文章编号：1005-8451（2005）12-0004-03

中铁信董事表决系统的设计及实现

王 刚[1]，陈光伟[2]，韩 臻[1]，危国洪[2]
（1.北京交通大学 软件学院，北京 100044；2.铁道部信息技术中心，北京 100844）

摘 要：在网络投票系统中，如何确保投票者的隐私以及确保投票有效是系统的关键。在对目前流行的几种投票协议分析的基础上，针对中铁信集团董事表决系统，提出了如何解决投票问题的具体方案，并在实际开发中实现了该方案。

关键词：网络投票；投票协议；数字签名；盲签名；CTF
中图分类号：TP39 **文献标识码**：A

Design and implementation of Director Voting System

WANG Gang[1], CHEN Guang-wei[2], HAN Zhen[1],WEI Guo-hong[2]
(1.School of Software, Beijing Jiaotong University, Beijing 100044, China;
2. Information Technology Center, Ministry of Railways, Beijing 100844, China)

Abstract: It was a key problem how to ensure the privacy of voter and the validity of voting in electronic voting. It was introduced several popular electronic voting protocols, proposed a solution to the key problem and implemented it in Director Voting System.

Key words: electronic voting; voting protocol; digital signature; blind signature; CTF

在网络投票系统中如何确保投票者的隐私以及确保投票有效是我们研究的重点，随着数据鉴别技术的成熟和完善，通过身份认证和报文鉴别，已经能较好地解决这个问题。网络投票是指用户通过网络对某个问题采用投票的方式进行表态，分为具名和匿名两种方式。一般来讲，无论具名还是匿名投票，都要满足下列要求：

（1）有授权的投票者可以参加投票；（2）人只能投一票；（3）没有人能够知道别人投票的情况；（4）没有人能够复制别人的投票；（5）没有人能够不被察觉地改变别人的投票；（6）每个投票者可以肯定他的投票被选举管理部门计票了；（7）可以知道谁投了票，谁没有投票。

本文在对目前流行的几种投票协议的研究基础上，提出了基于两个CTF（Central Tabulating Facility）的匿名投票的设计方案。

1 投票协议

要解决网络投票问题，主要是依靠数字签名技术。通过数字签名，可以获得以下安全服务：

同等实体认证，通过同等实体认证可以识别连接的实体的身份，只让授权的实体身份进入投票系统，这样就可以实现要求（1）。

数据完整性，因为数字签名可以保证数据的完整性（即保证数据没有被修改，插入，删除，重放），这样就可以实现要求（4）和（5）。

源不可否认性，数字签名还可证明消息是由特定方发出的，这样再结合具体的算法可以实现要求（7）。必须结合具体的投票协议。

仅通过数字签名技术，不能实现我们提出的所有安全要求，因此我们引入网络投票协议。

1.1 简单投票协议[4]

多数的投票系统都由两部分组成：投票者和记票中心。

最简单的具名投票协议是由CTF公布选票，每个投票人用自己的私钥对选票签名，用CTF的公钥将填写好的选票加密后送给CTF，CTF使用自己的私钥解密收到后的选票，用投票者的公钥检验签名的真实性，然后进行投票统计并公布结果。如果CTF是安全的，则这种办法可满足除（6）外的全部要求。

1.2 基于盲签名的投票协议[4]

盲签名是指签名人并不知道所签文件或消息的具体内容，而文件或消息的拥有者又可以从签名人在盲

收稿日期：2005-05-23
作者简介：王 刚，在读硕士研究生；陈光伟，研究员。

化文件或消息上的签名得到签名人关于真实文件或消息的签名。由于盲签名具有保护签名持有者匿名性的特点，因此很适合用于匿名电子投票协议中。

引入盲签名的目的是实现选票标识的投票者标识的分离，从而实现投票的匿名性，具体的做法基于cut-and-choose原理。协议算法如下：

（1）每个投票者产生10组合法的选票，每组选票都要求用一个足够大的随机数标识（起顺序号作用），从而与其他的选票相区分；（2）投票者将所有选票乘上盲因子，用自己的私钥加密之后送给CTF；（3）CTF首先对投票者的资格进行审查，若允许投票，则选择9组选票进行检查，要求投票者提供对应的盲因子；（4）CTF根据投票者提供的盲因子检查选票的内容，如果合格，则对投票者进行登记，同时对未检查的那个选票进行签名以证明其合法性。CTF将这个签名的选票返回给投票者；（5）投票者消去该选票的盲因子，记住其顺序号，填好内容后用CTF的公钥加密并送给CTF；（6）CTF将选票解密后要验证其签名和顺序号，投票者和顺序号都不允许重复。如果选票合法，则进行记票，同时对选票进行登记；（7）CTF最终公布所有的选票的内容和记票结果，供投票者检查。

通过这个协议，我们可以满足前面提出的要求（1）—（6），但不能防止CTF伪造选票，也不知道谁没投票。

1.3　基于两个CTF的投票协议[5]

基于盲签名的方法不能发现未投票的投票者。为了对投票者的投票情况进行监督，可以采用将申请选票和计票分开的方法。使得前者可以知道谁投了票，但不知道投票者选举的具体内容；后者了解选票的内容，但不知道它是谁投的。前一个CTF称为认证中心（Central Legitimization Agency—CLA），后者仍然称为CTF。协议如下：

（1）每个投票者以真实身份向CLA申请一个合法号码；（2）投票者用这个号码作为选票标识，填写选票后用CTF的公钥加密并送给CTF；（3）CLA保留合法号码与投票者身份的对照表，但将已颁发的合法号码表交给CTF，用以验证选票的合法性和唯一性；（4）CTF对选票进行验证并计票，最终向投票者公布计票结果和合法号码与选票的对照表，供投票者检验计票的正确性；向CLA公布从收到的选票中获得的合法号码表，供CLA检查投票者的投票情况。

这种方法可以说满足网络投票的所有安全要求，但前提是CLA和CTF是安全的和诚实的，因为它们两者联合是可以发现投票者的投票情况的。

2　基于双CTF的董事表决系统的设计及实现

董事表决系统是基于铁道部PKI/CA安全平台的一个应用，该系统目的是要实现多个董事可以在不同的地方实现表决，完成投票。在该系统中最重要的就是用户身份的确认和投票的不可抵赖性。董事和董事长，以及其他可访问此系统的工作人员的权限各不相同，所以身份的确认和权限的分配都是通过PKI/CA平台来完成。

之前的董事表决系统主要实现了具名投票，该系统主要缺点：CTF完全掌握各投票者的投票信息，不能真正满足投票的匿名性。因此，在新设计方案中，表决系统是用双CTF的投票协议来实现匿名投票的，根据前面对双CTF投票协议的描述，投票者和CLA以及CTF的关系如图1，其中的平台是指铁道部统一身份认证和授权平台。

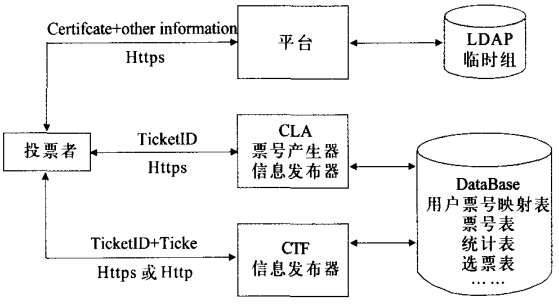

图1　匿名投票示意图

投票者认证授权是通过平台进行的，解决方案与具名投票一致，首先为匿名投票议案建立临时组，然后把相关用户加入到临时组中。投票者到CLA注册之前，先到平台认证授权，然后CLA将检测用户是否已经注册，如果已经注册，则返回原有选票标识，没有则通过票号产生器分配给投票者一个选票标识TicketID，并一同返回CLA对TicketID签名，随后把TicketID和投票者标识UserID对应关系存入用户票号映射表中，UserID采用密文存储方式。

表1　用户票号映射表

MotionID	TicketID	RegisterTime	UserID	SignCLA(MotionID‖TicketID‖RegisterTime‖UserID)

RegisterTime为注册时间。CLA同时把发布的TicketID存储到票号表中，供CTF检索用。

表2 票号表

MotionID	TicketID	SignCLA（MotionID‖TicketID）

投票者与平台和CLA之间以Https协议交互，双向认证，保证通信信道的安全性。

投票者在获取票号后，向CTF提交选票和票号，CTF收到选票数据后，访问CLA的票号表，对提交的票号进行检索，然后验证CLA对票号的签名。检索不成功或者验证有误，则返回用户错误提示信息。确认票号正常后，CTF将对用户提交的数据进行处理，检测用户是否已经投过票，是则用新选票覆盖用户的旧选票，重新签名存储，否则把选票数据存储到选票表中，返回用户投票成功标志。同时CTF还返回它对选票的签名。

表3 选票表

MotionID	TicketID	Attitude	Cause	VoteTime	$Sign_{CTF}$	(MotionID‖TicketID‖Attitude‖Cause‖VoteTime)

投票者可以通过CTF和CLA的信息发布器获得投票结果，获取票号库和选票库进行投票验证，保证投票的公正性。票号库和选票库在选举结束后向投票全体公布。系统匿名表决的流程如图2所示。

匿名模块的设计存在一个假设：CLA和CTF是安全和诚实的，两者不会在表决过程中联合作弊。在这个前提下，匿名投票的7个要求均能满足。并且用户在选举结束之前可以更改自己的投票数据，多次投票。CLA与CTF独立性和安全性通过行政手段和部署方式来保证。它们是两个独立的Web模块，需要部署在不同的服务器上，划归不同职员管理，保证两者的证书独立性。此外数据库系统建立严格的用户管理体系和授权机制也是非常重要的。

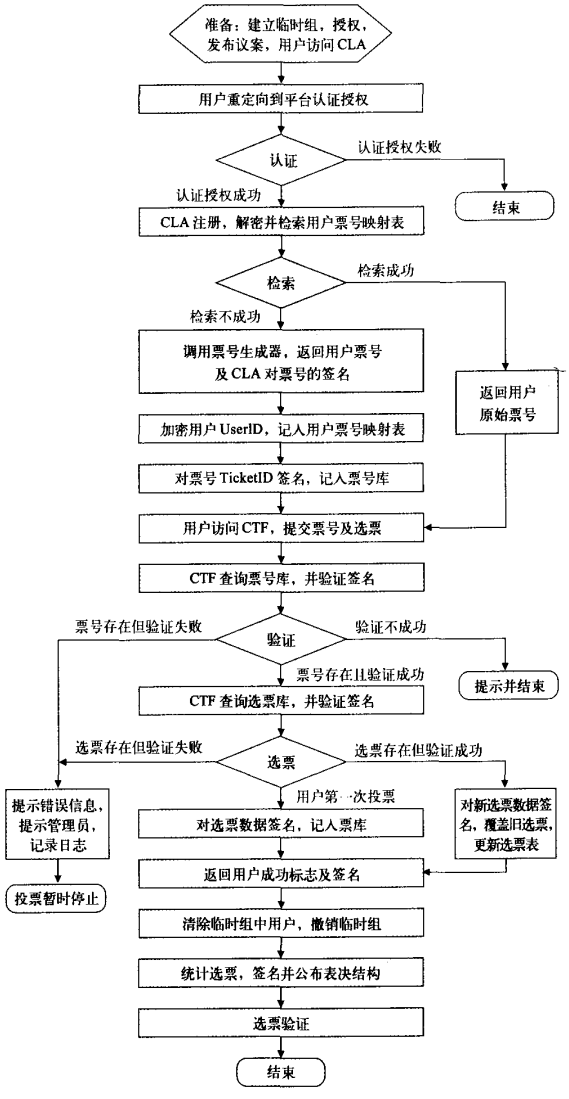

图2 表决系统匿名表决流程图

3 结束语

基于两个CTF的投票协议实际上已能基本实现我们所提出的所有安全要求。但前提是CLA和CTF本身的安全性。当投票者希望没有中央机构干涉投票过程或结果，或者当一个临时团体需要对某一问题进行表决时，这种协议是无法解决，需要进一步研究。因此研究一个无需中央机构的电子投票协议有较大的意义。

参考文献：

[1] Subariah Ibrahim , Maznah Kamat, Mazleena Salleh, and Shah Rizan Abdul Aziz, Secure E-Voting With Blind Signature, 4' National Conference on Telecommunication Technology Proceedings[C]. Shah Alam, Malaysia, 2003.

[2] William Stallings. 密码编码学与网络安全—原理与实践[D].（第三版）刘玉珍，王丽娜. 北京电子工业出版社，2004，1.

[3] 龚 俭，陆 晟，王 倩. 计算机网络安全导论[M]. 厦门：东南大学出版社，2000，5.

[4] 2 Radwin M j. An Untraceable. Universally Verifiable Voting Scheme[J]. Seminar in Cryptology Pyoli. ~ssor Philip Klein. 1995，1 2.