一种电子投票方案*

李彦江[1,3+], 马传贵[2], 黄刘生[1,3]

[1](中国科学技术大学 计算机科学技术系,安徽 合肥 230027)

[2](解放军信息工程大学 应用数学系,河南 郑州 450002)

[3](高性能计算与应用省部共建重点实验室,安徽 合肥 230027)

An Electronic Voting Scheme

LI Yan-Jiang[1,3+], MA Chuan-Gui[2], HUANG Liu-Sheng[1,3]

[1](Department of Computer Science and Technology, University of Science and Technology of China , Hefei 230027, China)

[2](Department of Applied Mathematics, PLA Information Engineering University, Zhengzhou 450002, China)

[3](Anhui Province-MOST Co-Key Laboratory of High Performance Computing and Application, Hefei 230027, China)

+ Corresponding author: Phn: +86-551-3624134, E-mail: yjli@mail.ustc.edu.cn, http://www.ustc.edu.cn

Received 2004-02-10; Accepted 2005-03-10

Li YJ, Ma CG, Huang LS. An electronic voting scheme. *Journal of Software*, 2005,16(10):1805−1810. DOI: 10.1360/jos161805

Abstract: A dynamic multi-secrets sharing threshold scheme is presented to apply to a large scale electronic voting system with many talliers (tallying authorities). Even if there exist adaptive adversaries, this scheme can guard the ballot's producing, encrypting, transmitting, decrypting and final tallying in spite of the adversaries's attack, so the scheme guarantees robustness. In this paper, the verifiability of the voters' qualification and talliers' identification will be solved by a dynamic multi-secret sharing scheme without invoking more zero knowledge proof to maintain privacy, universal verifiablitlity, and anonymity of ballots. It holds more communication efficiency and more security than the proposed schemes in early time.

Key words: dynamic multi-secrets; threshold scheme; electronic voting; universal verifiability; large scale election

摘 要: 提出了把动态多密门限体制应用于大规模选举的电子投票系统,它可以允许系统中存在多个监票人(机构).即使在选票的生成、加密、传输及解密、统计过程中存在自适应敌手,也不影响选举的正常进行,因此具有强壮性.提供的电子投票方案,无须调用多次交互式的零知识证明验证投票人的选举资格和监票人的身份,而是利用动态多密门体制方便地实现了选票的秘密性、广泛可验证性、公平性和匿名性,较之以前的投票方案具有较高的通信效率和安全性.

关键词: 动态多密;门限体制;电子投票;广泛可验证性;大规模选举

* Supported by the National Natural Science Foundation of China under Grant Nos.10071001, 90104035 (国家自然科学基金), the National Grand Fundamental Research 973 Program of China under Grant No.G1998030403 (国家重点基础研究发展规划(973))

作者简介: 李彦江(1973－),男,甘肃陇西人,博士生,助理研究员,主要研究领域为密码分析,信息安全;马传贵(1962－),男,博士,教授,主要研究领域为代数组合,网络密码,信息安全;黄刘生(1957－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为分布式算法,并行分布式系统,网络安全,软件工具与环境,KDD,面向对象的系统模型和设计方法,OODB.

中图法分类号: TP309 文献标识码: A

电子投票系统有利于防范选举中出现舞弊现象,并且计票速度更快,结果更准确.电子投票一般有投票人、监票人及候选人.Chaum[1]在 1981 年明确地提出了基于公钥密码的电子邮件概念,它也是电子选票的雏形;Josh[2],Magkos[3],Cranor[4]分别着手实现了保密、无收据性和安全实用的投票方案.1985 年,Josh[2]提出了电子选举的概念.1994 年,Benaloh[5]引入了电子投票的无收据性(receipt-free).1997 年,Cranor[6]设计并完成了一个能用于因特网的投票协议 Sensus.Cranor[7]于 1996 年提出了电子投票需要满足 7 个性质:准确性(accuracy)、民主性(democracy)、秘密性(privacy)、可验证性(verifiablity)、方便性(convenience)、灵活性(flexibility)以及移动性(mobility).2000 年,Martin[8]指出,Benaloh 方案只有在一个监票机构的情况下才具有无收据性.真正具有无收据性的电子投票方案是 Lee[9]在 2000 年提出来的.他引入了诚实的监票人,是建立在监票人完全可信的基础之上的.本文考虑到网络环境的复杂性,设计了可抵抗自适应敌手(破坏选举正常进行或影响投票人正常投票或干扰计票工作的人或机构)的投票方案,并总是假设选票 $(Y_1,...,Y_m)$ 分别在分布式网络系统中的服务器的端口 $(ID_1,...,ID_m)$ 上完成它的初始化、加密、传送、解密、计算及最后的统计工作.Canetti[10]从不同角度对端口进行了描述,概括地说,端口在信息交换过程中对应于通信的进程,在信息存取过程中对应于存储区的数据区段.

1 动态多密门限体制的基本思想及方法

由 m 个投票人 V_i 和 k 个候选人 C_j,n 个监票机构 AV_j 构成的电子投票方案,即对应于管理者 P_d(每个投票人 V_i)向 n 个参与者(监票人)分发 m 个秘密(投票人对候选人选票的私钥)的 m-门限多密共享体制.特别需要注意的是,这时投票者即为管理者 P_d(在动态多密门限体制中,P_d 有 m 个,其实质可以理解为只有一个 P_d,但要分发 m 个秘密,因为每个投票人的私钥不同).监票人作为参与者接收由 P_d 分发给他的影子多项式及子密多项式,进而又向其他的监票人分发子密;候选人实际上也成了旁观者.监票人知道 CA 发送给他的关于投票人合法身份的公钥,监票人获得的其他消息全部来源于公告牌,与旁观者掌握的知识一样多,在 (n,k_i,t)-m 多密门限共享体制中,$1\le i\le m$ .k_i 是投票人 V_i 的私钥 S_i 的门限值,n 表示监票人个数,t 表示敌手的最大量.选两个大素数 p,q,使得 $q|p-1$,并且 $q>n$, $\phi(q-1)>m+2$($\phi(n)$ 表示欧拉函数).令 G 表示 Z_p 的 q 阶乘法子群,并设 $g_0,g_1,\ldots,g_m,h$ 为 G 的 $m+2$ 个生成元,对监票人 AV_j,$1\le j\le n$,计算 $\log_{g_j} h$, $\log_{g_0} h$ 不可行.

1.1 选票私钥的生成及初始化

1.1.1 投票人私钥的初始化及其影子多项式、随机多项式的选取

这里假设 m 个投票人所具有的私钥组为 $(S_1,\ldots,S_m)$,其所对应的门限值分别为 $(k_1,\ldots,k_m)$,每个密钥 S_i 相应地由 (k_i,t,n)-门限体制分发.选 m 个至多 k_i-1 次的二变元多项式 $f_i(x,y)\in Z_p[x,y]$ 作为分发投票人私钥的影子多项式,并使得 $f_i(0,0)=S_i$,$1\le i\le m$;选 $k-1$ 次双变元多项式 $f(x,y)\in Z_p[x,y]$ 作为分发投票人私钥的随机多项式,其中 $k=\max(k_1,...,k_m)$, $f_i(x,y)=\sum_{j,l=0}^{k_i-1} f_{ijl}x^j y^l$, $f(x,y)=\sum_{j,l=0}^{k-1} f_{jl}x^j y^l$.

1.1.2 对有关参数的说明

管理者 P_d 一次性地向每个监票人 $AV_r(1\le r\le n)$ 发送 m 个影子多项式 $a_{ir}(y)=f_i(r,y)$,$1\le i\le m$,发送 m 个子密多项式 $b_{ir}=f_i(x,r)$,发送两个随机多项式 $a_r(y)=f(r,y)$,$b_r(x)=f(x,r)$,并且一同发送具有身份验证和比特承诺功能的约束向量 $D(A_r^{(0)},B_r^{(0)},h_{ra},h_{rb})$,其中

$$A_r^{(0)}=(A_{r0}^{(0)},A_{r1}^{(0)},...,A_{rn}^{(0)}),\ B_r^{(0)}=(B_{r0}^{(0)},B_{r1}^{(0)},...,B_{rn}^{(0)}),\ h_{ra}=(h_{ra,0},...,h_{ra,n}),\ h_{rb}=(h_{rb,0},...,h_{rb,n}).$$

这里, $h_{ra,j}=H(A_r^{(j)})$, $h_{rb,j}=H(B_r^{(j)})$.定义 $A_{rj}^{(0)}=g_r^{f_r(0,j)}h^{f(0,j)}$, $B_{rj}^{(0)}=g_r^{f_r(j,0)}h^{f(j,0)}$.其中 H 为具有强抵抗碰撞性的单向 Hash 函数,即由 $H(X)=H(Y)$ 可以得出 $X=Y$,设 $A_r^{(i)}=(A_{r0}^{(i)},A_{r1}^{(i)}...,A_{rn}^{(i)})$, $B_r^{(i)}=(B_{r0}^{(i)},B_{r1}^{(i)},...,B_{rn}^{(i)})$ 表示在共享秘密 S_r 时与监票人 AV_i 关联的两个 $n+1$ 元向量.对 $j\in[0,n]$,$r\in[1,n]$, $A_{rj}^{(i)}=g_r^{a_{ri}(j)}h^{a_i(j)}$, $B_{rj}^{(i)}=g_r^{b_{ri}(j)}h^{b_i(j)}$.

$2(m+1)$ 个多项式保密,即这些多项式的系数 f_{ijl} 是保密的.与此同时,对每个 $S_i=f_i(0,0)$,管理者 P_d 计算出自己的公钥 $Y_i=g_0^{s_i}\pmod p$,并把它发向公告牌.同时,将 $g_0,g_1,\ldots,g_m,h$ 发到公告牌.该方案所允许的自适应敌手的最

大量为 $t=\min(k_1-1,\ldots,k_m-1)$.

1.2 投票人私钥的分发(这里假设$k_i\geq(n+t+1)/2$)

1.2.1 分发投票人私钥的影子秘密

管理者(每个投票人 V_r)一次性地发送给监票人 AV_j 共 $2(m+1)$条消息及约束向量 D_r,即

$$V_r \xrightarrow{a_{1r}(y),a_{2r}(y),\ldots,a_{mr}(y),a_r(y),b_{1r}(x),b_{2r}(x),\ldots,b_{mr}(x),b_r(x),D_r} AV_j,$$

其中 $r\in[1,n]$,投票人私钥影子秘密组$(S_{1r},\ldots,S_{mr})$的分发阶段完成.

1.2.2 分发投票人私钥的子密

当每个监票人 AV_j 接收到 P_d 发给他的消息时,这些监票人在密钥组$(S_1,\ldots,S_m)$对应的不同端口 $ID.1,\ldots,ID.m$ 上产生 Echo 消息.实际上,从监票人 AV_r 发向 AV_j 的 Echo 消息为{Echo 消息,$D_r,a_{1r}(j),\ldots,a_{mr}(j),a_r(j),b_{1r}(j),b_{2r}(j),\ldots,b_{mr}(j),b_r(j)\}$.$f_i(0,0)=S_i,1\leq i\leq m$ 为待分发的秘密.

对每个 $i\in[1,m]$,P_d 发送 m 个投票人 V_i 的 n 个私钥影子秘密多项式 $a_{i1}(y),a_{i2}(y),\ldots,a_{im}(y)$,$n$ 个私钥子密多项式 $b_{i1}(x),b_{i2}(x),\ldots,b_{in}(x)$,两个随机多项式 $a_i(y)$及 $b_i(x)$及约束向量 D_i 给每个监票人 AV_r,注意到 P_d 发送了 mn 个长度为 $O(kn)$ 的消息.当监票人 AV_r 接收到这些消息后,对每个 $j\in[0,n],r\in[1,n],i\in[1,m]$,它又以发送者的身份向其他监票人 AV_j 发送如下消息:包含 m 个 $a_{ir}(j)=f_i(r,j)$,m 个 $b_{ir}(j)=f_i(j,r)$与两个随机数 $a_r(j)=f(r,j),b_r(j)=f(j,r)$及约束矩阵 $D_r=(A_r^{(0)},B_r^{(0)},h_{ra},h_{rb})$.

1.3 投票人私钥的验证

n 个监票人得到的 m 个投票人 V_i 的 m 个秘密选票的影子秘密多项式及子密多项式.只要投票人 V_r 与监票人 AV_j 或者监票人之间传送的数据通过了定理 5 的核对或验证,则说明投票人具有了选举资格或监票人取得了监票资格.

1.3.1 对多项式及端口的核对、验证及对影子秘密的验证过程

定理 **1**. 核对多项式在分发投票人 V_r 的选票原始私钥 S_r 时,若监票人 AV_i 接收到 P_d(这时就是 V_r)发送的 (D_r,i,A_r,B_r),如果对 $r\in[1,m],i\in[1,n]$,分别考查 $A_{ri}^{(0)}=B_{r0}$, $B_{ri}^{(0)}=A_{r0}$, $h_{ra,i}=H(A_r)$, $h_{rb,i}=H(B_r)$ 成立,那么,A_r,B_r 是正确的.

定理 **2**. 核对端口 (C_r,γ_r,γ) C_r 是在分发投票人 V_r 选票的原始私钥 S_r 时对 γ_r 和 γ 的承诺⇔对 $r\in[1,m]$,分别考查 $C_r=g_r^{\gamma_r}h^{\gamma}$.

定理 **3**. 验证多项式(D_r,i,a_r,a,b_r,b),这里,$a_{r1},a_{r2},\ldots,a_{rn},a_r,b_{r1},\ldots,b_{rn},b_r$ 是 k_r-1 次多项式,若这些多项式是正确的⇔对 $r\in[1,m]$,分别考查核对多项式(D_r,i,A_r,B_r)成立,其中

$$A_r=(A_{r0},A_{r1},\ldots,A_{rn}),B=(B_{r0},B_{r1},\ldots,B_{rn}),\ A_{rj}=g_r^{a_r(j)}h^{a(j)},\ B_{rj}=g_r^{b_r(j)}h^{b(j)}.$$

定理 **4**. 验证端口$(D_r,i,m,A_r,B_r,\alpha_r,\alpha,\beta_r,\beta)$,这里,$A_r,B_r$ 是监票人 AV_i 在共享投票人 V_r 选票的原始私钥 S_r 时接收到的从监票人 AV_m 发送来的 $n+1$ 元向量.验证 $\alpha_r=f_r(m,i)$, $\alpha=f(m,i)$, $\beta_r=f_r(i,m)$, $\beta=f(i,m)$ 对约束向量 D_r 成立,其中 $r\in[1,m]$⇔对 $r\in[1,m]$,分别考查核对多项式(D_r,m,A_r,B_r)、核对端口(A_{ri},α_r,α)及核对端口(B_{ri},β_r,β)同时成立.

定理 **5**. 验证影子秘密(D_r,m,σ_r,σ),其中(σ_r,σ)是监票人 AV_m 在共享投票人 V_r 选票的原始秘密 S_r 时关于约束向量 D_r 获得的影子秘密,(σ_r,σ)是正确的⇔对 $r\in[1,m]$,分别考查 $g_r^{\sigma_r}h^{\sigma}=A_{rm}^{(0)}$.

1.3.2 验证的正确性

现考虑监票人 AV_i 与 AV_j 之间的通信.对投票人 V_r 的私钥 S_r,AV_i 传送给 AV_j 的信息为

$$AV_i \xrightarrow{D_r,A_r^{(i)},B_r^{(i)},f_r(i,j),f(i,j),f_r(j,i),f(j,i)} AV_j,$$

监票人 AV_j 获得的关于选票密钥 S_r 的影子秘密为 $S_{rj}=\bar{a}_{rj}(0)=f_r(j,0)=\sum_{i=0}^{k-1}f_{ri0}j^i$,$k_r$ 个影子秘密利用 Larange 插值公式联合恢复的秘密设为 z_r,反设恢复出来的秘密 $z_r\neq S_r$,这说明至少有一个监票人 AV_i 计算出来的结果 $\bar{a}_{rj}(y)\neq f_r(i,y)\Rightarrow AV_i$ 从某个被破坏的监票人 AV_m 处接收了 Echo 消息 $\alpha_r\neq f_r(m,i)$,但由于监票人 AV_i 通过了验证端口$(D_r,i,m,A_r,B_r,\alpha_r,\alpha,\beta_r,\beta)$、核对多项式$(D_r,m,A_r,B_r)$及核对端口$(A_{ri},\alpha_r,\alpha)$,如果 $A_r^{(i)}\neq A_r\Rightarrow$核对多项式

(D_r,m,A_r,B_r)失败,从而否定了 Hash 函数的强抵抗碰撞性的假设,也与求解离散对数是困难的这一前提假设矛盾.

2 基于动态多密体制的电子投票

以下的投票方案都限定在一个投票周期内,当投票时间截止时,各种秘密及选票将被刷新,两个相继投票周期的相应信息不具有任何继承性.假设有 m 个投票人 $V_r(1\le r\le m)$,n 个监票人(机构)$AV_j(1\le j\le n)$.取 Z_q 中的 $m+1$ 个独立生成元(指在计算上生成元间相互无法表出或相互表出的难度极大)g_r 及 h,$1\le r\le m$,代表不同的选票.相应地,监票人看到每个投票人 $V_r(1\le r\le m)$对候选人 C_j 的投票为$(x,y)=(g_r^{\beta},h^{\alpha}G_{rj})$,投票人 V_r 对候选人 C_j 的选票内容 G_{rj} 保密,α 为投票人 V_r 选票的原始私钥分配给监票人 AV_j 的影子秘密.对于每个投票者,Lee[9]指出先到 CA 处进行注册,以取得投票资格,CA 发放有效证书给投票者 V_r,同时给每个监票人发送具有投票资格的选举人的证书.根据第 1.3.1 节,在投票前,可以用它行使 CA 的关键功能(提供监票人身份合法性的验证).投票时,监票人 AV_j 合作产生最终选票,并由计票人公布结果.

2.1 验证投票人V_r身份的合法性

利用一般的 Elgmal 加密模型,对每个监票人 AV_j 广播 $\omega_{rj}=x^{s_{rj}}$,并用多密共享的方式,保护选票的秘密性,最先验证投票人身份的合法性、选票的有效性,防止候选人与监票人以及监票人之间相互勾结伪造有效选票,最后产生最终选票交给计票人.每个投票人 V_r 选一个二元多项式 $f_r(x,y)$ 用来分发私钥 s_r 和公开验证监票人身份.从而在监票人 AV_j 相互验证彼此的身份时,不需要证书机构(CA)的介入.但是每个投票人 V_r,在投票前必须到 CA 处注册自己的公钥 $K_r=g_r^{s_r}=g_r^{f_r(0,0)}$,使 $s_r=f_r(0,0)$作为自己的私钥.发送对候选人 C_j 的选票前,先发送 $f_r(ID.j,y)$ 到每个监票人 AV_j,其中 $ID.j$ 为监票人 AV_j 所对应的终端服务器的 ID 标识号.根据第 1.3 节的内容,在投票人 V_r 与监票人 AV_j 之间可以有效地完成两个任务:一是 AV_j 可以清楚地知道 V_r 是否有选举权(因为 CA 在每次投票前已事先向 AV_j 发送过有效投票人的证书,即公钥 $g_r^{s_r}$);二是 AV_j 部分地得到了一些选票的加密信息(即每个 AV_j 从 V_r 处获得了$(X_j,Y_j)=(g_r^{\bar{a}_{r\,ID.j}(0)},h^{\bar{a}_{r\,ID.j}(0)}G_{rj})$).

2.2 选票的生成

在验证投票人 V_r 的过程中(第 1.1 节),监票人 AV_j 已知部分选票的加密信息(X_j,Y_j),令Δ为任意 t 个监票人的集合,由 Lagrange 插值公式可知,t 个监票人(机构)联合生成秘密 $s_r=\sum s_{rj}\lambda_{rj,\Delta}$,$\lambda_{r\,j,\Delta}=\prod_{l\in\Delta\setminus\{l\}}\frac{ID.l}{ID.l-ID.j}$,其中 $ID.i(1\le i\le k)$为监票人 AV_i 的 ID 标识号,$s_{r\,j}=\bar{a}_{r\,ID.j}(0)$,投票人 V_r 的选票为 $(x,y)=(g_r^{\omega_r},h^{\omega_r}m)$,而选票所含的内容可不用恢复投票人原始选票的私钥 S_r 而得到.这是因为

$$h=g_r^{s_r}=g_r^{\sum s_{r\,j}\lambda_{r\,j,\Delta}}=\prod g_r^{s_{r\,j}\lambda_{r\,j,\Delta}}$$

$$\Rightarrow h^{\alpha}=(\prod_{j\in\Delta}g_r^{s_{r\,j}\lambda_{r\,j,\Delta}})^{\alpha}=\prod_{j\in\Delta}(g_r^{\alpha s_{r\,j}})^{\lambda_{r\,j,\Delta}}=\prod_{j\in\Delta}(x^{s_{r\,j}})^{\lambda_{r\,j,\Delta}}=\prod\omega_{r\,j}^{\lambda_{r\,j,\Delta}}\Rightarrow m=y/h^{\alpha}=y\Big/\prod\omega_{r\,j}^{\lambda_{r\,j,\Delta}}.$$

2.3 验证选票的有效性

选票的正确性需要对(x,y)的有效性进行验证.考虑 ElGamal 加密模型(G_{ij} 表示投票人 V_i 对候选人 C_j 的选票内容,g_i 为投票人 V_i 分发选票私钥 S_i 所用的生成元),并且 V_i 对 k 个候选人一次性投票.具体的交互过程如下(其中$\Gamma=\{i_1,\ldots,i_k\}$为$\{1,\ldots,k\}$的置换):

验证者(AV_j)	证明者(V_i)
选 $\alpha_i\in Z_q$,	
$(x_i,y_i)=(g_i^{\alpha_i},h^{\alpha_i}G_{i\,j})$,	
计算 $a_{i_j}=g_i^{\omega_{i_j}},b_{i_j}=h^{\omega_{i_j}}$	
对 $t\in\Gamma\setminus\{i_j\}$,选 $d_t,r_t\in Z_q$,	
计算 $a_t=g_i^{r_t}x^{d_t},b_t=h^{r_t}(y/g_t)^{d_t}$	

$\xrightarrow{x,y,a_{i_1},a_{i_2},\cdots,a_{i_k},b_{i_1},b_{i_2},\cdots,b_{i_k}}$

$\xleftarrow{\text{将随机数 } c \text{ 发向证明者}}$ 选 $c \in Z_q$

计算 $d_{i_j} = c - \sum_t d_t$,

其中 $t \in \Gamma \setminus \{i_j\}$, $R_{i_j} = \omega_{i_j} - \alpha_t d_{i_j}$ $\xrightarrow{d_{i_1},\ldots,d_{i_k},R_{i_1},\ldots,R_{i_k}}$ 对 $t \in \Gamma$,验证:

$c ? = \sum_{t\in\Gamma} d_t$, $a_t ? = g_i^{R_t} x_i^{d_t}$,

$b_t ? = h^{R_t}(y_i / g_t)^{d_t}$

2.4 选票计数

在本文的方案中,对候选人 C_l,$1\le l\le k$,监票机构 AV_j,$1\le j\le n$,投票人 V_r 把选票(x_r,y_r)投向布告栏、监票人 AV_j,计票人在端口 $ID.j$ 上选择 $AV_i \in \Delta$ ($|\Delta| = k_i$,Δ为任意 k_j 个 AV_j 组成的子集),要知道候选人 C_j 获得的选票,计算 $(X,Y) = (\prod_{r=1}^{k_j} x_r, \prod_{r=1}^{k_j} y_r)$,然后利用门限 Elgamal 加密,计算出 $W = Y / X^{s_r}$,由前面分析可知,计票人不需要恢复出 V_r 的私钥 s_r.最后,利用 $W = g_r^{T_j} = \prod g_r^{G_{i_j}}$,这里,对 m 个投票人和 n 个候选人,用 Shanks' baby-step giant-step 算法计算出 T_j.T_j 表示候选人 C_j 最后获得的总选票(赞成票票数与反对票票数的差额).如果有 Super Voter 投反对票,则视该候选人得票数为 0.

2.5 性能分析

2.5.1 投票方案的优点

监票人 AV_j 无法与任何机构勾结来泄露投票人的秘密.在有效投票周期内,允许投票人一次性地对多个候选人进行投票,并且不同的投票人可以并行作业;除了验证投票人的合法性需要 CA 的中介,其余的投票环节都由多密门限体制进行动态管理,不需要像 Lee[9]方案那样引入可信的第三方(监票机构).选举结果一旦宣布,除了保留相应的选举结果,要求 AV_j 把其余中间信息清除.在不同的投票周期内,与选票相关的所有信息全部刷新,不具有任何继承性.但由于每个 AV_j 持有 CA 发送给它的投票人 V_i 的公钥 $G_j^{s_i}$,故该方案中要求 AV_j 有监票的义务.陈晓峰等人[11]提出了一种基于半信任模型的电子投票方案,较好地实现了选票的无收据性,但在监票人(机构)数≥2 时显得很繁杂,并且随着投票人与监票人数目的增加,交互式的零知识证明需要消耗较大的网络通信开支,只能用于中小规模的选举活动.本文的投票方案可满足大规模选举的要求.

2.5.2 复杂度分析

通信复杂性分析:通常的 m 重电子投票的消息复杂度为 $O(mn^2)$,而本文方案中考查的对象是分布式网络系统中分别承担投票和监票的 m 和 n 个服务器,其通信复杂度为 $O(mn\lg n)$.

时间复杂度分析:假定每一个进程的每一个任务的时间上界为 l,在每一通道队列中传递最早消息的时间上界为 d,因每一进程的发送缓冲区的最大长度和每一通道队列的最大长度都为 n,所以进程的发送缓冲区中的标识 ID(连同选票信息)放在相邻通道中最多需要时间 nl,而在通道队列中的 ID 被下一进程接收,则最多需要时间 nd,因此总共的时间复杂度为 $O(mn^2(l+d))$.但在分布式网络系统中,并非每个缓冲区和队列的长度都为 n,因此,在任意公平运行中,选票信息从重建启动到首次成功重建所需时间最多为 $O(mn(l+d))$.

2.5.3 投票方案的进一步改进

投票方案中用零知识证明了选票(x,y)的有效性,从证明过程可以看出,选票的产生和发送都是由投票人 V_r 来完成的,所以该方案不具有选票的无收据性.在本文的方案中,如果在证明者与验证者之间增加了一次有随机数参加的交互零知识证明,就可以实现选票的无收据性.

3 结 论

本文基于动态多密门限体制设计了一种可供大规模选举的电子投票方案.由于投票方案具有广泛的可验证性,选票受到严密保护,动态地实现了电子选票的秘密性、广义可验证性和公平性.当然,对加密选票的高效传

送及对存在于计算机网络系统中的敌手数量、权限的监测、限制,仍是需要进一步研究的问题.

致谢 在此,我们向对本文的工作给予支持和建议的同行,尤其是中国科学技术大学信息科学技术学院的黄刘生教授、解放军信息工程大学应用数学系马传贵教授领导的讨论班上的同学和老师表示感谢.

References:

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

[2] Cohen JD, Fischer MJ. A robust and verifiable cryptographically secure election scheme. In: IEEE Computer Society, ed. Proc. of the 26th IEEE Symp. on Foundations of Computer Science. New York: IEEE Press, 1985. 372−382.

[3] Magkos E, Burmester M, Chrissikopoulos V. Receipt-Freeness in largescale elections without untappable channels. In: Schmid B, *et al*., eds. Proc. of the 1st IFIP Conf. on ECommerce/E-business/E-Government. Zurich: Kluwer Academics Publishers, 2001. 683−693.

[4] Cranor LF, Cy RK. Sensus: A security-conscious electronic polling system for the Internet. In: Proc. of the Hawaii Int'l Conf. On System Sciences. 1997. http://lorrie.cranor.org/pubs/hicss/

[5] Benaloh J, Tuinstra D. Receipt-Free ballot elections. In: Proc. of the 26th Symp. on Theroy of Computing (STOC'94). Montreal, 1994. 544−553.

[6] Cranor L. Electonic voting: Computerized polls may save money, protect privacy. In: Proc. of the Hawaii Internet of Conf. on System Science. Huawaii, 1997. 116−124. http://www.acm.org/crossroads/xrds2-4/voting.html

[7] Cranor LF, Cytron RK. Design and implementation of a security-conscious electronic polling system. Technical Report, WUCS-96-02, Washington University, 1996.

[8] Martin H, Sako K. Efficient receipt-free voting based on homomorphic encryption. In: Preneel B, ed. EUROCRYPT 2000. LNCS 921, Berlin: Springer-Verlag, 2000. 393−403.

[9] Lee B, Kin K. Receipt-Free electronic voting through collaboration of voter and honest verifier. In: Proc. of the JWISC 2000. Okinawa, 2000. 101−108. http://citeseer.ist.psu.edu/lee00receiptfree.html

[10] Canetti R. Studies in secure multiparty computation and applications [Ph.D. Thesis]. Weizmann Institute of Science, Department of Computer Science and Applied Mathematics, 1995.

[11] Chen XF. Receipt free electronic voting based on semi-trusted model. Chinese Journal of Computers, 2003,26(5):557−562 (in Chinese with English abstract).

附中文参考文献:

[11] 陈晓峰,等.基于半信任模型的无收据的电子投票.计算机学报,2003,26(5):557−562.