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

中国科学院印刷厂 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。

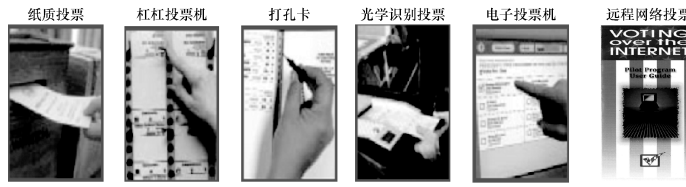

图 1.1 投票方式

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。

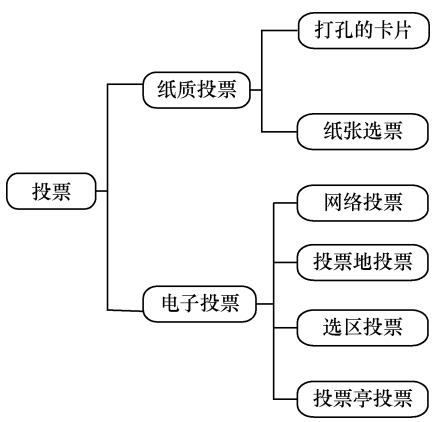

图 1.2 按照按票的介质进行分类

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。

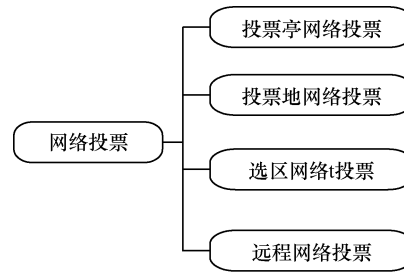

图 1.3　网络投票的分类

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,…,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,…,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。

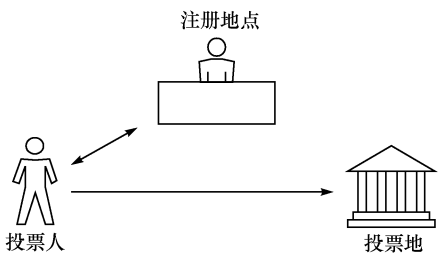

图 1.4 传统投票模型

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。

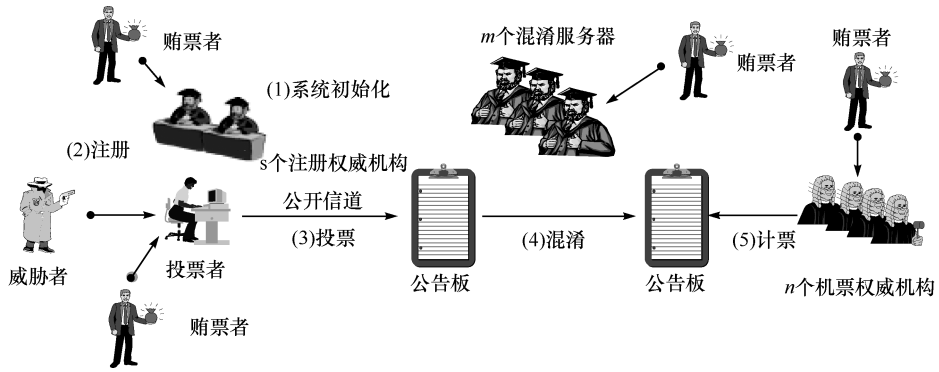

图 1.5　远程网络投票模型

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.

[8] Canetti R, Dwork C, Naor M, et al. Deniable encryption//Proceeding of the 17th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, 1997: 90～104.

[9] Cramer R, Franklin M, Schoenmakers B, et al. Multi-authority secret ballot elections with linear work// Proceeding of the 15th Annual International Conference on Theory and Application of Cryptographic Techniques, Saragossa, 1996: 72～83.

[10] Cramer R, Gennaro R, Schoenmakers B. A secure and optimally efficient multi-authority election scheme//Proceeding of 16th Annual International Conference on Theory and Application of Cryptographic Techniques, Konstanz, 1997: 103～118.

[11] Baudron O, Fouque P A, Pointcheval D, et al. Practical multi-candidate election system// Proceeding of the 12th Annual ACM Symposium on Principles of Distributed Computing, New York, 2001: 274～283.

[12] Damgard I, Jurik M. A generalization, a simplification and some applications of paillier's probabilistic public-key system//Proceeding of the 4th International Workshop on Practice and Theory in Public Key Cryptography: Public Key Cryptography, Cheju Island, 2001: 119～136.

[13] Damgard I, Jurik M, Nielsen J B. A generalization of paillier's public-key system with applications to electronic voting. International Journal of Information Security, 2010, 9(6): 371～385.

[14] Hirt M, Sako K. Efficient receipt-free voting based on homomorphic encryption// Proceeding of the 19th International Conference on Theory and Application of Cryptographic Techniques, Bruges, 2000: 539～556.

[15] Lee B, Kim K. Receipt-free electronic voting scheme with a tamper resistant randomizer// Proceeding of the 5th International Conference on Information Security and Cryptology, Seoul, 2002: 405～422.

[16] Rjaskova Z. Electronic Voting Schemes [Master Thesis]. Bratislava: Comenius University, 2002.

[17] Neff A. Detecting malicious poll site voting clients. http://votehere.com/vhti/documentation/psclients.pdf [2012-3-24].

[18] Kiayias A, Yung M. The vector-ballot approach for online voting procedures. Towards Trustworthy Elections, 2010: 155～174.

[19] Acquisti A. Receipt-free homomorphic elections and write-in voter verified ballot. Technical Report of International Association for Cryptologic Research and Carnegie Mellon Institute for Software Research International, 2004.

[20] 孟博. Internet 投票协议研究[博士后出站报告]. 武汉: 武汉大学, 2006.

[21] Meng B. A secure internet voting protocol based on non-interactive deniable authentication protocol and proof protocol that two ciphertexts are encryption of the same plaintext. Journal of Networks, 2009, 4(5): 370～377.

[22] Meng B, Li Z M, Qin J. A receipt-free coercion-resistant remote internet voting protocol without physical assumptions through deniable encryption and trapdoor commitment scheme. Journal of Software, 2010, 5(9): 942～949.

[23] Meng B. A critical review of receipt-freeness and coercion-resistance. Information Technology Journal, 2009, 8(7): 934～964.

第 2 章　相关的密码技术

2.1　公钥密码体制

公钥密码体制是密码编码学重要的组成部分，其加密算法和解密算法使用不同的密钥，一个是公钥，一个是私钥。这里主要介绍在远程网络投票协议中用到的 RSA、ElGamal[1~2]、BCP[3]和 Paillier[4~6]公钥加密体制。

2.1.1　RSA 公钥加密体制

(1) 密钥建立。

①随机选择两个素数 p 和 q，$|p| \approx |q|$。②计算 $n=pq$，$\phi(n)=(p-1)(q-1)$。③随机选取整数 e，满足 $1<e<\phi(n)$，$\gcd(e,\phi(n))=1$。④计算 d，$ed=1 \bmod \phi(n)$。⑤公钥(n,e)，私钥 d。

(2) 加密算法。

加密明文 m，$m<n$，则密文 $c=m^e \bmod n$。

(3) 解密算法。

解密密文 c，得到明文 $m=c^d \bmod n$。

2.1.2　ElGamal 公钥加密体制

(1) 密钥建立。

①随机选择素数 p。②g 是 Z_p 中的乘法群 Z_p^* 的一个生成元。③选择随机数 α，$1 \leqslant \alpha \leqslant p-2$，计算 $h=g^\alpha$。④公钥(p,g,h)，私钥 α。

(2) 加密算法。

随机选择 k，$0 \leqslant k \leqslant p-2$，则 m 的密文：$c=(x,y)=(g^k \bmod p, mh^k \bmod p)$。

(3) 解密算法。

解密密文 c，得到明文 $m=\dfrac{y}{x^\alpha} \bmod p$。

2.1.3　Paillier 公钥加密体制

(1) 密钥生成。

①选择两个大素数 p，q，令 $n=pq$，$\phi(n)=(p-1)(q-1)$，$\lambda=lcm(p-1,q-1)$。

②随机选择 $g(g\in Z_{n^2}^*)$,使得 g 满足 $\gcd(L(g^\lambda \bmod n^2),n)=1$,其中 $L(u)=\frac{u-1}{n}$,其中 $u\in S_n=\{u<n^2 \mid n^2=1 \bmod n\}$。明文域为 Z_n,密文域为 $Z_{n^2}^*$。③公钥(n,g),私钥(p,q)。

(2) 加密算法。

明文 m 且 $m<n$,选择随机数 r 且 $r\in Z_n^*$,则密文 $c=g^m \cdot r^n \bmod n^2$。

(3) 解密算法。

密文 $c<n^2$,明文 $m=\frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$。

2.1.4 BCP 公钥密码体制

2003 年,Bresson 等[3]提出 BCP 公钥密码体制,它保留了 Cramer-Shoup 模式的特点,同时基于两个陷门,具有两种不同解密模式,可看作是 ElGamal 密码体制的加法同态的变种。令 h 和 g 是最大界中 G 的两个元素。如果 $h=g^x$,$x\in_R[1,\lambda(N^2)]$,那么 x 就以很大的概率包含 $\mathrm{ord}(G)$,同时 h 是最大界。Z_N 是消息空间。

(1) 密钥生成。

选择一个随机数 $\alpha\in Z_{N^2}^*$,随机值 $a\in[1,\mathrm{ord}(G)]$,计算 $g=\alpha^2 \bmod N^2$ 和 $h=g^a \bmod N^2$。公钥是三元组(N,g,h),与之相对应的私钥是 a。

(2)加密算法。

Bob 得到 Alice 的公钥(N,g,h)。Bob 想加密明文 $m\in Z_N$ 发送给 Alice。计算:首先在 Z_{N^2} 中均匀选择 r,密文(A,B)是 $A=g^r \bmod N^2$,$B=h^r(1+mN) \bmod N^2$,然后发送(A,B)给 Alice。

(3) 解密算法。

从密文(A,B)中恢复明文 m,Alice 计算如下:

①一种情况,知道 a,Alice 通过 $m=\frac{B/(A^a)-1 \bmod N^2}{N}$恢复 m。②另外一种情况,如果知道因子分解结果:Alice 可以得到 $a \bmod N$ 和 $r \bmod N$。令 $ar \bmod \mathrm{ord}(G)=\gamma+\gamma_2 N$,那么可以非常高效得到 $\gamma=ar \bmod N$。Alice 根据 $m=\frac{D-1 \bmod N^2}{N} \cdot \pi \pmod N$可以恢复明文,其中,$\pi$ 是在 Z_N^* 的 $\lambda(N)$的逆。

2.2 秘密共享

1979 年,Shamir[7]和 Blakley[8]分别独立提出秘密共享思想,并分别给出了两种门限密码体制:拉格朗日内插多项式体制(是完善的)和矢量体制(是不完善的)。

设秘密 s 被分成 n 份部分信息，每一个部分信息被称为一个秘密分量或共享份额(也可以称为影子或秘密碎片)，每个秘密分量均有一个参与者持有，若通过其中任意 t 个或多余 t 个参与者所持有的秘密分量可以重构 s，而通过少于 t 个参与者所持有的密钥分量无法重构 s，则称这种方案为(t,n)秘密共享门限方案，其中 t 为方案的门限值。如果方案还满足任意一组参与者，若其个数少于 t，则由他们所持有的秘密分量得不到秘密 s 的任何信息，称(t,n)秘密共享门限方案是完善的。一个(t,n)秘密共享门限方案一般由两部分组成：一个是秘密分量的产生过程；另一个是秘密恢复过程。

Shamir 门限方案的构造基于多项式 Lagrange 插值公式。

设 $f(x_i)$，$i=1,2,\cdots,n$，$\{(x_1,y_1),\cdots,(x_t,y_t)\}$是平面上 t 个点构成的点集，其中 x_i，$i=1,\cdots,t$，均不相同，那么在平面上存在一个唯一的 $t-1$ 多项式 $f(x)$通过这 t 个点。若把秘密 s 取作 $f(0)$，n 个秘密分量取作 $f(x_i)$，$i=1,2,\cdots,n$，那么利用其中的任意 t 个秘密分量可重构 $f(x)$，从而可以得到秘密 s。

方案一般构造方式如下：设 $GF(q)$是一个有限域，其中 q 是一个大素数，满足 $q\geqslant n+1$，秘密 s 是 $GF(q)\backslash\{0\}$ 上均匀选取的一个随机数，表示为($i=1,2,\cdots,t-1$)。$t-1$ 个系数 $a_1,a_2,\cdots,a_{t-1}$的选取满足

$$a_i\in_R GF(q)\backslash\{0\},\quad i=1,2,\cdots,t-1$$

在 $GF(q)$上构造一个 $t-1$ 次的多项式

$$f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}$$

其中，$a_0=s$。

n 个参与者记为 $P_1,P_2,\cdots,P_n$，P_i 分到的秘密分量为 $f(i)$。如果任意 t 个 $P_{i_1},\cdots,P_{i_t}$ $(1\leqslant i_1<i_2<\cdots<i_t\leqslant n)$要想得到秘密 s，可以使用$\{(i_l,f(i_l))\mid l=1,\cdots,t\}$构造如下线性方程组：

$$\begin{cases}a_0+a_1(i_1)+\cdots+a_{t-1}(i_1)^{t-1}=f(i_1)\\ a_0+a_1(i_2)+\cdots+a_{t-1}(i_2)^{t-1}=f(i_2)\\ \qquad\cdots\\ a_0+a_1(i_t)+\cdots+a_{t-1}(i_t)^{t-1}=f(i_t)\end{cases}$$

因为 i_l $(1\leqslant l\leqslant t)$均不相同，所以可由 Lagrange 插值公式构造多项式

$$f(x)=\sum_{j=1}^{t}f(i_j)\prod_{\substack{l=1\\ l\neq j}}^{t}\frac{(x-i_j)}{(i_j-i_l)}(\mathrm{mod}q)$$

由多项式可得秘密 $s=f(0)$。

然而参与者仅需要知道 $f(x)$的常数项 $f(0)$，不需要知道整个多项式 $f(x)$，所以可以通过下式求出 s：

$$s=\sum_{j=1}^{t}f(i_j)\prod_{\substack{l=1\\ l\neq j}}^{t}\frac{-i_l}{(i_j-i_l)}(\mathrm{mod}q)$$

由此可知,如果由 t 个参与者那么一定能获得秘密 s。对于任何一个 $s\in GF(q)$存在唯一的多项式满足方程组 1(可设 $a_0=s$)所以若有 $t-1$ 个参与者,只能得到$t-1$ 个方程,而对 $f(x)$来说,共有 t 个未知数,所以得不到关于秘密 s 的任何信息,因此这个方案是完善的。

2.3 门限公钥加密

这里介绍 Pedersen[9] 提出的 RSA,Cramer 等[10,11] 提出的 ElGamal 以及 Baudron 等[12]提出的 Paillier 加密体制的门限版本。

2.3.1 RSA 公钥加密的门限版本

(1) 密钥生成算法。

可信中心随机选择两个强素数 p,q,使得 $p=2p'+1,q=2q'+1$,其中,p',q' 也是素数。令 $n=pq,n'=p'\times q'$,取素数 $e\in Z_{n'},e>l$。RSA 公钥为 $PK=(n,e)$。利用欧几里得算法计算 $d\in Z_{n'}$,使得 $de=1\bmod n'$。利用 Shamir 秘密共享模式:令 $f(0)=d$。对 $i=1,\cdots,t$,随机选择 $f_i\in Z_{n'}$,令 $f(X)=\sum_{i=0}^{t}f_iX^i$。秘密密钥$SK_i=d_i=f(i)\bmod n'$,验证密钥 $VK=v$,它是由 $Z_{n^2}^*$ 中的平方数构成的循环子群中的一个元素,子验证密钥 $VK_i=v^{d_i}\bmod n,i=1,\cdots,l$。

(2) 加密算法。

加密消息 m,计算 $c=m^e\bmod n$。

(3) 共享解密算法。

令 $\Delta=l!$,计算 $c_i=c^{2\Delta d_i}\bmod n$,并且用零知识证明 $\log_{c^{4\Delta}}c_i^2=\log_{VK}VK_i$。

(4) 秘密重构算法。

如果少于 t 个正确解密的秘密共享,则算法失败。否则令 S 是 $t+1$ 个秘密共享的集合。计算对于任意的 $i\in\{0,\cdots,l\},j\in S$,定义

$$\mu_{i,j}^{S}=\Delta\times\frac{\prod_{j'\in S\setminus\{j\}}(i-j')}{\prod_{j'\in S\setminus\{j\}}j-j'}\in Z$$

由 lagrange 插值公式得

$$\Delta f(i)=\sum_{j\in S}\mu_{i,j}^{S}f(j)\bmod m$$

因为 $f(0)=d$ 可得

$$m^{4\Delta^2}=c^{4\Delta^2 d}=c^{4\Delta^2 f(0)}=\prod_{j\in S}c^{4\Delta\mu_{0,j}^{S}f(j)}=\prod_{j\in S}c^{2\mu_{0,j}^{S}}\bmod n$$

根据 $\gcd(4\Delta^2,e)=1$ 可用扩展的欧几里得算法计算出 a,b 使得 $a\times4\Delta^2+b\times e=1$。得

$$m = m^{a\times 4\Delta^2} m^{b\times e} = (m^{4\Delta^2})^a \times c^b \bmod n$$

2.3.2　ElGamal 公钥加密的门限版本

(1) 密钥生成算法。

执行密钥生成协议[9],每个权威机构 A_j 都拥有秘密 s 的共享 $s_j \in Z_q$,其中,s 是 ElGamal 加密体制中的私钥。权威机构把 $h_j = g^{s_j}$ 公开。应用 Lagrange 插值可以从任何 t 个共享中重构秘密 s 如下:

$$s = \sum_{j\in\Lambda} s_j \lambda_{j,\Lambda}, \quad \lambda_{j,\Lambda} = \prod_{l\in\Lambda\setminus\{j\}} \frac{l}{l-j}$$

这正是 Shamir 的(t,n)门限秘密共享。公钥 $h = g^s$ 公开。

(2) 解密算法。

为不重构秘密 s,而可以解密$(x,y) = (g^a, h^a m)$,权威机构执行协议:①每个权威机构 A_j 广播 $w_j = x^{s_j}$,并且以零知识证明 $\log_g h_j = \log_x w_j$;②Λ 表示任意 t 个通过了零知识证明的权威机构集合。恢复明文

$$m = \frac{y}{x^s}, \quad x^s = x^{\sum_{j\in\Lambda} s_j \lambda_{j,\Lambda}} = \prod_{j\in\Lambda} w_j^{\lambda_{j,\Lambda}}$$

2.3.3　Paillier 加密的门限版本

(1) 密钥生成算法。

定义 $\Delta = l!$,其中,l 是服务器的个数。选择整数 n,n 是强素数 p,q 的乘积,令 $p = 2p' + 1$,$q = 2q' + 1$,$\gcd(n, \varphi(n)) = 1$。令 $m = p'q'$。随机选择 $\beta \in Z_n^*$,$(a,b) \in Z_n^* \times Z_n^*$。令 $g = (1+n)^a \times b^n \bmod n^2$。秘密密钥 $SK = \beta \times m$ 采用 Shamir(t,n)模式共享,令 $a_0 = \beta m$,随机选择 $a_i \in \{0, \cdots, n \times m - 1\}$,令 $f(X) = \sum_{i=0}^{t} a_i X^i$。服务器 P_i 的秘密共享 $S_i = f(i) \bmod nm$,公钥 $PK = (g, n, \theta = L(g^{m\beta}) = am\beta \bmod n)$,验证密钥 $VK = v$,它是由 $Z_{n^2}^*$ 中的平方数构成的循环子群中的一个元素,子验证密钥 $VK_i = v^{\Delta s_i} \bmod n^2$。

(2) 加密算法。

加密消息 M,随机选择 $x \in Z_n^*$,计算 $c = g^M x^n \bmod n^2$。

(3) 共享解密算法。

第 i 个参加者用自己的秘密共享 s_i 解密 $c_i = c^{2\Delta s_i} \bmod n^2$,并且以零知识证明 $\log_{c^{4\Delta}} c_i^2 = \log_{v^\Delta} v_i$。

(4) 秘密重构算法。

如果少于 t 个正确解密的秘密共享,则算法失败。否则令 S 是 $t+1$ 个秘密共享的集合。计算

$$M = l\left(\prod_{j\in S} c_j^{2\mu_{0,j}^{S}} \bmod n^2\right) \times \frac{1}{4\Delta^2\theta} \bmod n$$

其中

$$\mu_{0,j}^{S} = \Delta \times \prod_{j'\in S\setminus\{j\}} \frac{j'}{j'-j} \in \mathrm{Z}$$

2.4 盲 签 名

1983 年,Chaum[13]提出了盲签名的概念。盲签名在电子商务、电子政务中有着重要的应用。盲签名是一种特殊的数字签名,指签名者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通过脱盲后得到文件或消息的签名。盲签名的原理如图 2.1 所示。

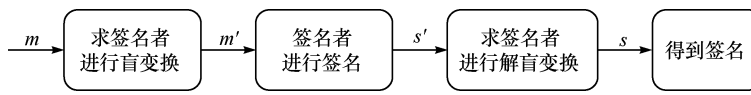

图 2.1 盲签名

需要签名者把要签名的消息 m 通过盲变换为 m',m'隐藏了明文 m 的内容。把 m'发送给签名生成者进行签名,得到签名 s'。需要签名者利用脱盲变换得到 m 的签名 s。这样请求签名者得到了 m 的签名 s,而签名者不知道 m 的内容。

下面介绍基于 RSA 的盲签名算法。

签名者的公钥(n,e),私钥 d。请求签名者想得到签名者对 m 的盲签名:①请求签名者盲化 m 为 $m'=mr^e \bmod n$,r 是随机数,$r\in_R \mathrm{Z}_n$;把 m'发送给签名者。②签名者生成 m'的签名 $s'=m'^d \bmod n$,发送给请求签名者;③请求签名者计算 $s=\frac{s'}{r}=\frac{m'^d}{r}=\frac{m^d r^{ed}}{r}=\frac{m^d r}{r}=m^d \bmod n$ 得到 m 的签名 s。

关于可证明安全的门限盲签名可以参看文献[14],[15]。

2.5 同 态 加 密

首先介绍同态加密、加法同态和乘法同态的概念,然后给出 RSA、ElGamal 和 Paillier 公钥加密体制具有的同态属性。

(1) 同态加密。

加密函数 $E()$是同态的,如果给定密钥 k,M 是明文集合,C 是密文集合,加密函数 $E()$满足

$$\forall m_1, m_2 \in M \quad E(m_1) \odot E(m_2) = E(m_1 \odot m_2)$$

(2) 乘法同态。

如果已经知道 $E(m_1)$,$E(m_2)$是明文 m_1,m_2 的密文,任何人都可以得到 $m_1 \times m_2$ 的密文 $E(m_1 \times m_2)$,即可以找到这样的运算⊗使得

$$\forall m_1, m_2 \quad E(m_1 \times m_2) = E(m_1) \otimes E(m_2)$$

(3) 加法同态。

如果已经知道 $E(m_1)$,$E(m_2)$是明文 m_1,m_2 的密文,任何人都可以得到 $m_1 + m_2$ 的密文 $E(m_1 + m_2)$,即可以找到这样的运算⊕使得

$$\forall m_1, m_2 \quad E(m_1 + m_2) = E(m_1) \oplus E(m_2)$$

(4) RSA 公钥加密体制。

假设公钥(n,e),私钥 d。$m_1, m_2 \in M$,$c_1 = E(m_1) = m_1^e \bmod n$,$c_2 = E(m_2) = m_2^e \bmod n$那么

$c_2 \times c_2 = E(m_1) \times E(m_2) = (m_1^e \bmod n) \times (m_2^e \bmod n) = (m_1 \times m_2)^e \bmod n = E(m_1 \times m_1)$

因此 RSA 算法具有乘法同态的性质。

(5) ElGamal 公钥加密体制。

假设公钥是(G, p, g, y),G 群,p 群的界,g 是生成元,$y = g^z \bmod p$,密钥 z,$m_1, m_2 \in M$,x_1,x_2 是随机数,则

$$c_1 = E_{x_1}(m_1) = (g^{x_1} \bmod p, y^{x_1} m_1 \bmod p), \quad c_2 = E_{x_2}(m_2) = (g^{x_2} \bmod p, y^{x_2} m_2 \bmod p)$$

$$\begin{aligned} c_2 \times c_2 &= E_{x_1}(m_1) \times E_{x_2}(m_2) = (g^{x_1} \bmod p, y^{x_1} m_1 \bmod p) \times (g^{x_2} \bmod p, y^{x_2} m_2 \bmod p) \\ &= (g^{x_1} g^{x_2} \bmod p, y^{x_1} y^{x_2} m_1 m_2 \bmod p) = (g^{x_1 + x_2} \bmod p, y^{x_1 + x_2} m_1 m_2 \bmod p) \\ &= E_{x_1 + x_2}(m_1 \times m_2) \end{aligned}$$

因此 ElGamal 具有乘法同态性质。

(6) Paillier 公钥加密体制。

Paillier 算法是概率公钥加密体制,公钥(n, g),私钥(p, q),$m_1, m_2 \in M$,x_1,x_2 是随机数,则加密算法 $E_x(m) = g^m x^n \bmod n^2$,解密算法 $D()$,存在

$$c_1 = E_{x_1}(m_1) = g^{m_1} x_1^n \bmod n^2, \quad c_2 = E_{x_2}(m_2) = g^{m_2} x_2^n \bmod n^2$$

$$\begin{aligned} c_1 \times c_2 &= E_{x_1}(m_1) E_{x_2}(m_2) = (g^{m_1} x_1^n \bmod n^2) \times (g^{m_2} x_2^n \bmod n^2) \\ &= g^{m_1 + m_2} (x_1 x_2)^n \bmod n^2 = E_{x_1 x_2}(m_1 + m_2) \end{aligned}$$

因此 Paillier 加密算法具有加法同态的性质。

加法同态属性如下:

$$\forall m_1, m_2 \in \mathbf{Z}_n, k \in \mathrm{N}$$

$$D(E(m_1) E(m_2) \bmod n^2) = m_1 + m_2 \bmod n$$

$$D(E(m)^k \bmod n^2) = \mathrm{k}m \bmod n$$

$$D(E(m_1) g^{m_2} \bmod n^2) = m_1 + m_2 \bmod n$$

$$D(E(m_1)^{m^2} \bmod n^2) = D(E(m_1)^{m^2} \bmod n^2) = m_1 m_2 \bmod n$$

自盲属性(self-blinding)如下：

$$\forall m_1, m_2 \in Z_n, r \in N$$

$$D(E(m) r^n \bmod n^2) = m$$

2.6 混 淆 网

混淆网(mix-net)是实现通信匿名性的一种关键技术。匿名性指用户在访问资源或服务时不能泄露其身份。2006 年，Tatli 等[16]把匿名性分为两种：通信匿名性和内容匿名性。通信匿名性受到人们的重点关注。他们同时指出有三种方法可以实现通信匿名性：代理、对等网和混淆网[17]。

基于代理的方法实现通信匿名性，发送方和接收方必须相信从发送方收到的消息已经进行了某种变换来隐藏发送方的身份。反之，当代理从接收方得到消息，把消息发送给真正的发送方。通常，基于代理的方法存在两个缺点：一个是用户必须无条件信任代理，另外一个是在用户和代理之间的信道没有保护机制。基于对等网实现通信匿名性，用户随机选择发送消息的路径，把消息发送给最终的接收者。这种方法不需要信任系统中的某一方。基于混淆网来实现通信匿名性，混淆网由一系列的实体：混淆服务器组成。每个混淆服务器都有自己的公钥。每个混淆服务器接收到加密的消息，然后解密，批处理，重新排序，隐藏发送者的相关信息后发送给接收者。在远程网络投票协议中，主要用这种方法实现匿名性。安全的混淆网应该具有正确性、隐私性、健壮性、高效性和普遍可验证性。正确性指如果所有的混淆服务器是诚实的，那么结果就是正确的。隐私性隐含着如果一个固定最小数量的混淆服务器是诚实的，那么发送方的隐私性就可以得到保证。健壮性是指如果一定数量的混淆服务器是诚实的，那么可以防止任何欺骗和攻击。高效性指验证者的负载与混淆服务器的数量之间没有关系。普遍可验证性是指解密结果的正确性可以被任何验证者验证。主要思想是通过洗牌改变和修改对象的顺序来隐藏最初的和最后的排序之间的对应关系。Chaum 把它作为匿名信道的一种实现方式。

1981 年，Chaum[17]提出第一个基于 RSA 的混淆网，并且证明可以抵抗被动攻击。被动攻击者可以监控在混淆服务器之间所有通信但是不能够得到混淆服务器内部每个混淆的排列。1990 年，Pfitzmann[18]指出发送方的主动攻击比简单的重复密文攻击更加的复杂。1995 年，Sako 和 Kilian[19]基于零知识证明，首先提出一个普遍可验证的混淆网。主要思想是每个混淆服务器必须提供其正确执行相关操作的零知识证明。1997 年，Ogata 等[20]证明健壮的混淆网同时也是普遍可验证的。2000 年，Mitom 和 Kurosawa[21]证明如果 κ 是安全参数，t 标识邪恶的混淆服

务器个数,那么每个混淆服务器的计算复杂度是 O(κtN),外部验证者的计算复杂度也是 O(κtN)。2000 年,Mitom 和 Kurosawa[21]指出在 Chaum 混淆网中应用的是 RSA 加密体制,因此,每个密文的大小与混淆服务器的个数是成正比关系。1998 年,Abe[22]设计了一个健壮的混淆网,其外部验证者计算复杂度是O(κN)。2000 年,Jakobsson[23]设计了一个更加高效健壮的混淆网,然而其不具有普遍可验证性,在 2000 年,Desmedt 和 Kurosawa[24]攻破了它。1999 年,Jakobsson[25]又提出一个健壮的混淆网(flash mixing),可以抵抗攻击[24]。2000 年,Mitom 和 Kurosawa[21]应用一个变种攻击[24],攻破了混淆网[25],同时他也给出了防止此攻击的解决方法。2007 年,Li 等[26]发现混淆网[27]不具有(t,N-2)适应性。1995 年,Pfitzmann[28]提出了一个通用的对混淆网的攻击方法。1996 年,Michels 和 Horster[29]又提出了其他的攻击方法。2003 年,Wikström[30]提出了对协议[31]的攻击方法。同年,Abe 和 Imai[32]独立发现了对混淆网[31,33]的攻击方法,同时给出了匿名性和健壮性的形式化模型,但是没有提出具有这些安全性的混淆网。2004 年,Wikström[34]提出了普遍可组合混淆网的思想,同时也给出了一个完整的构造和证明。一个非常重要的构造混淆网的工具是可证明的扰乱(proof of shuffle):通过每个混淆服务器执行一个可验证的扰乱,观察者可以确信每个混淆服务器在正确的运行。对多个数据项,如果多个相互不信任的实体连续的执行了多个可验证的扰乱,那么任何人不知道洗牌的结果。一个可验证的扰乱的输入是 n 个加密的消息,然后扰乱这些消息,也就是对它们进行随机排序,同时通过再加密替换掉原来的消息,输出扰乱的和再加密的消息。2001 年,Neff[35]、Furukawa 和 Sako[36]分别独立地提出了实现可验证扰乱高效算法。2003 年,Groth[37]对 Neff 的方法进行了扩展并且对其效率进行了改进。后来,其他的作者也对其进行了改进和完善[38,39]。2005 年,Wikström[40]首先提出一个基于 ElGamal 密码体制的混淆网。每个混淆服务器对输入部分的解密和洗牌,叫做发送方可验证。它没有用到再加密技术。同时基于 UC 框架证明了其存在任意少数混淆服务器腐败情况下的安全性。同时,他构造了第一个加密-置换扰乱的证明,表明其可以转换为 UC 框架下的零知识证明。2007 年,Adida 和 Wikström[41]基于 BGN 密码系统构造了一个解密扰乱和基于 Paillier 加密系统再加密扰乱,但是效率非常低。2012 年,Demirel 等[42]对混淆网的最新发展现状作了介绍。

下面介绍混淆网的基本结构,如图 2.2 所示。$E_{PK}(m)$表示用混淆服务器的公钥 PK 加密 m。

假设有 n 个消息的发送者 S_1,…,S_i,…,S_n,每个 S_i 想发送消息 m_i 给 R_i,如果采用混淆网,则 S_i 和 R_i 之间的对应关系是秘密的。

(1) 简单的混淆网匿名通道,存在一个混淆网 x 服务器。

每个 S_i 选择一个随机数 r_i,计算 $c_i = E_{PK_M}(r_i, R_i, E_{PK_{R_i}}(m_i))$,混淆网服务器

解密,丢掉 r_i,以字母排列发布 $R_i, E_{PK_{R_i}}(m_i)$。

在这个协议中,只有混淆网服务器知道 S_i 和 R_i 之间的对应关系,其他人都不知道。为了更好地隐藏 S_i 和 R_i 之间的对应关系,可以用 k 个混淆网服务器,$Mix_1, \cdots, Mix_k$。

(2) k 个混淆服务器的匿名通道,存在 k 个混淆服务器。

每个 S_i 选择一个随机数 r_i,计算

$$E_{PK_1}(r_1, E_{PK_2}(r_2, \cdots, E_{PK_k}(r_k, R_i, E_{PK_{R_i}}(m_i), \cdots)))$$

此时,一般说 S_i 发送 $R_i, E_{PK_{R_i}}(m_i)$到 k 个混淆匿名通道。

Mix_1 解密,丢掉 r_1,把 $E_{PK_2}(r_2, \cdots, E_{PK_k}(r_k, R_i, E_{PK_{R_i}}(m_i), \cdots))$,以字典顺序排列在公告板上。

$Mix_2, \cdots, Mix_{k-1}$ 执行相同的动作。

最后 Mix_k 把 $R_i, E_{PK_{R_i}}(m_i)$在公告板上以字典顺序排列。

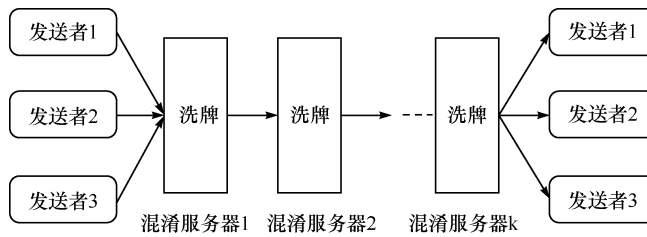

图 2.2 混淆网结构

在这个协议中,只要有一个混淆服务器诚实,那么 S_i 和 R_i 的对应关系就是秘密的。

2.7 Fiat-Shamir 启发式

1987 年,Fiat 和 Shamir[43]提出了一个通用方法,可以将验证者诚实的安全零知识协议转化为数字签名方案。把这种方法叫做 Fiat-Shamir 启发式。

一般用(commit,challenge,response)表示一个验证者诚实的零知识协议的副本,为了构造消息 $m \in \{0,1\}^*$ 的数字签名,应用散列函数 $HASH: challenge \leftarrow HASH(m \| commit)$。Fiat-Shamir 启发式是可以公开验证的,可以像验证数字签名那样验证隐藏在散列函数中的断言。

2.8 离散对数相等知识证明

离散对数相等的知识证明[8,10,11](proofs of knowledge for equality of discrete

logarithms)是用知识证明的方式来证明两个离散对数的相等。

示证者有$(g,x,h,y)(g,x,h,y\in Z_p)$。而且知道 $\alpha\in Z_p$ 满足 $x=g^{\alpha}$ 和 $y=h^{\alpha}$。验证者是诚实的验证者。图 2.3 描述的是交互式的版本。应用 Fiat-Shamir 启发式可以把图 2.3 中的交互式的版本变为非交互式的版本。

非交互式的版本如下:首先示证者还是按照非交互式版本中那样计算,只是令挑战 $c=HASH(a\| b\| x\| y)$。然后,验证者检查

$$c\overset{?}{=}HASH(g^{r}x^{-c}\| h^{r}y^{-c}\| x\| y)$$

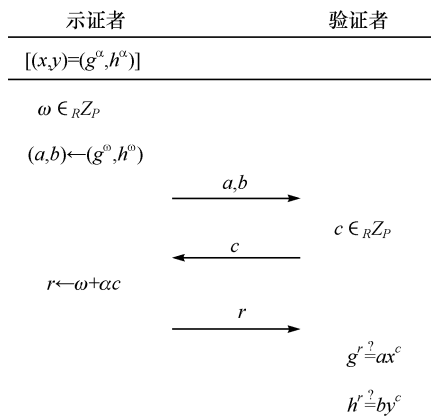

图 2.3　关于 $\log_g x=\log_h y$ 的知识证明

2.9　BCP 承诺方案

陷门承诺方案[44]的抗碰撞性是指除非知道陷门,否则找到两个不同的输入,产生相同的值是不可能的。另一方面,知道陷门信息可以很容易构造碰撞。一个陷门承诺方案是由密码生成算法、承诺函数和碰撞构造函数组成的。下面介绍陷门承诺的概念和 BCP 陷门承诺方案[3]。

(1) 陷门承诺。

陷门承诺也叫做变色龙承诺(chameleon commitment)。C 是一个函数,输入是(y_i,w,r),y_i 是验证者的公钥,对应的私钥是 x_i,w 是承诺的值,r 是一个随机数。C 是一个陷门承诺如果满足以下条件:

① 如果不知道 y_i 的秘密部分,承诺是绑定的,即不能够找到一对碰撞$(w_1,r_1),(w_2,r_2)$使得 $C(y_i,w_1,r_1)=C(y_i,w_2,r_2)$。

② 给出 y_i 和 $C(y_i,w,r)$,不能够计算出 w。

③ 利用 y_i 的秘密部分,很容易计算出任意数量的碰撞对。