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

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

最终可得如下结果:

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

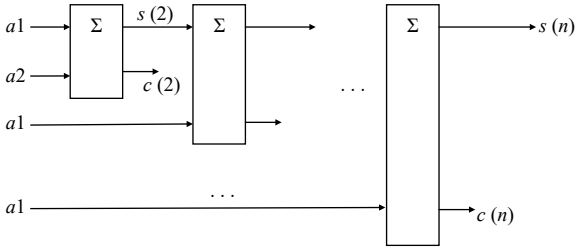

图 3 多比特计票器

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:

$$sum = M_1 + M_2 + \cdots + M_v = 2(\sum_{j=2}^{v} \boldsymbol{C}^{(j)}) + \boldsymbol{S} \tag{10}$$

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.

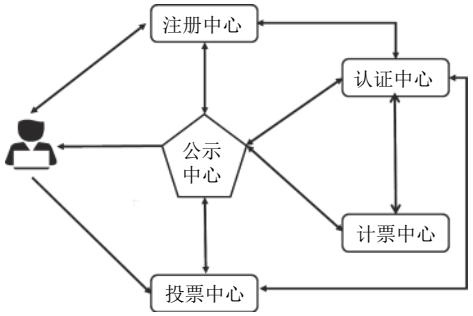

图 4 方案实体交互图

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]