基于 Harn 部分盲签名的安全电子投票方案

徐玲

中山职业技术学院计算机工程系 广东 528404

摘要：本文设计了一种新的 Harn 部分盲签名方案，并将此方案用于电子投票的设计中，形成了一个安全可靠的电子投票方案。这种电子投票方案不仅保证了投票者身份的匿名性和选票的安全、公平、保密性，还能实现投票的不可抵赖性。此方案是传统的盲签名电子投票方案的一个改进，是一个很实用的方案。

关键词：数字签名；电子投票；Harn 签名；部分盲签名

0 引言

本文利用 Harn 签名及其部分盲化性，提出了一个种基于 Harn 部分盲化签名的电子投票方案。此方案不仅保证了投票者身份的匿名性和选票的公平性、保密性，而且签名的部分盲化还能实现投票的可追踪性及不可抵赖性，从而令电子投票顺利进行，具有实用性。

1 基于 Harn 签名的部分盲签名

1.1 Harn 签名

设 p 为一个大素数，g 是 $GF(p)$ 的本原元，$H(\bullet)$ 是单向散列函数。每个用户都有一个私钥 $x\in[1,p-1]$ 且 $\gcd(x, p-1)=1$，公钥 $y=g^x(\mathrm{mod}\,p)$，待签的信息 $m\in[1,p-1]$。签名时，用户首先随机选择一个整数 $k\in[1,p-1]$，满足 $\gcd(k,p-1)=1$，然后计算 $r=g^k(\mathrm{mod}\,p)$ 和 $s=[x(H(m)+r)-k]\ \mathrm{mod}(p-1)$，由此得到消息 m 的签名为 $sig(m)=(r,s)$。验证时，通过计算 $y^{H(m)+r}=rg^s(\mathrm{mod}\,p)$ 来验证签名的有效性。

1.2 Harn 签名的部分盲化

设 A 为消息拥有者，B 为签名者，待签名的消息为 m，A 和 B 共同商定一个常数 c，称为部分盲因子，以便无须商量，在签名协议过程中使用。c 的长度为 $(k-2)$ bits，计算 $\tau(c)=2^{k-1}+2H(c)+1$，其中 $H(\bullet)$ 同上，$\tau(c)$ 的取值范围必须在 $2^{k-1}<\tau(c)<2^k$，当 $i\neq j$ 时，$\tau(c_i)$ 与 $\tau(c_j)$ 不能相互整除。签名者 B 的签名私钥为 $x\tau(c)$，相应的公钥为 $y=g^{x\tau(c)}\ \mathrm{mod}\,p$。基于 Harn 签名部分盲签名方案如下：

(1) A 与 B 商定一个常数 c，c 为签名者的信息或者签名者与用户商定的信息。

(2) 签名者 B 随机选取 $k\in Z_p$，计算 $r'=g^k\ \mathrm{mod}\,p$，并发送 r' 给用户 A。

(3) 用户随机选择 $t_1\in Z_p^*$，$t_2,t_3\in Z_p$，计算 $r=r'^{t_1}g^{t_2}y^{t_3}\ \mathrm{mod}\,p$，$m'=\left[(r+H(m,c)-t_3)t_1^{-1}-r'\right]\mathrm{mod}(p-1)$ 发送 m' 给签名者。

(4) 签名者计算 $s'=\left[x\tau(c)(m'+r')-k\right]\mathrm{mod}(p-1)$，发送 s' 给用户。

(5) 用户验证 $r'g^{s'}=y^{r'+m'}\ \mathrm{mod}\,p$ 是否成立，若成立，计算 $s=(s't_1-t_2)\mathrm{mod}(p-1)$，并公布 (r,s,c) 时关于消息 m 和公共信息 c 的部分盲签名。否则，输出“False”。

验证，任何人可通过检查 $rg^s=y^{r+H(m,c)}\ \mathrm{mod}\,p$ 来验证签名的有效性。

本文根据文献的效率比较结论，采用 $(t_1,t_2,t_3)=(1,t_2,t_3)$ 的方案，因为在签名阶段没有求逆运算，所以在 3 个方案中效率最高。

2 电子投票方案

2.1 方案概述

方案的参与者：投票人 V，发票中心，认证中心，投票中心，计票中心及验票中心(如图 1)。

(1) 投票人 $V_i(i=1,\cdots,n)$：表示可有 n 个投票人参与投

作者简介：徐玲(1983-)，女，硕士研究生，研究方向：网络安全。

票，在投票系统中事先导入应参与投票人的名单；

(2) 发票中心：发放选票及公钥，同时投票人利用私钥在所得选票进行签名；

(3) 认证中心：对投票人进行身份验证，投票人将选票进行部分盲化；

(4) 投票中心：投票人进行投票，投票结束后，被终止投票权利；

(5) 验票中心：根据选票可验证选票及投票人的有效性；

(6) 计票中心：统计选票，公布结果。

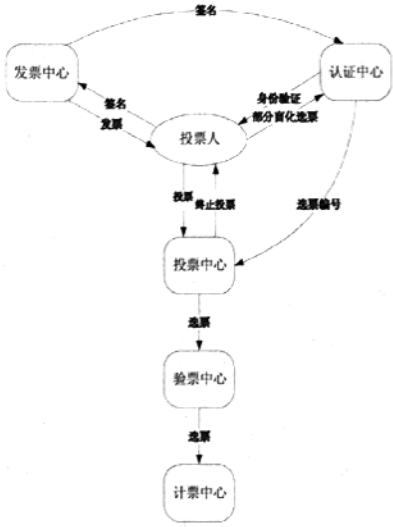

图 1 电子投票方案框架图

2.2 发票阶段

投票人以匿名的身份申请选票，为保证投票的保密性，选票的编号 $k(k=1,\cdots,n)$ 由投票系统随机分配，要保证每位投票人的选票编号不同，而且任何人或机构都不能知道和预测投票人与选票的分配情况。在每张选票上还有一个有效性标志 L，且 $L\in\{0,1\}$，当选票有效时，$L=1$，否则 $L=0$，这样可以防止一个投票人参与多次投票。

在投票前，举办方与所有应参与投票者商定一个公共信息 c，发票中心先选取一个大素数 p，同时还为每位投票人选取整数 x_i，并计算 $x_i\tau(c)$ 为投票人的 V_i 的私钥，$y_i=g^{x_i\tau(c)} \bmod p$ 为其相应的公钥，投票人随机选择 $k\in Z_p$，计算 $r'=g^k \bmod p$，将 (ID_i,r') 作为签名发送给发票中心，ID_i 是投票人的身份证号。

2.3 认证阶段

认证中心先验证签名中 ID_i 是否为合法投票人的身份证号，且是否在投票系统中，若均为是，则进行签名验证。

发票中心将签名发送给认证中心，认证中心随机选择 $t_1\in Z_p^*$，$t_2,t_3\in Z_p$，上节中令 $t_1=1$，计算 $r=r'g^{t_2}y_i^{t_3} \bmod p$，$m'=\left[\left(r+H(m,c)-t_3\right)-r'\right]\bmod(p-1)$，发送 m' 给投票人，投票人计算 $s'=\left[x\tau(c)\left(m'+r'\right)-k\right]\bmod(p-1)$，发送 s' 给认证中心，认证中心验证 $r'g^{s'}=y^{s'+m} \bmod p$ 是否成立，若成立，投票人为有效投票人，计算 $s=\left(s'-t_2\right)\bmod(p-1)$，公布 (r,s,c)，由此选票被部分盲化。

2.4 投票阶段

认证中心将验证有效的投票人的编号发送给投票中心，投票中心按接收的编号给每张选票发放待投票的文本 M，选票初始值为 0，有效值为 4、2、1，分别代表赞同、反对和弃权。投票人收到选票内容后，根据自己的态度为选票赋予相应的有效值，然后利用 Hash 函数得出 $H(M)$，再使用投票中心的公钥 e 进行加密该选票，得到 $E(M,H(M))$，将其发送给投票中心。

投票中心收到投票人的加密选票后，将该选票的有效性修改为 $L=0$。

2.5 验票阶段

在规定时间结束后，投票中心宣布终止投票，并将加密选票 $E(M,H(M))$ 和盲化签名 (r,s,c) 一起发送给验票中心。验票中心解密选票，首先验证选票是否是有效值，选择有效选票，然后对有效选票进行脱盲运算，验证投票人的合法性，最后将有效投票人的有效选票发送给计票中心。

2.6 计票阶段

计票中心收到有效选票后，统计投票结果，并通过投票系统公告公布投票结果。

3 方案安全性分析

合法性：投票人虽然以匿名申请选票，但是需将身份证 ID 随签名一并发给认证中心，认证中心首先要验证投票人的 ID 是否是投票系统中合法的投票人，由此可以保证合法的投票者参与投票，非法投票人即使申请到选票仍然无法参与投票。

保密性：选票采用盲签名技术，隐藏了投票人的身份，并且选票在传输过程中是加密的，隐藏了选票内容，因此无法把选票和具体投票人联系起来，从而确保了投票的保密性。

不可重复性：任何一名合法投票人只能投一张票，且认证中心只进行一次验证，若重复验证，则视为无效投票人。因此，投票人就不可能重复投票。

可验证性：选票是部分盲化，任何人无法伪造投票结果，

万方数据

投票结果可以被任何感兴趣的第三方检验，同时不泄露投票者的隐私；而且投票人可以检验自己的投票是否被正确计入计票结果，又不能抵赖参与投票的事实。

完备性：参与投票的选票均由发票中心发放，并标有惟一的编号，防止了非法伪造选票的情况发生，避免出现选票冲突的问题，以保证合法投票人的有效选票都计入投票结果。

健壮性：规定有投票资格的投票人未参与投票的作弃权处理，而参与投票的投票人必须提交有效的投票才能计入投票结果中。若有非法投票人欲参与投票，则在认证阶段中将阻止其继续参与投票，确保投票顺利进行。

4 结束语

本文结合 Harn 的部分盲签名技术提出了一个安全的电子投票方案。为了避免非法投票人冒充合法投票人参与投票，扰乱投票秩序，改变传统的完全盲签名投票，采用部分盲化签名方案，既能满足投票过程的保密性，也能通过半盲化选票追踪投票过程，防止中间任意一方，甚至投票人的欺诈行为。具有一定的安全性和实用性。

参考文献

[1]Wade Trappe,Lawrence C. Washington.密码学概论[M].北京:人民邮电出版社.2004.

[2]赵泽茂.数字签名理论.北京:科学出版社.2007.

[3]禹勇,杨波,杨国庆,张琴.Harn 签名的部分盲化.计算机工程.2007.

[4]Abe M,Fujisaki E. How to Date Blind Signatures[C]//Proceedings of Asiacrypt'96.Berlin: Springer-Verlag.1996.

[5]赖璀,范玉顺.一种新的安全、实用的电子投票方案.计算机科学.2003.

Secure electronic voting scheme based on Harn partial blind signature

Xu Ling

Zhongshan professional technology institute computer engineering department,Guangdong,528404,China

Abstract: In this paper,a new Harn partial blind signature method is built up,which was then applied to the designation of a secure and reliable electronic voting scheme.In this electronic voting scheme,the voters are anonymous,the votes are confidential,and the whole process of voting keeps secure and fair.Moreover,once the votes are voted,they are undeniable.As an improvement of traditional electronic voting schemes,this electronic voting scheme is very practical.

Keywords: Digital signature;Electronic voting; Harn signature;Partial blind signature

[上接 22 页]

参考文献

[1]曾旷怡,杨家海.访问控制列表的优化问题[J].软件学报.2007.

[2]Malik.王宝生,朱培栋,白建军译.网络安全原理与实践[M].北京:人民邮电出版社.2008.

[3]周游.校园网络安全解决方案之访问控制列表.电脑知识与技术.2009.

[4]刘军,王彩萍.ACL 在 IP 网络中的应用[J].计算机与数字工程.2009.

[5]贺斌.徐小华利用访问控制列表构建安全网络[J].科技信息.2010.

Security Strategies of Constructing a LAN Based on the Switch Technology

Meng Li

Library of Beijing Forestry University,Beijing,100083,China

Abstract:LAN technology has become very mature.Generally speaking its mainstream network model takes Gigabit three layer switches as the core to protect the various important resource servers.The paper puts forward security strategies of constructing a LAN based on the switch technology including optimum using VLAN,access control list,port security etc.

Keywords:LAN; Switch;VLAN;Access Control List;Security strategy

万方数据