安全远程网络投票协议

孟 博 王德军 著

科学出版社

安全远程网络投票协议

孟 博 王德军 著

科学出版社
北 京

内 容 简 介

本书共有十三章。系统全面地介绍了远程网络投票协议设计与分析的基本理论、关键技术及最新成果。主要内容包括远程网络投票协议的分类和模型、国内外发展现状、安全属性及其实现所需要的关键技术、典型远程网络投票协议、基于符号模型手工方式分析与验证无收据性、应用 PI 演算、一阶定理证明器 ProVerif、基于符号模型自动化分析与验证抗拒绝服务攻击性、无收据性和抗威胁性、概率进程演算、自动化安全协议证明器 CryptoVerif、基于计算模型自动化分析和验证抗威胁性等。

本书可供从事安全协议、密码学、计算机、通信和数学等专业的科技人员、硕士和博士研究生参考，也可供高等院校相关专业的师生参考。

图书在版编目(CIP)数据

安全远程网络投票协议 / 孟博，王德军著 . —北京：科学出版社，2013
ISBN 978-7-03-036826-3

Ⅰ. ①安… Ⅱ. ①孟…②王… Ⅲ. ①远程网络-计算机监控
Ⅳ. ①TP277②TP393. 2

中国版本图书馆 CIP 数据核字(2013)第 039474 号

责任编辑：孙伯元 / 责任校对：宋玲玲
责任印制：张 倩 / 封面设计：科迪亚盟

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com
源海印刷有限责任公司 印刷
科学出版社发行 各地新华书店经销
*
2013 年 6 月第 一 版 开本：B5(720×1000)
2013 年 6 月第一次印刷 印张：20 1/2
字数：395 640
定价：85.00 元
(如有印装质量问题，我社负责调换)

序

随着信息技术与产业的迅速发展和广泛应用，社会逐步实现了信息化。在信息化社会中，许多事务都采用信息化的方法进行处理。因此，如何使信息化的事务处理能够高效方便地进行并确保信息处理的安全就成为一个重要的问题。

投票是人们表达自己对某一事物意见的一种方式，已经广泛应用于选举、评奖、表决等事务处理中。用于传统事务处理的投票方式有举手、投石块、投金属币以及投纸票等。而在以计算机网络系统为基础的事务处理中，投票的方式发展成网络投票。由于投票所要处理的事务都是重要事务的裁决，涉及资源、利益和权力的分配等重要方面，所以确保投票系统的信息安全是一个重要问题。为此，网络投票系统综合采用了加解密、数字签名、密码协议、访问控制以及网络安全等多种信息安全技术。随着人们对网络投票理论与技术的研究和开发，网络投票系统已逐步走向实际应用。

本书作者长期从事网络投票的研究，重点研究投票协议及其安全性，取得了一系列重要成果。特别是在无物理约束条件下的安全远程网络投票协议、网络投票协议形式化分析与验证等方面的成果得到了国内外同行的好评。他们发表了一批高质量的学术论文，并培养了多名优秀的研究生。本书是他们这些研究成果的总结。本书的出版将为传播网络投票的基础知识、交流网络投票的理论与技术、扩大网络投票系统的应用做出贡献。

我作为孟博在博士后期间的合作导师以及王德军在攻读博士学位期间的老师，见证了他们的努力学习和刻苦研究。我为他们取得的研究成果和学术著作的出版感到由衷的高兴，并向他们表示衷心祝贺！

张焕国

2013 年

前　言

投票是人们表达自己对某一问题观点的一种方式。随着社会和经济的发展，采用投票方式来处理的事务越来越多。特别是信息技术的飞速发展使通过网络进行投票成为现实。目前远程网络投票已取代传统投票并广泛应用于商业和社会活动中。安全远程网络投票协议既是网络投票系统的基础和核心，又是安全协议研究领域的一个热点。由于远程网络投票的复杂性和特殊性，其安全性受到人们的重点关注。

作者从2004年便开始安全远程网络投票协议研究工作，在远程网络投票协议设计方面、对其安全属性实现的关键技术进行了深入研究，在无物理约束条件下提出了一个安全远程网络投票协议；在其形式化分析和验证方面，分别基于符号模型和计算模型，对典型的及提出的远程网络协议进行自动化分析和验证。在这期间，参加过多次国际国内相关学术会议，与国内外多名专家进行过学术交流，曾得到国家民委基金、国家自然科学基金、湖北省自然科学基金等课题的支持，取得了一批高水平的研究成果，培养了多名优秀研究生，发表了一批高质量学术论文，也在已出版的部分著作中反映了我们的一些研究成果。本书是作者长期从事远程网络投票协议研究的成果总结。

本书包括13章。第1、2章介绍了传统投票方式和分类、远程网络投票的分类和模型、远程网络投票的通信模型以及在安全远程网络投票协议设计中需要的关键技术等。第3、4章重点对远程网络投票协议安全属性中非常重要的无收据性和抗威胁性的发展现状做了阐述，同时对典型的与提出的远程网络投票协议及其安全性进行了深入分析和研究。第5～9章重点介绍了基于符号模型分析远程网络投票协议的国内外发展现状、手工方式分析与验证无收据性、应用PI演算、一阶定理证明器ProVerif、符号模型自动化分析与验证抗拒绝服务攻击性、无收据性和抗威胁性。第10～13章重点讨论了基于计算模型分析远程网络投票协议的国内外发展现状、概率进程演算、自动化安全协议证明器CryptoVerif、计算模型自动化分析和验证抗威胁性等。本书由中南民族大学孟博和王德军共同撰写，其中第1、2、6、7章由王德军撰写，其余章节由孟博撰写。全书最后由孟博统稿、王德军校稿。

本书的研究工作得到了国家民委基金（No. 12ZNZ008、12ZNZ009、10ZN09）、国家自然科学基金项目（No. 91018008、60603008）和湖北省自然科学基金（No.

2011CDC163)的支持以及其他课题(SZY11008,YZZ09008)的资助,在此表示衷心的感谢。

由于水平有限,对一些问题的理解和表述或有肤浅之处,诚请读者批评指正。

孟 博 王德军

2013年4月25日

目　录

第1章 绪 论

1.1 引 言

投票是人们表达自己对某一问题观点的一种方式。而这种表达方式随着科学技术发展水平的不同而不同，比如从古代的石头，到近代纸质投票、机械杠杆投票仪、打孔卡、光学识别投票，再到今天的直接记录电子投票系统、远程网络投票等，如图 1.1 所示。

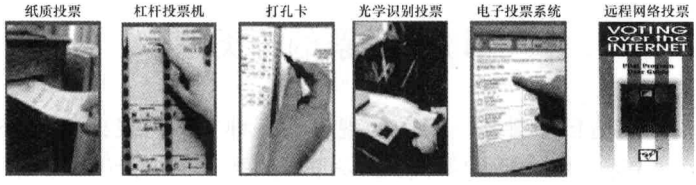

图 1.1 投票方式

随着计算机和通信技术的发展，计算机已经普及到千家万户。特别是随着网络的迅猛发展，由于网络本身所具有的特点，使人们利用计算机或者各种通信设备在任何地方通过网络进行投票成为现实。由于远程网络投票的方便性和实施成本的低廉，必将对社会经济的发展和国家民主进程产生积极而重大的影响。比如，可以吸引更多的人来投票，方便残疾人投票，投票的人数不受天气等状况的影响。远程网络投票不仅消除了票的运输和计算上的困难，也大大减少了投票者由于日常安排与投票日发生冲突而带来的不便，同时也为残疾人士参与相关活动提供了便利。

在商业应用领域，比如我国证券行业，股东可以利用远程网络投票的方式通过深圳或者上海证券交易所股东大会网络投票系统来对各种议案，如增发新股、配股、发行可转债、重大资产重组等事项发表自己的观点。在政治生活方面，2006 年 8 月，我国上海市闸北区宝山路街道第八届居委会的换届选举首次允许网络投票。选举所使用的电子投票系统提供了网络投票功能，无法现场投票的选民只要填写社保卡号码和发卡日期，就可以进行网络投票[1]。爱沙尼亚在网络投票选举方面的实践走在了世界的前列，它是全球第一个将远程网络投票方式运用于全国范围内地方选举的国家[2]。2000 年，爱沙尼亚政府规定可以在国家选举中采用 Internet 投票系统。2005 年 7 月，Internet 投票系统应用在本地政府选举中，2007 年 10

月，Internet 投票系统应用在国家选举中。根据 Brace 关于在美国国家选举中投票方式分类的报告，从 2000 年到 2008 年，使用电子投票的郡从 320 个增加到 1068 个，投票者使用电子投票的比例从 12.4%增加到 32.6%[3]。此外美国、日本、瑞士以及英国等国家在选举中大量进行远程网络投票实验，2000 年到 2011 年，瑞士实施了远程网络投票实验计划达到 36 个[4]。

在最近的二十多年中，人们对电子投票及远程网络投票展开了深入研究，提出了许多远程网络投票协议。但是，不论在实践还是在理论方面，目前都没有完善的解决方案。其中远程网络投票协议是实施远程网络投票系统的基础，我国目前对远程网络投票协议的研究还非常少，处在刚刚开始阶段。因此为了促进我国社会经济的发展和满足人们的需要，对远程网络投票协议进行研究具有重要的现实意义和巨大的经济价值。

1.2 投票的分类

投票是人们表达自己对某一问题的观点的一种方式。投票可以按照不同的标准进行分类：①按照票的介质的不同；②按照票的类型；③按照每张票的权重分类。

1.2.1 按照票的介质进行分类

按照票介质的不同，投票可以分为两大类：纸质投票和电子投票，如图 1.2 所示。

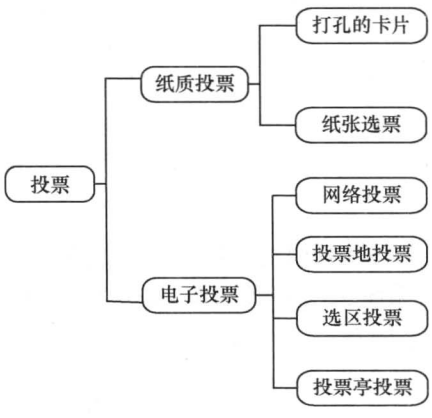

图 1.2 按照按票的介质进行分类

纸质投票的介质是纸张，它可以分为纸张选票、打孔的卡片等。纸张选票系统装置最简单，就是在写有候选人姓名的纸上选择出自己的支持者，在他旁边画个圈，再投进密封的票箱即可。1856 年澳大利亚首次运用该系统，美国直到 1889 年才在纽约首次使用。现在，在美国的少数民族和偏远农村等地区，还在使用这种投票方式。这种投票方式在我国的选举中是比较常用的一种方式。

打孔的卡片这种投票方式有点像学生考试用的答题卡。在卡上写着候选人的名字，投票者需在自己中意的候选人名字处打孔，然后将票投进票箱，与投票箱相连的计算机可以自动识别。这种系统在 1964 年的美国总统选举中首次被佛罗里达州选民使用。在 2000 年总统大选时，正是这种类别的选票导致佛罗里达州出现计票争议。因此，打卡装置也正在被淘汰。

电子投票所采用票的形式是电子的。电子投票根据投票地点的不同分为投票地投票、选区投票、投票亭投票与网络投票。

现在在美国使用的是直接记录(direct recording electronic)电子投票系统。此系统可以让投票者利用电子投票机方便地投票,机器上会显示候选人的名单,投票者只需按机器上的按钮,或者屏幕上的触摸式按键,就可完成投选程序。

选区投票限定在一定的区域内的投票者才可以投票。也就是说投票者只要在这个选区内,没有规定你在某一个特殊的投票地进行投票,都可以在这里投票。

投票亭投票指的是在某一个指定位置有投票官员来现场控制的一种投票方式。

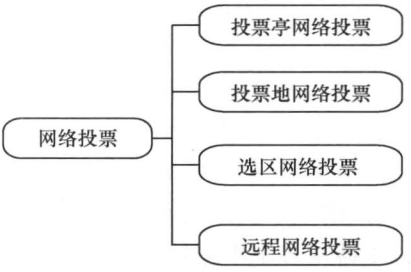

图 1.3 网络投票的分类

网络投票[5]是指投票者利用计算机通过远程网络来进行投票的方式,如图 1.3 所示。网络投票可以分为四种:①远程网络投票(remote internet voting);②投票亭网络投票(kiosk internet voting);③投票地网络投票(polling place internet voting);④选区网络投票(precinct internet voting)。

远程网络投票指不在投票管理员的现场控制下,利用计算机通过远程网络进行投票。投票者在家庭或者工作场所等通过各种互联网终端来进行投票,因此这种投票方式面临的安全风险最大。

投票亭网络投票指在某一个特定位置,在投票官现场控制下通过远程网络进行投票。

投票地网络投票指在任何有效的投票地,在投票官现场控制下通过远程网络进行投票。

选区网络投票在一定区域内的投票者,除了只能在某一特殊投票地投票的投票者之外,才可以投票。也就是说投票者只要在这个选区内,没有规定投票者在某一个特殊的投票地进行投票,都可以在这里投票。投票是在投票管理员的现场控制下通过远程网络进行的。

1.2.2 按照票的类型进行分类

常用的票的类型有如下六种:

(1) *yes/no voting*:投票者对问题进行 *yes* 或者 *no* 的回答。一般情况下用 1 表示 *yes*,用 0 表示 *no*。

(2) *1-out-of-L voting*:从 L 个可能的选择中选择一个。

(3) *K-out-of-L voting*:从 L 个可能的选择中选择 K 个,这 K 个元素是没有

次序关系的。

(4) *K-out-of-L ordervoting*：从 L 个可能的选择中选择 K 个，这 K 个元素是有次序关系的。

(5) *1-L-K voting*：投票者从 L 个选择中选择一个可能的选择，然后再在另一个可能的选择中选择 K 个。它的票的结构是 $(I, a_1, a_2, \cdots, a_K)$。比如在选举人大代表时，有 L 个不同的党派，共有 m 个候选人，投票人只能选自己所在的党派的候选人，那么这种选举方式就是 *1-L-K voting*。I 表示党派，$a_1, a_2, \cdots, a_K$ 表示自己党派的候选人中的 K 个。

(6) *write-in voting*：在投票时，可以投不在候选者名单中的票。

最初电子投票协议[6~8]只是支持简单的 *yes/no* 票类型，随着研究工作的深入，支持从多个中选择一个、或从多个中选择多个的电子/网络投票协议[9~16]被设计出来，同时支持 *write-in* 类型的远程网络投票协议[17~22]也被提了出来。

1.2.3 按照票的权重进行分类

按票的权重进行分类：① *equal-voting*：每个投票人的票的权重是一样的；② *weighted-voting*：投票人的票的权重是不相同的；几乎所有的电子/网络投票协议都没有特别明确这一点[23]。

1.3 传统投票模型

如图 1.4 所示，在传统投票中，首先投票者去注册地点进行注册，只有经过注册的投票者才可以投票。

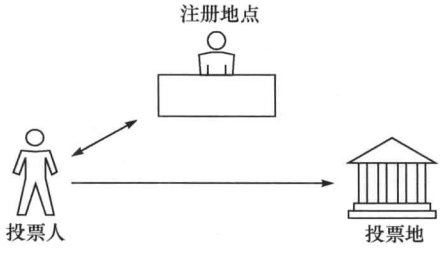

图 1.4 传统投票模型

注册完成后，领取票，票一般是由投票委员会提前制定的。然后到投票地进行投票。一般情况下，投票地有投票箱，在箱子的顶部有一个投票时用的小缝，在投票时，人们把填好的票投进投票箱。

投票结束后，根据投票委员会的决定，选择公开计票或者不公开计票。如果是公开计票，把投的票公开，然后进行计票，计票结果也当场公开。如果是不公开计票，则只公开计票结果。

传统投票需要花费大量的人力和物力来保证投票公正、公平的进行，防止破坏和舞弊行为的发生。

1.4 远程网络投票模型

在远程网络投票模型中，主要涉及的参与者有投票者、注册机构、证书颁发机构、计票机构、票的生成机构、贿票者与威胁者。当然也有另外的机构，比如监察机构等。

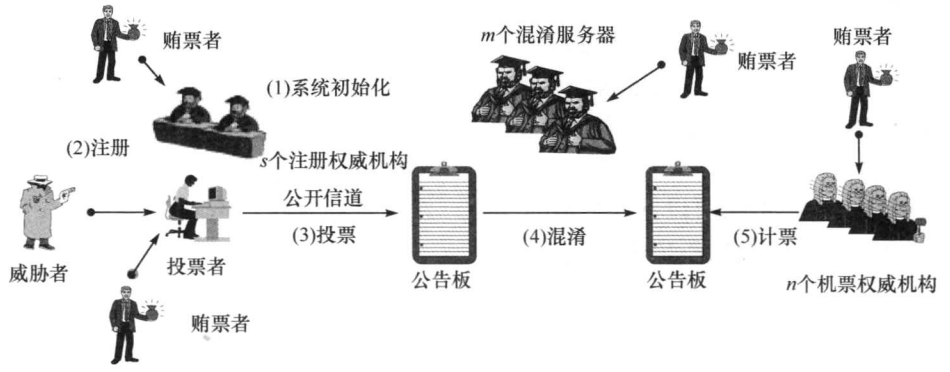

图 1.5 远程网络投票模型

远程网络投票模型[23]如图 1.5 所示，由四个阶段组成：系统建立阶段、注册阶段、投票阶段和计票阶段。在投票过程中，贿票者可以对权威机构进行贿赂，为了处理这种情况，门限加密通常被用在远程网络投票系统中。

(1) 系统建立阶段。权威机构建立投票系统，同时权威机构和投票者产生自己公/私钥。投票者和权威机构的私钥保密。权威机构生成票，然后将票和它的数字签名发送到公告板。

(2) 注册阶段。投票者通过一个安全的信道得到他的信任状，从公告板得到票。

(3) 投票阶段。投票者准备了一个加密的票，接着用可以验证的方式将它公布在公告板上，然后多个独立的混淆服务器以可验证的方式混淆被公布的票，使票的表现形式发生变化，投票者不能再识别出自己的票。在这个阶段，威胁者可能强迫投票者投一张特殊的票；贿票者可能贿赂投票者，干扰或者破坏投票。此时投票者可以使用一些技术产生一个假的信任状，然后使用它产生一个威胁者/贿票者不能验证的投票。

(4) 计票阶段。混淆完成以后，多个计票服务器用门限解密算法解密票的密文，计票，然后发布计票的结果。

在远程网络投票中常用的通信模型如下：

(1) 公告板(bulletin board)。任何参加投票的实体都可以通过公告板发布信息。任何人都可以访问公告板。任何人都可以在公告板上自己所属的区域进行写操作,但是不能删除和修改公告板上的信息。

(2) 不可泄漏通道(untappable channel)。不可泄漏通道是通讯双方之间的一个秘密通道。通过不可泄漏通道进行通信是物理上安全的。没有任何人,除了通信双方外,知道通道中传输的信息。同时通讯参加者也不能向任何人证明自己所发送的内容。

(3) 不可追踪的匿名通道或匿名通道(untraceable anonymous channel or anonymous channel)。通过这个通道传送信息可以保证信息的发送者的匿名性。信息的接收者不知道信息的发送者的身份。

(4) 不可泄漏的匿名通道(untappable anonymous channel)。它既可以保证发送者的匿名性,又可以保证传输的安全。发送者和接收者不能重演发送或接收的内容。没有人能监听传输的消息。

1.5 本章小结

随着信息技术的发展,远程网络投票已取代传统投票并广泛应用于商业和社会活动中,其安全性受到人们的重点关注。本章对传统投票方式和分类、远程网络投票的分类和模型、远程网络投票的通信模型进行了详细研究,为后面的研究工作打下了坚实的基础。

参考文献

[1] 上海宝山路街道. 首次网络投票选举居委会. 人民日报,2006-08-10(第 10 版).

[2] Hall T E, Alvarez M. Internet voting in comparative perspective: The case of estonia. Political Science & Politics, 2009, 42:497～505.

[3] Brace K W. Nation sees drop in use of electronic voting equipment for 2008 election-A first, election data service. http://www. electiondataservices. com [2012-3-24].

[4] U. S. Election Assistance Commission. A survey of internet voting. http://www. eac. gov/assets/1/Documents/SIV-FINAL. pdf [2012-3-24].

[5] Alvarez R M, Hall T E. Point, click, and vote: The future of internet voting. http://www. brookings. edu/press/books/pointclickandvote. html[2012-3-24].

[6] Benaloh J, Tuinstra D. Receipt-free secret-ballot elections//Proceeding of the 26th Annual ACM Symposium on Theory of Computing, New York, 1994: 544～553.

[7] Sako K, Kilian J. Receipt-free mix-type voting scheme//Proceeding of the 14th Annual International Conference on Theory and Application of Cryptographic Techniques, Saint-Malo, 1995: 393～403.