# 一个适合大规模电子选举的秘密投票方案 [1]

祁 明 肖国镇 *

(华南理工大学网络中心 广州 510641)
*(西安电子科技大学信息保密研究所 西安 710071)

**摘 要** 本文提出了一个适合大规模电子选举的秘密投票方案. 该方案不仅可使选举人进行等级选举, 而且可使选举人利用从管理者处获得的单一签名同时进行不同类型电子选举.

**关键词** 电子选举, 盲签名, 密码协议

**中图号** TN918.2

## 1 引 言

长期以来, 人们一直期盼各种投票系统实现电子化, 因为电子化的实现不但可以减少通常投票活动在管理, 选票收集和统计以及安全保密等方面所需花费的大量人力和物力, 而且可使投票者不必去为投票者专门设立的投票处. 就目前已提出的许多投票方案而言, 普遍存在以下问题: (1) 投票的中间结果容易被泄漏, 即公正性难以保证; (2) 一般方案均不允许投票者弃权, 而允许弃权的方案又无法防止假弃权者的欺骗; (3) 无法将投票者分类进行等级选举; (4) 投票者每投一次票就不得不从管理中心获得一次签名, 这种方式不适合投票者同时进行多种不同类型的投票. 本文提出了一个新的电子投票方案, 克服了上述存在的缺点. 我们给出了该方案的一个特殊实现方法, 并讨论了它的安全性及其性能.

## 2 投票方案及其特殊实现

2.1 方案的基本框架 新方案由投票者、公证人、管理中心和多个计票人共同实施完成. 下面我们在假设每个计票人分管不同类型的选举并且这些选举可同时进行的情况下, 给出新方案的框架, 此框架共包含七个大的步骤. 对此框架稍加修改, 就可变成进行同一类型选举的情况.

(1) 准备 管理中心计算有关参数.

(2) 申请 投票者选随机数并将此随机数盲化后, 连同自己的身份码一起作为投票申请送管理中心审核, 并设法获得中心的盲签名.

(3) 签名 管理中心对盲消息进行签名, 并将其签名送投票者.

(4) 投票 投票者从中心的签名得到盲签名后, 利用此签名可构造投向不同计票人的选票.

(5) 计票 各计票人对收到的选票进行编号并公开.

(6) 核查 投票者若发现自己所投选票未被公开或被改动, 可向公证人公开有关数据, 以确定计票人是否有问题. 若无异议, 则投票者将有关秘密数据送计票人.

(7) 公开 计票人核对选票并公开最终选举结果.

2.2 方案的特殊实现

[1] 1995-09-27 收到, 1996-12-30 定稿
中国博士后科学基金和广东省自然科学基金资助项目

**准备** (1) 设 $(e,d,n)$ 和 $(e_i,d_i,n_i)$ 分别是管理中心和投票者 $U_i(i=1,2,\cdots,n)$ 的 RSA 参数，$g$ 为 GF($p$) 和 GF($q$) 的本原元，这里 $n=p\cdot q$。$\mathrm{CID}_j$ 和 $\mathrm{ID}_i$ 分别为计票人 $C_j$，$(j=1,2,\cdots,m)$ 和投票者 $U_i$ 的身份码。

(2) 管理中心计算 $C_j$ 的秘钥和公钥：$x_j=\mathrm{CID}_j^{-d}\mathrm{mod}n$，$y_j=x_jg_j^x\mathrm{mod}n$。中心将 $(\mathrm{CID}_j,y_j)$ 向所有投票者公开，$x_j$ 由 $C_j$ 保密。

**申请** (1) $U_i$ 选随机数 $t_i$ 和 $r_i$ 并计算 $t_i'=t_i^{-1}r_i^e\mathrm{mod}n$ 和 $f_i=(t_i')^{d_i}\mathrm{mod}n_i$，$(n<n_i)$。

(2) $U_i$ 将 $(\mathrm{ID}_i,t_i',f_i)$ 作为投票申请提交给管理中心。

**签名** (1) 中心验证签名 $f_i$ 的合法性，以确信 $U_i$ 是否重复投票。如果中心确信 $U_i$ 是第一次投票，则中心为 $U_i$ 计算签名 $s_i'=(t_i')^d\mathrm{mod}n=t_i^{-d}r_i\mathrm{mod}n$。

(2) 中心将 $(\mathrm{ID}_i,s_i')$ 作为对申请的批文送 $U_i$。如果规定 $U_i$ 只能在某 $C_j$ 处投票，则中心可将 $(\mathrm{CID}_j,y_j)$ 和批文一起送 $U_i$，并将 $\mathrm{ID}_i$ 送 $C_j$。因此，$C_j$ 知道中心允许向自己投票的总人数。

**投票** (1) $U_i$ 利用 $s_i=s_i'/r_i=t_i^{-d}\mathrm{mod}n$ 从盲签名 $s_i'$ 得到中心关于 $t_i$ 的签名 $s_i$ 且只有 $U_i$ 知道 $s_i$。

(2) 设 $z_{ij}$ 为 $U_i$ 所选的向 $C_j$ 投票的真实内容，$w_{ij}$ 为随机数，并设 $v_{ij}=H(z_{ij}\|w_{ij})$，这里 $H$ 为单向杂凑函数。

(3) $U_i$ 计算：

$$K_{ij}=(y_j^e\mathrm{CID}_j)^{s_i}\mathrm{mod}n=g^{ex_js_i}\mathrm{mod}n,$$
$$C_{ij}=K_{ij}v_{ij}\mathrm{mod}n,$$
$$D_{ij}=s_ig^{s_i}\mathrm{mod}n.$$

(4) $U_i$ 经匿名信道向 $C_j$ 所投的选票为 $B_{ij}=(C_{ij},D_{ij})$。

**计票** $C_j$ 收到全部选票 $B_{ij}$ 后 $(i=1,2,\cdots,k)$ $(k\le n)$，对它们进行编号并公开。

**核查** (1) 如果 $U_i$ 发现自己向 $C_j$ 所投选票 $B_{ij}$ 未被公开或被改动，可向公证人提交 $(t_i,s_i,v_{ij})$ 以表示质疑。公证人利用这些数据可验证签名 $s_i$ 的正确性并可求得 $B_{ij}=(C_{ij},D_{ij})$，从而可发现计票人 $C_j$ 是否有误。

(2) 如果向 $C_j$ 提出质疑和异议的投票者较多，则公证人有权追究 $C_j$ 的责任或取消所有向 $C_j$ 所投选票的有效性，以便重新投票。

**公开** (1) 如果 $U_i$ 对 $C_j$ 的计票结果无异议，则将 $(l,t_i)$ 送 $C_j$。这里 $l$ 是选票 $B_{ij}$ 对应的编号。

(2) 计票人 $C_j$ 利用管理中心的公钥 $e$ 和自己的密钥 $x_j$ 计算：

$$K_{ij}=(D_{ij}^et_i)^{x_j}\mathrm{mod}n=g^{ex_js_i}\mathrm{mod}n,$$
$$v_{ij}=K_{ij}^{-1}C_{ij}\mathrm{mod}n,$$

并将 $(l,B_{ij},t_i,v_{ij})$ 公开。$U_i$ 由此可判别是否真正是 $C_j$ 收到了 $B_{ij}$。

(3) 若 $U_i$ 对公开结果无异议，便再将 $(l,s_i,z_{ij},w_{ij})$ 送 $C_j$。若 $s_i^et_i=1\mathrm{mod}n$（因为 $s_i=t_i^{-d}\mathrm{mod}n$）且 $v_{ij}=H(z_{ij}\|w_{ij})$ 成立，则 $C_j$ 公开最后的投票结果，如表 1 所示。如果 $U_i$ 利用 $s_i$ 同时进行了 $k$ 个不同类型的投票时，则将有 $k$ 个不同的投票结果。

表 1

| 编号 | 选票和相关参数 |
|---|---|
| ⋮ | ---------- |
| $l$ | $C_{ij}$, $D_{ij}$, $t_i$, $v_{ij}$, $s_{ij}$, $z_{ij}$, $w_{ij}$ |
| ⋮ | ---------- |

## 3 讨论和分析

(1) 由于特殊的选票结构，投票者的身份码 $\mathrm{ID}_i$ 和选票 $B_{ij}$ 之间的关系由盲签名方法所蕴藏．因此，所提方案保证了投票的匿名性．

(2) 在许多投票方案中，计票人容易将投票的中间结果泄漏给其他未投票者，这不但难以保证投票的公证性，而且还会在许多特殊的投票活动中引起投票者之间的不公平竞争．由于新方案采用在最后阶段公开 $(t_i, v_{ij})$ 的方法，从而保证了公证性．

(3) 在规定不许弃权的条件下，当选票总数未达到或超过 $C_j$ 应收到的总票数时，可以宣告投票无效．另外，由于 $U_i$ 向不同 $C_j$ 的投票中，最后结果中的 $t_i$ 和 $D_{ij}$ 总是相同的，因此，$C_j$ 很容易发现重复投票者．

(4) 由于每张选票都含中心签名，所以，任何未经许可的人无权投票．

(5) 如果有人删除或改动选票，投票人可以匿名提出质疑，从而该方案可防止任何人对选票进行的诈骗行为．

(6) 任何人都可以验证投票结果的正确性．

(7) 当使用多个 $C_j$ 时，既可进行同类型的投票，也可进行不同类型的投票．当进行后一种投票时，这些投票应同时进行或者各个不同的投票结果应同时公开，以防有人利用 $s_i$ 构造合法选票．

(8) 从 $B_{ij} = (C_{ij}, D_{ij}) = (K_{ij}v_{ij} \bmod n, s_i g^{s_i} \bmod n)$ 可知，它与已有各种选票均不相同．$C_{ij}$ 类似于 Sako 选票 [1] 中对 $v_{ij}$ 的加密，而 $D_{ij}$ 类似于 FOO 选票 [2] 中的签名 $y$，但与 $y$ 不同的是，签名 $s_i$ 被隐藏了起来。可见，$B_{ij}$ 吸收了许多已有选票的优点并具有较好的安全性．

(9) Koyama 方案 [3] 和新方案是目前所见到的仅有的两个四方投票协议．由于 Koyama 方案未采用盲签名技术，所以在匿名性和公证性方面存在许多问题．而这些问题对新方案均不存在．

(10) 若将此方案用于商业上的投标投票时，一旦 $B_{ij}$ 对应的选票中标，则为了确定 $B_{ij}$ 对应的投票者，该投票者只需将盲化消息的秘密参数 $r_i$ 公开即可．因为由 $t_i' = t_i^{-1} r_i^e \bmod n$ 和申请书 $(\mathrm{ID}_i, t_i', f_i)$ 是否对应即可作出判断。

(11) 当规定某些具有行使否决权的特殊投票者只能在某 $C_j$ 处投票时，则新方案可用于等级选举投票．

(12) 文献 [4] 曾提出过一个允许投票者弃权的投票方案，但该方案不能防止假弃权者进行欺骗．由于新方案在最后阶段实行两次公开法，从而可有效地防止假弃权者破坏投票的公正性．

## 4 论　结

本文讨论了在设立多个计票人的情况下实现安全而有效的投票途径，提出了一个实用的适合大规模和多功能电子选举的投票方法。值得进一步研究的问题是，如何在不使用盲签名的情况下构造安全而有效的投票方案。

## 参 考 文 献

[1] Sako K. Electronic voting system with objection to the center. In SCI92-13C, Tokyo, 1992, 1–6.

[2] Fujioka A, Okamoto T, Ohta K. A practical secret voting scheme for large scale election. Proc. of Auscrypt'92, Sydney; Springer-Verlag, 1993, 244–251.

[3] Koyama K. Secure secret voting system using the RSA public key cryptosystem. Trans. IEICE, 1985,J68-D(11):1956–1966.

[4] Chen L, Burmester M. A practical secret voting scheme which allows voters to abstain. Proc. of Chinacrypt'94, Xi'an: Science Press, 1994, 100–107.

# A PRACTICAL SECRET VOTING SCHEME FOR LARGE SCALE ELECTRONIC ELECTIONS

Qi Ming Xiao Guozhen*

(*Network Center of SCUT, Guangzhou* 510641)

*(*Xidian University, Xi'an* 710071)

**Abstract** This paper presents a practical secret voting scheme for large scale electronic elections. The scheme enables a voter to engage in not only the estate election, but also some different electronic elections simultaneously by using a single signature obtained from administrator.

**Key words** Electronic voting, Blind signature, Cryptographic protocol

祁 明: 男, 1957 年生, 博士后, 主要从事计算机网络安全, 认证技术和密码协议的研究.
肖国镇: 男, 1934 年生, 教授, 博士生导师, 主要从事密码和编码的研究工作.