基于多方排序协议的安全电子投票方案①

杨婷婷[1], 林昌露[1], 刘忆宁[2], 张胜元[1]

[1](福建师范大学 数学与计算机科学学院, 福州 350007)
[2](桂林电子科技大学 数学与计算科学学院, 桂林 541004)

摘 要: 与传统投票相比较, 电子投票拥有许多优势, 也存在重要的安全问题. 电子投票的全隐私性是评估投票方案安全的重要指标, 它是指对投票者的隐私保护和候选者的隐私保护, 特别是落选者的得票数的保护. 利用可验证秘密共享的思想提出了一个安全多方排序协议, 并将它运用到电子投票中, 设计了一个新的安全的电子投票协议, 本协议具有全隐私性.

关键词: 电子投票; 多方排序; 可验证秘密共享; 全隐私

Secure Electronic Voting Scheme Based on Multi-party Ranking

YANG Ting-Ting[1], LIN Chang-Lu[1], LIU Yi-Ning[2], ZHANG Sheng-Yuan[1]

[1](College of Electronic Science and Technology, Fujian Normal Univrsiety, Fuzhou 350007, China)
[2](School of Electronic Science and Technology, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: Compared with the traditional voting, electronic voting(e-voting) not only has many advantages, but also exists many security problems. The full privacy of electronic voting is an important index to evaluate the security of the voting scheme, it implies the privacy of the voters and candidates for privacy protection, especially the protection of total votes for the losers. This paper designs a secure multi-party ranking protocol via using the verifiable secret sharing. We propose a new secure electronic voting scheme based on the proposed multi-party ranking protocol. The e-voting scheme is full privacy.

Key words: electronic voting; multi-party ranking; verifiable secret sharing; full privacy

电子投票是密码学在现实生活中的一个重要应用, 它是以各种密码学技术为理论基础, 通过计算机以及相应网络来完成整个投票过程. 传统投票, 需要大量的人力、物力, 且效率低、统计票数耗时、检票繁琐. 电子投票能很好的弥补传统投票的这些缺陷, 它立足互联网络, 能突破时间空间限制, 在投票期间实现远程投票. 随着互联网和现代密码技术的发展, 电子投票得到了大力发展, 例如 Brace[1]在研究美国国家选举投票方式分类的报告中指出, 2000 年到 2008 年使用电子投票的郡从 320 个增加到 1068 个, 使用电子投票的投票者的比例从 12.4%增加到 32.6%.

电子投票协议作为电子投票的核心, 是电子投票能否走向实现的关键. 自电子投票协议的概念被提出以来, 国内外许多学者对此展开了深入研究, 提出许多电子投票协议. 1981 年, Chaum[2]基于混合网与 RSA 公钥体制提出了第一个电子投票协议. 1992 年, Fujioka、Okatnoto 和 Ohta[3]提出著名的 FOO 投票协议. 该协议是一个真正满足电子投票中的基本安全要求的大规模选举方案, 并使电子投票走向实用. 1997 年, Cramer 等人[4]第一次提出了多候选人选举问题, 设计了一个多选一的多候选人方案, 但方案只能处理“是/否”选票类型, 不能进行多选多选举, 不适合大规模选举. 2001 年, Damgard 等人[5]利用 Paillier 加密方案的同态性提出一个多选多的选举方案, 计算复杂度较高. 2006 年, 仲红等人[6]基于安全多方求和协议, 设计了一个多选多的无计票中心的投票协议, 除了获胜者之

① 基金项目:国家自然科学基金(61103247, 61363069);广西自然科学基金(2014GXNSFAA118364)
收稿时间:2014-10-28;收到修改稿时间:2014-12-25

外的其他人的票数也要公开, 无法实现落选者选票的隐私性. 2013 年, Yi 和 Okamoto[7]提出了基于同态加密的面向应用的网络电子投票协议. 同年, Rui 等人[8]提出一个端到端可验证的网络电子投票协议 EVIV. 2014 年, Rabin 和 Rivest[9]利用分裂值表示和随机部分检查设计了一个实际的端到端可验证投票协议.

电子投票在实际应用中暴露出许多安全问题. 因此, 电子投票不仅需要满足现实投票的要求外, 还要考虑电子投票特殊环境下的安全要求. 1992 年, Fujioka 等人[3]提出电子投票应该满足以下几个特性: (1)秘密性, (2)隐私性, (3)公平性, (4)唯一性, (5)完整性, (6)合法性, (7)可验证性. 1994 年, Benaloh 和 Tuinstra[10]首次提出投票协议的无收据性. 2005 年, Jules 与 Jakobsson[11]提出了投票协议抗胁迫性概念.

隐私性是投票的一个基本安全要求. 传统投票方式中, 以无记名投票的方式实现, 有利于投票者消除顾虑, 能够完全按照自己的意志行使投票权, 很好地维持了投票的公平性. 因此, 投票者隐私性的实现是评估一个电子投票方案安全性的重要指标. 2012 年, Pang 等人[12]提出了一个基于混合网以及 PET 协议的具有全隐私的电子投票协议, 该协议关注安全特性中的隐私保护问题. 投票协议的隐私性包括两方面内容: 选票内容的保密、选票和投票者之间关系的隐私. 但在计票阶段中, 候选者的得票数同样属于敏感信息, 破坏者根据候选者之间的得票数差异, 在下次投票时利用各种手段拉拢选票, 破坏选举的公平性. 因此, Pang 等人提出了电子投票中“全隐私”的概念, 既保护投票者的隐私(投票意愿不被泄露)又保护候选者的隐私(落选者的得票数不被泄露). 该方案利用混合网隐藏投票结果, 并利用 PET 协议来计票, 投票结束后只有获胜者的得票数及身份被揭示, 并提供能够公开验证的方法及票数证明.

安全多方排序协议又叫安全多方数据比较协议, 源于 Yao[13]在 1982 年提出的百万富翁问题. 安全多方排序协议是对百万富翁问题的扩展, 是指一群参与者分别拥有各自的数据, 在不泄漏自己数据的前提下, 知道自己数据的排名. 百万富翁问题提出以来, 许多学者提出了自己的解决方案, 在此基础上也出现了许多多方排序协议, 如 2001 年, Fischlin[14]基于 GM 加密方案设计了一个秘密比较协议; 2007 年, 刘文等人[15]基于 EIGamal 加密方案提出了安全多方多数据排序协议; 2011 年, 唐春明等人[16]利用秘密共享方案构造了一个有效的安全多方排序协议.

本文首先分析了“黄-仲”多方排序协议的安全问题, 从而基于可验证秘密共享设计了一个安全多方排序协议, 解决了原始方案可能存在主动敌手攻击的问题. 并应用此多方排序协议提出了一个满足全隐私性的电子投票方案. 与 Pang 等人的投票协议相比, 本文提出的方案的计票以及得到最终的结果不需要投票者的参与, 投票者投完票即可离开, 不需要参与之后的计票, 计票由候选者自行完成.

本文的内容安排如下: 下一节介绍了本文需要的一些基础知识. 第三节描述本文提出的多方排序协议及其安全分析. 第四节将给出新的安全电子投票方案. 第五节对所设计的电子投票方案进行安全分析第六节对电子投票方案进行复杂性分析及比较. 最后一节对本文做了总结.

1 预备知识

本节介绍下文将使用到的两个基本知识: 可验证秘密共享及“黄-仲”多方排序协议.

1.1 可验证秘密共享

1992 年, Pedersen[17]提出了可验证秘密共享方案. 在该方案中, 收到子秘钥的一方能验证所收到秘密的正确性, 即可验证与其他子秘钥是否保持一致.

设 q 是大素数, Z_q 是模 q 剩余类, g 是 Z_q 的一个生成元, 分发者(D)取 $h \in Z_q$, 且除了 D 外无人知道离散对数值 $\log_g h$, 要分发主秘密 $s \in Z_q$, n 个接收者 $P_1,...,P_n$, 有一个广播渠道, 且与每个 P_i 之间存在一个秘密通道, D 方案步骤如下:

(1) D 对 s 承诺: $E_0 = E(F_0, G_0) = E(s,t)$, t 是在 Z_q 中随机选的; 并选择多项式 $F(x) \in Z_q[x]$ 且指数不超过 $k-1$, 满足 $F(0) = s$.

$$F(x) = s + F_1 x + \cdots + F_{k-1} x^{k-1},$$

且计算 $s_i = F(i) \pmod q$, $i = 1,2,...,n$.

随机选择 $G_1,...,G_{k-1} \in Z_q$, 用 G_i 来承诺 F_i, 其中 $i = 1,2,...,k-1$.

$$G(x) = t + G_1 x + \cdots + G_{k-1} x^{k-1},$$

且计算 $t_i = G(i) \pmod q$, $i = 1,2,...,n$.

分发者广播 $E_i = E(F_i, G_i)(i = 1,2,...,k-1)$, 并秘密地发送 (s_i, t_i) 给 n 个接收者 P_i, 其中 $i = 1,2,...,n$.

(2) 当 P_i 接收到他的子秘钥 (s_i, t_i), 进行下面的

验证,

$$E(s_i,t_i)=\prod_{j=0}^{k-1}E_j^{i^j}=g^{\Sigma_{j=0}^{k-1}F_j i^j}h^{\Sigma_{j=0}^{k-1}G_j i^j}\left(\mathrm{mod}\,q\right).$$

验证通过, 即说明共享值正确, 则 P_i 接受 s_i; 验证不通过, 即说明共享值错误, 则 P_i 要求 D 重发, 直到验证通过.

这里的承诺按如下方式:

设 g,h 是 Z_q 中的元素, 且没人知道离散对数值 $\log_g h$, 这些元素可被可信第三方或者系统初始化生成. 这样要加密某个秘密 $s\in Z_q$ 时, 随机选 $s\in Z_q$, 计算承诺值为:

$$E(s,t)=g^s h^t\left(\mathrm{mod}\,q\right).$$

1.2 “黄-仲”多方排序协议

保护私有信息的多方排序有着很强的应用背景. 比如, 一个班级的考试成绩排名问题. 对于保护私有信息的多方排序问题的研究目前比较少, 2010 年, 黄宏升和仲红[18]提出了保护私有信息的多方排序协议(简称“黄-仲”协议), 该协议在半诚实模型条件下解决了保护私有信息的多方排序问题, 计算代价较小. 协议具体描述如下:

n 个参与方: $P_1,P_2,...,P_n$ 和第三方: C.

假设条件: 存在两两之间安全通信信道, 参与方都是半诚实的, 即各方正确遵守协议, 他们可以保留协议执行的中间结果来试图推导其他参与者的输入, 但不可以退出或恶意掺入虚假数据.

协议开始前 n 个参与方 P_i 都有自己的秘密数据 $m_i\left(i=1,2,...,n\right)$, 并且参与方秘密协商一个置换 π, C 不知道这个置换. n 个参与方与 C, 协商好是按升序(或是降序)排序. 协议执行如下:

(1) 参与方 P_i 产生 n 个随机数 $r_{ij}\in Z_q(j=1,2,...,n)$ 来隐藏自己的数据 $m_i(i=1,2,...,n)$, 计算

$$M_i=R_i\oplus(0,0,...,m_i,...,0),$$

其中 m_i 在 n 维向量 $(0,0,...,m_i,...,0)$ 的第 i 个数据位上, $R_i=(r_{i1},r_{i2},..,r_{ii},...,r_{in})$.

P_i 将置换后的 M_i, 即 $\pi(M_i)$ 发送给 C.

(2) C 收到每个参与方 P_i 发送来的数据后, 对所有 $\pi(M_i)$ 进行 $\oplus$ 运算得:

$$M=\pi(M_1)\oplus\cdots\oplus\pi(M_i)\oplus\cdots\oplus\pi(M_n).$$

(3) 每个参与方 P_i 对自己的 R_i 进行置换 π, 得 $\pi(R_i)$ 之后将其发给 P_n, 且 P_n 计算

$$R=\pi(R_1)\oplus\cdots\oplus\pi(R_i)\oplus\cdots\oplus\pi(R_n).$$

(4) C 收到 R 后, 进行运算得:

$$result=M\oplus R=(m_{\pi(1)},...,m_{\pi(i)},...,m_{\pi(n)}),$$

C 对所得到的 $result$ 进行排序, 将排序后的结果

$$result'=(m_{\pi(1)'},m_{\pi(2)'},...,m_{\pi(n)'}),$$

广播给 n 个参与方 P_i.

(5) 每个参与方 P_i 都可以通过查找结果 $result'$, 得知自己私有数据在这 n 个数据中的位置(排名).

注: 该协议是在半诚实模型下进行的, 且需要第 n 个参与方 P_n 做随机数的收集、计算与转发.

2 改进的多方排序协议

在“黄-仲”协议中, 参与者 $P_i\left(i=1,2,...,n-1\right)$ 都要把随机数的置换发给 P_n, 在半诚实模型的假设下, P_n 不会作假. 但此要求过高, 实际上 P_n 存在作假的可能, 即无法抵抗主动敌手攻击. 针对此点, 引入可验证秘密共享. 每个 $P_i\left(i=1,2,...,n\right)$ 对自己的随机数进行可验证共享, 再对所有收到的随机数的共享求和后发送给 C, 这样 C 不能恢复出每个 P_i 的随机数, 且无需 P_n 作随机数的汇总.

2.1 协议描述

改进后的多方排序协议具体描述如下:

n 个参与方 P_i 的秘密数据为 $m_i(i=1,2,...,n)$, 他们之间秘密协商一个置换 P_i, 第三方 C 不知道这个置换. 参与方与 C, 协商好是升序(或是降序)排序.

假设条件: 存在两两之间安全通信信道, 参与方部分是半诚实的, 即他们正确遵守协议, 保留协议执行的中间结果来试图推导其他参与者的输入, 但不可以退出或恶意掺入虚假数据. 部分被主动的攻击敌手收买, 被完全控制, 这些收买者会不忠的执行协议.

(1) 参与方 P_i 产生 n 个随机数 $r_{ij}(j=1,2,...,n)$ 用来隐藏自己的数据 $m_i(i=1,2,...,n)$, 计算

$$M_i=R_i\oplus(0,0,...,m_i,...,0),$$

其中 m_i 在 n 维向量 $(0,0,...,m_i,...,0)$ 的第 i 个数据位上, $R_i=(r_{i1},r_{i2},...,r_{ii},...,r_{in})$, 这里的加法是按位加.

P_i 将置换后的 m_i, 即 $\pi(M_i)$ 发送给 C.

(2) n 个参与方 P_i 对自己的 R_i 进行置换 π 运算得 $\pi(R_i)$, 并计算 B_i, B_i 为 R_i 所对应的十进制数. 例如数组 $(3,2,1,1)$ 对应十进制数 3211. 每个参与方 P_i 选择 $F_{i1},...,F_{in}$, 并令 $B_i=F_{i0}$, 得到多项式:

$$F_i(x)=F_{i0}+F_{i1}x+\cdots+F_{in}x^n,$$

选择 $G_{i0},G_{i1},...,G_{in}$, 得到多项式:

$$G_i(x)=G_{i0}+G_{i1}x+\cdots+G_{in}x^n,$$

公布承诺值 $E_i(F_{ij},G_{ij})$，其中 $j=0,1,...,n$，计算 $(F_i(j),G_i(j))$ 并秘密地发送给 $P_j(j=1,...,i-1,i+1,...,n)$.

(3) P_j 对收到的 $(F_i(j),G_i(j))$ 利用公布的 $E_i(F_{ij},G_{ij})$，$j=0,1,...,n$ 进行如下验证:

$$E(F_i(j),G_i(j))=\prod_{k=0}^{n}E_i^{j^k}=g^{\Sigma_{k=0}^{n}F_{ik}j^k}h^{\Sigma_{k=0}^{n}G_{ik}j^k},$$

验证不通过要求分发者重发; 验证通过后做如下计算:

$$f_i=F_1(i)+\cdots+F_i(i)+\cdots+F_n(i),$$

并将 f_i 发送给 C.

(4) C 收到每个参与方 P_i 发送来的数据后，对每个 $\pi(M_i)$ 进行按位加运算得:

$$M=\pi(M_1)+\cdots+\pi(M_i)+\cdots+\pi(M_n).$$

再用收到的 f_i 进行 Lagrange 插值算法，运算如下:

$$f=\Sigma_{i=1}^{n}\frac{\Pi_{j=1,j\neq i}^{n}(-j)}{\Pi_{j=1,j\neq i}^{n}(i-j)}f_i,$$

并将 f 转化回数组 $R=(r_1,r_2,..,r_i,...,r_n)$，$M$ 与 R 按位减，运算得:

$$result=M-R=(m_{\pi(1)},...,m_{\pi(i)},...,m_{\pi(n)}).$$

C 对所得到的 *result* 进行排序，将排序后的结果

$$result'=(m_{\pi(1)'},m_{\pi(2)'},...,m_{\pi(n)'}),$$

广播给 n 个参与方 P_i，其中 $i=1,2,...,n$.

(5) 每个参与方 P_i 都可以通过查找结果 $result'$，得知自己私有数据在这 n 个数据中的位置(排名).

2.2 协议分析

本协议沿用了原协议的使用随机数隐藏数据的思想，从而隐藏了数据与参与方之间的关系，有效的保护了参与方的数据隐私. 由第三方完成对匿名数据的排序并广播给每个参与方，协议结束后，每个参与方 $P_i(i=1,2,...,n)$ 只知道自己的位置(排名)，而不知道其他参与方的位置，有效的保护了参与方排名的隐私. 下面将具体的分析协议的安全性.

定理 1. 在主动敌手攻击下，本协议是一个安全的多方排序协议.

证明: 为了证明本协议是安全的，下面将从正确性和秘密性两个方面说明.

正确性: 首先，证明参与方 $P_i(i=1,2,...,n)$ 的数据 $m_i(i=1,2,...,n)$ 能够被第三方 C 正确接收. 协议第一步参与者 $P_i(i=1,2,...,n)$ 用随机数组 $R_i=(r_{i1},r_{i2},...,r_{ii},...,r_{in})$ 来隐藏自己的数据 $m_i(i=1,2,...,n)$，可得数组 $M_i=(r_{i1},r_{i2},...,r_{ii}+m_i,...,r_{in})$，置换后将数组发送给 C，这样 C 就获得了包含 m_i 的数组 $\pi(M_i)$，下面只需要随机数组能被 C 正确接收即可. 第二步参与者对自己的随机数组 $R_i=(r_{i1},r_{i2},...,r_{ii},...,r_{in})$ 进行上步同样的置换，并转化为十进制数 B_i，利用可验证秘钥共享协议将 B_i 共享出去. 第三步每个收到分享的参与者 $P_j(j=1,2,...,n)$ 对分享 $(F_i(j),G_i(j))$，通过分享者公开的参数 $E(F_i(j),G_i(j))(j=0,...,n)$，验证 $E(F_i(j),G_i(j))=\prod_{j=0}^{n}E_i^{i^j}$ 是否成立就可验证其所收到的分享的正确性，保证了随机数共享的正确性. 验证不通过可要求重发，验证通过后每个 P_i 把自己收到的所有随机数共享按位加得 f_i 并发送给 C. 第四步第三方 C 由 $f_i(i=1,2,...,n)$ 利用 Lagrange 插值算法可算出所有随机数的和 f 转化会数组的形式，这样 C 就正确接收到了随机数. C 再对所有 M_i 按位加，最后与随机数组按位减，即可得到所有需要排序的数据，这里按位减刚好把隐藏数据的随机数去掉，所以能得到正确的数据. 其次，证明数据被正确排序. 在不知道置换的情况下，第三方不能将数据与对应的参与方联系上，只能正确的给出排序.

秘密性: 参与方 $P_i(i=1,2,...,n)$ 的数据 $m_i(i=1,2,...,n)$ 被第三方 C 接收时是经过了随机数的隐藏与置换，所以第三方 C 在不知道随机数与置换的情况下，得到数组 $M_i=(r_{i1},r_{i2},...,r_{ii}+m_i,...,r_{in})$ 也不能确定 m_i 的值，从而保护了数据的秘密性. 对于随机数，C 得到的是所有随机数的按位加，不能得到每个参与方对应的随机数，最后去除随机数是所有数据同时去除，从而保证了数据的秘密性.

3 安全的电子投票方案

本节将第 2 节设计的多方排序协议应用到电子投票中，构造了一种新的多选多安全电子投票方案. 由于多方排序协议的使用，使得本协议满足全隐私性.

3.1 安全假设与方案组成

假设: 投票者都愿意按照投票要求进行正确投票，且所投票合理. 胁迫者不知道候选者的密钥，从而不能得知投票者的投票内容. 本假设是合理的，因为候选者如果把自己的密钥告诉他人，可能会泄露自己某些信息.

方案由以下五部分实体组成:

① 投票者: 具有投票资格, 投票开始前需身份认证.

② 候选者: 投票开始前需生成自己的公、私钥对, 投票后自行统计自己的票, 最后参与多方排序协议.

③ 注册中心: 对投票者的身份进行认证, 给投票者数字证书用以投票, 实现投票者匿名.

④ 公告板: 投票者可以把选票公布, 且不能被篡改; 候选者可通过公告板上的票进行计算选票.

⑤ 第三方: 最后参与多方排序, 可以是除了候选者的任何人担任, 因为多方排序中票数与候选者的关系是被隐藏的.

3.2 方案描述

该投票方案是属于多选多候选人的类型, 它包括三个步骤: 初始化、投票阶段及计票阶段. 投票流程如图 1, 具体描述如下:

(1) 初始化

n 个投票者 $P_1,P_2,...,P_n$ 投票, 要求在不泄露投票者意愿与落选者得票数的情况下, 在 m 个候选者 $C_1,C_2,...,C_m$ 中选出 k 个获胜者.

系统生成参数 g. 候选者产生自己的 ElGamal 公钥加密的私/公钥对 (x_i,y_i), 其中 $y_i=g^{x_i}\pmod p$, $i=1,2,...,m$, 注册中心产生自己的 ElGamal 公钥加密的私/公钥对 (x_c,y_c), 其中 $y_c=g^{x_c}\pmod p$, 下文的加密均采用 ElGamal 加密体制. 投票者在注册中心注册(见图 1, ①), 得到数字证书 $C(P_i)=(ID_i,Sig(ID_i))$ (见图 1, ②), 并发送至公告板, 其中 ID_i 为身份标识, $Sig(ID_i)$ 为注册中心对用户身份的数字签名. 建立一张 T^k 与 k 的对应关系表, 如通过 2^k 表, 1024 对应是 10, 其中 $T=2$, $k=10$.

(2) 投票阶段

每个投票者 P_i 产生投票向量 $V_i=(v_{i1},v_{i2},...,v_{im})i=1,2,\ldots,n$, 其中 v_{ij} 代对于候选者 C_j 的意愿:

$$v_{ij}=\begin{cases}T & \text{赞成;}\\ 1 & \text{反对。}\end{cases}\quad j=1,2,...,m。$$

这里, T 可为除 1 的任意数值, 弃权票等同于反对票, 默认为 1.

对于投票结果向量 $V_i=(v_{i1},v_{i2},...,,v_{im})i=1,2,\ldots,n$, 中的第 j 列用 C_j 的公钥 y_j 以及注册中的公钥 y_c 加密, 并发送至公告板(见图 1, ③):

$$e(V_i)=(E_{y_1y_c}(v_{i1}),E_{y_2y_c}(v_{i2}),...,E_{y_my_c}(v_{im}))$$
$$=((g^{k_{i1}}\pmod p),v_{i1}(y_1y_c)^{k_{i1}}\pmod p),...)。$$

注: k_{ij} 为加密时所选的随机数.

(3) 计票阶段

投票阶段结束时, 注册中心计算 $(\Pi_{i=1}^n g^{k_{ij}}\pmod p)^{x_c}$ 并发送给对应的第 j 个候选者 C_j (见图 1, ④⑤), 每个候选者 $C_j(j=1,2,...,m)$ 对公告板投票结果的第 j 列求积得 $\Pi_{i=1}^n E_{y_j}(v_{ij})$ (见图 1, ④), 用自己的私钥 x_j 解密以及注册中心发来的信息解密, 即

$$D(\Pi_{i=1}^n E_{y_jy_c}(v_{ij}))$$
$$=\frac{y^{\Sigma_{i=1}^n r^{ij}}\Pi_{i=1}^n v_{ij}}{(\Pi_{i=1}^n g^{k_{ij}}\pmod p)^{x_c}(g^{\Sigma_{i=1}^n k^{ij}})^{x_j}}\pmod p$$
$$=\Pi_{i=1}^n v_{ij}\pmod p=T^k,$$

得 $T_j=T^k$, 再通过投票前建立的 T^k 与 k 之间建立的对应表, 即可知道自己的得票数 k, 这里的得票数是赞成票-反对票的净得票数.

当所有候选者都得知自己的票数后, 再与第三方执行第 3 节所设计的多方排序协议(见图 1, ⑥), 第三方返回排序结果(见图 1, ⑦), 候选者得到票数高低的排名. 排名前 k 位候选者即可宣布自己获胜, 并解密出自己的选票来证明.

表 1 公告板上的票

投票者 ID	C_1	…	C_m
ID_i	$E_{y_1y_c}(v_{11})$	…	$E_{y_my_c}(v_{1m})$
⋮	⋮	⋮	⋮
ID_i	$E_{y_1y_c}(v_{n1})$	…	$E_{y_my_c}(v_{nm})$

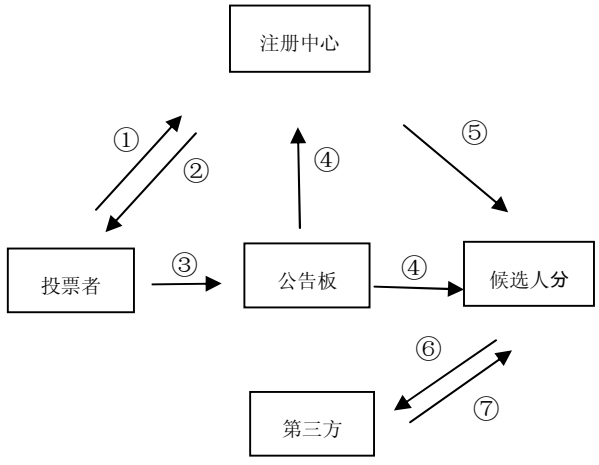

图 1 投票流程

例如, 有 4 个候选者选 2 人获胜, 他们的得票分别是 5、7、3、4, 他们在知道自己票数后, 和第三方 C 执行多方排序协议, 前两人知道自己的得票数分别排第一和第二, 就公开宣布获胜, 并解出自己对应列的选票证明自己获胜. 后两人知道自己的得票数比获胜者的低, 就知道落选, 这样保护了落选者的隐私.

4 安全性分析

本节将对所提出的电子投票方案的安全性进行详细分析.

(1) 正确性

计票时, 第 j 个候选者拿出公告板中第 j 列, 由 ElGamal 加密的同态性, 计算

$$\Pi_{i=1}^{n}E_{y_jy_c}(v_{ij})=(g^{\Sigma_{i=1}^{n}r^{ij}},y^{\Sigma_{i=1}^{n}k^{ij}}),$$

再拿出自己的私钥 x_j 以及注册中心发来的信息 $(\Pi_{i=1}^{n}g^{k_{ij}}\pmod p)^{x_c}$ 秘密地解密:

$$\begin{aligned}&D(\Pi_{i=1}^{n}E_{y_jy_c}(v_{ij}))\\&=\frac{y^{\Sigma_{i=1}^{n}r^{ij}}\Pi_{i=1}^{n}v_{ij}}{(\Pi_{i=1}^{n}g^{k_{ij}}\pmod p)^{x_c}(g^{\Sigma_{i=1}^{n}k^{ij}})^{x_j}}\pmod p\\&=\Pi_{i=1}^{n}v_{ij}\pmod p=T^k,\end{aligned}$$

故所有候选者执行完此步, 可得知自己票数, 再与第三方进行多方排序协议, 得到票数的排序, 排名前 k 个宣布获胜, 并解密自己的选票进行证明.

(2) 全隐私性

定理 2. 若本方案所使用的多方排序就是安全的, 则本方案满足全隐私性.

证明: 投票时, 投票者 $P_i(i=1,2,...,n)$ 发送用候选者及注册中心的公钥共同加密后的选票 $\mathrm{e}(\mathrm{V}_i)$ 到公告板, 身份认证是用数字证书 $C(P_i)=(ID_i,Sig(ID_i))$, 候选者不能把数字证书与投票者联系上, 即保护了投票者的隐私. 即使候选者能把数字证书与投票者联系上, 但由于加密时利用了注册中心的公钥, 使得候选者不能单独解密投票者的选票, 保证了选票内容的隐私性. 计票时, 候选者在计票中心的帮助下才能解密出自己得票列积, 且此时注册中心提供的信息 $(\Pi_{i=1}^{n}g^{k_{ij}}\pmod p)^{x_c}$ 不能帮助候选者解密单张选票, 没有破坏选票内容的隐私性. 候选者得知自己的得票数后, 与第三方进行多方排序协议, 由定理 1 多方排序的安全性知只要第三方不知道置乱数据所用的置换, 数据与候选者的对应关系就得到保护, 从而保护到了落选候选者的得票数的隐私. 因此, 方案一方面保护投票者的隐私, 一方面保护了候选者的隐私, 满足全隐私性.

(3) 秘密性

方案中 $P_i(i=1,2,...,n)$ 的选票通过加密得到数组 $e(V_i)=\left(E_{y_1y_c}(v_{i1}),E_{y_2y_c}(v_{i2}),\ldots,E_{y_my_c}(v_{im})\right)$ 之后再发送到公告板, 除投票者外, 选票内容不被他人所知. 候选者即使能将投票者与投票者的 ID 对应, 但在不知道注册中心私钥的情况下, 不能解密选票, 即不能获得投票者的选票内容. 候选者在计票时, 由注册中心提供的信息 $(\Pi_{i=1}^{n}g^{k_{ij}}\pmod p)^{x_c}$ 也不能解密单张选票, 无法获得选票内容. 因此, 满足秘密性.

(4) 公平性

投票者在投票时, 投票内容需用对应候选者的公钥及注册中心的公钥共同加密后发到公告板公开. 而选票一旦加密后 $e(V_i)$ 只有候选者与注册中心同时解密才能解开, 强迫者在不知道某一方私钥的情况下都无法解密, 无法核实投票者是否按要求投票, 则要求投票者投指定的候选者无意义, 投票结果体现投票者意志, 选票在投票过程中一直处于被加密的状态, 最后解密也是解密一列的积, 并不影响单张选票的加密, 不会泄露中间结果. 故本方案中, 投票者可以按照自己的意愿进行投票, 不用担心投票内容泄露, 满足公平性.

(5) 唯一性

本方案中, 若同一个 ID 的投票者重复多次投票, 则所投出加密后的选票在公告板中会以时间上的最后一张保留且有效, 即后来的选票会覆盖前面的选票, 故本方案满足选票的唯一性.

(6) 完整性

计票阶段由候选者 $C_j(j=1,2,...,m)$ 对公告板投票结果的自己的得票列求积得 $\Pi_{i=1}^{n}E_{y_j}(v_{ij})$, 用自己的私钥 x_j 解密, 即可知道自己的得票数. 若候选者少计, 则不利于自己获胜, 故此情况不可能发生; 若候选者多计且使得自己获胜, 则最后获胜候选者也需要解密自己的得票来证明, 此时会暴露自己造假, 故此情况也不可能发生. 因此本方案确保了所有有效选票都被正确计入, 从而选举结果是真实可信.

(7) 合法性

本方案中, 初始化阶段只有经过身份认证的合法

的投票者才会获得数字证书 $C(P_i)=(ID_i,Sig(ID_i))$，投票阶段具有数字证书 $C(P_i)=(ID_i,Sig(ID_i))$ 的合法投票者才能参与投票，所以此方案满足合法性.

5 复杂性分析及比较

本节将对所提出的电子投票方案的复杂性进行分析，并与本文所提到的其他一些典型电子投票方案进行比较.

投票阶段，每个投票者需要执行 ElGamal 加密 m 次，每次加密需要执行 2 次幂运算和 2 次模乘运算. 计票阶段，m 位候选者需要执行 $2n$ 次模乘运算，再进行解密，需要 1 次幂运算和 1 次模除运算. 执行多方排序协议时，m 个候选者用随机数掩盖票数时需要 1 次按位加运算即 m 次加运算，进行 m 次随机数多项式分享，每次要进行 $m-1$ 次加运算、$m-1$ 次模乘运算和 $m-2$ 次幂运算，第三方排序需要 m 次加运算，$m(m-1)$ 次模乘运算，1 次减法运算.

用 M_1 表示幂运算，M_2 表示模乘运算，M_3 表示模除运算，M_4 表示模加运算，M_5 表示模减运算，则方案总计算量为:

$$(2mn+m+m^2(m-2))M_1+(2m+2nm+m^2(m-1)+m(m-1))M_2+(m)M_3+(m+m^2(m-1)+m)M_4+M_5。$$

由于其它运算相对于幂运算的计算量可忽略，因此本方案计算复杂度为 $O(km^3)$.

本文方案的方案与 Pang 等人方案[12]相比较，解密只需要候选者自行进行，不需要投票者的参与，简化了计票过程，且一般来说候选者数会比投票者人数小很多，即 $m<<n$，故 Pang 等人方案复杂度 $O(kn^2m)$ 大于本方案的复杂度 $O(km^3)$，本文提及的一些典型电子投票方案与本方案的对比如表 2.

表 2 一些典型电子投票方案与本方案的对比

方案的性质	文献[11]	文献[4]	Pang 方案[12]	本文
全隐私性	×	×	√	√
无收据性	√	×	√	√
计票不需要投票者参与	√	√	×	√
计算复杂度	$O(n^2)$	$O(n^{\frac{m-1}{2}})$	$O(kn^2m)$	$O(km^3)$
选举类型	多选多	多选一	多选多	多选多

注：表中的 n 为投票者个数，m 为候选者个数，k 为多选多选举中需要选出的获胜者个数. 一般地,$m<<n$.

6 总结

本文主要的成果有两方面：一是利用可验证秘密共享的思想设计了一个可验证的多方排序协议，可验证秘密共享的引入使得排序协议能够抵抗主动敌手攻击；二是将此多方排序协议运用到电子投票协议中，给出了一个安全的多选多的电子投票方案，多方排序协议的使用使得投票者与落选者的隐私都能被保护，满足了全隐私性. 与其它电子投票协议相比，本方案降低了计算的复杂度.

参考文献

1 Brace KW. Nation Sees Drop in Use of Electronic Voting Equipment for 2008 Election-A First. Manassas, VA: Election Data Services Inc.

2 Chaum D. Untraceable electronic mail, return addresses and digital pseudonyms. Communications of ACM, 1981, 24(2): 84–88.

3 Fujioka A, Okamoto T, Ohta K. A practical secret voting scheme for large scale elections. In: Seberry J, ed. Advances in Cryptolog(AUSCRYPT'92). Berlin, Heidelberg. Springer Berlin Heidelberg. LNCS718. 1992. 244–251.

4 Cramer R, Gennaro R, Schoenmakers B. A secure and optimally efficient multi-authority election scheme. European Transactions on Telecommunications. Hoboken. John Wiley & Sons, Ltd. 1997, 8(5): 481–490.

5 Damgard I, Jurik M. A generalisation, as simplication and some applications of Paillier's probabilistic public-key system. In: Kim K, ed. Public Key Cryptography. Berlin, Heidelberg. Springer Berlin Heidelberg. LNCS1992. 2001. 119–136.

6 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.

7 Yi X, Okamoto E. Practical internet voting system. Journal of Network and Computer Applications, 2013, 36(1): 378–387.

8 Rui J, Paulo F, Carlos R. EVIV: An end-to-end verifiable internet voting system. Computers and Security, 2013, 32(2): 170–191.

9 Rabin MO, Rivest LR. Practical end-to-end verifiable voting via split-value representations and randomized partial checking. CalTech/MIT Voting Technology Project Working. 2014. 122.

10 Benaloh J, Tuinstra D. Receipt-free secret-ballot elections. Proc. of the 26th ACM Symposium on Theory of Computing. New York. ACM. 1994. 544–553.

11 Jules A, Catalano D, Jakobsson M. Coercion-resistant electronic elections. Workshop on Privacy in the Electronic Society (WPES). New York. ACM. 2005. 61–70.

12 Pang L, Sun M, Luo S, Wang B, Xin Y. Full privacy preserving electronic voting scheme. Journal of China Universities of Posts and Telecommunications, 2012, 19(4): 86–93.

13 Yao AC. Protocols for secure computation. Proc. of 23rd Annual IEEE Symposium On the Foundation of Computer Science(FOCS'82). 1982. l60–164.

14 Fischlin M. A cost-effective pay-per-multiplication comparison method for millionaires. David Naccache. Topics in Cryptology(CT-RSA 2001). Berlin, Heidelberg. Springer Berlin Heidelberg. LNCS2020. 2001. 457–471.

15 刘文,罗守山,陈萍.利用 EIGamal 密码体制解决安全多方多数据排序问题.通信学报,2007,28(11):1–5.

16 唐春明,石桂花,姚正安.排序问题的安全多方计算协议.中国科学,2011,41(7):789–797.

17 Pedersen TP. Non-interactive and information-theoretic secure verifiable secret sharing. Advances in Cryptology (CRYPTO'91). Berlin, Heidelberg. Springer Berlin Heidelberg. LNCS576. 1992. 129–140.

18 黄宏升,仲红.保护私有信息的多方排序协议.微计算机信息(管控一体化),2010,26(6-3):67–68.