第35卷 第13期 计 算 机 工 程 2009年7月
Vol.35 No.13 Computer Engineering July 2009
·安全技术· 文章编号：1000—3428(2009)13—0137—02 文献标识码：A 中图分类号：TP393.08

基于匿名消息广播的电子选举方案

唐西林[1]，杨智勇[1]，杨长海[1,2]
(1. 华南理工大学理学院，广州 510640；2. 南昌陆军学院科文教研室，南昌 330103)

摘 要：利用盲签名和匿名消息广播技术，并根据选票形式的结构差异，构造普通选票和超级选票模型，提出一种具有超级选票的电子选举方案，使特权选民不但拥有超级选票的投票权，而且可拥有投普通票以及弃权票的机会，仿真实验结果表明，该方案满足电子选举的基本安全要求，适合小规模的电子选举，具有一定应用价值。

关键词：超级选票；盲签名；中央制表机构

Electronic Voting Scheme Based on Anonymous Message Broadcast

TANG Xi-lin[1], YANG Zhi-yong[1], YANG Chang-hai[1,2]
(1. College of Science, South China University of Technology, Guangzhou 510640;
2. Teaching & Research Room of Science & Arts, Nanchang Military Academy, Nanchang 330103)

【Abstract】By using technology of blind signature and anonymous broadcast, and according to different structures of common vote and super ballot, the models of both of them are set up. The electronic voting scheme with super ballot is proposed, which makes privileged voters have the rights to vote super ballot, common ballot and abstention ballot. Experimental results show this scheme meets basic security of election scheme and is suitable for electronic voting in a small scale. It has the value of application.

【Key words】super ballot; blind signature; central tabulating facility

1 概述

自上世纪80年代，文献[1]提出第1个电子选举方案以来，电子选举就凭借其高效、安全的优点逐步取代传统的人工选举。在这个过程中，随着零知识证明、盲签名、位委托及ANDOS(All-or-Nothing Disclosure Of Secrets)等密码技术在电子选举中的应用，电子选举的形式更多样化，功能也更强大，使得电子选举除了能达到实际选举同样安全性，即满足选民身份合法性、投票的保密性、计票的完整性及选举结果的可验证性等基本要求外，还使一些电子选举方案满足无收据性、选票的完善保密性、计票的公平性和无争议性等新的要求[2]。

电子选举方案按选票的权重分有2类：(1)电子选举方案各选票权重相同，即所谓的普通电子选举；(2)在选举中有特权选民，由于他们比其他人拥有更大的权利，因此可以投超级选票，当然特权选民也可以放弃自己的特权而投普通票及弃权票。这类有超级选票的选举在现实生活中确实存在，它可以是公司结构的一部分，在这里某些人有比其他人更大的权利或者他是联合国做法的一部分，其中，某些国家比其他国家有更大的权利。

文献[3]提出带有超级选票的选举问题，提出存在一个七方委员会，他们定期开会对一些问题秘密表决，其中有两方有超级选票。有些学者提出一个一票否决的电子选举方案，并且利用多方计算解决了选民同时得到选举结果的解决方案。文献[4]提出了一个具有完善保密性和自披露性的匿名广播协议。

本文基于盲签名并改进了Gorth J提出的匿名广播协议，得到一个可以投超级选票的电子选举方案[4]，其安全性依赖于盲签名和零知识证明的安全性，而其选票的完善保密性、计票的公平性和无争议性等则依赖于Gorth J的匿名消息广播协议的安全性。经分析，改进的方案在小规模的电子选举中具有较高的效率。

2 相关概念

本文在文献[5]的基础上提出以下几个名词，并将其作为具有超级票的电子选举安全性的必要条件，现作如下解释：

(1)特权选民：指该选民拥有比其他选民更大的权利，他可以投出直接否决被选举人的一票，当然他也可以放弃特权改投普通票。

(2)自披露性：一旦最后一个投票者发送出消息，任何人都可以知道所有选票的内容。

(3)弱完善保密性：对于选票不同的2组选民，只有其中一组选民中的N-t个串通起来才能得到本组剩余t个选民的选票，而无法得到其他组任何选民的选票内容。

3 电子选举

3.1 电子选举模型

(1)通信信道。通信信道采用授权的广播信道模型[2]。

(2)参与方。设有 N 个特权选民，M 个普通选民，共计 n 个人，即 $n=N+M$。

(3)选票结构。令 $V_i = a^{k_i}b^{l_i}c^{p_i}d^{t_i}$，其中，$a, b, c, d$ 为 q 阶群 G_q 中的元素；$k_i, l_i, p_i, t_i \in \{0,1\}$，$i=1, 2, \cdots, n$。在超级选票中，赞成、反对、弃权分别表示为 $a^0b^1, a^1b^0, a^0b^0=1$；在普通选票中，赞成、反对、弃权分别表示为 $c^0d^1, c^1d^0, c^0d^0=1$。

基金项目：国家自然科学基金资助项目(10571061)
作者简介：唐西林(1962－)，男，教授、博士，主研方向：代数和密码学；杨智勇，硕士研究生；杨长海，讲师、硕士研究生
收稿日期：2009-01-25 **E-mail：**xilintang@21cn.com

3.2 电子选举方案

假设选民都是合法的投票人，方案分为获取证书、注册、表决、计算选票 4 个阶段。其中，获取证书可以利用基于 RSA 的盲签名技术[6]，签名的公钥为 e，私钥为 d，k 为安全参数。

(1)获取签名证书

1)CTF(中央制表机构)随机选择一个大的随机数 R_0，并以广播的形式发送给各个选民。

2)普通选民准备 N_0 份小于 R_0 的随机数组成的文件，特权选民选取一个大于 R_0 随机数组成的文件。

3)若 P_i 为普通选民，则用不同的盲因子隐藏每份文件，并把这 N_0 份文件连同自己的身份 ID_i 发送给 CTF，若 P_i 为特权选民则随机选择一个盲因子隐藏文件并连同自己的身份 ID_i 发送给 CTF。

4)CTF 对普通选民 P_i 发送的 N_0 份文件中随机选择 N_0-1 份文件，并向 P_i 索要每份文件的盲因子，而对特权选民的文件直接签名，然后发给 P_i。

5)CTF 打开普通选民的(去掉盲因子) N_0-1 份文件，并相信他们是正确的，然后对第 N_0 份文件签名并把它发送给 P_i。

6) P_i 把所得签名脱盲后得到 $S_K(R_i)$。

(2)注册

该协议在上述的一个阶为素数 q 的群 G_q 上进行，g 为 G_q 的生成元。选民 P_i 随机选择一个与 q-1 互素的元素 x_i，计算 $h_i = g^{x_i} \bmod q$，并公布 h_i，利用零知识证明其知道 x_i。任何不公布 h_i 和不能证明其知道 x_i 的选民将被取消选举资格。

(3)表决

选民投票的顺序由匿名消息广播协议决定。

1)选民 P_1 选择随机数 r_1，投出选票 $(s_1,u_1,v_1)=(S_K(R_1), g^{r_1},(\prod_{j=2}^{n} h_j)^{r_1}V_1)$，把 (s_1,u_1,v_1) 以匿名广播形式发送出去，并把自己正确按照协议进行的证明以附加消息的形式按匿名广播协议发送出去。

2)选民 P_2 首先检查 P_1 按照协议进行的证明，然后选择随机数 r_2，加密自己的投票为 $(s_2,u_2,v_2)=(S_K(R_2), g^{r_2}, (\prod_{j=2}^{n} h_j)^{r_2}V_2)$，并利用自己的私钥 x_2 计算出 $v_1' = u_1^{-x_2}$，$v_1 = (\prod_{j=3}^{n} h_j)^{r_1}V_1$ 和 $v_2' = u_2^{-x_2}V_2 = (\prod_{j=3}^{n} h_j)^{r_2}V_2$，将 (s_1,u_1,v_1') 和 (s_2,u_2,v_2') 通过置换后发送给 p_3。

3)假设 S 表示已经投出选票的选民的集合，T 表示未投票的选民的集合，当选民 P_i 投票时，S 包含 i。设 $\{(s_j,u_j,v_j)\}_{j\in S\setminus\{i\}}$ 是 P_i 投票时收到的消息。P_i 先检查他收到的选票附加的正确性证明，然后利用自己的私钥 x_i 加密自己的选票为 $(s_i,u_i,v_i)=(S_K(R_i),u^{r_i},(\prod_{j\in T\cup\{i\}} h_j)^{r_i}V_i)$，$P_i$ 利用 S 上的一个随机置换 π_i 将 $\{(s_j,u_j,v_j)\}_{j\in S}$ 置换为 $\{(s_j',u_j',v_j')\}_{j\in S}$，并利用自己的私钥 x_i 计算 $\{v_j = v_j' u_j^{-x_i}\}_{j\in S}$，则选票变为 $\{(s_j,u_j,v_j)\}_{j\in S} = (S_K(R_j), g^{r_j},(\Pi_{j\in T} h_j)^{r_j}V_j)$。$P_i$ 将其以广播形式发送给下一个选民，并附上其遵守协议的证明。

4)最后一个选民计算出 $\{(s_j,u_j,v_j)\}_{j\in S} = \{(S_K(R_j), g^{r_j},V_j)\}_{j\in S}$。为防止最后一个选民先知道投票结果，可使 CTP 作为最后一个选民投出 $(S_K(R), g^{r_0},(\Pi_{j\in T} h_j)^{r_0}V_o)$，计算出 $\{(s_j,u_j,v_j)\}_{j\in S} = \{(S_K(R_j), g^{r_j},V_j)\}_{j\in S}$，其中，$h_0 = g^{x_0}$；$r_0$ 为 CTP 选择的随机数，并将 $\{(S_K(R), g^{r_j},V_j)\}_{j\in S}$ 发给所有投票者。

(4)计票阶段

CTP 根据 $\{(S_K(R), g^{r_j},V_j)\}_{j\in S}$ 计算各张选票内容，将所得各种选票结果相加，并公布选举结果。

(5)检验

CTP 在公布选举结果的同时，公布所有选民的签名证书列表 $S_K(R_i)$，若选民怀疑某些普通选民投出超级选票，可通过 CTF 的公钥对签名证书进行鉴别。同时各选民亦可通过 CTP 公布的选票检查自己的选票是否被正确统计，并自行计算投票结果。

4 性能分析

(1)匿名性。由于选票的内容被加密，在投票阶段任何人无法知道内容，且任何人只能在最后把超级选票和特权选民联系起来，而普通选民只能和普通选票联系起来，因此具有匿名性。

(2)公平性。在投票阶段需要全体选民包括 CTF 的参与，而只有当每个 P_i 都使用自己的 x_i 对选票进行解密后才可以计票，同时由于 CTF 作为最后一个选民参与，因此单个选民即使与其他选民合作也无法提前计票，即该方案具有公平性。

(3)弱完善保密性。由于投票人把 CTF 的盲签名证书作为身份，因此只有当 N 个特权选民中的 $N-1$ 个串通才能得到另外一个特权选民的秘密选票。同样只有当 M 个特权选民中的 $M-1$ 个串通才能得到另外一个普通选民的秘密选票。

(4)计票的完整性。任何选民都可以通过 CTF 最后发送的消息 $\{(S_K(R_j), g^{r_j},V_j)\}_{j\in S}$ 查看自己的选票是否被统计进去。

(5)无争议性。全体选民根据 $\{(S_K(R_j), g^{r_j},V_j)\}_{j\in S}$ 共同统计选举结果，若一个或少数 P_i 公布结果与多数人公布结果不同，则证明其欺骗性。

(6)可检验性。任何选民都能利用 CTF 发送的信息 $\{(S_K(R_j), g^{r_j},V_j)\}_{j\in S}$ 计算选举结果，从而验证选举结果是否正确。

(7)健壮性。如果有 m 个合格候选人中途退出，则将导致选举无法进行，由于是小规模的电子选举方案，因此可以让剩余的 $n-m$ 个选民重新进行投票，方案具有健壮性。

5 计算复杂度

每个选民进行 $O(1)$ 次运算来完成密钥注册，每个密钥的大小为 $O(k)$。为证明密钥的正确性需用 $O(n)$ 次运算，在投票阶段利用文献[7]的方法，通过 $O(n)$ 运算来计算新的密文组和知识证明，这样一个组的大小为 $O(nk)$。共需 $O(n^2)$ 运算来验证所有选民的证明。

6 结束语

电子选举正在以不可逆转的趋势代替传统的人工选举，在这一过程中问题接踵而至，对电子选举安全性及其他性能的要求也越来越高。本文讨论在具有超级选票的情况下实现安全电子选举的安全有效途径，在基于 DDH 问题的困难性和离散对数的零知识证明安全性的前提下，提出一个适合小规模选举的电子选举方案，经分析满足电子选举的安全性要求。该方案的缺点是安全性依赖于可信的第三方 CTF，如何在没有可信第三方的情况下构造具有超级选票的电子选举是值进一步研究的问题。

(下转第 159 页)