计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(4):386−391 [doi: 10.15888/j.cnki.csa.008421]

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

基于安全多方计算的多候选人电子投票方案①

李亚伟, 王维琼, 谢　琼

(长安大学 理学院, 西安 710064)
通信作者: 王维琼, E-mail: wqwang@chd.edu.cn

摘　要: 多候选人的电子投票方案在很多实际选举场景中有重要的应用价值. 全隐私性是安全电子投票方案关注的一个重要性质, 是指对选民和候选人的隐私保护. 本文基于安全多方计算提出了一个多选多的电子投票方案. 此方案将选民的投票意见映射为数组的形式, 结合 ElGamal 同态加密系统, 在半诚实模型下由选民和候选人通过交互计算输出选举结果, 实现了全隐私性且无需第三方计票机构参与. 此外, 为了避免有争议的选举结果, 本方案首次将反对票数考虑.

关键词: 电子投票; 安全多方计算; ElGamal 加密系统; 全隐私; 隐私保护

引用格式: 李亚伟,王维琼,谢琼.基于安全多方计算的多候选人电子投票方案.计算机系统应用,2022,31(4):386–391. http://www.c-s-a.org.cn/1003-3254/8421.html

Multi-candidate Electronic Voting Scheme Based on Secure Multi-party Computation

LI Ya-Wei, WANG Wei-Qiong, XIE Qiong

(School of Science, Chang'an University, Xi'an 710064, China)

Abstract: Multi-candidate electronic voting schemes play an important role in elections. Full privacy implies privacy protection for both voters and candidates, which is an important property of secure electronic voting schemes. A "*k*-out-of-*m*" electronic voting scheme based on secure multi-party computation is proposed in the study. In the scheme, voters' willingness is mapped into the form of an array. Combined with the ElGamal homomorphic encryption system, the scheme outputs election results through the interactive computing of voters and candidates in a semi-honest model, which achieves full privacy and does not require the participation of a third-party vote-counting agency. Furthermore, the number of dissenting votes is taken into account for the first time in order to avoid controversial election results.

Key words: electronic voting; secure multi-party computation; ElGamal encryption system; full privace; privacy protection

电子投票是基于密码学技术设计并通过网络实现的一种投票方式. 与传统的唱票表决相比, 电子投票的投票和计票过程更高效、选举结果更准确. 随着互联网与密码学技术的发展, 电子投票得到大力发展. 近年来, 电子投票系统在许多西方国家的选举中得到应用, 其中爱沙尼亚首先在国家层面的选举使用电子投票. 目前, 美国、加拿大等地的议会和立法中已开始使用电子投票. 我国部分领域也在尝试使用电子投票, 其中2005 年上海市长宁区某街道进行团支部直选时首次在政治领域使用电子投票.

最早的电子投票方案可追溯到 1981 年, 由 Chaum[1] 基于混合网络和 RSA 公钥加密体制提出. 1992 年, Fujilka 等人[2] 基于盲签名提出了可适用于大规模选举的 FOO 方案, 使电子投票走向实用. 1997 年, Cramer 等人[3] 首次提出了多候选人的电子投票问题, 并利用 ElGamal 加密系统设计了一个多选一的电子选举方案,

① 基金项目: 国家自然科学基金 (11901049); 陕西省自然科学基础研究计划 (2020JQ-343); 陕西省高校科协青年人才托举计划 (20200505)
收稿时间: 2021-06-05; 修改时间: 2021-07-07, 2021-07-23; 采用时间: 2021-08-12; csa 在线出版时间: 2022-03-22

该方案需要可信的计票中心参与接收并统计选票. 2001 年, Damgård 等人[4] 基于 Paillier 加密系统提出了一个多选多的电子投票方案, 该方案无法避免重复投票现象且需要可信计票机构参与. 2006 年, 仲红等人[5] 基于安全多方求和提出一个无需第三方计票机构参与的多选多电子投票方案, 但选举结束后会公开所有候选人的得票数. 2012 年, Pang 等人[6] 基于混合网络和 PET 协议提出一个多选多电子选举方案. 2015 年, 杨婷婷等人[7] 基于安全多方排序协议设计了一个多选多电子投票方案, 但方案使用的排序协议要求参与者两两之间有安全信道, 对通信环境要求较高. 2018 年, 娄宇等人[8] 基于全同态加密算法提出一个多候选人的电子投票方案, 其计票工作由第三方计票中心完成且公开所有候选人得票数. 2019 年, 刘霆等人[9] 将随机线性分组码的秘密分享应用于多候选人电子投票方案中, 解决了防投票记录篡改、关键信息存储的安全性等问题. 同年, 付伟伟等人[10] 基于随机矩阵提出一个多选一电子投票方案, 该方案满足可验证性, 但需要计票中心参与. 2021 年, 邵清等人[11] 基于 ElGamal 强盲签名和区块链技术提出了电子投票方案, 此方案没有明确选举场景、选票形式等, 重点关注选票的可验证性、不可篡改性等问题, 且用智能合约取代可信第三方完成计票. 文献 [12–16] 等结合区块链、同态加密等技术提出了完整的安全电子投票系统.

保密选票内容是安全电子投票方案的一个基本要求. 但在计票阶段, 候选者得票数同样属于关键信息. 因为破坏者可能根据候选人之间得票数的差异, 在下次选举时通过拉拢选票的手段, 破坏选举的公平性. 因此, 文献 [6] 首次提出了投票方案中“全隐私”的概念, 是指既保护选民选票内容又保护候选人得票数. 上述文献 [6,7] 提出的方案保护了落选者得票数.

为保密选票内容, 可以用加密技术对选票信息进行加密. 同时为方便后续计票, 加密后的信息需要满足一定的同态性质. 而同态加密[17] 满足上述需求, 能够在不解密密文的前提下, 通过对密文的操作实现对相应明文的计算. 姚期智[18] 提出的安全多方计算主要解决互不信任的数据拥有者之间的安全协同计算问题, 基于此思想设计电子投票方案可解决计票时第三方机构参与的问题.

尽我们所知, 已有的电子投票方案仅统计候选人的赞成票数. 然而在实际的选举场景中, 时常会遇到以下情况: 某些候选人赞成票数名列前茅, 但选民对其反对声音也很高. 例如, 在有 50 位合法选民的选举活动中, 有两位候选人得票情况如表 1. 根据已有的电子投票方案候选人 2 获胜, 但是候选人 1 当选更能反映选民的意愿.

表 1 可能的得票情况

得票情况	赞成票数	反对票数
候选人1	27	2
候选人2	28	22

为了避免上述有争议的选举结果出现, 本文在综合考虑候选人赞成票数和反对票数的前提下, 基于安全多方计算, 结合 ElGamal 同态加密系统提出一个无需第三方计票机构参与、全隐私的多选多电子投票方案.

1 预备知识

1.1 半诚实模型及其安全性定义

本文在半诚实模型下考虑方案的安全性. 半诚实参与者是指参与者会忠实执行协议, 但他们会利用收到的中间信息试图推断其他参与者的输入.

设 n 个参与者P_i $(i=1,2,\cdots,n)$分别持有私密信息 X_i, 记$X=\{X_1,X_2,\cdots,X_n\}$. 他们利用协议π合作计算函数 $f(X)=(f_1(X),\cdots,f_n(X))$, 计算结束后$P_i$收到$f_i(X)$. 协议 π执行过程中, 记$P_i(i=1,2,\cdots,n)$的视图为$VIEW_i^{\pi}(X)$. 对于部分参与者$\tau=\left(P_{i_1},P_{i_2},\cdots,P_{i_s}\right)\subset(P_1,P_2,\cdots,P_n)$, 记:

$$VIEW_{\tau}^{\pi}(X)=\left(\tau,VIEW_{i_1}^{\pi}(X),\cdots,VIEW_{i_s}^{\pi}(X)\right) \quad (1)$$

定义 1 (半诚实模型下协议的安全性[19]). 当参与者都是半诚实参与者时, 若存在概率多项式时间算法 S, 使得对于任意的τ, 都有式 (2) 成立,

$$\left\{S\left(\tau,X_{i_1},X_{i_2},\cdots,X_{i_s},f_{\tau}(X)\right)\right\}\overset{c}{\equiv}\{VIEW_{\tau}^{\pi}(X)\} \quad (2)$$

则称协议π保密地计算了函数$f(X)$, 其中符号$\overset{c}{\equiv}$表示计算上不可区分.

1.2 ElGamal 加密系统

ElGamal 加密系统[20] 是一种具有乘法同态性的公钥加密系统, 本文将使用文献 [21] 中构造的具有加法同态性的门限 ElGamal 加密系统, 描述如下:

(1) 密钥生成算法

对给定安全参数 k, 系统生成一个 k 比特的大素数 p 和循环群Z_p^*的一个生成元 g. 每个P_i $(i=1,2,\cdots,n)$

选取随机数x_i作为其持有的私钥份额, 公布$h_i = g^{x_i} \bmod p$, 则公钥为$h = \prod_{i=1}^{n} h_i = g^{\sum_{i=1}^{n} x_i} \bmod p$.

(2) 加密算法 E

对于消息$M\left(M \in Z_p^*\right)$, 选取随机数 r, 密文为: $E(M) = (c_1, c_2) = \left(g^r \bmod p, g^M h^r \bmod p\right)$.

(3) 解密算法 D

对于密文$E(M) = (c_1, c_2)$, $P_i(i = 1,2,\cdots,n)$计算$w_i = c_1^{x_i} \bmod p$并公布, 所有参与者共同解密得:

$$g^M = c_2 \cdot \left[\prod_{i=1}^{n} w_i\right]^{-1} \bmod p \tag{3}$$

与 ElGamal 加密系统类似, 该加密系统具有语义安全性. 需要注意的是此加密系统不具有完全解密性, 解密算法仅可得明文 M 的幂值g^M.

1.3 *IsEq* 协议

Kissner 等人[22] 研究隐私集合运算时提出了 *IsEq* 协议. 根据此协议, 对于用同一公钥加密所得的密文C_1和C_2, 若C_1和C_2是同一明文的密文, 则$IsEq(C_1, C_2) = 1$; 否则, $IsEq(C_1, C_2) = 0$.

2 多选多电子投票方案的设计

2.1 投票场景

本文假设有 n 位选民和 m 位候选人取得了合法身份标识$P_1, P_2, \cdots, P_n$和$C_1, C_2, \cdots, C_m$, 有资格进入投票系统参与投票和计票. 选民将从 m 位候选人中选出 k 位获胜者. 本方案规定每位获胜者的反对票数均不能超过阈值 t. 记所有的获胜候选人构成集合 W.

2.2 表决方式

选民$P_i(i = 1,2,\cdots,n)$对候选人$C_j(j = 1,2,\cdots,m)$进行表决得一个三元数组$\left(v_{i,3j-2}, v_{i,3j-1}, v_{i,3j}\right)$, 其 3 个分量分别对应赞成、反对和弃权 3 种表决意见. 若选民的表决意见为赞成, 则对应数组为(1,0,0); 若选民的表决意见是反对或弃权, 其对应数组为(0,1,0)或(0,0,1). P_i $(i = 1,2,\cdots,n)$对每位候选人依次表决完毕后, 得到数组$V_i = (v_{i,1}, v_{i,2}, \cdots, v_{i,3m})$, V_i为P_i表决后的选票.

2.3 投票方案

本文设计的投票方案分为初始化阶段、投票阶段和计票阶段, 具体过程如下:

2.3.1 初始化阶段

基于门限 ElGamal 加密系统生成大素数p和循环群Z_p^*的生成元g. 选民$P_1, P_2, \cdots, P_n$和候选人$C_1, C_2, \cdots, C_m$分别选取$x_i(i = 1,2,\cdots,n+m)$作为其持有的私钥份额, 计算$h_i = g^{x_i} \bmod p$并公开. 所有选民和候选人计算公钥$h = \prod_{i=1}^{n+m} h_i = g^{\sum_{i=1}^{n+m} x_i} \bmod p$. 每位候选人$C_j$ $(j = 1,2,\cdots,m)$选取随机数r_j, 计算密文$E_s = E(s) = (g^{r_j} \bmod p, g^s h^{r_j} \bmod p)$ $(s = 1,2,\cdots,n)$, 并保存E_s以备在计票阶段使用.

2.3.2 投票阶段

选民$P_i(i = 1,2,\cdots,n)$依据第 2.2 节所述方式表决得选票$V_i = (v_{i,1}, v_{i,2}, \cdots, v_{i,3m})$. 接着, $P_i(i = 1,2,\cdots,n)$利用门限 ElGamal 加密系统加密选票V_i的每个分量得加密选票$B_i = (E(v_{i,1}), E(v_{i,2}), \cdots, E(v_{i,3m}))$, 其中$E\left(v_{i,j}\right) = (g^{r_{i,j}} \bmod p, g^{v_{i,j}} \cdot h^{r_{i,j}} \bmod p)$, $r_{i,j}$为P_i加密时选取的随机数, 并将加密选票B_i发送给每位候选人.

2.3.3 计票阶段

计票阶段由所有选民P_i $(i = 1,2,\cdots,n)$和候选人C_j $(j = 1,2,\cdots,m)$通过交互计算完成, 过程如下.

(1) 每个候选人C_j $(j = 1,2,\cdots,m)$执行如下计算:

① 将所有加密选票B_i的第$3j-2$列和$3j-1$列中元素求积得:

$$w_j = \prod_{i=1}^{n} E\left(v_{i,3j-2}\right), s_j = \prod_{i=1}^{n} E\left(v_{i,3j-1}\right) \tag{4}$$

② 计算密文:

$$L_j = E\left(IsEq\left(s_j, E_0\right) + \cdots + IsEq\left(s_j, E_t\right)\right) \tag{5}$$

③ 选取 n 个随机数$q_{ji}(i = 1,2,\cdots,n)$, 计算密文数组:

$$U_j = \left(u_{j1}, u_{j2}, \cdots, u_{jn}\right) \tag{6}$$

其中, $u_{ji} = E\left(IsEq\left(w_j, E_i\right) \cdot IsEq\left(L_j, E_1\right)\right)$.

(2) C_1将$Z_1 = U_1$发给C_2. 对于每个$j = 2,3,\cdots,m$, 候选人C_j收到C_{j-1}发来的Z_{j-1}后, 执行以下操作:

① C_j 计算$Z_j = U_j \cdot Z_{j-1}$, 其中$U_j \cdot Z_{j-1}$由U_j和Z_{j-1}对应分量相乘得到.

② C_j将Z_j发送给$C_{j+1 \bmod m}$.

③ C_1最后收到密文数组

$$Z_m = U_1 \cdot U_2 \cdot \cdots \cdot U_m = (z_1, z_2, \cdots, z_n) \tag{7}$$

并公开.

(3) 候选人$C_j(j = 1,2,\cdots,m)$从$i = n$至$i = 1$依次计算$IsEq(z_n \cdot z_{n-1} \cdots z_i, E_k)$, 直到找出 q 使式 (8) 成立,

$$IsEq\left(z_n \cdot z_{n-1} \cdot \cdots \cdot z_q, E_k\right) = 1 \tag{8}$$

停止计算.

(4) 所有人从$i=n$至$i=q$共同解密z_i. 每位候选人将满足条件$D(z_i)\neq 1$的 i 保存至集合 X, 记集合$X=\{x_1, x_2,\cdots,x_e\}(1\leqslant e\leqslant k)$.

(5) 候选人$C_j(j=1,2,\cdots,m)$计算:

$$Y_j=E\left(\sum_{u=1}^{e} IsEq\left(E_0\cdot w_j^{IsEq(L_j,E_1)},E(x_u)\right)\right) \quad (9)$$

并公开.

(6) 所有人共同解密Y_j $(j=1,2,\cdots,m)$, 若$D\left(Y_j\right)\neq 1$, 则$C_j\in W$, 最后输出集合 W.

3 方案分析与比较

3.1 正确性分析

定理 1. 本方案的选举结果是正确的, 即对选民$P_i(i=1,2,\cdots,n)$的选票V_i, 方案能够输出集合 W.

证明: 投票阶段将其加密选票B_i发送给每位候选人. 计票阶段, 所有选民和候选人利用B_i进行交互计算, 输出选举结果, 其具体分析如下:

第 1 步. 首先, 由门限 ElGamal 加密系统的加法同态性, 式 (4) 中$w_j=\prod_{i=1}^{n}E\left(v_{i,3j-2}\right)=E\left(\sum_{i=1}^{n}v_{i,3j-2}\right)$, 同理$s_j=E\left(\sum_{i=1}^{n}v_{i,3j-1}\right)$, 其中$\sum_{i=1}^{n}v_{i,3j-2},\sum_{i=1}^{n}v_{i,3j-1}$分别为$C_j$所得赞成票数和反对票数. 其次, 根据式 (5) 当$\sum_{i=1}^{n}v_{i,3j-1}>t$时, $L_j=E(0)$, 此时根据式 (6), 密文数组U_j的分量$u_{ji}(i=1,2,\cdots,n)$全为密文$E(0)$; 当$\sum_{i=1}^{n}v_{i,3j-1}\leqslant t$时, $L_j=E(1)$, 密文数组U_j的某一个分量u_{ji}为密文$E(1)$, 其余的均为密文$E(0)$, 且若分量$u_{ji}=E(1)$, 表示候选人C_j的赞成票数为i.

第 2 步. 候选人交互计算得到式 (7), 其中$z_i=\prod_{j=1}^{n}u_{ji}(i=1,2,\cdots,n)$. 由式 (6) 中$u_{ji}$的计算公式知$z_i=\left(g^{\sum_{j=1}^{m}q_{ji}} \bmod p, g^{\sum_{j=1}^{m}IsEq\left(w_j,E_i\right)\cdot IsEq\left(L_j,E_1\right)}_h{}^{\sum_{j=1}^{n}q_{ji}} \bmod p\right)$若记$k_i=\sum_{j=1}^{m}IsEq\left(w_j,E_i\right)\cdot IsEq\left(L_j,E_1\right)$, 则得赞成票数为$i$的候选人有$k_i$位.

第 3 步. 由于找到的q使得式 (8) 成立, 根据门限 ElGamal 加密系统的加法同态性及协议 $IsEq$ 协议可知$k_n+k_{n-1}+\cdots+k_q=k$. 进一步, 可知获胜的赞成票数为集合$\{q,q+1,\cdots,n\}$中的元素.

第 4 步. 由本文使用的门限 ElGamal 加密系统的不完全解密性可知, i满足$D(z_i)\neq 1$当且仅当$k_i\neq 0$, 因此, 候选人所得集合X由所有获胜的赞成票数构成.

第 5 步. 对于式 (9) 得到的密文Y_j, 根据门限 ElGamal 加密系统的加法同态性, 若候选人C_j的反对票数没有超过阈值 t 且赞成票数与某个获胜票数相等时, $Y_j=E(1)$; 否则$Y_j=E(0)$. 再由此加密系统的不完全解密性可知, 当$D\left(Y_j\right)\neq 1$时, 候选人C_j获胜.

第 6 步. 结束时所有获胜候选人将被输出.

综上所述, 该方案的选举结果是正确的.

3.2 全隐私性分析

全隐私性[10] 是指在整个选举过程中, 所有选民的选票信息和候选者的得票数均是隐私的.

定理 2. 在半诚实模型下, 本方案满足对所有选民选票信息的隐私保护.

证明: 由于任意 n–1 位选民和所有的候选者合谋, 可以产生最大程度的攻击. 因此, 在此合谋结构下, 证明方案满足对所有选民投票信息的隐私保护即可. 此处用模拟范例[19] 的方法证明. 由于每位选民的地位是平等的, 不妨设选民$P_1,P_2,\cdots,P_{n-1}$和所有候选者$C_1,C_2,\cdots,C_m$合谋获得P_n的选票V_n, 记合谋者构成的集合为$\tau=\{P_1,\cdots,P_{n-1},C_1,\cdots,C_m\}$. 对于$\tau$中的参与者, 需构造相应的模拟器 S 使式 (10) 成立.

$$\{S(V_1,V_2,\cdots,V_{n-1},W)\}\overset{c}{\equiv}\{VIEW_{\tau}^{\pi}(V_1,V_2,\cdots,V_n)\} \quad (10)$$

S 构造门限 ElGamal 加密系统, 其主私钥为x', 对应的公钥为h'. 用此加密系统的公钥计算密文$E'_s=E'(s)=(g^r \bmod p, g^s h'^r \bmod p)(s=1,2,\cdots,n)$, S 接收输入$\{V_1,V_2,\cdots,V_{n-1},W\}$, 按如下方式运行:

(1) S构造一个数组$V_n'=\left(v'_{n,1},v'_{n,2},\cdots,v'_{n,3m}\right)$, 使得$\pi(V_1,V_2,\cdots,V_{n-1},V_n')=W$.

(2) S利用数组$V_1,V_2,\cdots,V_{n-1},V_n'$模拟投票阶段, 计算得到加密选票$B_1,B_2,\cdots,B_{n-1},B'_n$, 其中$B_{n'}=(E(v_{n,1'}),E(v_{n,2'}),\cdots,E(v_{n,3m'}))$.

(3) S利用$B_1,B_2,\cdots,B_{n-1},B'_n$模拟计票阶段. 执行第 1 步得$\left\{w'_j,s'_j,L'_j,q'_{ji},U'_j\right\}$, 其中$j=1,2,\cdots,m$, $i=1,2,\cdots,n$, w'_j和s'_j为密文, q'_{ji}为随机数, U'_j为密文数组. 执行第 2 步得密文数组$Z'_m=\left(z'_1,z'_2,\cdots,z'_n\right)$. 进一步, S按照第 3、4 步计算得q'和集合$X'=\left\{x'_1,x'_2,\cdots,x'_e\right\}$ $(1\leq e\leq k)$. 继续执行第 5、6 步, 计算得密文Y'_j, 解密Y'_j并输出W'. 综上, S在模拟过程中得到的信息序列为:

$$\{S(V_1,V_2,\cdots,V_{n-1},W)\}=\left\{V_1,V_2,\cdots,V_{n-1},w'_j,s'_j,q'_{ji},L'_j,U'_j,Z_m',q',X',Y'_j,W'\right\} \quad (11)$$

其中, $j=1,2,\cdots,m$, $i=1,2,\cdots,n$, $W'=\pi(V_1,\cdots,V_{n-1},V_n')$.

而在整个方案执行过程中:

$$VIEW_\tau^\pi\{V_1,V_2,\cdots,V_n\}=\left\{V_1,V_2,\cdots,V_{n-1},w_j,s_j,q_{ji},L_j,U_j,Z_m,q,X,Y_j,W\right\} \quad (12)$$

其中, $j=1,2,\cdots,m$, $i=1,2,\cdots,n$.

由于门限 ElGamal 加密系统具有语义安性, 因此, 对于τ中所有参与者而言有:

$$\left\{w_j',s_j',L_j',U_j',Z_m',Y_j'\right\}\overset{c}{\equiv}\left\{w_j,s_j,L_j,U_j,Z_m,Y_j\right\}$$

其中, $j=1,2,\cdots,m$. 因为随机数计算不可区分, 则$r_{j,i}'\overset{c}{\equiv}r_{j,i}$, 其中$j=1,2,\cdots,m$, $i=1,2,\cdots,n$. 根据q'和集合X', τ中所有参与者不能推断出选民P_n的隐私信息V_n, 且$W'=\pi(V_1,V_2,\cdots,V_{n-1},V_n')=W$, 因此式 (13) 成立.

$$\{S(V_1,V_2,\cdots,V_{n-1},W)\}\overset{c}{\equiv}\{VIEW_\tau^\pi(V_1,V_2,\cdots,V_n)\} \quad (13)$$

定理 2 得证, 即本方案满足对选民选票信息的隐私保护.

由于本方案仅输出获胜候选人的名单, 且即使在计票阶段每位候选人保存了获胜候选者对应的获胜票数, 但其无法将票数与候选人对应起来, 则方案满足对获胜者得票数的隐私保护. 同时, 由于门限 ElGamal 加密系统的特性, 任何人都无法解密式 (4) 中的w_j,s_j, 因此无法得到落选者的得票数, 即方案满足对落选者得票数的隐私保护.

综上, 本方案满足全隐私性, 并且保护了所有落选者的得票数.

3.3 其它安全性质分析

(1) 无收据性是指任何选民都无法向他人证明自己的选票. 本方案中每位选民将加密选票发送给所有候选人, 由于门限 ElGamal 加密系统的特性, 选民靠自己不能解密任何密文, 则无法向候选人证明自己的选票.

(2) 公平性是指所有选民同时得到选举结果. 该方案的选举结果在计票阶段结束之后输出, 任何人都无法提前获知选举结果. 因此, 本方案满足公平性.

3.4 复杂性分析与比较

本文设计的方案使用了门限 ElGamal 加密系统, 分析时只考虑费时的模指数运算, 每次加密操作需要 2 次模指数运算, 每次解密操作需要$n+m+1$次模指数运算.

投票阶段, 所有选民需要$3nm$次加密. 计票阶段, 所有选民和候选人最多执行$m(n+2+k)$次加密和$m+k$次解密. 因此投票阶段和阶段最多需要模指数运算$2[3nm+m(n+2+k)]+(m+k)(n+m+1)$次. 计票阶段, 最多需要调用$m(3n+2k+t+1)$次 IsEq 协议, 根据文献 [23], 本文执行 IsEq 协议所需模指数运算复杂度$\mathrm{O}(n^2m)$. 综上所述, 本方案的计算复杂度为$\mathrm{O}(n^2m)$.

将本文设计的方案与文献 [6,7] 中提出的全隐私多候选人电子投票方案进行对比, 如表 2 所示. 本方案考虑了候选者所得反对票数, 且其全隐私性实现了对所有候选者得票数的保护.

表 2 全隐私电子投票方案的对比

方案的性质	全隐私性			是否考虑反对票数的影响	是否需要安全信道	计算复杂度
	选民	获胜者	落选者			
文献[6]	√	×	√	×	×	$\mathrm{O}(kn^2m)$
文献[7]	√	×	√	×	√	$\mathrm{O}(km^3)$
本方案	√	√	√	√	×	$\mathrm{O}(n^2m)$

4 结语

为使选举结果更符合选民的意愿, 本文首次考虑了候选人反对票数. 在此基础上提出了一个满足全隐私性、无需第三方参与的多选多电子投票方案, 并且本方案的全隐形实现了对所有候选人得票数的保护. 此外, 分析表明方案同时满足公平性和无收据性. 下一步工作将研究符合实际应用场景需求、满足更多安全性质且高效的电子投票方案.

参考文献

1 Chaum DL. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 1981, 24(2): 84–90. [doi: 10.1145/358549.358563]

2 Fujioka A, Okamoto T, Ohta K. A practical secret voting scheme for large scale elections. Workshop on the Theory and Application of Cryptographic Techniques. Gold Coast: Springer, 1993. 244–251.

3 Cramer R, Gennaro R, Schoenmakers B. A secure and optimally efficient multi-authority election scheme. International Conference on the Theory and Applications of Cryptographic Techniques. Konstanz: Springer, 1997. 103–118.

4 Damgård I, Jurik M. A generalisation, a simplification and some applications of Paillier's probabilistic public-key system. 4th International Workshop on Public Key Cryptography. Cheju Island: Springer, 2001. 119–136.

5 仲红, 黄刘生, 罗永龙. 基于安全多方求和的多候选人电子选举方案. 计算机研究与发展, 2006, 43(8): 1405–1410.

6 Pang L, Sun MH, Luo SS, *et al*. Full privacy preserving electronic voting scheme. The Journal of China Universities of Posts and Telecommunications, 2012, 19(4): 86–93. [doi: 10.1016/S1005-8885(11)60287-2]

7 杨婷婷, 林昌露, 刘忆宁, 等. 基于多方排序协议的安全电子投票方案. 计算机系统应用, 2015, 24(8): 25–32. [doi: 10.3969/j.issn.1003-3254.2015.08.005]

8 娄宇, 朱更明. RLWE 同态加密算法的多候选人电子投票协议. 计算机工程与科学, 2018, 40(3): 472–480. [doi: 10.3969/j.issn.1007-130X.2018.03.012]

9 刘霆, 崔喆, 蒲泓全, 等. 基于随机线性分组码的秘密分享在电子投票中的应用. 工程科学与技术, 2019, 51(6): 175–181.

10 付伟伟, 王晓京, 彭行一, 等. 基于随机矩阵的一种新型电子投票方案. 计算机应用, 2019, 39(S2): 280–283.

11 邵清, 洪皓洁, 李斌. 基于 Elgamal 强盲签名的区块链电子投票方案研究. 小型微型计算机系统, 2021: 1–8. [doi: 10.3969/j.issn.1000-1220.2021.01.001]

12 Gupta SP, Tripathi AM. E-voting using blockchain. Journal of Physics: Conference Series, 2021, 1911: 012001. [doi: 10.1088/1742-6596/1911/1/012001]

13 张育衔. 基于区块链的匿名投票系统研究 [硕士学位论文]. 北京: 北京邮电大学, 2020.

14 吴昊天. 高效可验证电子选举系统的研究与设计 [硕士学位论文]. 西安: 西安电子科技大学, 2020.

15 Choi S, Kang JH, Chung KS. Design of blockchain based e-voting system for vote requirements. Journal of Physics: Conference Series, 2021, 1944: 012002. [doi: 10.1088/1742-6596/1944/1/012002]

16 Geetha SK, Sathya S, Sakthi ST. A secure digital e-voting using blockchain technology. Journal of Physics: Conference Series, 2021, 1916 012197.

17 Rivest RL, Adleman L, Dertouzos ML. On data banks and privacy homomorphisms. Foundations of Secure Computation. New York: Academic, 1978. 169–179.

18 Yao AC. Protocols for secure computations. 23rd Annual Symposium on Foundations of Computer Science. Washington: IEEE, 1982. 160–164.

19 Goldreich O. Foundations of Cryptography: Volume II Basic Applications. London: Cambridge University Press, 2004. 599–764.

20 Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 1985, 31(4): 469–472. [doi: 10.1109/TIT.1985.1057074]

21 窦家维, 刘旭红, 周素芳, 等. 高效的集合安全多方计算协议及应用. 计算机学报, 2018, 41(8): 1844–1860. [doi: 10.11897/SP.J.1016.2018.01844]

22 Kissner L, Song D. Privacy-preserving set operations. 25th Annual International Cryptology Conference on Advances in Cryptology. Santa Barbara: Springer, 2005. 241–257.

23 Kissner L, Oprea A, Reiter MK, *et al*. Private keyword-based push and pull with applications to anonymous communication. Second International Conference on Applied Cryptography and Network Security. Yellow Mountain: Springer, 2004. 16–30.