Dec_{sk}(\boldsymbol{C})$:

$$\boldsymbol{S}\boldsymbol{C}=\boldsymbol{E}+\boldsymbol{M}\boldsymbol{S}\boldsymbol{G}(\bmod q) \tag{5}$$

则, 根据上式输出明文矩阵

$$\boldsymbol{M}=\left(\left\lceil\left\langle\boldsymbol{s}_i,\boldsymbol{c}_{j\ell-1}\right\rangle\right\rfloor_2\right)_{i,j\in[r]}\in\{0,1\}^{r\times r} \tag{6}$$

5) Evaluate 算法包括两种: 同态加法和同态乘法.

① Add: 设输入两个密文$\boldsymbol{C}_1$和$\boldsymbol{C}_2$, 则有:

$$\boldsymbol{C}_{\mathrm{add}}:=\boldsymbol{C}_1+\boldsymbol{C}_2\in\mathbf{Z}_q^{(n+r)\times N} \tag{7}$$

② Mult: 设输入两个密文$\boldsymbol{C}_1$和$\boldsymbol{C}_2$, 则有:

$$\boldsymbol{C}_{\mathrm{mult}}:=\boldsymbol{C}_1\boldsymbol{G}^{-1}(\boldsymbol{C}_2)\in\mathbf{Z}_q^{(n+r)\times N} \tag{8}$$

6) 方案安全性

循环安全: k是由安全参数λ决定的密钥空间. f是k到c的函数. 一个全同态加密方案$HE=\{KeyGen,Enc,Dec,Eval\}$对于函数$f$是循环安全的[15].

该方案的安全性直接依赖于$DLWE_{n,q,\chi}$以及循环安全. 在目前的技术情况下, DLWE 问题以及循环安全假设都无法在有限的计算资源下被攻破, 故该方案安全.

2 同态计票器

2.1 进位溢出问题

电子投票方案中的计票操作是在正整数$\mathbf{Z}^+$上进行的, 然而, 上述 GSW 方案的明文空间却是$\{0,1\}^{r\times r}$. 为了实现二进制上的加法与乘法和十进制上加法与乘法的对应, 需要设计出一种合理可行的编解码方案, 这样在最终的解密结果中可以得到每个人的具体票数.

$$\mathbf{Z}^+\overset{\text{编解码}}{\longleftrightarrow}\{0,1\}^{r\times r}\overset{\text{RAO-GSW方案}}{\longleftrightarrow}\mathbf{Z}_q^{(n+r)\times N}$$

直观上看, 直接将$\mathbf{Z}$通过进制转换成二进制数$\{0,1\}^r$, 再将$\{0,1\}^r$转变成一个对角矩阵$\{0,1\}^{r\times r}$即可. 然而, 这种方式并不直接适用于本文电子投票中的计票问题.

例如对于两个十进制数$A=\overline{a_3a_2a_1a_0}$, $B=\overline{b_3b_2b_1b_0}$, 其中$a_i,b_i=0,1$, 则有: $C=A+B=\overline{a_3a_2a_1a_0}\oplus\overline{b_3b_2b_1b_0}=\overline{c_3c_2c_1c_0}$, 其中$c_i=a_i\oplus b_i,i=0,1,2,3$, $\oplus$模二加法, 若$a_3=b_3=1$, 则$C=1\overline{c_3c_2c_1c_0}\neq\overline{c_3c_2c_1c_0}$. 其中的 1 是由模二加法运算产生的进位而导致的溢出问题, 极端情况下, 若每一次$c_i=a_i\oplus b_i$都发生一次进位, 则累积到高位a_3和b_3会导致更严重的溢出问题. 若将大量的数相加, 溢出问题将更加严重, 并且计算结果会溢出多次. 因此需要设计出一种能够解决如下问题的计票器: (1) 能够识别何时发生了溢出; (2) 溢出了多少次.

文献[17]中设计了一种半加器, 可以解决单比特加法计票. 但是对于本文打包的多比特选票, 该方法并不适用. 如果直接借用半加器或全加器, 由于进位次数是不可知的, 一旦发生进位就会溢出, 则会导致解码的失败, 不能有效处理该问题. 基于此, 本文借助半加器和全加器的思想设计了一种密文加法器, 以解决进位溢出导致的解码失败问题.

2.2 同态计票器原理与设计

由于全同态加密算法可以对加密数据做任意功能的运算, 运算的结果解密后相当于对明文做同样运算的结果. 因此, 以下以对明文做的运算为例说明该算法, 该算法同样适用于密文计算. 首先以最简单的两个比特的加法为例:

设$a_1,a_2\in\{0,1\}$, 记$\oplus$为模二加法, $\otimes$为模二乘法. 令$s=a_1\oplus a_2$, $c=a_1\otimes a_2$, 则$sum=a_1+a_2=2c+s$.

类似地, 对于n个比特$a_1,a_2,\cdots,a_n$相加, 则可以通过如下方式计算:

$$s=\bigoplus_{i=1}^{n}a_i$$

$$c^{(j)} = s^{(j-1)} \otimes a_j,$$

$$s^{(j)} = \bigoplus_{i=1}^{n} a_i, j = 2,3,\cdots,n$$

最终可得如下结果:

$$sum = a_1 + a_2 + \cdots + a_n = 2\left(\sum_{j=2}^{n} c^{(j)}\right) + s \quad (9)$$

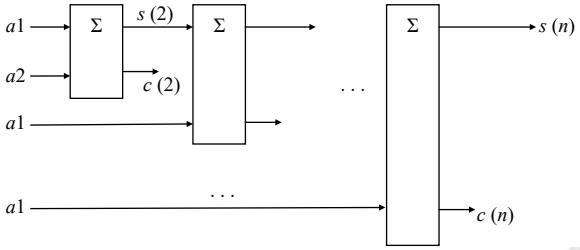

图 3 多比特计票器

为了效率的提升, 使用打包技术, 具体来说, 即将第i个选民的选票重塑为一个矩阵, 该矩阵如下:

$$\boldsymbol{M}_i = \begin{pmatrix} m_1^{(i)} & & & \\ & m_2^{(i)} & & \\ & & \ddots & \\ & & & m_u^{(i)} \end{pmatrix}$$

其中, 下标u表明候选人数目. 对于v个投票人的选票, 通过如下方式统计最终选票:

$$sum = \boldsymbol{M}_1 + \boldsymbol{M}_2 + \cdots + \boldsymbol{M}_v = 2\left(\sum_{j=2}^{v} \boldsymbol{C}^{(j)}\right) + \boldsymbol{S} \quad (10)$$

其中:

$$\boldsymbol{S} = \bigoplus_{i=1}^{v} \boldsymbol{M}_i$$

$$\boldsymbol{C}^{(j)} = \boldsymbol{S}^{(j-1)} \otimes \boldsymbol{M}_{(j)}, j = 2,3,\cdots,v$$

$$\boldsymbol{S}^{(j)} = \bigoplus_{i=1}^{j} \boldsymbol{M}_i$$

其中, $\boldsymbol{C}^{(j)}$表示是否发生了溢出, $\boldsymbol{C}^{(j)}$的总个数表明溢出发生的次数.

3 全同态加密多候选人电子投票方案

3.1 方案描述

在满足电子选举公平性、唯一性、匿名性等八个基本特性的基础上, 本方案根据上述数字签名算法进行身份验证; 采用上述同态加密算法, 对选票进行打包, 同时对加密的选票进行计算, 最后通过解密得到最终投票结果. 方案实体交互图如图 4.

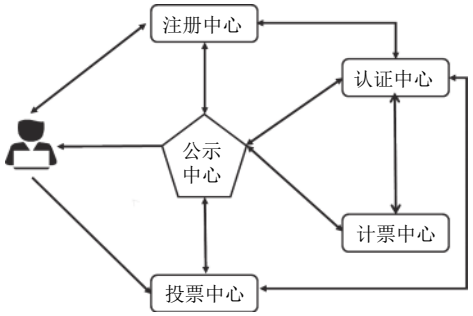

图 4 方案实体交互图

3.2 系统初始化

方案中的实体: 注册中心、投票中心、计票中心使用 ECDSA 签名算法生成签名所需的密钥对, 这些实体用自己生成的公钥请求认证中心 (CA) 生成证书, 认证中心 (CA) 根据业务准则对这些实体的身份进行认证, 确认收到的公钥确实为这些实体本身所有, 认证中心用自己的私钥对实体的公钥施加数字签名并生成证书, 认证中心公布这些实体的数字证书, 数字证书中包含这些实体的身份信息以及自己的公钥.

其中签名所需密钥对的生成过程为: 设 ECDSA 数字签名算法的域参数为$(F_q, E, G, q, a, b, n, h)$, 其中$F_q$是有限域, E是F_q上的椭圆曲线, G是E上的一个有理点, G称为基点, G的阶为q(q为素数), n是G在F_q中规定的序号 (一个质数), a, b是椭圆曲线E的系数, h是一单向安全的哈希函数. 随机从$[1, n-1]$中随机选取一个数d, 计算$Q = dG$. 其中d为私钥, Q为公钥.

签名算法$SIG(M)$:

① 选择一个随机数$k, k \in [1, n-1]$;

② 计算$kG = (x_1, y_1)$;

③ 计算$r = x_1 \bmod n$, 如果$r = 0$, 则跳转到第一步;

④ 计算 $e = H(m)$;

⑤ 计算$s = k^{-1}(e + dr) \bmod n$, 如果$s = 0$, 则跳转到第一步;

⑥ 对消息m的签名为(r, s).

验证算法$VER(r, s)$:

① 检验$r, s \in [1, n-1]$, 若不成立, 返回拒绝签名;

② 计算$e = H(m)$;

③ 计算$u_1 = es^{-1} \bmod n, u_2 = rs^{-1} \bmod n$;

④ 计算$X = u_1 G + u_2 Q = (x_1, y_1)$, 如果$X =$零点, 则验证改签名无效;

⑤ 计算$v = x_1 \bmod n$;

⑥ 如果$v = r$, 则签名有效, 否则签名无效.

各个实体的密钥对如下:

注册中心: $pk_R = Q_R, sk_R = d_R$

投票中心: $pk_V = Q_V, sk_V = d_V$

计票中心: $pk_S = Q_S, sk_S = d_S$

由于投票人的身份信息不需要对外公布, 故投票人采用 ECDSA 算法生成自己的密钥对, 由自己保留, 不需要到认证中心进行认证. 投票人的密钥对为: $pk_O = Q_O, sk_O = d_O$.

此外, 认证中心需要根据描述的同态加密算法中的密钥生成算法以及候选人的数量来生成投票密钥对, 投票密钥对如下: 公钥 $pk := \left(\left\{\boldsymbol{P}_{(i,j)}\right\}_{i,j\in[r]}, \boldsymbol{B}\right)$, 私钥 $sk := \boldsymbol{S}$, 其中 r 为候选人的数量. 认证中心需要以安全的途径将公钥发送给注册中心, 将私钥发送给计票中心.

3.3 注册阶段

投票人需要使用自己的身份材料在注册中心进行注册, 注册中心会根据投票人递交的身份信息验证该投票人是否具有投票权以及是否为首次投票, 一旦验证通过, 则投票中心向该投票人发放与身份信息无关的唯一身份标识 ID_{V_i}、唯一投票标识 B_{V_i}、空白选票以及投票公钥 pk, 并使用自己的私钥对 $ID_{V_i}\|B_{V_i}$ 进行签名发送给投票人.

$$ID_{V_i}\|B_{V_i}\|SIG_R(ID_{V_i}\|B_{V_i})$$

投票人对收到的签名进行验证, 若验证通过, 确实为来自注册中心的合法签名, 则投票人保存 $ID_{V_i}\|B_{V_i}\|SIG_R(ID_{V_i}\|B_{V_i})$. 同时注册中心需要将 $ID_{V_i}\|SIG_R(ID_{V_i}\|B_{V_i})$ 发送到公示中心, 投票人可以到公示中心查看自己是否已经被公布为合法的投票人.

3.4 投票阶段

假设投票人需要对 r 个候选人进行投票, 则一个投票人对多位候选人的投票表示为以下形式, 其中对角线存放的是对每个候选人的投票信息, 赞成即为 1, 反对为 0, 即 $m_i \in \{0,1\}, i = 1,2,\cdots,r$, 则选票的形式如下:

$$\begin{pmatrix} m_1 & & & & \\ & \ddots & & & \\ & & m_i & & \\ & & & \ddots & \\ & & & & m_r \end{pmatrix} \in \{0,1\}^{r\times r}$$

通过以下方式实现对选票的加密:

$$\boldsymbol{C} = \boldsymbol{BR} + \sum_{i,j=[r];M[i,j]=1} \boldsymbol{P}_{(i.j)}$$

投票人用自己的公钥对身份标识 ID_{V_i} 以及投票标识 B_{V_i} 进行签名, 并将身份标识 ID_{V_i}、投票标识 B_{V_i}、自己的签名公钥 pk_O、加密后的选票 $\boldsymbol{C}_i$ 以及签名一同发送到投票中心.

$$ID_{V_i}\|B_{V_i}\|pk_o\|C_i\|SIG_O(ID_{V_i}\|B_{V_i})$$

投票中心收到上述信息后, 首先根据投票人发送的签名信息和公钥验证投票人的签名是否合法, 若合法, 则使用注册中心的公钥验证 $SIG_R(ID_{V_i}\|B_{V_i})$ 中的 $ID_{V_i}\|B_{V_i}$ 是否和 $SIG_O(ID_{V_i}\|B_{V_i})$ 中的 $ID_{V_i}\|B_{V_i}$ 相一致, 若一致, 则可确定该投票人是注册中心认证过的合法投票人; 其次, 再根据 B_{V_i} 验证选票的唯一性, 若通过验证, 则可将选票纳入统计中, 如果没有通过上述任何一项验证, 则丢弃该选票, 不纳入统计. 投票中心将通过验证的选票进行签名发送到公示机构进行公示.

$$S\|C^{(i)}\|SIG_V(ID_{V_i}\|B_{V_i}\|C_i)$$

3.5 计票阶段

待投票截止后, 计票中心从公示中心获得所有选票, 并根据投票中心的公钥验证 $SIG_V(ID_{V_i}\|B_{V_i}\|C_i)$ 的合法性, 若验证通过, 则开始计票, 使用上述构造的同态计票器中的算法对加密选票进行计算得到最终结果 $\boldsymbol{S}, \boldsymbol{C}^{(j)}$. 并对 $\boldsymbol{S}, \boldsymbol{C}^{(j)}$ 进行签名, 将 $\boldsymbol{S}\|\boldsymbol{C}^{(j)}\|SIG_S(\boldsymbol{S}\|\boldsymbol{C}^{(j)})$ 发送到公示中心.

计票中心使用投票私钥对投票结果 $\boldsymbol{S}, \boldsymbol{C}^{(j)}$ 进行解密, 得到最终投票结果, 将该结果发送到公示中心以待监督.

4 安全性分析

(1) 合法性. 在注册阶段每位投票人都会使用自己的身份材料去注册中心进行注册, 注册中心会对投票人的身份信息进行审核, 只有通过审核的投票人才能参与投票.

(2) 匿名性. 首先在投票人通过注册中心的审核后, 注册中心会给投票人发放一个和自己身份信息无关的身份标识, 这样很好的隐藏了投票人的真实身份信息; 其次, 在投票阶段, 投票人利用同态加密方案中的公钥对选票进行加密, 因此, 除了投票人本身, 其他任何人都不能通过加密的选票获得选票的真实内容, 也不能将选票和投票人的身份对应起来.

(3) 唯一性. 首先在注册阶段, 通过注册中心认证的合法投票人会获得唯一投票标识, 因此, 每位投票人只拥有一次投票机会.

(4) 公正性. 在本方案中, 投票私钥由计票中心持有, 计票中心在计算选票之后, 使用该私钥进行解密, 得到最终结果. 由于同态加密算法是对于密文进行计

算, 因此该计算可交给任何一个可信第三方, 因此保证了方案的公正性.

(5) 完备性. 在投票阶段, 投票中心首先会根据注册中心的信息对投票人的身份进行认证, 保证投票人身份合法, 其次会根据投票人的投票编号来检查选票的唯一性, 而且通过使用数字签名技术可以对选票内容的完整性进行验证, 只有全部通过上述认证的选票才会被投票中心正确的统计, 如若有一项没有通过验证, 则会被丢弃, 最终的计票结果只会统计合法选票.

(6) 可验证性. 在投票阶段, 投票中心将收集到的选票公布在了公示中心, 每位投票人都可以根据公告栏上的信息和自己持有的信息进行比对, 以确认自己的选票是否有被正确统计.

(7) 正当性. 方案的每个阶段都会进行身份认证来防止恶意的投票者破坏投票.

(8) 无争议性. 由于本方案是基于 ECDSA 和全同态加密, 因此方案的安全性是可证明的, 方案中的各方的公钥都是公开的, 任何投票人或第三方都可验证方案过程的正确性.

5 结束语

本文基于 ECDSA 数字签名算法和基于 LWE 的同态加密方案提出了一种多候选人电子投票方案. 在该方案中, 利用安全性较高, 密钥长度短的签名算法进行身份认证, 从而提高了认证效率. 而且还使用 SIMD 技术对选票进行打包, 节省了计算成本; 设计了一种同态计票器解决计票中存在的编解码问题; 在计票阶段直接对密文进行计算, 确保了选票的完全保密, 本方案是一个匿名的可公开验证的安全可行的电子投票方案.

参考文献

1 Lee B, Boyd C, Dawson E, *et al*. Providing receipt-freeness in mixnet-based voting protocols. In: Lim JI, Lee DH, eds. Information Security and Cryptology–ICISC 2003. Berlin, Heidelberg: Springer, 2004. 245–258.

2 Chaum D, Ryan PYA, Schneider S. A practical voter-verifiable election scheme. In: De Capitani Di Vimercati S, Syverson P, Gollmann D, eds. Computer Security–ESORICS 2005. Berlin, Heidelberg: Springer, 2005. 118–139.

3 Fujioka A, Okamoto T, Ohta K. A practical secret voting scheme for large scale elections. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology. Queensland, Australia. 1992. 244–251.

4 Radwin MJ. An untraceable, universally verifiable voting scheme. Seminar in Cryptology. 1995. http://www.radwin.org/michael/project/voting.pdf.

5 Kim K, Kim J, Lee B, *et al*. Experimental design of worldwide internet voting system using PKI. SSGRR, 2001.

6 杨婷婷, 林昌露, 张胜元. 安全的多候选人电子投票方案的改进. 福建师大学报 (自然科学版), 2015, 31(3): 32–38.

7 Anggriane SM, Nasution SM, Azmi F. Advanced e-voting system using Paillier homomorphic encryption algorithm. 2016 International Conference on Informatics and Computing. Mataram, Indonesia. 2017. 338–342.

8 黄仕杰, 洪璇. 基于同态实现多候选人的电子投票方案. 计算机应用与软件, 2017, 34(3): 284–288. [doi: 10.3969/j.issn.1000-386x.2017.03.051]

9 朱正阳, 刘镭, 唐春明, 等. 基于 LWE 同态加密的电子投票方案. 信息网络安全, 2013, (5): 8–11. [doi: 10.3969/j.issn.1671-1122.2013.05.003]

10 Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security, 2001, 1(1): 36–63. [doi: 10.1007/s102070100002]

11 Gentry C. Fully homomorphic encryption using ideal lattices. Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing. Bethesda, MD, USA. 2009. 169–178.

12 Van Dijk M, Gentry C, Halevi S, *et al*. Fully homomorphic encryption over the integers. Gilbert H. Advances in Cryptology–EUROCRYPT 2010. Berlin, Heidelberg: Springer, 2010. 24–43.

13 Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. Cambridge, MA, USA. 2012. 309–325.

14 Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. Canetti R, Garay JA. Advances in Cryptology (CRYPTO 2013). Berlin, Heidelberg: Springer, 2013. 75–92.

15 Hiromasa R, Abe M, Okamoto T. Packing messages and optimizing bootstrapping in GSW-FHE. In: Katz J, ed. Public Key Cryptography (PKC 2015). Berlin, Heidelberg: Springer, 2015. 699–715.

16 Regev O. On lattices, learning with errors, random linear codes, and cryptography. Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing. Baltimore, MD, USA. 2005. 84–93.

17 王永恒, 徐晨, 陈经纬, 等. 基于 HElib 的安全电子投票方案. 计算机应用研究, 2017, 34(7): 2167–2171. [doi: 10.3969/j.issn.1001-3695.2017.07.055]