第 34 卷 第 20 期 计 算 机 工 程 2008 年 10 月
Vol.34 No.20 Computer Engineering October 2008
·安全技术· 文章编号：1000—3428(2008)20—0184—03 文献标识码：A 中图分类号：TP311

无收据性电子选举方案

王 旭，黄根勋
(解放军信息工程大学理学院数理系，郑州 450001)

摘 要：提出一种多选一的电子选举方案，基于门限 ElGamal 公钥密码体制，选民通过与验证者的交互生成具有向量形式的选票，计票结果不再是一个离散对数难求问题，便于操作，具有无收据性及无强迫性。该方案不仅适用于“多选一”的电子选举，也适用于“多选多”的电子选举，适合于大规模选举。

关键词：电子选举；门限 ElGamal 公钥密码体制；零知识证明

Receipt-free Electronic Election Protocol

WANG Xu, HUANG Gen-xun
(Department of Mathematics and Physics, Institute of Science, PLA Information Engineering University, Zhengzhou 450001)

【Abstract】This paper proposes receipt-free electronic election protocol by using the threshold ElGamal cipher. Every voters have a ballot of vector form. Result of the election is not a difficult discrete logarithm problem, so it is more applicable. The scheme is of receipt-freeness and incoercibility. It can be applied to the case of 1-out-of-L as well as the case of k-out-of-L. The scheme is fit for electronic election protocol of large scale.

【Key words】 electronic election; threshold ElGamal cipher; zero-knowledge proof

1 概述

随着计算机技术和网络通信技术的发展，人们可以借助计算机网络提供一种在较短时间内、以较低成本为大量用户所使用的选举方式——电子选举。电子选举的投票系统具有如下安全性要求：(1)秘密性；(2)完整性；(3)稳固性；(4)唯一性；(5)合法性；(6)公正性；(7)可验证性；(8)鲁棒性；(9)广义可验证性；(10)无收据性；(11)无强迫性。其中，(1)~(8)在大多数电子投票方案中得到了满足，而且实现起来也比较容易。但(9)、(10)在实现时常常冲突。当前对电子投票的研究集中于实现同时满足无收据性和广义可验证性的实用电子投票方案。“多选多”(k-out-of-L)的电子选举方案也是电子选举研究的一个重要方面。

“无收据的电子投票”[1]最早由Benaloh和Tuinstra提出，2000 年Byoungcheon Lee和kwangjo Kim提出一种无收据性的电子选举方案[2]，该方案满足上述电子选举方案的基本安全性要求及无收据性，但计票结果的计算是一个离散对数难求的问题，特别是选民规模比较大时，不适用于实际操作。2002 年Byoungcheon Lee和kwangjo Kim对该方案进行了修改[3]，提出了“防篡改智能卡”(tamper-resistant smart card)的概念，在一定程度上解决了秘密信道的瓶颈，但是计票结果的计算仍是一个离散对数难求的问题。

2 预备知识

2.1 ElGamal 公钥密码体制

设 p,q 是一个大素数且 $q|p-1$，g 是有限域 Z_p^* 的一个 q 阶子群 G_q 一个生成元，$s\in Z_q$ 是用户的私钥，$h=g^s \bmod p$ 是公钥，$m\in Z_p$ 是明文消息。对 m 的加解密过程如下：

(1)加密过程

随机选取 $k\in_R Z_q$，计算 $x\equiv mh^k \bmod p$，$y\equiv g^k \bmod p$，$(x,y)=(g^k \bmod p, mh^k \bmod p)$ 就是对 m 加密的密文；

(2)解密过程

$$m\equiv \frac{x}{y^s} \bmod p$$

2.2 门限 ElGamal 公钥密码体制

2.2.1 shamire 门限方案

$s\in Z_q$ 为 n 个主体共享的密钥，每个主体 $A_j(1\le j\le n)$ 拥有一个密钥管理中心(KMC)分发的子密 $s_j\in Z_q$。这些主体中任意 t 个组成的子集 Λ 利用 Lagrange 插值公式及公开的参数计算相应的 Lagrange 系数及自己的子密钥可以计算出秘密 s，为叙述方便，设 Lagrange 系数为

$$\lambda_{j,\Lambda}=\prod_{l\in\Lambda\setminus\{j\}}\frac{l}{l-j}$$

则

$$s=\sum_{j\in\Lambda}s_j\lambda_{j,\Lambda}$$

2.2.2 (t,n)门限 ElGamal 加密方案

p,q,g,s,h 的取法同 2.1 节，$(x,y)=(g^k \bmod p, mh^k \bmod p)$ 是相应明文 m 的密文。为了在不重构秘密钥 s 的情况下对密文 $(x,y)=(g^k \bmod p, mh^k \bmod p)$ 进行解密，计票员联合执行以下协议：

(1)计票员 T_j 公布 $\omega_j=x^{s_j} \bmod p$，并利用协议证明 $\log_g h_j=\log_x \omega_j$；

(2)假设 Λ 是通过(1)中零知识证明的 t 个计票员的集合，则 $m=y/\prod_{j\in\Lambda}\omega_j^{\lambda_{j,\Lambda}}$。

作者简介：王 旭(1981－)，男，硕士研究生，主研方向：信息安全；黄根勋，副教授、博士

收稿日期：2007-11-13 **E-mail：**wangxu450001@sohu.com

而如果参与者的个数小于 t，则无法重构 s，也就无法解密选民的选票。

2.3 同指数零知识证明方案

基于有限域上的 ELGamal 公钥体制的同指数零知识证明可以描述为：一个人(设为 Prover)想向另一个人(设为 Verifier)证明 $u=g^{\beta}$ 与 $v=h^{\beta}$ 拥有共同的指数 β，而又不暴露 β，即证明 $\log_g{}^u=\log_h{}^v$。基于 ELGamal 公钥体制的同指数零知识证明如下：

证明人(P)　　验证人(HV)

$(u,v)=(g^{\beta},h^{\beta})$

$\omega\in_R Z_q$

$(a,b)\longleftarrow(g^{\omega},h^{\omega})$

$c=H(a,b)$

$r\longleftarrow\omega+\beta c$

$\xrightarrow{a,b,r}$

$g^r\stackrel{?}{=}au^{H(a,b)}$

$h^r\stackrel{?}{=}bv^{H(a,b)}$

2.4 合法性知识证明协议(VKPP)

合法性知识证明协议：假设存在一个明文消息 $m=\{m_1,m_2\}$ 和一个密文 (x,y)，证明人 P 欲向验证人 HV 证明 (x,y) 是对 m 中的某一个明文 m_i 的加密，但并不透漏 m_i 本身，即要证明命题“对于 $m=\{1,X\}$ 和 (x,y)，$\exists m_i\in m$，$k\in Z_q$，使得 $(x,y)=(g^k,h^k m_i)$ 成立”，或者 $\log_g{}^x=\log_h{}^{y/m_1}\vee\log_h{}^{y/m_2}$，VKPP 的协议流程如下：

证明人(P)　　验证人(HV)

$\omega,d_j,r_j\in_R Z_q$

$(a_i,b_i)\longleftarrow(g^{\omega},h^{\omega})$

For　$j\neq i$

$(a_j,b_j)\leftarrow(g^{r_j}x^{d_j},h^{r_j}(y/X)^{d_j})$

$c\leftarrow H(a_1,b_1,a_2,b_2)$

$d_i=c-\sum_{j\neq i}d_j$

$r_i=\omega-\beta d_i$

$(A,B)=(a_1,b_1),(a_2,b_2)$

$(D,R)=(d_1,r_1),(d_2,r_2)$

$\xrightarrow{(x,y)\ \ (A,B)\ \ (D,R)}$

$d_1+d_2\stackrel{?}{=}H(g^{r_1}x^{d_1},h^{r_1}(y/m_1)^{d_1},$

$g^{r_2}x^{d_2},h^{r_2}(y/m_2)^{d_2})$

2.5 加密知识证明协议(EKPP)

加密知识证明协议：对于一个明文消息 m 和一个密文消息(x, y)，证明人 P 欲向一个指定的验证人 HV 证明(x, y)确实是在加密公钥 h 下对 m 的正确加密，即存在一个随机数 k，使得 $(x,y)=(g^k,h^k m)$。假定 s_{HV} 和 $h=g^{s_{HV}}\bmod p$ 分别表示 HV 的私钥和公钥，对 EKPP 协议的描述如下：

证明人 P 执行以下操作：

(1)从 Z_q 中随机选择 ω,r,t；

(2)计算 $(a,b)=(g^{\omega},h^{\omega})$，$d=g^r h_{HV}^t$；

(3)计算 $c=H(a,b,d,x,y)$，$u=\omega-k(c+r)$；

(4)将 (c,r,t,u) 作为证据发送给 HV。HV 判断等式 $c=H(g^u x^{c+r},h^u(y/m)^{c+r},g^r h_{HV}^t,x,y)$ 是否成立，如果成立，表示(x, r)确实是对 m 的正确加密，否则不然。

证明人(P)　　验证人(HV)

$\omega,r,t\in_R Z_q$

$(a,b)\leftarrow(g^{\omega},h^{\omega})$

$d\leftarrow g^r h_{HV}^t$

$c\leftarrow H(a,b,d,x,y)$

$u=\omega-k(c+r)$

$\xrightarrow{(c,r,t,u)}$

$c\stackrel{?}{=}H(g^u x^{c+r},h^u(y/m)^{c+r},$

$g^r h_{HV}^t,x,y)$

2.6 电子公告板协议

投票人和管理员之间，以及管理员和计票人之间的通信信道是一个具有存储能力的公共的广播通道，称为“电子公告板”(BBS)，它应具有以下性质：(1)任何人可以读取它的信息；(2)每一个合法用户可以而且只能在属于他的指定位置写信息；(3)任何人不能擦除他人的信息。

3 协议描述

3.1 参与实体

本文的投票方案包括以下实体：系统管理员，证书管理机构(CA)，m 个投票人 $(v_1,v_2,\cdots,v_m)$，n 个计票人 $(T_1,T_2,\cdots,T_n)$ 及验证人。

3.2 投票协议的过程

本投票协议的过程可分为 4 个阶段：

(1)系统初始化阶段

系统管理员生成 Elgmal 加密体制的公开参数 (p,q,g,h) 及 Z_p^* 上的小整数 $\beta\neq1$，并且 $\beta^m<p$，计票机构执行密钥生成协议，n 个计票人 $(T_1,T_2,\cdots,T_n)$ 和系统管理员联合起来执行(t, n)一门限 ElGama1 加密方案中的密钥生成协议，生成系统的秘钥 s，而且让每个计票人 T_j 获得一个对 s 的共享子密钥 s_j，在公告板上公布以下数据：

1)Elgmal 加密体制的公开参数 (p,q,g,h)；

2) Z_p^* 上的小整数 $\beta\neq1$；

3)计票人公布对自己的共享密钥 s_j 的承诺 $h_j=g^{s_j}$。

(2)注册阶段

选民向 CA 注册，CA 向每一位合法的选民颁发数字证书，选民获得投票权，CA 在公告板上公布所有合法的选民的数字证书。

(3)投票阶段

投票人 v 和验证者联合起来产生最终的加密选票，主要步骤如下：

1)选民 v 按照自己的意愿对 L 个候选人 $(p_1,p_2,\cdots,p_L)$ 表达自己的意愿，给出一个投票向量 $(v_1,v_2,\cdots,v_L)$，其中，

$$v_j=\begin{cases}1 & v\text{不选候选人}p_j\\ \beta & v\text{选候选人}p_j\end{cases}$$

2)选民 v 对 1)中投票向量的每个分量进行加密得最初选票(First Ballot, FB)：

$$FB=\{(x_1,y_1)(x_2,y_2)(x_L,y_L)(x_{L+1},y_{L+1})\}=$$
$$\{(v_1y^{z_1}\bmod p,g^{z_1}\bmod p)(v_2y^{z_2}\bmod p,g^{z_2}\bmod p)\cdots$$
$$(v_Lh^{z_L}\bmod p,g^{z_L}\bmod p)(v_{L+1}=\prod_{j=1}^{L}v_j h^{\sum_{j=1}^{L}z_j},g^{\sum_{j=1}^{L}z_j})\}$$

其中，z_j 是对 v_j 进行加密的随机数。

3)选民向验证者提供数字证书 $Cert_v$ 和选票 FB 及自己对

选票 FB 的签名 $Sign_{sv}(FB)$ (sv 是选民 v 用于签名选票的私钥)，计算选票 FB 合法性证据，其中，包括选票 FB 的前 L 项的合法性证据集 $VP=\{VP_1,VP_2,\cdots,VP_L\}$ 及最后一项对 X 加密的证据 EP，并将 EP 和 VP 及它们的签名 $Sig_{sv}(EP),Sig_{sv}(VP)$ 发送给验证者。

4)验证者通过选民的数字证书验证选民身份的合法性，通过选民的合法性证据 EP 和 VP 验证选票的合法性，随机选取 $\beta\in Z_q$，计算 $(u,v)=(g^{\beta},h^{\beta})$，计算它的同指数证据 CE，计算最终选票

$$LB=\{(x_1',y_1')(x_2',y_2')\cdots(x_L',y_L')(x_{L+1}',y_{L+1}')\}=$$
$$\{(x_1u,y_1v)(x_2u,y_2v)\cdots(x_Lu,y_Lv)(x_{L+1}u,y_{L+1}v)\}$$

并利用自己的私钥 SHV 对 LB, EP, VP, CE 分别签名，得到 $Sign_{SHV}(LB),Sign_{SHV}(EP),Sign_{SHV}(VP)$, $Sign_{SHV}(CE)$，然后将 $LB\|CE\|Sign_{SHV}(LB)\|Sign_{SHV}(EP)\|Sign_{SHV}(VP)\|Sign_{SHV}(CE)$ 发送给选民 v。

5)选民计算 (u,v)，通过 CE 验证对选票再加密的正确性，对 LB 签名得到 $Sign_{SV}(LB)$，将 $LB\|Sign_{SV}(LB)\|Sign_{SHV}(LB)$ 发送到公告板上。这样在公告板上得选票集如下：

$$LB_1=\{(x_{11}',y_{11}')(x_{12}',y_{12}')\cdots(x_{1L}',y_{1L}')(x_{1L+1}',y_{1L+1}')\}$$
$$LB_2=\{(x_{21}',y_{21}')(x_{22}',y_{22}')\cdots(x_{2L}',y_{2L}')(x_{2L+1}',y_{2L+1}')\}$$
$$\cdots$$
$$LB_m=\{(x_{m1}',y_{m1}')(x_{m2}',y_{m2}')\cdots(x_{mL}',y_{mL}')(x_{mL+1}',y_{mL+1}')\}$$

(4)计票阶段

等过了投票的最后期限，系统就不再接受选票，开始如下计票过程：

1) 管理员 A 从 BBS 上收集所有的合法选票 $LB_i(1\le i\le m)$。为方便起见，假设所有投票人提交的选票都是合法的，即合法选票的个数为 m。

2)A 计算合法选票中同列加密选项的乘积，得

$$(X,Y)=\{(X_1,Y_1),(X_2,Y_2)\cdots(X_L,Y_L),(X_{L+1},Y_{L+1})\}=$$
$$\{(\prod_{i=1}^{m}x_{i1},\prod_{i=1}^{m}y_{i1})(\prod_{i=1}^{m}x_{i2},\prod_{i=1}^{m}y_{i2})\cdots$$
$$(\prod_{i=1}^{m}x_{iL},\prod_{i=1}^{m}y_{iL})(\prod_{i=1}^{m}x_{iL+1},\prod_{i=1}^{m}y_{iL+1})\}$$

并将其发布到公告板上。

3)n 个计票人联合起来执行(t, n)一门限 ElGama1 加密方案中的解密协议，从 (X_j,Y_j) 中计算得出 $W_j=Y_j/X_j^{s}$。由于 s 被 n 个计票人按照特定的方式秘密共享，因此只要有 t 个计票人诚实合作，就一定能得出 W_j，而且无须在计算过程中重构 s。通过解密，可得

$$W=(W_1,W_2,\cdots,W_L,W_{L+1})=(\beta^{r_1},\beta^{r_2},\cdots,\beta^{r_L},\beta^{r_{L+1}})$$

即投票结果，$r_j(1\le j\le L)$ 表示第 j 个候选人所得的票数，且满足 $\sum_{j=1}^{L}r_j=r_{L+1}$。由 β 的取法可知，要得出 $r_j(1\le j\le L+1)$ 的值不再是离散对数难求问题。

4 安全性分析

本文的投票方案能够满足电子投票的安全性要求，分析如下：

(1)秘密性：在计票过程中并不对单个选票解密，而是对所有合法加密选票中的各个独立的加密选项的乘积进行解密，得到最终的投票结果。即使有 l 个计票人和“买选票者”相勾结，试图解密某个投票人的加密选票，但由于不诚实的选民个数 $l<t$，因此他们的企图不会成功。

(2)完整性：所有投票人的选票和相应的证据，以及投票人和验证者的签名都发布在公告板上，因此，任何人都可以验证这些选票的合法性，以及选票收集和投票结果的正确性，从而确保了所有合法选票都能被正确计入。

(3)稳固性：由于不诚实的选民不能通过合法性证明协议，因此不合法的选票不会被验证者签名，不会被计票，从而保证了投票的稳固性。

(4)唯一性：每个选民只能在公告板上公布一张自己签名的选票，保证了选票的唯一性。

(5)合法性：只有经过注册合法的选民才能参加选举，保证了合法性。

(6)公平性：选民和验证者都得不到对方任何部分信息，保证了选举的公平性。

(7)鲁棒性：使用的(t, n)门限 ElGama1 加密方案保证了只要有 t 个计票人诚实合作，就能使投票顺利进行下去，得到最终的投票结果。因此，即使有 $l(l\le n-t)$ 个计票人不合作或出现问题，系统也能正常运作。

(8)无收据性：由于选民 v_i 最终的选票

$$LB_i=\{(x_{i1}',y_{i1}')(x_{i2}',y_{i2}')\cdots(x_{iL}',y_{iL}')(x_{iL+1}',y_{iL+1}')\}$$

是选民的第一张选票

$$FB_i=\{(x_{i1},y_{i1})(x_{i2},y_{i2})\cdots(x_{iL},y_{iL})(x_{iL+1},y_{iL+1})\}$$

的每一个分量与验证者产生的随机对 $(u,v)=(g^{\alpha},h^{\alpha})$ 相乘得到的，因此选民要证明自己选了第 j 个候选人，即要证明

$$(x_{ij}',y_{ij}')=(\beta h^{z_{ij}+\alpha},g^{z_{ij}+\alpha})$$

则选民要出示 $Z_{ij}+\alpha$，这是做不到的，不能提供收据证明自己选的是某候选人。

(9)广义可验证性：任何人可以根据公告板上发布的选票、证据和签名信息来验证每个选票的合法性，同时所有合法加密选项的乘积以及计票的最终结果也是公共可验证的。

5 结束语

本文对文献[1]的电子选举方案作了改进，通过使用知识证明协议 EKPP, VKPP，给出了一个“1-out-of-L”的无收据的电子选举方案。理论分析和实验验证表明该方案是无收据的，而且满足了电子投票的安全性需求，具有很好的实用性。与文献[1]方案的性能相比，该方案可迅速计算选举结果，是高效的且可用于大规模选举。同时，在选民生成选票 FB 阶段中，只要将 FB 最后一项的加密证据更改为对 β^k 加密，就可在不增加复杂性的情况下将原协议扩展为“k-out-of-L”的无收据的电子选举方案。

参考文献

[1] Benaloh J, Tuinstra D. Receipt Free Secret-ballot Elections[C]//Proc. of the 26th Symp. on Theory of Computing. New York, USA: [s. n.], 1994.

[2] Hirt M, Sako K. Efficient Receipt Free Voting Based on Homomorphic Encryption[C]//Proc. of EUROCRYPT'00. [S. l.]: Springer-Verlag, 2000.

[3] Lee B, Kim K. Receipt-free Electronic Voting Scheme with a Tamper-resistant Randomizer[C]//Proceedings of ICISC'02. [S. l.]: Springer-Verlag, 2002.