河海大学

硕士学位论文

盲签名理论研究及应用

姓名：龚少麟

申请学位级别：硕士

专业：通信与信息系统

指导教师：赵泽茂

20050601

摘 要

随着计算机网络技术的发展，网络信息安全问题日益突出。作为信息安全核心技术基础之一的数字签名技术，被广泛应用于军事、通信、电子商务等领域，并且随着“电子签名法”的颁布和实施，这种应用将变得越来越普遍。

首先，本文简单介绍了数字签名、盲签名、数字证书、哈希函数等基本概念以及典型的盲签名方案，如 RSA 盲签名方案、Schnorr 盲签名方案和 ElGamal 盲签名方案，并介绍了盲签名技术在电子现金系统和电子投票系统中的应用现状。然后，对谭作文等人提出的代理盲签名方案进行了改进，设计了一种基于 Schnorr 盲签名的代理盲签名方案，并进行了理论证明和实验分析。该方案能够满足代理盲签名的安全性要求，并且缩短了计算时间，提高了计算效率。

其次，在 ElGamal 强盲签名的基础上设计了一种多重盲签名方案，对安全性进行了理论分析。该方案实现了多人同时对消息的盲签名，并且具有盲性和不可追踪性等性质。基于盲签名技术提出了一种匿名电子投票协议，该协议能够保证投票人身份的匿名性，并且可以防止一人多票或一票多投现象的发生。在这个协议的基础上提出了匿名电子投票系统的设计方案，对系统各功能模块进行了详细的设计，并编程实现了部分功能。最后，提出了盲签名技术的进一步改进和研究设想，并对未来的发展趋势进行了展望。

关键词：数字签名；盲签名；代理盲签名；多重盲签名；电子投票

Abstract

With the development of computer network technology, network information security problem becomes more and more important. Digital signature as one of key technology of the information security is widely used in military, communication, e-commerce, etc. With "electronic signature law" being put into practice, the application of digital signature will become more and more popular.

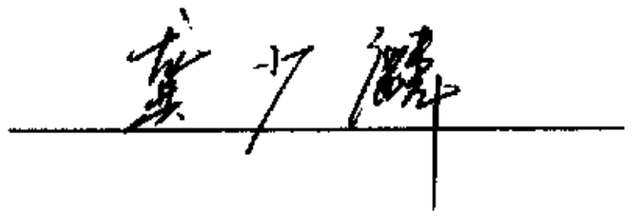
The paper firstly introduces some basic conceptions of cryptography, such as digital signature, blind signature, digital certification, hash function etc and typical blind signature schemes, for instance, RSA blind signature scheme, Schnorr blind signature scheme and ElGamal blind signature scheme. The wide use of blind signature theory in e-vote system and e-cash system is also summarized. Besides, Tan's proxy blind signature scheme is improved and a proxy blind signature scheme based on Schnorr blind signature is designed with the theory proving and test analysis. Our scheme could satisfy security request of proxy blind signature. Compared with Tan's scheme, the improved proxy blind signature scheme shortens the time of signing and improves the efficiency of signing effectively.

Secondly, A multiple blind signature scheme based on ElGamal strong blind signature scheme is designed with theory analysis to the security of the scheme. It is possible for many signers to sign at the same time by using this scheme and this scheme has both properties of blind and untraceable. Finally, this paper presents an anonymous electronic vote protocol on the basis of blind signature technology and security analysis of this protocol is presented in detail. The protocol can realize anonymity of voter of identity and prevent that one people have two votes or the same vote is thrown many times. Then an anonymous electronic vote system scheme based on this protocol is proposed. This paper provides the design of function modules in detail and a part of programming code is given. In the end, this paper presents the assumption of the further improvement and research of blind signature theory and looks forward to the development trend of blind signature theory in the future.

Keyword: digital signature; blind signature; proxy blind signature; multiple blind signature; electronic vote

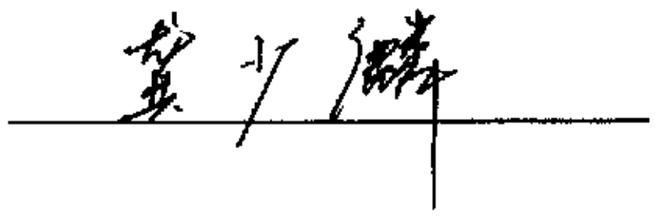
学位论文独创性声明：

本人所呈交的学位论文是我个人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果。与我一同工作的同事对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。如不实，本人负全部责任。

论文作者（签名）：  2005 年 6 月 8 日

学位论文使用授权说明

河海大学、中国科学技术信息研究所、国家图书馆、中国学术期刊（光盘版）电子杂志社有权保留本人所送交学位论文的复印件或电子文档，可以采用影印、缩印或其他复制手段保存论文。本人电子文档的内容和纸质论文的内容相一致。除在保密期内的保密论文外，允许论文被查阅和借阅。论文全部或部分内容的公布(包括刊登)授权河海大学研究生院办理。

论文作者（签名）：  2005 年 6 月 8 日

第一章 绪 论

1.1 研究背景

随着电子信息技术的迅速发展，人类已步入信息社会。由于整个社会将形成一个巨大的计算机网络，所以信息安全、计算机网络安全问题已引起了各国的高度重视。计算机作为国家的关键基础设施和战略命脉，其安全状况直接关系到国家的安全和发展。随着我国信息化进程的加快，网络化将向政府机关、经济部门、军队、学校、社会团体以及家庭等方面延伸，先进的计算机系统把整个社会乃至军队联结起来。

我国的信息安全形势不容乐观。2000 年以来，建设了一批信息安全基础设施，加强了互联网信息内容的安全管理，信息安全保障工作取得一些成效。由于基础薄弱，工作人员防范意识淡薄，安全隐患巨大。首先，网上的重大失窃密案件多有发生；反动邪教法轮功和民运分子等境内外敌对势力利用因特网从事各种违法犯罪活动，对社会稳定和政权巩固造成了许多负面影响。其次，我国网络金融安全隐患巨大，我国银行网络每年因安全问题包括外部攻击、内外勾结、内部人员违法犯罪和技术缺陷引起的经济损失数以亿计。再次，全国各地都发生过涉及个人隐私、名誉权遭到侵害的网络信息案件，而遭受的更多是意识形态的文化方面的渗透，这也是利用信息战进行和平演变的一个重要方面。信息网络存在严重隐患还表现在，不能快速有效抑制各种计算机病毒的入侵，2003 年初至年底我国连续遭受“口令”、“冲击波”、“大无极”等病毒袭击，这些病毒都给计算机用户造成了较严重的损失，究其造成损失的原因，均属于没有及时做软件的漏洞修补。根据国家计算机病毒应急处理中心的调查显示：2003 年中国计算机病毒感染率高达 85.57%，因病毒感染造成经济损失的比率达到了 63.57%。上述安全问题，已覆盖了各个重要敏感的安全领域，随着国家信息化的进一步发展，还将更充分更深入地暴露出我国信息网络的安全隐患，遭受更大的威胁和风险。

信息安全技术在信息化迅速发展的今天已进入了高速发展的新时期，形成了密码技术、可信计算技术、电磁辐射泄露防护技术、系统入侵检测技术和计算机病毒检测消除技术等多个安全防护技术门类。由于网络和信息技术本身均属于高科技的范畴，因此技术因素在网络及信息安全领域内的作用是不可替代的，但同时应充分认清的一点是，网络及信息安全问题并不只是单纯的技术因素能解决的问题。

人们在网络空间中的活动模式与常规的以地域为分界的国家政权管理模

式存在很大的差异性，这种差异性将直接导致许多技术手段无法有效发挥作用，特别是在涉及到跨国的审计追踪和责任追查等问题上。现阶段网络空间暂时的管理真空以及个人在网络空间对各类信息的超强获取能力所导致人们自我意识的过度膨胀和政府权威性的下降，将进一步降低了管理措施实施的有效性。因此网络及信息安全的全面解决方案将是一个涉及到管理、法律、技术等多方面的综合性措施，必须对整个网络及信息安全事业的发展进行全局的规划。

面向新世纪信息化建设的需要，政府把采取技术手段与加强日常管理和健全体制紧密结合起来，使信息安全由应对防护向综合保障转变：抓好组织管理体系建设，完善信息安全管理体制；加快法制建设步伐，健全信息安全保障体系；加强国民安全意识教育，增强信息安全防范意识；加强人才培养与管理，提高信息安全运行效率；加快制定相关技术标准，建立中国的信息安全标准体系；加大资金投入力度，扶植关键技术研发和产业化。

1.2 研究的目的及意义

在现实生活中，长期以来文件上的手写签名一直被用作签名者身份的证明。这是因为：签名是可信的；签名是不可伪造的；签名是不可重用的；签名的文件是不可改变的；签名是不可抵赖的。在未来社会的生活中，电子文档将逐步代替纸质的文件成为信息交流的主体。证明某一个电子文件是某作者所作的有效办法是模拟普通的手写签名在电子文档上进行电子签名，即在电子化文件中添加可以标记自己的一段特征数据来实现签名。作者可以通过数字签名表明自己的身份，读者可以通过数字签名验证作者的身份。

数字签名[1][2][3]的应用是有效解决网络身份识别认证、网络资源授权、网络公文处理和法律证据等问题的重要途径之一，可广泛地应用于证券、银行、电子商务、政务办公系统和企业安全应用网关等，市场前景极为广阔、潜力巨大。2000 年，中国人民银行牵头，由 13 家商业银行共同出资成立了中国最具权威的 CA 机构---中国金融认证中心（CFCA）。河北省电子商务认证有限公司开发的 3SAS 系统，成功的解决了 WEB 站点的用户身份认证和交易的数字签名问题，保障企业电子商务活动的安全进行。数字签名技术是网络通信中保障信息安全的关键技术，特别是盲签名技术，它对于具有匿名性要求的网络通信具有独特的地位和作用，被广泛的应用于电子支付系统和电子投票系统中。

“电子签名”是法律上的重要的创新概念，将其作为种种电子认证技术在法律上的总括，得到许多国家的采纳。不仅如此，联合国国际贸易法委员会电子商务工作组一直以《电子签名统一规则》作为拟定草案的标题，并得到为数众多国家的一致认同，而欧盟相关指令也同样以“电子签名”为题。自世界上第一部电子签名立法——美国犹它州《数字签名法》颁布实施以来，迄今为止，

意大利、德国、马来西亚、新加坡、韩国、美国、爱尔兰等也相继颁布了自己的电子签名法。

2004 年 3 月 24 日国务院常务会议原则通过了《电子签名法(草案)》;

2004 年 4 月 6 日十届全国人大常委会第八次会议初审《电子签名法(草案)》;

2004 年 6 月 21 日十届全国人大常委会第十次会议二审《电子签名法(草案)》;

2004 年 8 月 23 日十届全国人大常委会第十一次会议三审《电子签名法(草案)》;

2004 年 8 月 28 日十届全国人大常委会第十一次会议表决通过《电子签名法》。

几经周折，作为我国信息网络法律开山之作的《电子签名法》也于 2004 年 8 月 28 日十届全国人大常委会第十一次会议表决通过，被享有“首部真正意义上的信息化法律”的殊荣。

电子签名法的出台既是适应信息化发展的应急之需，也是根本之路，它将对我国电子商务、电子政务的发展起到极其重要的促进作用。该法对确定电子签名的法律效力、规范电子签名的行为、明确电子认证服务机构的法律地位及电子签名的安全保障措施等多个方面作了具体规定，使电子商务和电子政务的实施有了明确的法律主体。可以说，电子签名法是我国电子商务发展的里程碑，标志着我国法律体系正式迈入网络时代。

1.3 盲签名理论研究现状

数字签名是认证的主要手段之一，也是现代密码学的主要研究内容之一。数字签名是日常生活中手写签名的电子对应物，它的主要功能是实现用户对电子形式存放消息的认证。目前有关数字签名的研究内容非常丰富，可分为普通签名和特殊签名两类。特殊签名包括群签名、盲签名、带消息恢复的签名、代理签名、不可否认签名、公平盲签名、门限签名等，各种签名与具体的应用环境密切相关。

传统的数字签名的一个基本的特征是签名者知道所签消息的内容。但在某些特殊情况下，人们并不希望这样。盲签名[4][5][6]正是这样一种特殊的签名，一个盲签名方案不仅保留有数字签名的各类特性，而且还拥有以下一些特殊的性质：

(1) 盲性：消息的内容对签名者是不可见的。

(2) 不可追踪性：签名者后来看到签名时不能把签名和盲消息对应起来。

正是这些特点，使得盲签名这种技术可广泛用于许多领域，如电子投票系统和电子支付系统等。近年来，国内外学者对盲签名理论进行了深入的探讨与

研究，并取得了丰富的研究成果。1982年，Dr.Chaum[7]首次提出了盲签名的概念。随后，人们分别基于因子分解问题（即FP）、离散对数问题（即DLP）、二次剩余（即QR）相继提出各种盲签名方案。

基于因子分解问题的盲签名方案的研究成果主要有：

1983年，Chaum[8]基于RSA公钥密码系统提出了一个盲签名方案。1992年，Solms[9]等提出一种完美的勒索和洗钱的方法。1993年，Micali提出公平密码系统的概念以防止犯罪分子对密码系统的滥用。然而，Stadler等[10]认为匿名性和不可追踪性仍有可能被犯罪分子所滥用。为了避免犯罪分子的这种行为，Stadler建议在匿名支付系统中应该建立一个可信的第三方，例如法官。Cohen等[11]认为一个签名伪造策略（消息选择攻击的一个分支）可能会给RSA数字签名系统带来麻烦。因此，Fan等[12]提出了一个盲签名方案以增强Chaum盲签名方案的随机性，这样攻击者就不能计算出签名者的签名以避免消息选择攻击的威胁。2001年，Chien等[13]基于RSA公钥密码系统提出了一个部分盲签名方案，该方案可以减少数据库的大小以及避免电子现金系统的重复花费。

基于离散对数问题的盲签名方案的研究成果主要有：

1992年，Okamoto[14]基于Schnorr签名体制提出了一个盲签名方案。1994年Camenisch等[15]基于离散对数问题提出了两个盲签名方案。第一个方案来源于DSA的变形，第二个方案是以Nyberg-Rueppel签名体制为基础的。然而，1995年Harn[16]指出这两个方案都不能满足不可追踪性的要求，签名者可以追踪到消息拥有者并获得消息签名对。2000年，Mohammed等[17]基于ElGamal数字签名体制提出了一个盲签名方案。

关于二次剩余问题，学者们也做了许多工作，取得了一些成果。Fan等[18]于1996年提出一个盲签名方案，该方案的安全性是基于二次剩余方根的难解性。1998年，Fan等[19]提出一个部分盲签名方案，该方案能减少电子现金系统的计算量和数据库的大小。然而，Hwang等[20]指出该方案不能满足不可追踪性的要求。同一年，Fan等[21]又提出一个盲签名方案以提高方案[15]的计算效率。2001年，Fan等给出了一个Shao方案的攻击方法，该方法可以伪造一个合法的签名以替代合法签名者的签名。

现有的大多数电子现金系统都是基于由单个银行发行电子现金的模型，所有的用户与商家在同一家银行拥有帐户。而在现实世界中，电子现金可能是在一个中央银行监控下，由一群银行发行的。为了适应多银行电子现金系统的需求，因此，A.Lysyanskays和Z.Ramzan [22]将盲签名和群签名相结合提出了群盲签名的概念并给出了一个具体的方案，该方案是通过在 J.Camenish和M.Stadler的群签名基础上增加盲性质实现的。

人们考虑到电子现金可能是由开户银行的一个有效分支机构进行盲签名，

因此，2000 年 Lin 和 Jan[23]将代理签名和盲签名相结合提出了第一个代理盲签名方案。在此以后，Z. Tan, Z. liu 和 C. Tang[24]于 2002 年提出了一个基于 Schnorr 盲签名的代理盲签名方案，S. Lal 和 A. K. Awasthi[25]于 2003 年提出了一个基于 Mambo 代理签名的代理盲签名方案。

2001 年，祁明等[26]基于一个特殊的 ElGamal 型签名方案建立了一个新型盲签名方案，并在此基础上构造了一个多重盲签名方案，它使得多个签名人能够共同对盲化的消息实施签名。2002 年，黄少寅等[27]基于 Schnorr 体制提出了一个必须经多人同时盲签名才可生效的新方案，可以方便应用在电子现金需银行多个部门同时进行盲签名后才可生效的情形中。这些新方案在电子商务中具有广泛的应用。

盲签名一提出便受到广泛关注，但尚有许多问题需要进一步研究和解决：

(1) 目前很多盲签名方案还存在隐患，各种盲签名方案的安全性还有待进一步的检验；

(2) 目前大部分盲签名方案的计算复杂度高、通信量大、计算效率低，因此如何设计简单有效的盲签名方案还有待进一步研究；

(3) 如何更好的将盲签名和其它特殊签名相结合，如群签名、代理签名，构造群盲签名、代理盲签名；

(4) 如何有效的将盲签名技术运用于实际环境中以解决匿名认证的需求；

综上所述，盲签名技术对于具有匿名性要求的网络通信具有独特的地位和作用，研究盲签名技术具有理论上的前瞻性，应用上的可行性。同时，随着计算机网络技术的发展，人们对信息安全的要求也将越来越高，这将极大地推动盲签名技术的研究和应用，毫无疑问，盲签名技术具有比较长远的发展空间和广阔的市场前景。

1.4 作者所做的工作

盲签名是一种特殊的数字签名，盲签名所具有的匿名性使得这种技术可广泛用于许多领域。本文对盲签名理论进行了系统、深入地研究，对各种典型的盲签名方案及代理盲签名方案进行了分析及改进，并探讨了盲签名技术的应用。作者在这期间所做的工作总结如下：

(1) 对现有的盲签名体制进行了深入地分析和研究，并总结了盲签名技术在电子现金系统、电子投票系统中的广泛应用。

(2) 对谭作文等人的代理盲签名方案进行了分析，指出了方案中存在的不足，然后基于Schnorr盲签名设计了一种代理盲签名方案，对其进行了理论证明和试验分析。将其与谭作文等人的代理盲签名方案对比，结果表明该方案缩短了计算时间，提高了计算效率；

(3)对祁明提出的多重盲签名方案进行了分析，指出了方案中存在的不足，然后基于ElGamal强盲签名设计了一种多重盲签名方案，分析表明该方案可以实现多人同时对消息进行盲签名，并且在安全性上具有强盲性，可以同时满足盲性和不可追踪性。

(4)本文基于盲签名技术提出了一种匿名电子投票协议，对其安全性进行了详细的分析，结果表明该协议能够实现投票人身份的匿名性，并且可以防止一人多票或一票多投现象的发生。然后基于该协议设计了一个匿名电子投票系统，对该系统进行了详细设计，并给出了部分算法的实现。

1.5 论文结构与组织

本文的论文结构主要分为以下几章：

第一章主要介绍网络时代的数字签名技术发展趋势以及分析课题的研究现状。

第二章简要介绍了密码学概论，以及哈希函数、数字签名、盲签名、计算复杂性、安全协议等密码学基本概念，其中详细介绍了几种典型的盲签名方案，以及盲签名技术在计算机网络中的广泛应用。

第三章对谭作文等人的代理盲签名方案进行了分析和研究，基于 Schnorr 盲签名方案设计了一种代理盲签名方案，并将其与谭作文等人的代理盲签名方案进行了对比分析。

第四章对祁明提出的多重盲签名方案进行了分析和研究，基于 ElGamal 强盲签名设计了一个多重盲签名方案，对其进行了详细的分析。

第五章基于盲签名技术提出了一种匿名电子投票协议，对其进行了安全性分析，然后基于该协议提出了一个匿名电子投票系统，并给出了系统的详细设计以及部分算法的实现。

第二章 基本概念

密码学是一门既古老又年轻的学科，其历史可以追溯到几千年以前。在1949年之前，密码技术基本上可以说是一门技巧性很强的艺术，而不是一门科学。在这一时期，密码专家常常是凭借直觉和信念来进行密码设计和分析，而不是推理证明。

1949年C.E.Shannon发表了“保密系统的通信理论(Communication Theory of Security Systems)”一文，为密码学奠基了坚实的理论基础，使密码学成为一门真正的科学，标志着现代密码学的诞生。1976年，W.Diffie和M.E.Hellman发表了“密码学中的新方向(New Direction in Cryptography)”一文，提出了一种崭新的密码设计思想，导致了密码学的一场革命。他们首次证明了从发送端到接收端无密钥传输的保密通信是可能的，从而开创了公钥密码学的新纪元。从此，现代密码学理论的研究和工程应用双双进入了疾驰的快车道。算法标准、公钥密码、身份证明与消息认证、数字签名标准、椭圆曲线密码、量子力学、混沌密码、序列密码等现代密码新理论的成果不断涌现。

一个密码体制(cryptosystem)通常由五部分组成：

(1)明文空间：全体明文的集合。

(2)密文空间：全体密文的集合。

(3)密钥空间：全体密钥的集合。通常每个密钥都由加密密钥和解密密钥组成，加密密钥和解密密钥可能相同也可能不同。

(4)加密算法：由加密密钥控制的加密变换的集合。

(5)解密算法：由解密密钥控制的解密变换的集合。

如果一个密码体制的加密密钥和解密密钥相同，则称其为单密钥密码体制或对称密码体制；否则，称其为双密钥密码体制或非对称密码体制。

对称加密系统最著名的是美国数据加密标准DES、AES(高级加密标准)和欧洲数据加密标准IDEA。1977年美国国家标准局正式公布实施了美国的数据加密标准DES，公开它的加密算法，并批准用于非机密单位和商业上的保密通信。加密与解密的密钥和流程是完全相同的，区别仅仅是加密与解密使用的子密钥序列的施加顺序刚好相反。但是，经过20多年的使用，已经发现DES很多不足之处，对DES的破解方法也日趋有效。AES将会替代DES成为新一代加密标准。

在对称密码系统中解密密钥和加密密钥相同或容易从加密密钥推出，因此加密密钥的暴露将会使系统变得不安全。非对称密码系统[28]解决了这些问题。在私钥密码系统中解密密钥和加密密钥不同，相互间也很难推出，通信双方不需要预先传递密钥。公钥密码的观点是1976年Diffie和Hellman首先提出来的，并导致了密码学的一场革命。1978年Rivest，Shamir和Adleman提出了

第一个比较完善的公钥密码算法 RSA。随后人们基于上面讨论的不同 NPC 问题，提出了大量的公钥密码算法，主要有 ElGamal 算法、Rabin 算法、Merke—Hellman 背包算法、McEliece 算法、二次剩余算法和椭圆曲线算法等。

2.1 哈希函数

哈希函数[29]是一种将任意长消息压缩到固定长消息摘要的函数。Hash 函数可分为两大类：一类是强碰撞自由的 Hash 函数，另一类是弱碰撞自由的 Hash 函数。将 Hash 函数应用到数字签名里可带来如下好处：

(1)可破坏数字签名方案的某些数学性质，如同态性。

(2)通过对消息摘要签名取代对消息签名，可以提高签名的速度。

(3)签名可以不包括原消息，增强了保密性。

(4)可以用公钥密码实现保密用私钥密码实现数字签名，从而将签名和加密分开处理。

Hash 函数除了可用于数字签名之外，还可以用于其他方面，譬如消息的完整性检测、消息的来源认证检测等方面。为保证消息的完整性，及时发现消息是否被非法篡改，可以在消息传输之前先对消息做 Hash 变换，然后对消息进行传输，对于接收到的消息也做 Hash 变换。将传输前的消息的 Hash 变换值与接收到的消息的 Hash 变换值作比较，如果两者相同，则可以认为消息在传输过程中没有被篡改，否则消息一定被非法篡改了。

Hash 函数的安全性是指：在现有的计算资源下，找到一个碰撞是不可能的。

综上所述，一个密码学上安全的 Hash 函数应具有以下性质：

(1) $H(\cdot)$ 的输入可以任意长。

(2) $H(\cdot)$ 的输出长度固定。

(3)对于任意消息 $H(m)$，计算 m 是不容易的。

(4)给定 $H(\cdot)$，找出一对碰撞消息在计算上不可行的。

目前已经设计出大量的 Hash 函数，如 Rabin Hash 方案、Merkle Hash 方案、N—Hash 算法、MD4 算法、MD5 算法、SHA 等。在 2004 年 8 月 17 日召开的国际密码学会议（Crypto'2004）上，来自山东大学的王小云教授做了破译 MD5、HAVAL-128、MD4 和 RIPEMD 算法的报告，引起全球密码学界的广泛关注。

2.2 数字签名

在现实生活中，人们常常需要进行身份鉴别、数据完整性认证和抗否认。

身份鉴别允许我们确认一个人的身份；数据完整性认证则帮助我们识别消息的真伪、是否完整；抗否认则防止人们否认自己曾经做过的行为。传统商业中的契约以及个人之间的书信等常常采用手书签名、印章和封印等手段便获得在法律上认可的身份鉴别、数据完整性认证和抗否认效果。

1、数字签名的定义与分类

一般数字签名方案包括 3 个过程：系统的初始化过程、签名产生过程和签名验证过程。系统的初始化过程产生数字签名方案用到的一切参数；签名产生过程中，用户利用给定的算法对消息产生签名；签名验证过程中，验证者利用公开的验证方法对给定消息的签名进行验证，得出签名的有效性。下面给出数字签名的形式化定义：

(1)系统的初始化过程

产生签名方案中的基本参数$(\mathrm{M,S,K,SIG,VER})$，其中：M 是消息集合，S 是签名集合，K 是密钥集合，包含私钥PK 和公钥SK，SIG 是签名算法集合，VER 签名验证算法集合。

(2)签名产生过程

对于密钥集合K，相应的签名算法为$\mathrm{sig_K} \in \mathrm{SIG}$，$\mathrm{sig_K} : \mathrm{M} \to \mathrm{S}$，对任意的消息$m \in \mathrm{M}$，有$s = \mathrm{sig_K}(m)$，那么$s \in \mathrm{S}$为消息$m$的签名，将$(m,s)$发送到签名验证者。

(3)验证签名过程

对于密钥集合K，有签名验证算法

$$\mathrm{ver_K} : \mathrm{M} \times \mathrm{S} \to \{\mathrm{True,False}\}$$

$$\mathrm{ver_K}(m,s) = \begin{cases} \mathrm{True}, & s = \mathrm{sig_k}(m) \\ \mathrm{False}, & s \neq \mathrm{sig_k}(m) \end{cases}$$

签名验证者收到(m,s)后，计算$\mathrm{ver_K}(x,y)$，若$\mathrm{ver_K}(x,y) = \mathrm{True}$，签名有效；否则，签名无效。

按照不同的标准，数字签名方案有不同的分类方法。

(1)基于数学难题的分类

根据数字签名方案所基于的数学难题，数字签名方案可以分为基于离散对数问题的签名方案和素因子分解问题的签名方案。ElGamal 数字签名方案和 DSA 数字签名方案都是基于离散对数问题的数字签名方案，而 RSA 数字签名方案是基于素因子分解问题的数字签名方案。将离散对数问题和因子分解问题结合起来，又可以产生同时基于离散对数和素因子分解问题的数字签名方案。例

如，1994 年 Harn 设计的一种数字签名方案；1997 年 Laih 和 Kuo 设计的一种新的数字签名方案。二次剩余问题可以认为是素因子分解问题的特殊情况，因此，基于二次剩余问题同样可以设计多种数字签名方案，例如 Rabin 数字签名方案，1997 年 Nyang 和 Song 所设计的快速数字签名方案。

(2)基于签名用户的分类

根据签名用户的情况，可将数字签名方案分为单个用户签名的数字签名方案和多个用户的数字签名方案。一般的数字签名是单个用户签名方案，而多个用户的签名方案又称多重数字签名方案（multisignature scheme）。根据签名过程的不同，多重数字签名可分为有序多重数字签名方案（sequential multisignature scheme）和广播多重数字签名方案（broadcasting multisignature scheme）。

(3)基于数字签名所具有特性的分类

根据数字签名方案是否具有消息自动恢复特性（message recovery），可将数字签名方案分为两类：一类不具有消息自动恢复的特性，另一类具有消息恢复的特性。一般的数字签名不具有消息自动恢复特性，例如最初的 ElGamal 数字签名。1994 年，Nyberg 和 Ruepple 首次提出一类基于离散对数问题的具有消息自动恢复特性的数字签名方案。

2、数字签名的特征与作用

数字签名的作用主要有两个：第一，信源识别(或称身份认证)，即接收者能够核实发送者发送的报文签名，发送者事后也不能否认发送的报文签名；第二，检验发送消息的完整性(或称为消息认证)，即验证消息在传送的过程中是否被篡改、重放或延迟。数字签名应具有以下特性：

(1)签名是可信的。签名使消息的接收者相信签名者慎重地签署了该消息。

(2)签名是不可伪造的。除了合法的签名者之外，任何其他人伪造其签名是困难的。

(3)签名是不可复制的。对一个消息的签名不能通过复制变为另一个消息的签名。如果对一个消息的签名是从别处复制得到的，则任何人都可以发现消息和签名之间的不一致性，从而可以拒绝签名的消息。

(4)签名后的消息是不能更改的。一旦签名的消息被篡改，则任何人都可以发现消息和签名之间的不一致性。

(5)签名是不可否认的。签名者不能事后声称他没有签署过该消息。

3、数字签名的应用

在网络的数字化社会中，由于 Internet 的自身特点，人们在通过网络进行活动时，迫切需要一种能够进行身份鉴别、数据完整性认证和抗否认的技术，这样，数字签名（Digital Signature）技术应运而生，推动和加速了网络电子商

务活动的发展。

SET（Secure Electronic Transaction）由 Visa 和 MasterCard 所开发，是为了在 Internet 上进行在线交易时保证信用卡支付的安全而设立的一个开放的规范。它得到了 IBM，HP，Microsoft，Netscape，VeriFone，GTE，Verisign 等很多大公司的支持。SET 所使用的加密技术有对称密码体制（如 DES）、非对称密码体制（如 RSA）、数字信封、数字签名、消息摘要以及双重签名。双重签名使订单信息和个人帐号信息隔离，将包括持卡/帐号信息的订单送到商家时，商家只能看到定货信息，而看不到持卡人的帐户信息。湖南邮电、IBM 及中国银行湖南分行联手合作，已推出中国第一套基于 SET 的电子商务系统。该系统包括电子身份发放机制、支付网关、商业服务器和电子钱包，目前这个系统已投入运行。

盲签名是一种很有用的密码技术，实际上是一种特殊的数字签名，除了满足一般数字签名的基本特征外，它还满足两个附加条件：①签名者对其所签的信息是不可见的，即签名者不知道他所签的信息内容；②签名信息不可追踪，即当签名信息被其所有者公布后，签名者无法知道这是他哪一次签名。现在盲签名技术被广泛应用在很多重要的实际工作中，特别是那些强调用户隐私性的服务，例如安全的投票，智能网中的电话投票业务，Internet 上的电子银行、数字现金等。荷兰有一家公司 Digicash 已经开发出基于数字现金协议的密码产品。

2.3 盲签名

2.3.1 盲签名概述

随着 Internet 电子商务的发展和金融电子化的普及，传统的交易方式正在发生着一场深刻的变革。电子现金作为电子商务中的一种重要支付手段，日益受到国内外学者的重视，其研究也在不断深入。由于用户的个人消费信息（如时间、形式、内容等）对商家、银行或非法组织具有极其重要的意义，因此电子现金系统必须保护用户的隐私，即所谓的匿名性。实现匿名性的关键技术是 D. Chaum 提出的盲签名。

D. Chaum 关于盲签名曾经给出一个非常直观的说明：所谓盲签名，就是先将要隐蔽的文件放进信封里，当文件在一个信封中时，任何人都不能读它。对文件签名就是通过在信封里放一张复写纸，当签名者在信封上签名时，他的签名便透过复写纸签到了文件上。一个盲签名方案不仅保留有数字签名的各类特性，而且还拥有一些特殊的性质，如下所示：

(1) 盲性：消息的内容对签名人来说是盲化的，签名人看不到消息的内容。

(2) 不可追踪性：签名者仅知 $sig(m')$，而不知 $sig(m)$，其中 m, m' 分别为原

始消息和盲化消息。即使签名者保留签名 $sig(m')$ 及其它有关数据，仍难以找出 $sig(m)$ 和 $sig(m')$ 之间的内在联系，不可能对消息 m 的拥有者进行追踪。

到目前为止，虽然提出了许多种不同的盲签名，但还没有对各种盲签名进行系统的分类。祁明[30]将盲签名分为盲消息签名、盲参数签名、弱盲签名和强盲签名。作者认为，严格说来这不能作为一种分类方法，但是，沿着祁明的思路可以进行如下的分类：

(1)按照不同的盲化对象划分：

盲消息签名方案：盲消息签名仅对待签名的消息 m 进行了盲化。在盲消息签名方案中，签名者对盲消息 m' 签名，并不知道真实消息 m 的具体内容。这类签名的特征是 $\mathrm{sig}(m)=\mathrm{sig}(m')$ 或 $\mathrm{sig}(m)$ 含 $\mathrm{sig}(m')$ 中的部分数据。盲消息签名方案在电子商务中一般不用于构造电子货币支付系统。

签名被盲化方案：在盲参数签名方案中，签名者知道所签消息 m 的具体内容，消息拥有者仅对签名 $\mathrm{sig}(m')$ 进行了盲化，即改变 $\mathrm{sig}(m')$ 而得到新的签名 $\mathrm{sig}(m)$，但又不影响对新签名的验证。盲参数签名的这些性质可以用于电子商务系统 CA 中心为交易双方颁发口令，另外，利用盲参数签名方案还可以构造代理签名机制中的原始签名人和代理签名人之间的授权方程，以用于多层 CA 机制中证书的签发和验证。

(2)按照消息拥有者对签名人是否可以追踪进行分类：

弱盲签名：在弱盲签名方案中，消息拥有者对消息 m 和签名 $\mathrm{sig}(m')$ 进行了盲化。若签名者保留 $\mathrm{sig}(m')$ 及有关数据，待 $\mathrm{sig}(m)$ 公开后，签名者可以找出 $\mathrm{sig}(m')$ 和 $\mathrm{sig}(m)$ 的内在联系，从而达到对消息 m 拥有者的追踪。

强盲签名：在强盲签名方案中，消息拥有者对消息 m 和签名 $\mathrm{sig}(m')$ 进行了盲化。即使签名者保留 $\mathrm{sig}(m')$ 及其它有关数据，仍难以找出 $\mathrm{sig}(m)$ 和 $\mathrm{sig}(m')$ 之间的内在联系，不可能对消息 m 的拥有者进行追踪。在电子支付系统和电子投票系统中，为了保障用户和投票者的匿名性及保密性，往往都采用强盲签名技术。

(3)按照签名人数的多少来划分：

简单盲签名(同盲消息签名方案)：如果签名人为一个人，则这时的签名就是普通的盲签名。

多重(群)盲消息签名：若签名人为一群人，则这时的签名就是多重(群)盲消息签名。该类签名方案必须经多人同时盲签名才可生效。

(4)按照签名人是否接受别人的代理来来划分：

简单盲签名：如果签名人不受别人委托，这时的签名就是普通的盲签名。

代理盲签名：如果原始签名人委托代理签名人行使其签名权，则这时的签名就称为代理盲签名。

2.3.2 典型的盲签名方案

1、RSA 盲签名方案

D.Chaum 在 1982 年 CRYPTO'82 上提出"用于不可跟踪支付的盲签"一文，文中提出一个基于 RSA 数字签名体制的盲签名方案。该方案是第一个盲签名方案，它主要用于电子选举系统和电子支付系统中保护用户的匿名性。该方案是目前性能最好的一个方案，大多数电子货币系统和电子投票系统的设计都采用此方案。签名协议如下：

(1)初始化阶段

签名者 B 取两个大素数 p,q，$n=p\cdot q$，$\varphi(n)=(p-1)(q-1)$，随机选取 e 满足 $1<e<\varphi(n)$ 且 $\gcd(e,n)=1$，计算 d 满足 $1<d<\varphi(n)$ 且 $de\equiv 1 \bmod \varphi(n)$，B 的公钥是 (n,e)，私钥是 d，$\mathrm{h}(\cdot)$ 是具有无碰撞性的哈希函数。

(2)签名阶段

步骤 1：消息拥有者 A 随机选取与 n 互素的 k，计算 $\tilde{m}=\mathrm{h}(m)\cdot k^e \bmod n$，并将 $\tilde{m}$ 发送给签名者 B.

步骤 2：B 接收到 $\tilde{m}$ 后，计算 $\tilde{s}=\tilde{m}^d \bmod n$，并将 $\tilde{s}$ 发送给 A.

步骤 3：A 接收到 $\tilde{s}$ 后，计算 $s=k^{-1}\tilde{s} \bmod n$，$s$ 是 B 对 $\mathrm{h}(m)$ 的签名，即 $s=\mathrm{h}(m)^d \bmod n$.

(3)验证阶段

计算 $\mathrm{h}'(m)\equiv s^e \bmod n$，若 $\mathrm{h}'(m)=\mathrm{h}(m)$ 成立，则验证了 s 是 B 对 $\mathrm{h}(m)$ 的盲签名，否则拒绝接受。

2、Schnorr 型盲签名方案

1992 年，Okamoto[31]基于 Schnorr 签名体制构造了一个盲签名方案，该方案的安全性依赖于离散对数问题的难解性。Schnorr 盲签名协议较复杂，需要

较多的交互过程。现将该签名协议描述如下：

(1)初始化阶段

签名者选择两个大素数 p,q，满足 $q|(p-1)$，$p \geq 2^{512}$ 及 $q \leq 2^{160}$，$g \in Z_p^*$ 且满足 $g^q = 1 \bmod p$，选取私钥 $1 < x < q$，令 $y = g^x \bmod p$，p,q,g,y 为公钥。$h(\cdot)$ 是具有无碰撞性的哈希函数。

(2)签名阶段：

步骤 1：签名者 B 随机选择 $k \in Z_q^*$，计算 $r = g^k \bmod p$，并将 r 发送给消息拥有者 A；

步骤 2：A 接收到 r 后，选择随机数 $\alpha,\beta \in Z_q^*$，然后计算 $r' = rg^{-\alpha} y^{-\beta} \bmod p$，$e' = h(r',m) \bmod q$，$e = e' + \beta \bmod q$，并将 e 发送给 B；

步骤 3：B 接收到 e 后，计算 $s = k - ex \bmod q$，并将 s 发送给 A；

步骤 4：A 接收到 s 后，计算 $s' = s - \alpha \bmod q$，则 (e',s') 即为消息 m 的盲签名。

(3)验证阶段

计算 $r'' = g^{s'} y^{e'} \bmod p$，若 $h(r'',m) = e'$ 成立，则接受 (e',s') 是对消息 m 的盲签名。否则拒绝接受。

3、ELGamal 型盲签名方案

2000 年，姚亦峰等[32]提出了利用二元仿射变换，以 Harn 和 Xu 提出的十八种安全广义 ELGamal 型数字签名方案为基础构造盲签名方案，利用该方法得到十八种相应的盲签名方案，进一步分析得到其中十二种方案是强盲签名方案，其余的六种方案只能构造弱盲签名方案，并给出一个具体的方案。ElGamal 型数字签名方案要求每次选取一个随机数，这可以保证对同一消息的两次签名的结果是不同的，这是一个很有价值的特性，而 RSA 数字签名方案则不具备这种特点。

方案一：

(1)初始化阶段

签名者选择大素数 p，g 是 Z_p^* 的一个生成元。选取私钥 $x \in Z_p^*$，令 $y = g^x \bmod p$，p,g,y 为公钥。

(2)签名阶段

步骤 1：签名者 B 任取 $\tilde{k} \in Z_{p-1}^*$，计算 $\tilde{r} = g^{\tilde{k}} \bmod p$，并将 $\tilde{r}$ 发送给消息

拥有者 A;

步骤 2: A 接收到 $\tilde{r}$ 后，任取 $\alpha,\beta \in Z_{p-1}^{*}$，计算 $r=\tilde{r}^{\alpha} g^{\beta} \bmod p$，$\tilde{m}=\alpha m \tilde{r} r^{-1} \bmod (p-1)$，并将 $\tilde{m}$ 发送给 B;

步骤 3: B 接收到 $\tilde{m}$ 后，利用自己的私钥 x 计算 $\tilde{s}=(x\tilde{r}+\tilde{k}\tilde{m}) \bmod (p-1)$，并将 $\tilde{s}$ 发送给 A;

步骤 4: A 接收到 $\tilde{s}$ 后，计算 $s=(\tilde{s} r \tilde{r}^{-1}+\beta m) \bmod (p-1)$，则 (r,s) 即是消息 m 的盲签名。

(3) 验证阶段

验证等式 $g^{s} \equiv y^{r} r^{m} \bmod p$ 是否成立。若成立，则接受 (r,s)，否则拒绝接受。

在上述盲签名方案中，如果签名者 B 保留 $(\tilde{m},\tilde{r},\tilde{s})$，则当消息拥有者 A 公开 (m,r,s) 后，B 可求得 α,β，从而确认 $\mathrm{sig}(m)$ 和 $\mathrm{sig}(\tilde{m})$ 相对应，即签名者能够把签文件的行为与签了名的文件联系起来，达到对消息拥有者追踪的目的。这说明上述方案是一个弱盲签名方案。

方案二:

(1) 初始化阶段

同方案一。

(2) 签名阶段

步骤 1:签名者 B 随机选取 $\tilde{k} \in Z_q^{*}$，$\tilde{k} \neq 1$，计算 $\tilde{r}=g^{\tilde{k}} \bmod p$，并将 $\tilde{r}$ 发送给消息拥有者 A。

步骤 2:设 m 为待签名的消息，则 A 随机地选取三个整数 $\alpha,\tau,\beta \in Z_{p-1}^{*}$，计算 $r=\tilde{r}^{\alpha} y^{\tau} g^{\beta} \bmod p$，$\tilde{m}=\alpha^{-1}\tilde{r}^{-1}(mr-\tau) \bmod (p-1)$，并将 $\tilde{m}$ 发送给 B。这里可以将 k 看成是 $k=\alpha\tilde{k}+\tau x+\beta \bmod (p-1)$。

步骤 3:B 接收到 $\tilde{m}$ 后，计算 $\tilde{s}=\tilde{r}\tilde{m}x-\tilde{k} \bmod (p-1)$ 并将 $\tilde{s}$ 发送给消息拥有者 A。

步骤 4:消息拥有者 A 接收到 $\tilde{s}$ 后，计算 $s=\alpha\tilde{s}-\beta \bmod (p-1)$，则 (r,s) 为消息 m 的盲签名。

(3) 验证阶段

消息接收者或签名验证人接收到$(m,(r,s))$后，验证等式$g^s r = y^{mr} \bmod p$是否成立。若成立，则确信(r,s)是有效的盲签名。

在上述盲签名方案中，如果签名者 B 保留$(\tilde{m},\tilde{r},\tilde{s})$，则当消息拥有者 A 公开$(m,r,s)$后，B 若想求出$\alpha,\tau,\beta$，需面临求解离散对数问题。因此，签名者不能把签文件的行为与签了名的文件联系起来。即使他记下了他所作的每一个盲签名，当用到一个签了名的文件时，他也不能确定什么时候他签了该文件。这说明上述方案是一个强盲签名方案。

2.3.3 盲签名的应用

盲签名是一种特殊的数字签名，国内外学者对其进行了深入的探讨与研究并取得了丰富的研究成果。盲签名所具有的匿名性使得这种技术可广泛用于许多领域，如电子现金系统和电子投票系统的构造等。

电子现金又称为数字现金，它最大的特点是能满足用户的匿名要求，也就是它能够保证用户的身份不能被他人知道。而在电子信用卡支付系统和电子支票支付系统中，用户的身份能够被银行知道，银行可以跟踪用户的消费情况，从而无法保护用户的隐私权。电子现金的安全性和可靠性等主要是依靠密码技术来实现的，主要有分割选择技术、零知识证明、认证、盲签名等。电子现金支付具有其特殊性，目前已经有 Digicash、Netcash、Modex 等三种系统开始时使用。

电子投票作为消息认证系统的重要课题之一和作为盲签名的重要应用，近年来之所以受到广泛关注，主要是由于它可以省去通常投票活动在组织工作、选票采集、选票统计和安全保密等方面所需花费的大量人力和物力；其次，投票人也可以不必去有关管理部门所设置的特定的投票处。因此，与通常的投票相比，电子投票既省钱、省力又安全。

2.4 数字证书

为保证网上数字信息的传输安全，除了在通信传输中采用更强的加密算法等措施之外，必须建立一种信任及信任验证机制，即参加电子商务的各方必须有一个可以被验证的标识，这就是数字证书。数字证书是各实体(持卡人/个人、商户/企业、网关/银行等)在网上信息交流及商务交易活动中的身份证明，其作用类似于日常生活中的身份证。该数字证书具有唯一性。它将实体的公开密钥同实体本身联系在一起，为实现这一目的，必须使数字证书符合 X.509 国际标

准，同时数字证书的来源必须是可靠的。这就意味着应有一个网上各方都信任的机构，专门负责数字证书的发放和管理，确保网上信息的安全，这个机构就是 CA 认证机构。

数字证书认证中心（Certficate Authority,CA）是整个网上电子交易安全的关键环节。它主要负责产生、分配并管理所有参与网上交易的实体所需的身份认证数字证书。每一份数字证书都与上一级的数字签名证书相关联，最终通过安全链追溯到一个已知的并被广泛认为是安全、权威、足以信赖的机构-根认证中心（根 CA）。

电子交易的各方都必须拥有合法的身份，即由数字证书认证中心机构（CA）签发的数字证书，在交易的各个环节，交易的各方都需检验对方数字证书的有效性，从而解决了用户信任问题。CA 涉及到电子交易中各交易方的身份信息、严格的加密技术和认证程序。基于其牢固的安全机制，CA 应用可扩大到一切有安全要求的网上数据传输服务。

数字证书认证解决了网上交易和结算中的安全问题，其中包括建立电子商务各主体之间的信任关系，即建立安全认证体系（CA）；选择安全标准（如 SET、SSL）；采用高强度的加、解密技术。其中安全认证体系的建立是关键，它决定了网上交易和结算能否安全进行，因此，数字证书认证中心机构的建立对电子商务的开展具有非常重要的意义。

2.5 本章小结

本章简要介绍了密码学概论和哈希函数、数字签名、盲签名、数字证书等密码学基本概念，然后详细介绍了典型的盲签名方案，并总结了盲签名技术在电子现金系统、电子投票系统中的广泛应用。

第三章 基于 Schnorr 盲签名的代理盲签名设计

3.1 引言

代理签名[33][34]是一种非常有用的密码学工具。借助于代理签名，原始签名人能将其数字签名权力委托给代理签名人。在盲签名方案中,消息的内容对签名者是不可见的。若签名被接收者泄露，签名者也不能追踪签名。代理签名和盲签名有着各自的特点，在实际中分别有着广泛的应用。在某些现实情况下，我们需要同时应用它们，比如一个匿名的代理电子投票系统。在该系统中，我们需要授权代理机构实施电子投票，并且在电子投票过程中需要对选票进行盲签名以使选票生效。因此，在该系统中我们需要用到代理盲签名，其签名过程如图3.1所示。

2002年，谭作文等人提出了一个基于Schnorr盲签名的代理盲签名方案。本章对该方案进行了分析与研究，提出了一种攻击方法，然后以该方案的构造思想为基础，提出了一种基于Schnorr盲签名的代理盲签名方案，并进行了详细的理论证明和实验分析。结果表明，我们的代理盲签名方案能够满足代理盲签名的基本安全性要求，并且减少了运算量，提高了计算效率。

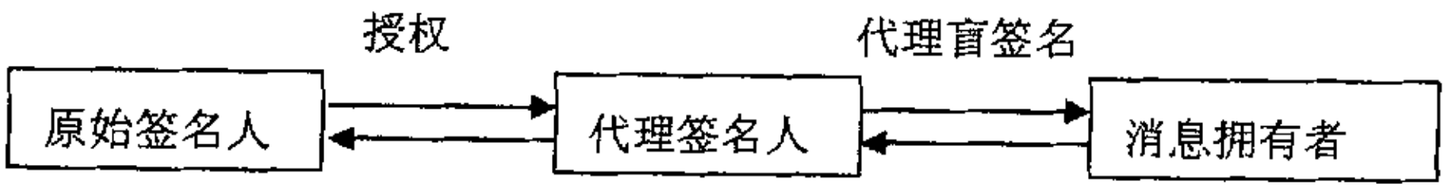


图3.1 代理盲签名示意图

3.2 基于Schnorr盲签名的代理盲签名方案的不足

谭作文[26]等人在2002年提出了一种基于Schnorr盲签名的代理盲签名方案，该方案包括初始化、代理、签名和验证四个阶段，该方案的主要思想是：原始签名人首先使用自己的私钥产生一个普通的数字签名，然后将其发送给代理签名人。代理签名人将得到的签名和自己的私钥处理产生一个代理签名私钥，可以进行代理签名。消息拥有者选取两个随机数对消息盲化，然后发送给代理签名人。代理签名人使用代理签名私钥对盲化的消息进行签名，然后将签名发送给消息拥有者。消息拥有者对收到的签名进行去盲处理得到代理签名人对原始消息的合法签名。验证方需要同时使用原始签名人和代理签名人的公钥才能验证代理盲签名的合法性。

针对该方案提出了一种攻击方法，利用该攻击方法消息拥有者C可以伪造$(m,(u,s,e))$是原始签名人F委托签署的，虽然F可能根本没有将签名权授予任何人。在代理签名阶段，消息拥有者C在交互过程中用$u'=\left(\tilde{r}y_A{}^{\tilde{r}}\right)^{-e+b}y_F{}^{-e}\bmod p$来替代$u=\left(\tilde{r}y_A{}^{\tilde{r}}\right)^{-e+b}y_A{}^{-e}\bmod p$，其他等式不变。这样，消息拥有者C可以声称签名$(m,(u',s,e))$是由原始签名人F委托代理签名人B签署的合法签名。并且，该签名满足以下的验证等式$r'=g^s y_B{}^{-e}y_F{}^{e}u\bmod p$，$e=h(r',m)\bmod q$。验证等式证明如下：

$$r'=g^s y_B{}^{-e}y_F{}^{e}u\bmod p=g^{s'+b}y_B{}^{-e}y_F{}^{e}u\bmod p=g^{k+b}g^{s'e'}y_B{}^{-e}y_F{}^{e}u\bmod p$$

$$=tg^b g^{\tilde{s}e'}y_B{}^{e'-e}y_F{}^{e}u\bmod p=tg^b g^{\tilde{s}(e-a-b)}y_B{}^{(-a-b)}y_A{}^{e}u\bmod p$$

$$=tg^b\left(\tilde{r}y_A{}^{\tilde{r}}\right)^{e-b}\left(\tilde{r}y_A{}^{\tilde{r}}\right)^{-a}y_B{}^{-a-b}y_A{}^{e}u\bmod p$$

将$u'=\left(\tilde{r}y_A{}^{\tilde{r}}\right)^{-e+b}y_F{}^{-e}\bmod p$作为$u$代入上式，即可以得到

$r'=tg^b y_B{}^{-a-b}\left(\tilde{r}y_A{}^{\tilde{r}}\right)^{-a}\bmod p=r\bmod p$，从而满足等式$e=h(r',m)\bmod q$。综上所述，消息拥有者利用该方法可以成功伪造一个合法的代理盲签名。

3.3 基于Schnorr盲签名的代理盲签名方案的改进

上一节对谭作文等人提出的代理盲签名方案的构造思想进行了研究和分析，提出了一种攻击方法。本节以其构造思想为基础，对消息盲化及签名方程进行了技术处理，构造了一种基于 Schnorr 盲签名的代理盲签名方案，然后对方案进行了理论证明和实验分析。结果表明，该方案能够满足代理盲签名的基本安全性要求，并且与谭作文等人的代理盲签名方案相比，减少了签名的运算量，提高了签名的计算效率。现将该方案描述如下：

(1)初始化阶段

系统参数定义如下：选择两个大素数p,q满足$q|(p-1)$，$p\geq 2^{512}$及$q\leq 2^{160}$，$g\in Z_p^*$且满足$g^q=1\bmod p$。$1<x_B<q$，$1<x_C<q$分别为代理签名人 B、原始签名人 C 的秘密密钥，y_B,y_C分别为它们的公开密钥，且$y_B=g^{x_B}\bmod p$，$y_C=g^{x_C}\bmod p$．p,q,g,y_B,y_C公开．h为单向哈希函数。

(2)代理阶段

步骤 1：原始签名人 C 首先随机选取整数 $k_C \in Z_p^*$，且 $k_C \neq 1$，计算 $r_C = g^{k_C} \bmod p$，$s_C = x_C + k_C r_C \bmod q$，将 (r_C, s_C) 通过安全通道发送给 B。然后计算 $y_P = g^{s_C} y_B \bmod p$，$y_p$ 是代理签名人的签名公钥，并在系统内公开 y_p。

步骤 2:B 收到 (r_C, s_C) 后，首先验证等式 $g^{s_C} = y_C r_C^{r_C} \bmod p$ 是否成立。若等式成立则接受 C 的委托。然后计算 $s_P = s_C + x_B \bmod q$，s_P 实际上是代理签名人的签名密钥。

(3)代理签名阶段

步骤 1：代理签名者 B 随机选择 $k \in Z_q^*$，计算 $r = g^k \bmod p$，并将 r 发送给消息拥有者 A；

步骤 2：消息拥有者 A 接收到 r 后，选择随机数 $\alpha, \beta \in Z_q^*$，然后计算 $r' = r g^{\beta} y_P^{\alpha} \bmod p$，$e' = h(r', m) \bmod q$，$e = e' - \alpha \bmod q$，并将 e 发送给 B；

步骤 3：B 接收到 e 后，计算 $s = k - e s_p \bmod q$，并将 s 发送给 A；

步骤 4：A 接收到 s 后，计算 $s' = s + \beta \bmod q$，则 (e', s') 即为消息 m 的代理盲签名。

(4)签名验证阶段

消息接收者将消息签名对 $(m, (e', s'))$ 发送给签名验证方，签名验证方首先计算 $r'' = g^{s'} y_P^{e'} \bmod p$，$e'' = h(r'', m) \bmod p$。若 $e'' = e' \bmod p$ 成立，则 (e', s') 是对消息 m 的有效代理盲签名。

原始签名人 C		代理签名人 B
随机选取整数 $k_C \in Z_p^*$，$k_C \neq 1$，		
计算 $r_C = g^{k_C} \bmod p$，		
$s_C = x_C + k_C r_C \bmod q$，		
$y_P = g^{s_C} y_B \bmod p$，并公开 y_p	$\xrightarrow{(r_C, s_C)}$	
		验证等式 $g^{s_C} = y_C r_C^{r_C} \bmod p$
		计算 $s_P = s_C + x_B \bmod q$，

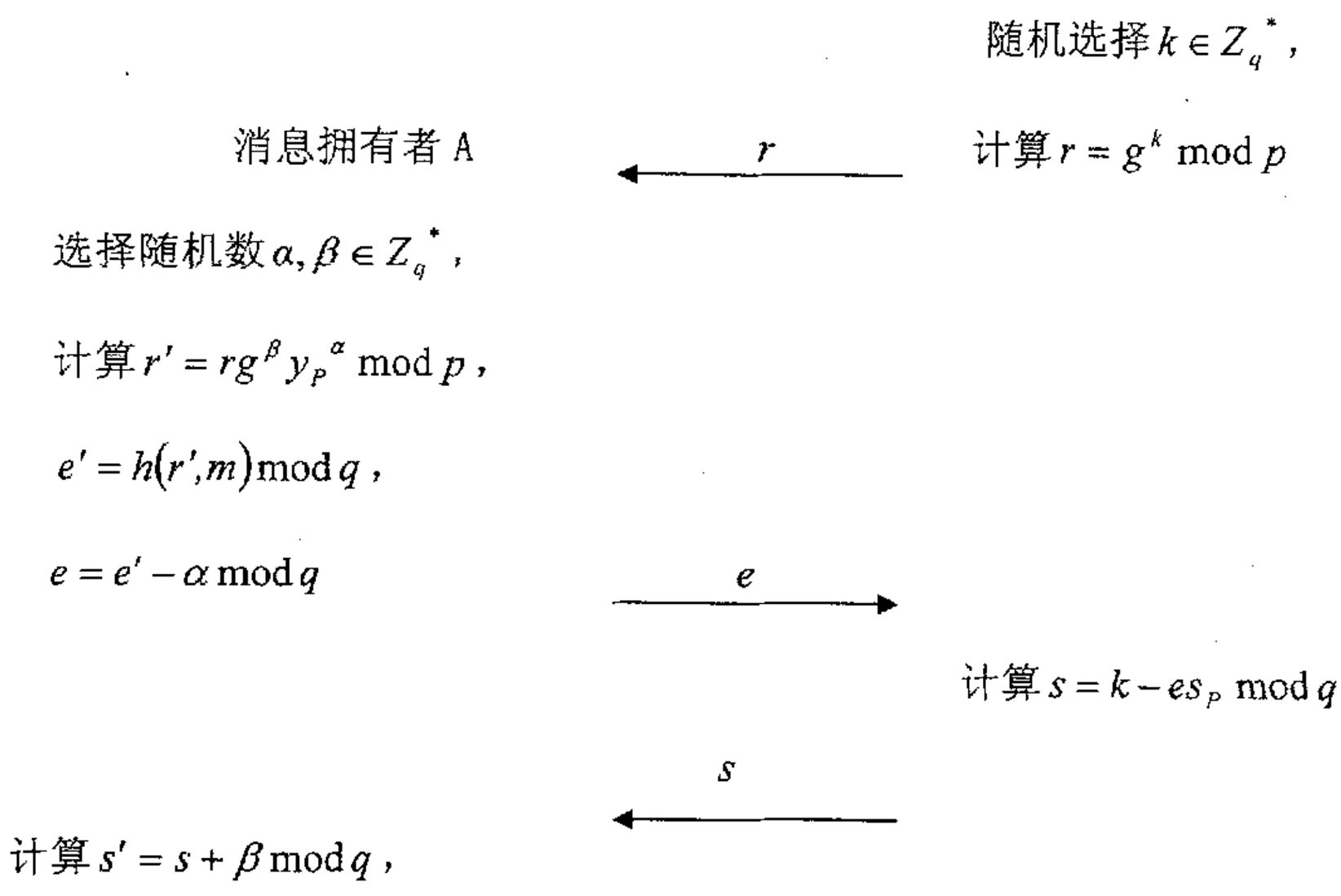


图 3.2 基于 Schnorr 盲签名的代理盲签名方案

3.4 正确性和安全性分析

1、方案的正确性

在代理签名阶段，原是签名人将 (r_C, s_C) 发送给代理签名人，代理签名人验证等式 $g^{s_C} = y_C r_C^{r_C} \bmod p$ 是否正确，若等式正确则接受原始签名人的委托，行使代理签名权，否则拒绝接受。验证等式的正确性可以证明如下：

$$s_C = x_C + k_C r_C \bmod p \Rightarrow g^{s_C} = g^{x_C} \cdot g^{k_C r_C} \bmod p$$

因为 $r_C = g^{k_C} \bmod p$，所以得到 $g^{s_C} = y_C r_C^{r_C} \bmod p$。

当消息拥有者将最终得到的代理盲签名 (e', s') 发送给验证方，验证方首先计算 $r'' = g^{s'} y_P^{e'} \bmod p$，　$e'' = h(r'', m) \bmod p$。若 $e'' = e' \bmod p$ 成立，则 (e', s') 是对消息 m 的有效代理盲签名。验证等式 $e' = h(r'', m) \bmod p$ 的正确性证明如下：

由于 $e' = h(r', m) \bmod q$，因此只要证明 $r'' = r' \bmod p$ 即可。

$$r'' = g^{s'} y_P{}^{e'} \bmod p$$

$$= g^{s'} \cdot g^{s_p \cdot e'} \bmod p$$

$$= g^{s'+s_p e'} \bmod p$$

$$= g^{s+\beta+s_p(e+\alpha)} \bmod p$$

$$= g^{k+\beta+s_p\alpha} \bmod p$$

$$= r g^{\beta} y_P{}^{\alpha} \bmod p$$

$$= r' \bmod p$$

正确性得证。

2、安全性分析

从验证方程 $r'' = g^{s'} y_P{}^{e'} \bmod p$， $e' = h(r'', m) \bmod p$ 可以看出，由于 y_p 同时含有原始签名人 C 和代理签名人 B 的公钥 y_C, y_B，所以验证方程本身已经反映出签名 (e', s') 是由授权方和代理方共同完成的。同时，这个方案所满足的安全性分析如下：

性质 1：任何签名人都不能伪造原始签名人的签名。

证明：在这个代理盲签名协议中，B 从 A 处得到 (r_C, s_C)，然后可以根据等式 $r_C = g^{k_C} \bmod p$ 求解出 k_c，再根据等式 $s_C = x_C + k_C r_C \bmod p$ 求解出 x_C，但是他必须面临求解离散对数方程的难题，因此他难以求解出 x_C，从而无法伪造 C 的原始数字签名。同样，任何其他攻击者都无法求解出 x_C，因此难以伪造 C 的原始数字签名。

性质2：任何签名人都不能伪造代理签名人的签名。

证明：在这个方案中，s_p 是代理签名人的签名私钥，y_p 是对应的签名公钥。由等式 $s_p = s_C + x_B \bmod q$ 可以看出，在等式中存在B的私钥 x_B，因此只有B才能生成签名私钥 s_p，包括原始签名人都无法知道签名私钥 s_p。攻击者可以通过求解等式 $y_B = g^{x_B} \bmod p$ 来得到 x_B，但是必须面临求解离散对数的难题。因此除了B以外，任何其他人(包括A)都难以伪造一个合法的代理签名。

性质3：原始签名和代理签名可以有效区分。

证明：在签名验证阶段我们使用不同的等式来验证原始签名和代理签名的有效性。从验证方程$r'' = g^{s'} y_P^{e'} \bmod p$， $e' = h(r'', m) \bmod p$可以看出，验证人使用代理签名公钥y_p对签名进行验证，由于y_p同时含有原始签名人C和代理签名人B的公钥y_C和y_B，因此若验证等式通过，则可以看出此签名是一个合法的代理签名。所以通过验证等式中使用的公钥的不同很容易将代理签名和原始签名区分开。

性质4：原始签名人不可抵赖其授权给代理签名人行使签名权。

证明：由于除了原始签名人外的任何人都不知道原始签名人的私钥x_c，攻击者若要通过等式$y_C = g^{x_C} \bmod p$来计算x_c，则要面临求解离散对数的难题，因此任何人都无法伪造一个原始签名人C的合法的数字签名，所以C不能否认他的一个有效的 数字签名。

性质5：代理签名人不能抵赖其对消息的盲签名。

证明：从定理2可以得到，除了代理签名人B以外，任何人都不能伪造B的代理签名，若试图通过求解等式$y_B = g^{x_B} \bmod p$来得到x_B，必须面临求解离散对数的难题。通过计算验证等式$r'' = g^{s'} y_P^{e'} \bmod p$，若$e' = h(r'', m) \bmod p$成立，则B不能否认他使用了私钥$x_B$对消息进行了签名。

性质6：原始签名人C可以收回B的代理签名权。

证明：如果原始签名人 C 想收回 B 的代理签名权，即注销 B 所拥有的代理签名密钥s_P，那么就可以在系统内向用户“广播”消息（这个消息应该由 C 签名），宣布y_P不再有效。而验证方在验证签名时需要使用y_P计算$r'' = g^{s'} y_P^{e'} \bmod p$，因此，B 生成的所有代理签名随之失效。

3.5 计算效率分析

1、理论分析

在进行签名的过程中，占据大部分计算时间的是取模意义下的求幂运算、乘法运算以及求逆运算。本文将谭作文等人提出的代理盲签名方案和上面提出的基于 Schnorr 盲签名的代理盲签名方案进行了比较，并将两个代理盲签名方

案的计算量列入表 3.1 中。为了方便，本文使用以下记号作为标记：

T_e：计算一次模指数运算所花时间；

T_m：计算一次模乘法运算所花时间；

T_v：计算一次模逆元运算所花时间。

T_h：计算一次哈希函数所花时间。

表 3.1 各代理盲签名方案的计算量比较

	谭作文的方案	新的方案
代理阶段	$2T_e+2T_m$	$3T_e+3T_m$
签名阶段	$7T_e+7T_m+4T_v+1T_h$	$3T_e+3T_m+1T_h$
验证阶段	$3T_e+3T_m+1T_v+1T_h$	$2T_e+2T_m+1T_h$
总运算量	$12T_e+12T_m+5T_v+2T_h$	$8T_e+8T_m+2T_h$

由表 3.1 可以看出，我们的代理盲签名方案计算量要小于谭作文的代理盲签名方案，尤其是签名阶段的计算量有明显的减少。因此，从理论上可以证明我们提出的基于 Schnorr 盲签名的代理盲签名方案与谭作文的代理盲签名方案相比计算时间少，计算效率高。

2、实验分析

本实验采用 2.0GHz PentiumIV 处理器在 256M 的内存下进行测试，使用 VC 作为开发工具编程实现了上述两方案的整个代理签名过程，并计算了上述两方案在各个阶段的运算时间。在整个代理盲签名过程中，需要原始签名人、代理签名人之间多次交互通信才能完成。但是考虑到消息在网络中的传输时间受到多方面的影响，具有不确定性，因此本实验不考虑消息在网络中的传输时间，只是对各个阶段的计算时间进行测试。经过对比分析表明，我们的代理盲签名方案和谭作文的代理盲签名方案相比，减少了各个阶段的计算时间，提高了计算效率。

目前，绝大多数的公钥密码体制都建立在 512 到 1024 位的大整数运算之上。而大多数的编译器只能支持到 64 位的整数运算，即我们在运算中所使用的整数必须小于等于 64 位，这远远达不到实验的需要，于是需要专门建立大整数运算类来解决这一问题。

本章将大整数表示为一个 N 进制数组，对于目前的 32 位系统而言 N 可以取值为 2 的 32 次方，假如将一个二进制为 1024 位的大数转化成 0x10000000 进制，它就变成了 32 位，而每一位的取值范围就是 0~0xffffffff，我们正好可以用一个无符号长整数来表示这一数值。所以 1024 位的大数就是一个有 32 个元素的 unsigned long 数组，针对 unsigned long 数组进行各种运算所需的循环规模至多 32 次而已。任何整数运算最终都能分解成数字与数字之间的运算，在 0x100000000 进制下其“数字”最大达到 0xffffffff，其数字与数字之间的运算，

结果也必然超出了目前 32 系统的字长。在 VC++中，存在一个__int64 类型可以处理 64 位的整数。

本章以 VC 作为开发工具，以大整数为基础编写了一个大整数类 CBigInteger，实现了大整数的加、减、乘、除、取余、模幂、模逆等运算，为签名方案的实现奠定了基础。

```
class CBigInteger
{
    public:
    //构造函数
    CBigInteger ();
    //析构函数
    ~ CBigInteger ();
    //Add，求大数与大数的和
    void Add(CBigInteger & a，CBigInteger & b，CBigInteger & c);
    //Sub，求大数与大数的差
    void Sub(CBigInteger & a，CBigInteger & b，CBigInteger & c);
    //Mul，求大数与大数的积
    void Mul(CBigInteger & a，CBigInteger & b，CBigInteger & c);
    //Div，求大数与大数的商
    void Div(CBigInteger & a，CBigInteger & b，CBigInteger & c);
    //Mod，求大数与大数的模
    void Mod(CBigInteger & a，CBigInteger & b，CBigInteger & c);
    // Cmp，大数的比较运算
    int Cmp(CBigInteger & a，CBigInteger & b);
    // modexp，幂模运算
    void modexp(CBigInteger x, CBigInteger y, CBigInteger z, CBigInteger
w); // modinv，模逆运算
    void modinv (CBigInteger x, CBigInteger n, CBigInteger w);
    //modmul，模乘运算
    void modmul(CBigInteger x, CBigInteger y, CBigInteger z, CBigInteger
w);
    // bytes_to_big，从字符数组输入到大数
    void bytes_to_big(char *ptr, CBigInteger x);
    // big_to_bytes，将大数输出到字符数组
    void big_to_bytes(CBigInteger x, char *ptr);
```

};

以新的代理盲签名方案为例，首先选取合适的参数如图 3.3 所示，p 为 512 个二进制位，q 为 160 个二进制位，并且 p,q 满足 $q|(p-1)$，$g \in Z_p^*$ 且满足 $g^q = 1 \bmod p$。$1 < x_B < q$，$1 < x_C < q$ 分别为代理签名人 B、原始签名人 C 的秘密密钥，y_B, y_C 分别为它们的公开密钥，且 $y_B = g^{x_B} \bmod p$，$y_C = g^{x_C} \bmod p$。

图 3.3 系统初始化参数

在代理阶段，原始签名人首先计算一个普通签名 (r_C, s_C)，然后将其发送给代理签名人。代理签名人验证等式 $g^{s_C} = y_C r_C^{r_C} \bmod p$ 是否成立。若等式成立则接受原始签名人的委托，否则拒绝接受委托，终止协议。现将该过程的伪代码显示如下，这里我们用**来表示指数运算：

```
输入 kc;
rc=g** kc mod p;
temp1= (kc* rc )mod q;
sc= (xc+ temp1)mod q;
```

```
temp2= g** sc mod p;
yp= (temp2* yb) mod p;
temp3= rc** rc mod p;
 temp4= (yc* temp3) mod p;
 temp5= g** sc mod p;
 if(temp4= temp5) sp= (sc+xb) mod q;
      else 终止协议
```

在签名阶段，消息拥有者选取两个随机数对消息盲化，然后发送给代理签名人。代理签名人使用代理签名私钥对盲化的消息进行签名，然后将签名发送给消息拥有者。消息拥有者对收到的签名进行去盲处理得到代理签名人对原始消息的合法签名(e',s')。其中哈希函数采用 SHA-1 算法来实现。现将该过程的伪代码显示如下：

```
输入 k,a,b
r= g** k mod p;
temp6= g** b mod p;
temp7= yp** a mod p;
temp8= r* temp6 mod p;
r'= temp8* temp7mod p;
e'=h(r1,m)modq;
e=(e'-a)modq;
temp9= e* sp mod q;
s=(k- temp9)modq;
s'=(s+b)modq;
```

在验证阶段，消息接收者将消息签名对$(m,(e',s'))$发送给签名验证方，签名验证方首先计算$r'' = g^{s'} y_p^{e'} \bmod p$，　$e'' = h(r'',m) \bmod p$。若$e'' = e' \bmod p$成立，则(e',s')是对消息m的有效代理盲签名。现将该过程的伪代码显示如下：

```
temp10= g** s' mod p;
temp11= yp** e' mod p;
r''= temp10* temp11modp;
e''=h(r'',m);
if(e'=e'') 接受签名
   else 拒绝接受
```

本实验使用 QueryPerformanceFrequency()和 QueryPerformanceCounter()函

数实现了精确计时。这两个函数要求计算机从硬件上支持精确定时器，函数原型如下所示：

```
BOOL   QueryPerformanceFrequency(LARGE_INTEGER *lpFrequency);
BOOL   QueryPerformanceCounter(LARGE_INTEGER *lpCount);
```

在进行定时之前，先调用 QueryPerformanceFrequency()函数获得机器内部定时器的时钟频率，然后在需要严格定时的事件发生之前和发生之后分别调用QueryPerformanceCounter()函数，利用两次获得的计数之差及时钟频率，计算出事件经历的精确时间。其定时误差不超过 1 微秒，精度与 CPU 等机器配置有关。实现精确计时的源代码如下所示：

```
LARGE_INTEGER litmp;
LONGLONG QPart1,QPart2;
double dfMinus, dfFreq, dfTim;
QueryPerformanceFrequency(&litmp);
dfFreq = (double)litmp.QuadPart; // 获得计数器的时钟频率
QueryPerformanceCounter(&litmp);
QPart1 = litmp.QuadPart; // 获得初始值
 ……
QueryPerformanceCounter(&litmp);
QPart2 = litmp.QuadPart;// 获得中止值
dfMinus = (double)(QPart2-QPart1);
dfTim = dfMinus / dfFreq; // 获得对应的时间值，单位为秒
CString   str2;
str2.Format("%.6f",dfTim);
```

现将实验中各个阶段的参数变量以及计算时间显示如下：（图 3.4～3.6）

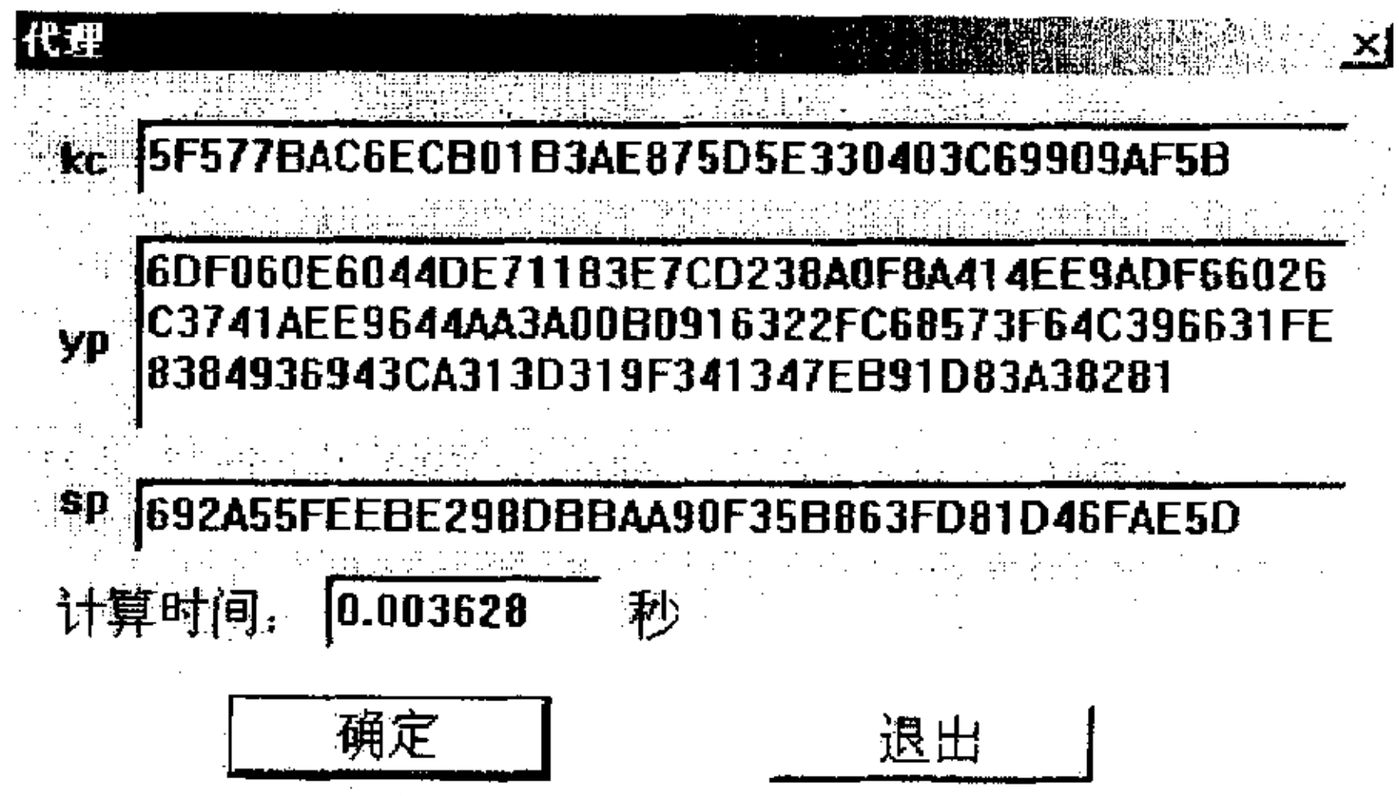


图 3.4 代理阶段变量显示界面

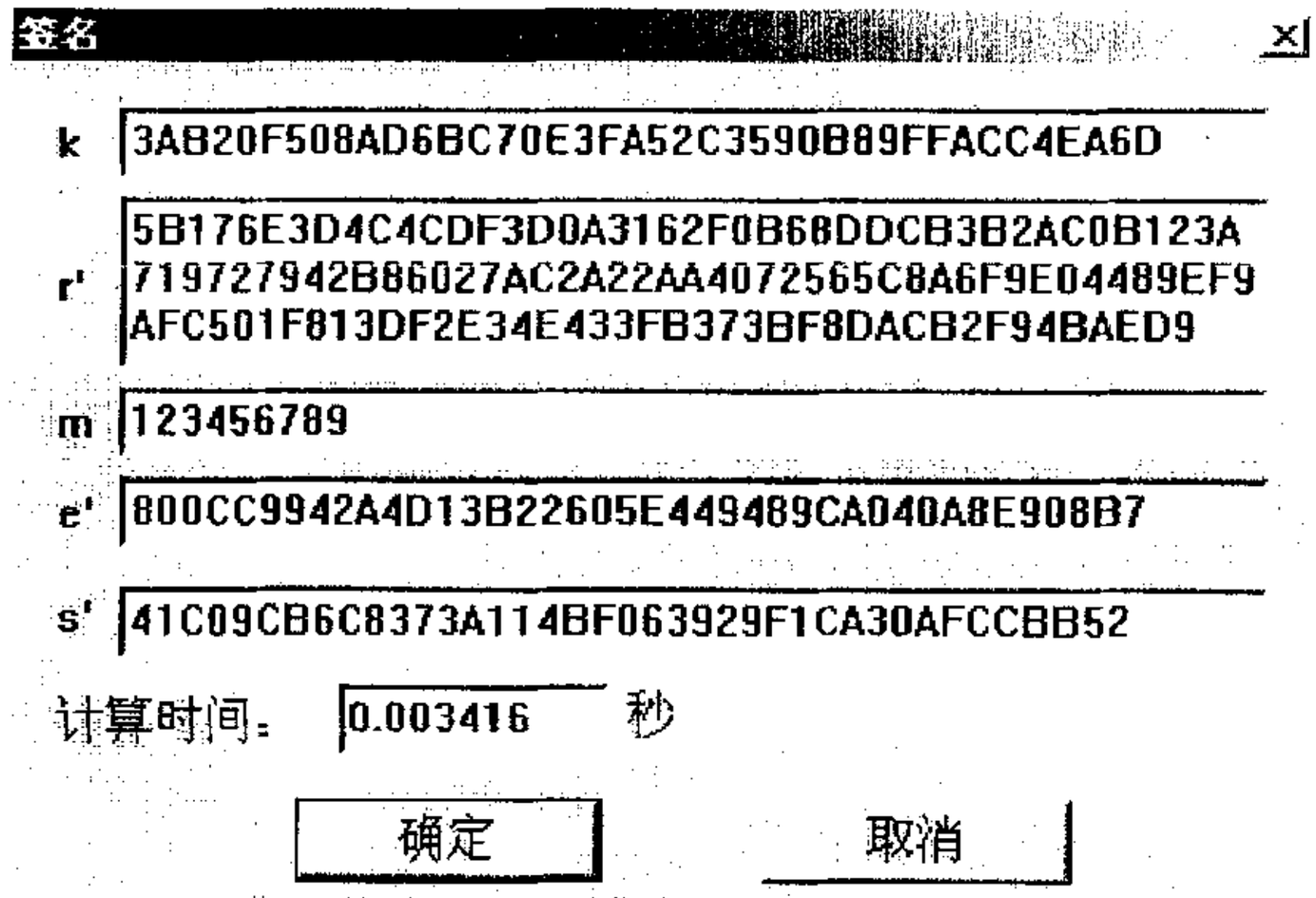


图 3.5 签名阶段变量显示界面

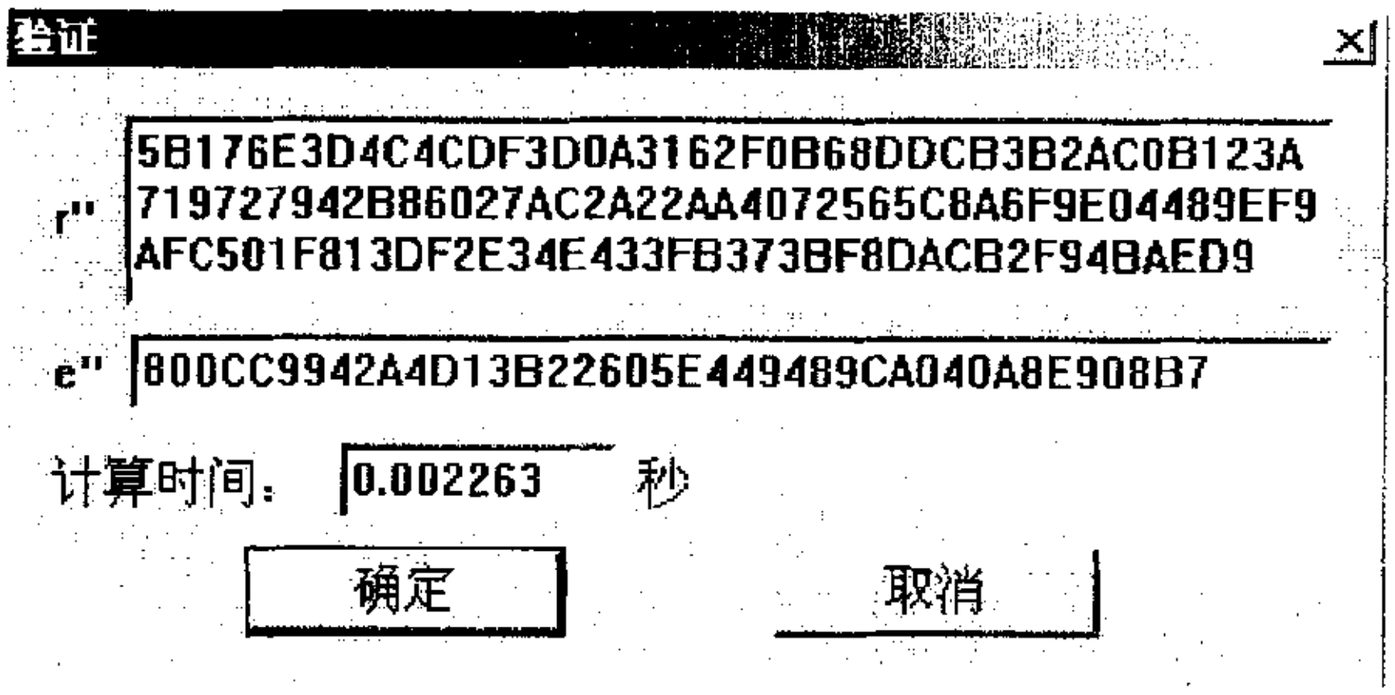


图 3.6 验证阶段变量显示界面

参照以上方法，同样可以获得谭作文的方案的计算时间，这里不再重复叙述。将得到的上述两方案的计算时间 (不包括消息在网络中的传输时间) 列入表 3.2 中，经过对比可以看出我们的方案在签名、验证阶段的计算时间要少于谭作文的方案，总的计算时间缩短了约 5 毫秒，提高了计算效率。

表 3.2 代理盲签名方案的计算时间比较（单位：毫秒）

	谭作文的方案	我们的方案
代理阶段	2.416	3.628
签名阶段	7.819	3.416
验证阶段	3.943	2.263
总计算时间	14.178	9.307

结论：本章提出的代理盲签名方案能够实现代理盲签名的基本功能，满足代理盲签名的基本安全性要求，并且与谭作文等人的代理盲签名方案相比，减

少了计算时间，提高了计算效率。

3.6 本章小结

本章首先对谭作文等人的代理盲签名方案进行了分析，然后基于 Schnorr 盲签名构造了一种代理盲签名方案，将其与谭作文等人的代理盲签名方案进行了对比分析。分析表明，该代理盲签名方案满足代理盲签名方案的安全性要求，并且缩短了计算时间，提高了计算效率。

第四章 基于 ElGamal 强盲签名的多重盲签名设计

4.1 引言

我们把能够实现多个用户对同一消息进行签名的数字签名称为多重数字签名(Digital Multisignature)。根据签名过程的不同，多重数字签名方案可分为两类:有序多重数字签名(Sequential Multisignature)和广播多重数字签名(Broadcasting ultisignature)。 两类方案中的参与方包含消息发送者、消息签名者、签名验证者，在广播签名方案中还包含签名收集者。

从电子商务的实际应用来看，在许多情况下不但需要进行盲签名，而且需要进行多重盲签名(如图4.1所示)，即多个人同时对消息进行盲签名。比如，对数字货币，特别是对大额数字货币的签发就需要多个人对货币的发放进行签发，目的是在保障隐私性的同时，加强其安全性。但目前此类研究成果并不多。

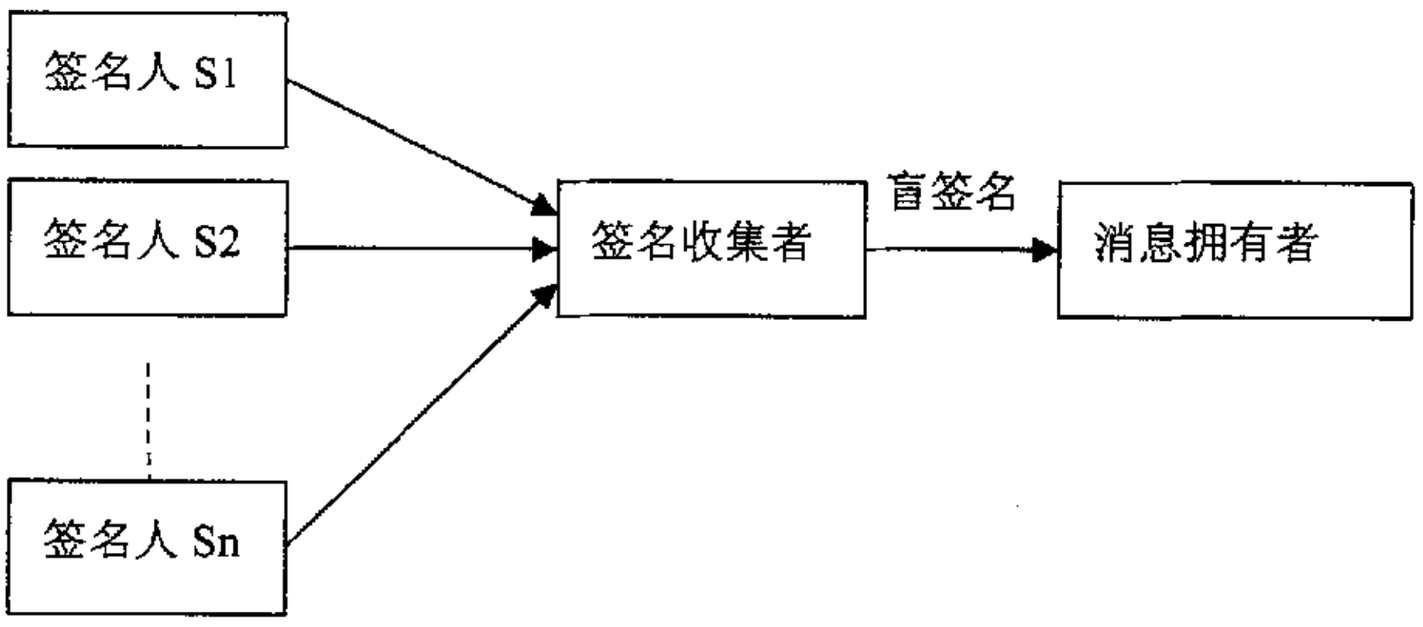


图4.1 广播多重盲签名示意图

4.2 祁明等提出的多重盲签名方案的不足

祁明[26]等人在2001年提出了一种多重盲签名方案，该方案包括初始化、签名和验证3个阶段。该方案的主要思想是：首先消息拥有者随机选取两个参数对消息进行盲化，然后将盲化的消息发送给所有的签名人。所有签名人使用自己私钥共同对盲化的消息进行签名，然后将签名发送给消息拥有者，消息拥有者对签名去盲，即可得到所有签名人对原始消息的共同签名。该方案能够实现多人同时对消息进行盲签名。

上述方案可以满足消息的盲性，即签名者不能获得有关消息 m 的任何信息。但是，该方案不能满足签名的不可追踪性，即签名者根据他所掌握的有关数据能够追踪他所签署的签名。在上述盲签名方案中，如果签名者 $S_i(i=1,2,\Lambda\ ,n)$ 保

留$(\tilde{m},\tilde{r},\tilde{s})$，则当消息拥有者U公开$(m,r,s)$后，$S_i(i=1,2,\Lambda,n)$可以通过求解以下的方程组

$$\begin{cases}\tilde{m}=a^{-1}mr\tilde{r}^{-1}\bmod(p-1)\\ s=rm\tilde{r}^{-1}\tilde{m}^{-1}\tilde{s}+b\bmod(p-1)\end{cases}$$

得到$a,b\in Z_{p-1}^{*}$。因此，签名者可以把签文件的行为与签了名的文件联系起来，达到追踪的目的。所以，上述多重弱盲签名方案是一种弱盲签名方案。

4.3 一种基于ElGamal强盲签名的多重盲签名方案

上一节对祁明的多重盲签名方案进行了分析，分析表明该方案是一个弱盲签名方案。本章以祁明提出的方案的构造思想为基础，构造了一种基于 ElGamal 强盲签名的多重盲签名方案。该方案的不同之处在于，在消息盲化阶段选取了三个参数以满足签名的不可追踪性，并且增加了一个签名收集者，提高了方案的可操作性。在下面的方案中，设 A 为消息拥有者，$B_i(i=1,2,\Lambda,n)$为签名者，C 为签名验证者，D 为签名收集者。

(1)初始化阶段

签名者$B_i(i=1,2,\Lambda,n)$共同选择大素数p，g是Z_p^{*}的一个生成元。分别选取私钥$x_i\in Z_p^{*}$，令$y_i=g^{x_i}\bmod p$，$y=\prod_{i=1}^{n}y_i$，p,g,y为公钥。

(2)签名阶段

步骤 1:签名者$B_i(i=1,2,\Lambda,n)$分别随机选取$\tilde{k}_i\in Z_q^{*}$，$\tilde{k}_i\neq 1$，计算$\tilde{r}_i=g^{\tilde{k}_i}\bmod p$，然后将$\tilde{r}_i$发送给签名收集者 D，D 计算$\tilde{r}=\prod_{i=1}^{n}\tilde{r}_i\bmod p$，并将$\tilde{r}$发送给消息拥有者 A。

步骤 2:设m为待签名的消息，则 A 随机地选取三个整数$\alpha,\tau,\beta\in Z_{p-1}^{*}$，计算$r=\tilde{r}^{\alpha}y^{\tau}g^{\beta}\bmod p$，$\tilde{m}=\alpha^{-1}\tilde{r}^{-1}(mr-\tau)\bmod(p-1)$，并将$\tilde{m}$发送给签名收集者 D。这里可以将$k$看成是$k=\alpha\tilde{k}+\tau x+\beta\bmod(p-1)$。

步骤 3：签名收集者 D 将$\tilde{m}$分别发送给$B_i(i=1,2,\Lambda,n)$，$B_i(i=1,2,\Lambda,n)$接收到$\tilde{m}$后，分别计算$\tilde{s}_i=\tilde{r}\tilde{m}x_i-\tilde{k}_i\bmod(p-1)$，然后发送给签名收集者 D。D 计

算 $\tilde{s}=\sum_{i=1}^{n}\tilde{s}_i \bmod(p-1)$，并将 $\tilde{s}$ 发送给消息拥有者 A。

步骤 4:消息拥有者 A 接收到 $\tilde{s}$ 后，计算 $s=\alpha\tilde{s}+\beta \bmod(p-1)$，则 (r,s) 为消息 m 的多重盲签名。

(3)验证阶段

签名验证人接收到 $(m,(r,s))$ 后，验证等式 $g^s r=y^{mr} \bmod p$ 是否成立。若成立，则确信 (r,s) 是有效的盲签名。

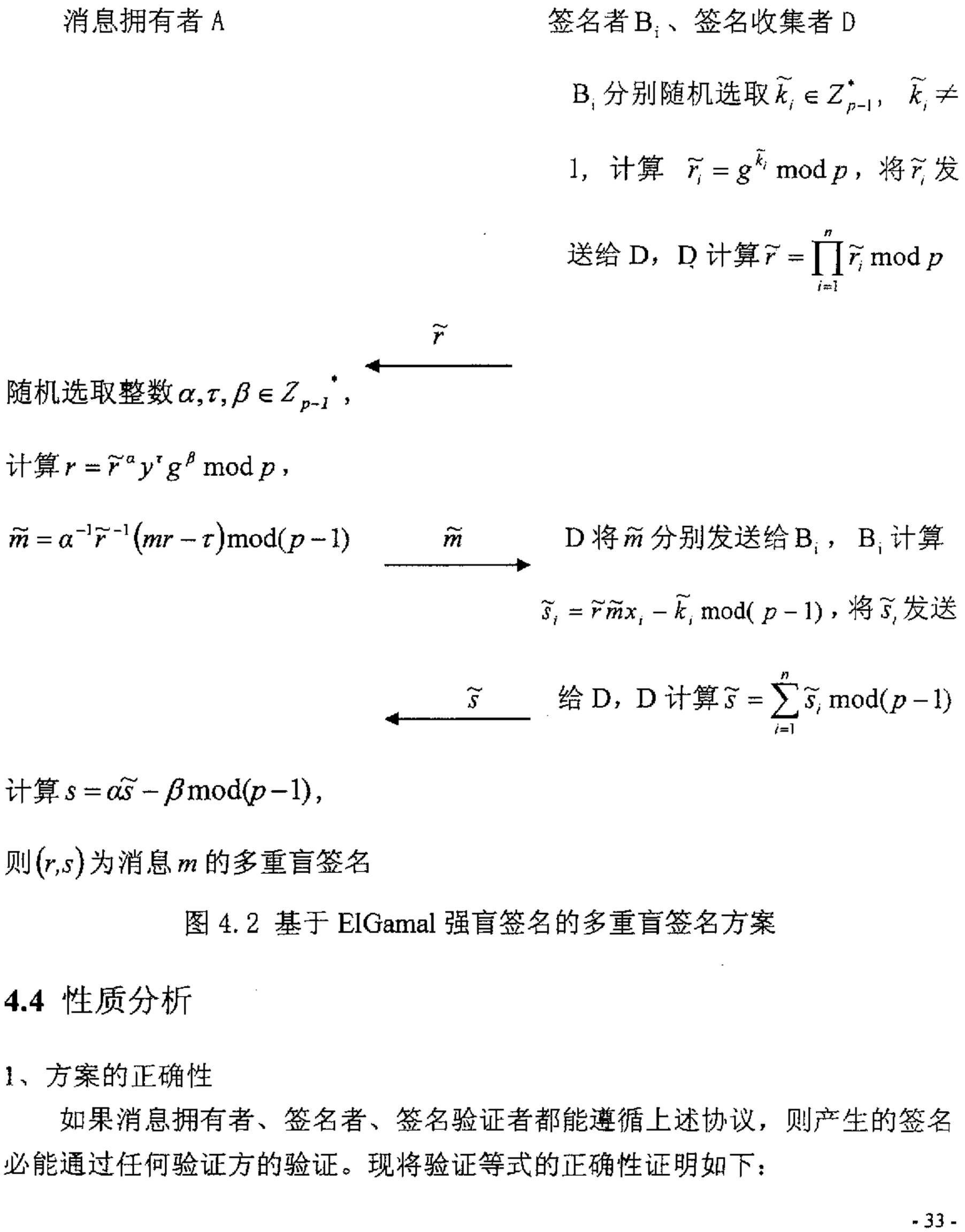


图 4.2 基于 ElGamal 强盲签名的多重盲签名方案

4.4 性质分析

1、方案的正确性

如果消息拥有者、签名者、签名验证者都能遵循上述协议，则产生的签名必能通过任何验证方的验证。现将验证等式的正确性证明如下：

$$\begin{aligned}\tilde{s} &= \sum_{i=1}^{n}\tilde{s}_i \bmod(p-1)\\ &= \sum_{i=1}^{n}\left(\tilde{r}\tilde{m}x_i - \tilde{k}_i\right)\bmod(p-1)\\ &= \tilde{r}\tilde{m}\sum_{i=1}^{n}x_i - \sum_{i=1}^{n}k_i \bmod(p-1)\end{aligned} \tag{4-2}$$

将 $\tilde{m} = \alpha^{-1}\tilde{r}^{-1}(mr-\tau)\bmod(p-1)$，

$s = \alpha\tilde{s} - \beta \bmod(p-1) \Rightarrow \tilde{s} = \alpha^{-1}(s+\beta)\bmod(p-1)$ 代入式（4-2），得

$$\alpha^{-1}(s+\beta) = \alpha^{-1}\tilde{r}\tilde{r}^{-1}(mr-\tau)\sum_{i=1}^{n}x_i - \sum_{i=1}^{n}k_i \bmod(p-1)$$

$$\Rightarrow s + \alpha\sum_{i=1}^{n}k_i + \tau\sum_{i=1}^{n}x_i + \beta = mr\sum_{i=1}^{n}x_i \bmod(p-1)$$

$$\Rightarrow g^s r = y^{mr} \bmod p$$

正确性得证。

2、方案的盲性

首先我们将证明，签名者不能获得有关消息 m 的任何信息。从协议过程可以看出，在整个签名过程中消息拥有者对消息 m 进行了盲化，其表达式为 $\tilde{m} = \alpha^{-1}\tilde{r}^{-1}(mr-\tau)\bmod(p-1)$，其中 $r = \tilde{r}^{\alpha}y^{\tau}g^{\beta} \bmod p$。显然，在计算 $\tilde{m}$ 的过程中使用了随机数 α,τ,β，而这些随机数是用户秘密选择的，签名者并不能得到。因此签名者无法从获得的数据 e 出发，从用户那里获得有关 m 的任何信息，从而在整个签名过程中，签名者没有获得有关消息 m 的任何信息。

其次，我们考虑协议的不可追踪性，即签名者不能根据他所掌握的有关数据来追踪他所产生的签名。在上述盲签名方案中，如果签名者 $B_i(i=1,2,\Lambda,n)$ 保留 $(\tilde{m},\tilde{r},\tilde{s})$，则当消息拥有者 A 公开 (m,r,s) 后，$B_i(i=1,2,\Lambda,n)$ 可以通过求解以下方程组

$$\begin{cases} r = \tilde{r}^{\alpha}y^{\tau}g^{\beta} \bmod p \\ \tilde{m} = \alpha^{-1}\tilde{r}^{-1}(mr-\tau)\bmod(p-1) \\ s = \alpha\tilde{s} - \beta \bmod(p-1) \end{cases}$$

得到 α,τ,β，但是可以发现求解该方程组需要面临求解离散对数的难题。因此，

签名者不能把签文件的行为与签了名的文件联系起来。即使他记下了他所作的每一个盲签名，当用到一个签了名的文件时，他也不能确定什么时候他签了该文件。这说明上述方案是一个强盲签名方案。

3、方案的安全性

上述方案与一般性盲签名方案的不同之处在于签名过程改由多人来完成，安全性得到了加强；与一般多重签名方案相同，本方案仅增加了 $B_i(i=1,2,\Lambda\ ,n)$ 的计算量，与消息拥有者无关，也不增加数字签名 (r,s) 的长度。本文从以下几个方面来说明该多重盲签名协议是安全的。

性质1：只有所有签名人都正确执行协议，才能生成正确的盲签名。

证明：从协议的执行过程可以看出，各签名人使用各自的私钥 x_i 进行同时签名，而在进行签名验证时使用的是各个签名人的公钥之积 $y=\prod_{i=1}^{n} y_i$。如果在签名过程中，有一位签名人没有参与签名，则在使用 $y=\prod_{i=1}^{n} y_i$ 验证签名等式 $g^s r = y^{mr} \bmod p$ 的过程中会发现签名不正确。因此，该方案可以保证只有在所有签名人共同参与的情况下才能得到合法的盲签名。

性质 2：在签名过程中，用户不能获得签名者的密钥之和 $\sum_{i=1}^{n} x_i$。

证明：从上述的多重盲签名协议可以看出，用户在签名过程中得到的数据是 $\tilde{r}$，$\tilde{s}$，其表达式为

$$\begin{cases} \tilde{r} = \prod_{i=1}^{n} \tilde{r}_i \bmod p \\ \tilde{s} = \sum_{i=1}^{n} \left(\tilde{r}\tilde{m}x_i - \tilde{k}_i\right) \bmod (p-1) \end{cases}$$

用户可以试图从以上方程组推导出 $\sum_{i=1}^{n} x_i$，但是 $\tilde{k}_i \in Z_q^*$ 是签名人选取的随机整数，用户无法知道 $\tilde{k}_i$ 的具体数值，试图通过等式 $\tilde{r}_i = g^{\tilde{k}_i} \bmod p$ 获得 $\tilde{k}_i$ 必须面临求解离散对数的难题，并且每一次签名选取的 $\tilde{k}_i$ 都不一样，因此用户无法通过求解以上方程组得到签名者的密钥之和 $\sum_{i=1}^{n} x_i$。

性质3：第三方不能伪造一个合法的盲签名。

证明：从协议的执行过程可以看出，各签名人使用各自的私钥x_i进行同时签名，而在进行签名验证时使用的是各个签名人的公钥$y=\prod_{i=1}^{n} y_i$。第三方不知道签名者密钥x_i，因此无法伪造签名者的签名。而计算密钥x_i由前面的分析可知，要面临计算离散对数的难题。所以第三方不能伪造一个签名者的合法签名。

性质4：签名收集者也不能伪造一个合法的盲签名。

证明：签名收集者将一次签名过程中的信息$(\tilde{r},\tilde{m},\tilde{s}_i)$保留下来，在下一次签名时签名收集者试图伪造签名者的合法签名。签名收集者将保留的$\tilde{r}$发送给消息拥有者从而得到$\tilde{m}'$，签名收集者试图从以下方程组

$$\begin{cases}\tilde{s}_i=\tilde{r}\tilde{m}x_i-\tilde{k}_i \bmod(p-1)\\ \tilde{s}_i'=\tilde{r}\tilde{m}'x_i-\tilde{k}_i \bmod(p-1)\end{cases} \qquad (\text{i=1, 2, ……, n})$$

求解出$\tilde{s}_i'$。从以上方程组可以明显看出，该方程组中存在3个未知数$\tilde{k}_i,x_i,\tilde{s}_i'$，而从前面定理的证明可以知道，试图求解$\tilde{k}_i,x_i$必须面临离散对数的难题。因此签名收集者无法从以上方程组中推导出各个签名者的合法签名$\tilde{s}_i'$，从而无法得到$\tilde{s}'=\sum_{i=1}^{n}\tilde{s}_i' \bmod(p-1)$。

4.5 本章小结

本章对祁明提出的多重盲签名方案进行了深入的分析和研究，并基于一个ElGamal 强盲签名方案构造了一个多重盲签名方案。分析表明，该方案能够实现多人对消息进行盲签名，并且能够同时满足盲签名的两个基本性质，即盲性和不可追踪性，具有强安全性。

第五章 基于盲签名的匿名电子投票系统

5.1 引言

电子投票[35][36][37][38]作为消息认证系统的重要课题之一和作为盲签名的重要应用，近年来之所以受到广泛关注，主要是由于它可以省去通常投票活动在组织工作、选票采集、选票统计和安全保密等方面所需花费的大量人力和物力；其次，投票人也可以不必去有关管理部门所设置的特定的投票处。因此，与通常的投票相比，电子投票既省钱、省力又安全。

1884年，Thomas Edison发明了一种电子投票装置，想将其卖给Massachusetts市的立法机关进行电子投票，但没有成功。这时人们仍然采用手工方式进行投票选举。但人们对电子投票方式的憧憬一直未改。随着计算机的出现，人们开始利用计算机进行电子选举的实践。1958年，哥伦比亚广播公司选举总部开始利用计算机对投票结果进行预测。1964年，美国的五个县在九月选举中使用了计算机。在1992年，这一美国大选年的民主党的全国代表大会上，代表们通过触摸屏进行投票，而在共和党的全国代表大会上，则使用了计算机系统进行管理。在巴西，到2001年为止，在全国范围内已经开始实行了通过触摸屏投票装置进行投票的民主选举。但这些电子选举的实践大多只停留在利用计算机或一些打孔设备、光读取设备进行日常的选举管理，这种选举方式要设立投票站，到了投票选举的时候，人们需要到投票站进行投票。真正能应用Internet进行投票选举的例子还不多见。在2000年美国的总统选举中，在佛罗里达州等少数几个地方对部分选民试行了通过Internet进行投票选举。

从上面的例子我们可以看出，要满足电子投票安全性要求的困难很大，所以人们将更多的签名技术应用到了电子投票领域，如盲签名等。2003 年，汪保友，杨风，胡运发[39]提出了一个基于盲签名的在线选举方案；陈晓峰，王育民[40]提出了一个基于匿名通讯信道的安全电子投票方案；周伯丹, 张曙光, 付志峰[41]提出了一个基于盲签名的电子选举方案。大部分电子投票协议为了满足大型电子投票的安全需要而设计的相当复杂，并且还只是处于理论探索、实验摸索阶段。

5.2 匿名电子投票应满足的基本性质

在现实生活中,一个普通的投票系统的安全性是显而易见的，对于投票人而言至少要保证：任何有资格的选民必须拥有一张选票(除非他弃权)、一个人只能限投票一次而不能随意投二次或多次(被委托投票者需出示委托书且限制委

托一次)、每个人的投票内容要保密、任何人不能伪造假选票。对于选举组织者而言,他必须做到这些要求：审查选民的合法性、只能给有资格的人才能颁发选票且一人只能颁发一张、没有资格的人不能投票、能识别假冒的选票、所有的投票被正确计入、计票结果是诚实的等。

而匿名电子投票方案至少应达到普通投票系统所具备的性质和要求，而且还应该满足普通选举不能满足的要求，使得电子投票更科学、更合理。一个安全的匿名电子投票协议应满足下列基本性质[41]：

(1)合法性：只有合法选民才能投票，非法选民或冒充他人均能被识别和跟踪。

(2)保密性：除了投票者外，选票的内容不能被其他人知道。

(3)匿名性：指无法将所投选票和投票人联系起来，即无法根据选票跟踪投票人。

(4)完备性：所有合法选票应被正确统计。

(5)正当性：不诚实的选举者无法扰乱和破坏选举。

(6)不可重复性：任何选举者不可重复投票。

(7)公平性：任何事情不能影响选举结果，特别是投票的中间结果不可泄露。

(8)公正性：任何选票不能被修改,修改过的选票能被识别并被剔除。

(9)可验证性：任何人可以检验自己的选票是否被计入,任何人都可以选票结果是否正确，任何人均可对其进行验证。如果发生选票被改动和漏掉而未公布，则很容易被选举人发现。

5.3 匿名电子投票协议的设计

5.3.1 匿名电子投票协议

一个匿名电子投票协议由以下四部分组成。协议包括认证中心(Certificate Authority)、管理机构(Management Administration)、投票人(Votor)和计票机构(Count Administrator)。认证机构负责分别向管理机构、计票机构和所有投票人发放数字证书，数字证书中存放各个参与方的身份信息以及公钥信息；管理机构负责对投票人的资格进行审核，并对电子选票进行盲签名；计票机构负责发放电子选票，以及对提交的电子选票进行验证，统计选票，并将选举结果公布。投票人投票后可验证投票结果是否公正，自己的选票是否被计入。下面首先给出电子投票协议的详细过程。

首先给出所需要的参数和符号：设CA：认证中心，A：管理机构，V：投票人，C：计票机构。因为RSA公钥密码体制成熟简单，易实现，并且既可以用于加密也可以用于数字签名，因此在我们的匿名电子投票协议中采用了RSA公

钥密码体制来实现加密及数字签名的功能。整个匿名电子投票协议描述如下：

(1)系统初始化

所有参与方应到CA处申请数字证书，CA审查参与方的身份后，向申请人颁发数字证书，数字证书中应包含公钥以及CA的签名。各参与方可以以此作为自己的身份证明，与之对应的私钥由各参与方自己保存。在RSA公钥密码体制下， A的公钥为PKa，私钥为SKa；C的公钥为PKc，私钥为SKc。所有投票人均从CA处获得相应的公钥证书，他们的公钥和私钥分别记为PKv，SKv。

(2)注册协议

Step1：投票人 V 到投票管理机构 A 处进行注册，填上身份证号码 IDv 和一个随机数 Rv，并用私钥对信息进行签名 $SIG_V(IDv||Rv)$，然后发送给 A。

Step2：A 首先用 V 的公钥验证签名的正确性，然后判断 V 是否具有选举资格，如果 V 通过验证，则 A 向他颁发一个统一的投票编号 Nv(该号具有唯一性,只有合法的投票人才能领取这样一个编号)，并计算编号 Nv 的认证码 MACv=H(IDv||Rv||Nv)，H(·)为哈希函数。A 用自己的私钥进行签名 $SIG_{SKa}(Nv||MACv)$，并将 $SIG_{SKa}(Nv||MACv)$发送给 V，同时保留投票人的身份信息(IDv,Nv,MACv)，以便将来发生纠纷时对不诚实的投票人进行追踪。

Step3：V 收到 A 的签名后，用 A 的公钥计算得到(Nv)'||(MACv)'。如果(MACv)'=H(IDv||Rv||(Nv)')成立，则说明 A 的签名有效，而且只有 V 才能进行验证，因为任何人不知道 V 选取的随机数 Rv。V 保留 $Rv||SIG_{SKa}(Nv||MACv)$，以此证明自己是经过认证的合法的投票人。

Step4：A 完成对所有投票人的认证工作后，将 V 的投票编号 Nv 和相应的签名 $SIG_{SKa}(Nv||MACv)$ 发送给计票中心 C，同时公布所有的(Nv，$SIG_{SKa}(Nv||MACv)$)，并宣布在某一时刻开始投票。

(3)选票签名协议

Step1：投票人 V 将选票编号 Nv 和 A 的签名 $SIG_{SKa}(Nv||MACv)$发送给计票中心 C，C 对 $SIG_{SKa}(Nv||MACv)$进行验证，若签名正确则将 C 的签名 $SIG_{SKc}(Nv)$ 发送给 V。

Step2：投票人 V 根据自己的意愿填入选票内容 M，对 M||Nv 进行盲化处理得 M'，并用 A 的公钥加密 $SIG_{PKa}(Nv||SIG_{SKc}(Nv)||M')$，将其发给 A。

Step3：A 收到后，验证 V 的选票是否合法。A 首先用私钥 SKa 解密得到 $Nv||SIG_{SKc}(Nv)||M'$，然后用 C 的公钥 PKc 验证签名 $SIG_{SKc}(Nv)$是否正确。如果正确，则说明 V 的选票有效，同时对 M'进行签名 $SIG_{SKa}(M')$，然后传送给 V。

Step4：V 对 $SIG_{SKa}(M')$进行去盲处理后，得到 A 的签名 $SIG_{SKa}(M||Nv)$。

(4)计票协议

Step1： V 用 C 的公钥 PKc 加密得 $SIG_{PKc}(M||Nv||SIG_{SKa}(M||Nv))$，然后传

递给 C。

Step2：C 收到后，用私钥解密得 $M||Nv||SIG_{SKa}(M||Nv)$，首先验证 $SIG_{SKa}(M||Nv)$是否正确。如果正确，则说明是经 A 签名过的投票，同时判断是否存在 Nv 或是否是第二次计票，以保证正确计票，这时将所有参加投票的 Nv 公布，使得投票人知道自己的选票是否被计入。

Step3：第一阶段投票结束后，C应将投票人的编号予以公布。如果投票人没有发现自己的编号Nv，则可以在规定的一段时间进行重新投票，以保证所有的投票都能被有效地接收，而不漏掉任何一个人。

5.3.2 协议的安全性分析

本章中提出的基于盲签名技术的电子投票系统在满足电子投票系统基本要求的基础上，很好的解决了投票人匿名性的问题，现对方案的安全性分析如下：

(1)合法性

只有合法选民才能投票，非法选民或冒充他人均能被识别和跟踪。攻击者可能伪装成某个合法的投票人注册投票。但是在管理协议阶段，每一个投票人都用私钥对身份证号码 IDv 和随机数 Rv 进行了签名得到 $SIG_V(IDv||Rv)$，然后发送给管理机构 A。管理机构 A 用每一个投票人的公钥验证，攻击者无法获得合法的投票人的私钥，因此不能伪装成某个合法的投票人获得选票编号。

(2)保密性

除了投票人外，选票的内容不能被其他人知道。在电子选票签名阶段，投票人对 M||Nv 进行盲化处理得 $M'=h(M||Nv)k^e \bmod n$，并用 A 的公钥加密得到 $SIG_{PKa}(Nv||SIG_{SKc}(Nv)||M')$，将其发给 A。管理机构并不知道选票的具体内容，只是对投票人盲化后的电子选票进行签名，使电子选票合法化。

(3)匿名性

指无法将所投选票和投票人联系起来，即无法根据选票跟踪投票人。恶意的攻击者在投票结果公开后只能获得 M||Nv，即每一个序列号以及对应的选票内容。假设攻击者获得了 MACv=H(IDv||Rv||Nv)，由于哈希函数是单向函数，因此无法将每一个序列号 Nv 和投票人的真实身份 IDv 联系起来，也就无法知道所投选票对应的投票人的真实身份 IDv。除了管理机构外，任何人都不能获知投票人的身份及其选票内容。

(4)完备性

所有合法选票应被正确统计。假设投票者遵守选举协议进行了投票，但投票被管理中心拒绝。在协议中，投票者的选票被管理中心拒绝可能发生在两个阶段:签名阶段和统计阶段。第一阶段投票结束后，C 将投票人的编号予以公布，

如果投票人没有发现自己的编号 Nv，则可以在规定的一段时间进行重新投票，以保证所有的投票都能被有效地接收，而不漏掉任何一个人。

(5)正当性

不诚实的选举者无法扰乱和破坏选举。在电子注册阶段，投票人需要用自己的私钥对提交的信息进行签名；在申请领取正式选票阶段，投票人需要凭借选票编号 Nv 和 A 的签名 Sv 到计票中心 C 申请领取正式选票；在投票阶段投票人需要提交管理机构对电子选票的签名。可以看出，电子投票协议中的每一阶段都有相应的签名和认证过程来防止恶意的攻击行为。

(6)不可重复性

任何选举者不可重复投票。因为每一份电子选票有一个对应的序列号 Nv，投票人将电子选票提交给机票机构 C，拍卖方通过将提交的电子标书的序列号 Nv 和数据库中已经提交的电子选票的序列号进行对比，可以发现重复提交的电子选票，有效防止重复提交电子选票的现象发生。

(7)公平性

任何事情不能影响选举结果，特别是投票的中间结果不可泄露。投票人 V 在投票的过程中使用计票机构 C 的公钥 PKc 对电子选票及 A 的签名进行加密得到 $SIG_{PKc}(M||Nv||SIG_{SKa}(M||Nv))$并传递给 C。攻击者无法不知道计票机构的私钥，因此无法得知电子选票的内容。

(8)公正性

任何选票不能被修改，修改过的选票能被识别并被剔除。在投票阶段，投票人将电子选票 M||Nv 进行盲化处理得 $M'=h(M||Nv)k^e \bmod n$，然后提交给管理机构，管理机构对 M'进行签名 $SIG_{SKa}(M')$，然后传送给 V。V 去盲后得到得到 A 的签名 $SIG_{SKa}(M||Nv)$，并传递给 C。C 验证 $M||Nv=D_{PKa}(SIG_{SKa}(M||Nv))$是否成立？如果成立，则说明是经 A 签名过的投票。如果选票被修改过，则验证等式不能成立，修改过的选票能够成功的被识别出来。

(9)可验证性

投票结束后，计票中心将电子选票 M||Nv 公开，任何人根据自己选票的序列号 Nv 可以检验自己的选票是否被计入，并且可以验证选票结果是否正确。其他任何人均可以通过等式 $M||Nv=D_{PKa}(SIG_{SKa}(M||Nv))$对选票的合法性进行验证。如果发生选票被改动和漏掉而未公布，则很容易被选举人发现。

本章基于盲签名技术构造了一个匿名电子投票系统，有效的解决了投票者匿名性的问题，计票机构无法追踪到投票者的真实身份，并且该系统可以有效防止一人多票或一票多投现象的发生，使得整个投票系统更加公正、安全。同时，借助 CA 中心该系统可以对投票过程中各参与方的真实身份进行认证识别，具有很高的实用价值。

5.4 系统设计

这里假设有四个实体：包括认证中心(Certificate Authority)、管理机构(Management Administration)、投票人(Votor)和计票机构(Count Administrator)。认证中心负责发放各个参与方的数字证书，数字证书中包含各个参与方的身份信息和公钥信息；管理机构负责审核投票人的资格，防止“一人多票”的现象发生，并对提交的选票进行盲签名，使其具有合法性；计票机构负责对提交的选票进行验证，防止“一票多投”的现象发生，并统计选票，公布结果。匿名电子投票系统组成如图6.1所示。

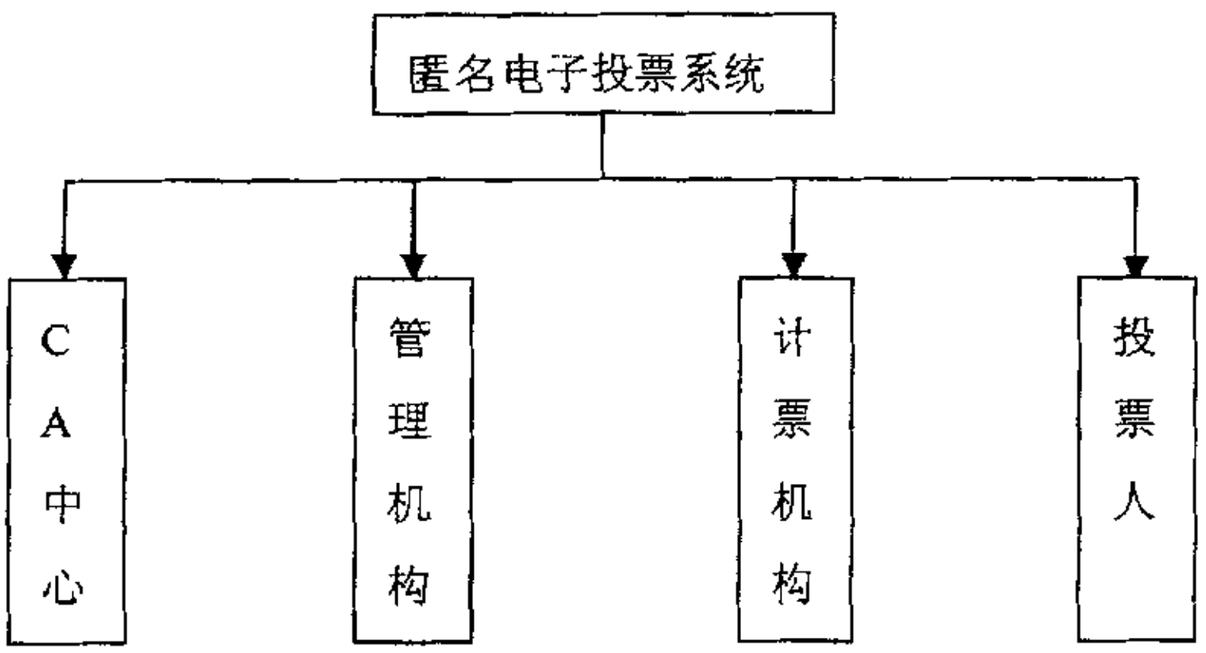


图 6.1 匿名电子投票系统组成图

整个系统的流程如图 6.2 所示

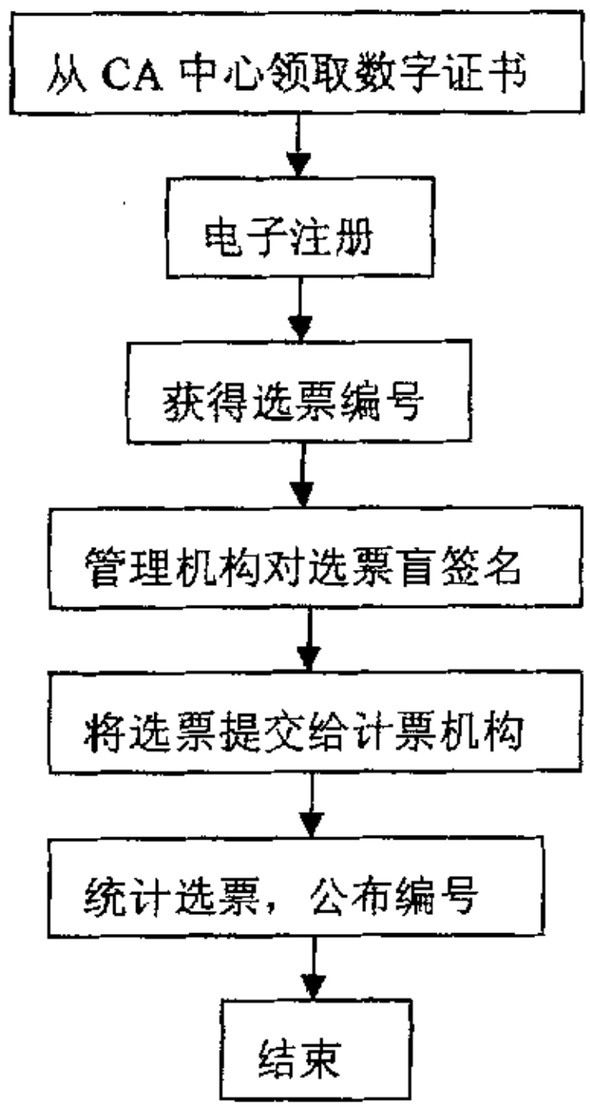


图 6.2 匿名电子投票系统流程图

本系统主要划分为以下几个模块:系统初始化模块、注册模块、选票签名模

块、计票模块。此外，在该系统中使用了多种加密解密、数字签名等算法以满足匿名电子投票系统的安全性。系统中使用到的主要算法如图 6.3 所示。

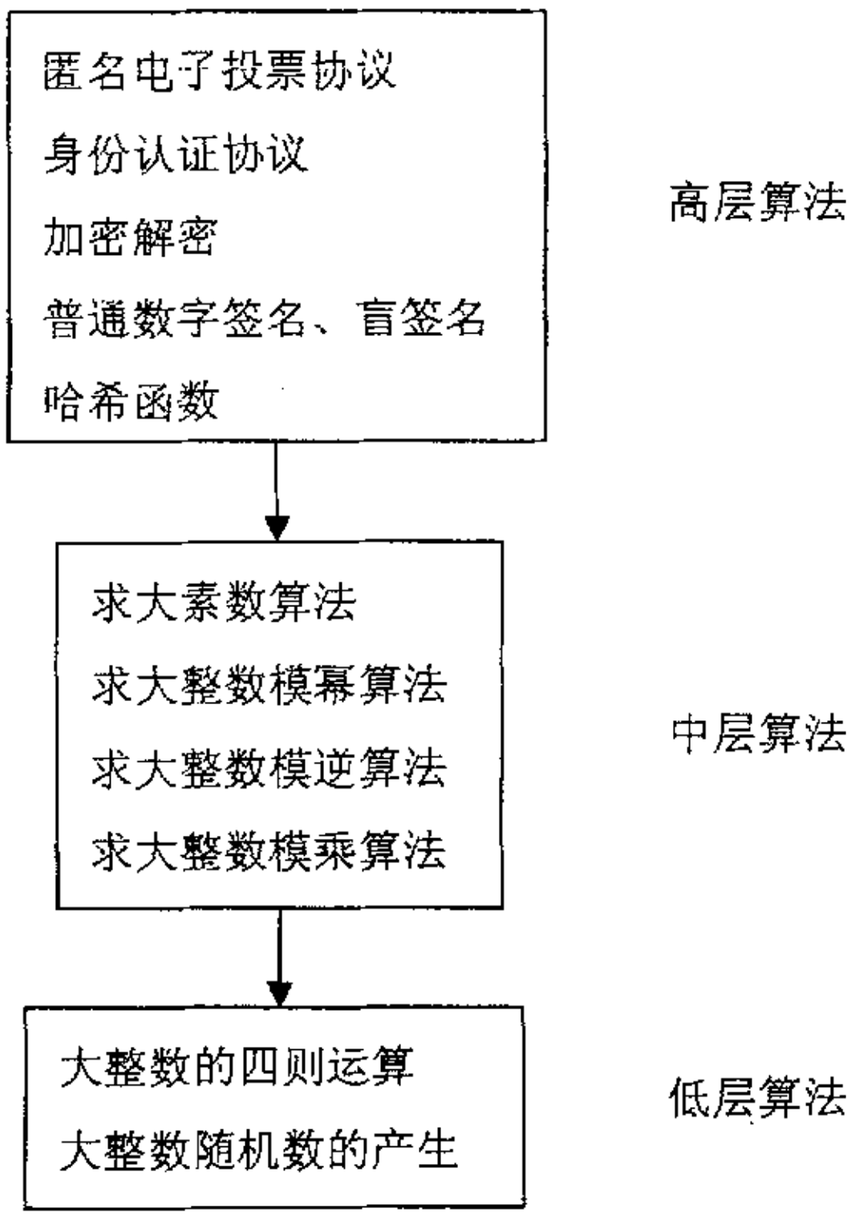


图 6.3 系统中使用的主要算法

5.4.1 系统初始化模块的设计

为了实现上述协议，我们采用 RSA 公钥密码体制，系统初始化参数包括：管理认证机构 A 随机地选取两个大素数 p,q (二进制位为 512 位)，计算 $n=p\cdot q$，$\varphi(n)=(p-1)(q-1)$，然后随机地选取 e 满足 $1<e<\varphi(n)$ 且 $\gcd(e,n)=1$，并计算 d 使得 $1<d<\varphi(n)$ 且 $de\equiv 1 \bmod \varphi(n)$ 成立，则 A 的公钥是 PKa=(n,e)，私钥是 SKa=d (公钥和私钥的二进制位为 1024 位)。

RSA 算法需要生成一对 1024 位的公钥和私钥，而产生公钥和私钥需要用到大素数。显然，通过对一个随机数进行因子分解，我们可以判断这个随机数是否为素数。但是，大整数的因子分解是一个难解的问题，到目前为止我们还没有找到一个快速有效的算法来大整数进行因子分解。因此，我们不能试图通过对随机数进行因子分解来生成大素数。

我们考虑对生成的随机数先测试它是否为素数，而不是对它进行因子分解。这种素数测试比因子分解要容易得多。已经有许多素性测试方法能够确定一个随机数是否为素数。如果合数通过一个素性测试的概率足够小，则这个素

性测试是很可靠的。实际上，对于许多素性测试方法，合数通过测试的概率可以受到控制，也就是说，我们可以把合数通过测试的概率设定的足够小。

目前最快的算法是拉宾-米勒测试算法，其定义如下：令$n-1=2^l m$，其中l是非负整数，m是正奇数。若$b^m \equiv 1 \bmod n$或$b^{2^j m} = -1 \bmod n$，$0 \le j \le l-1$，则称n通过以b为基的拉宾-米勒测试。若n通过一次测试，则n不是素数的概率为 25%，若n通过 t 次测试，则n 不是素数的概率为$1/4^t$。因此，在实际应用中让b取不同的值对n进行 5 次测试，若全部通过则判定n为素数。并且，可首先用 300－500 个小素数对n进行测试，以提高拉宾－米勒测试通过的概率，从而提高测试速度。

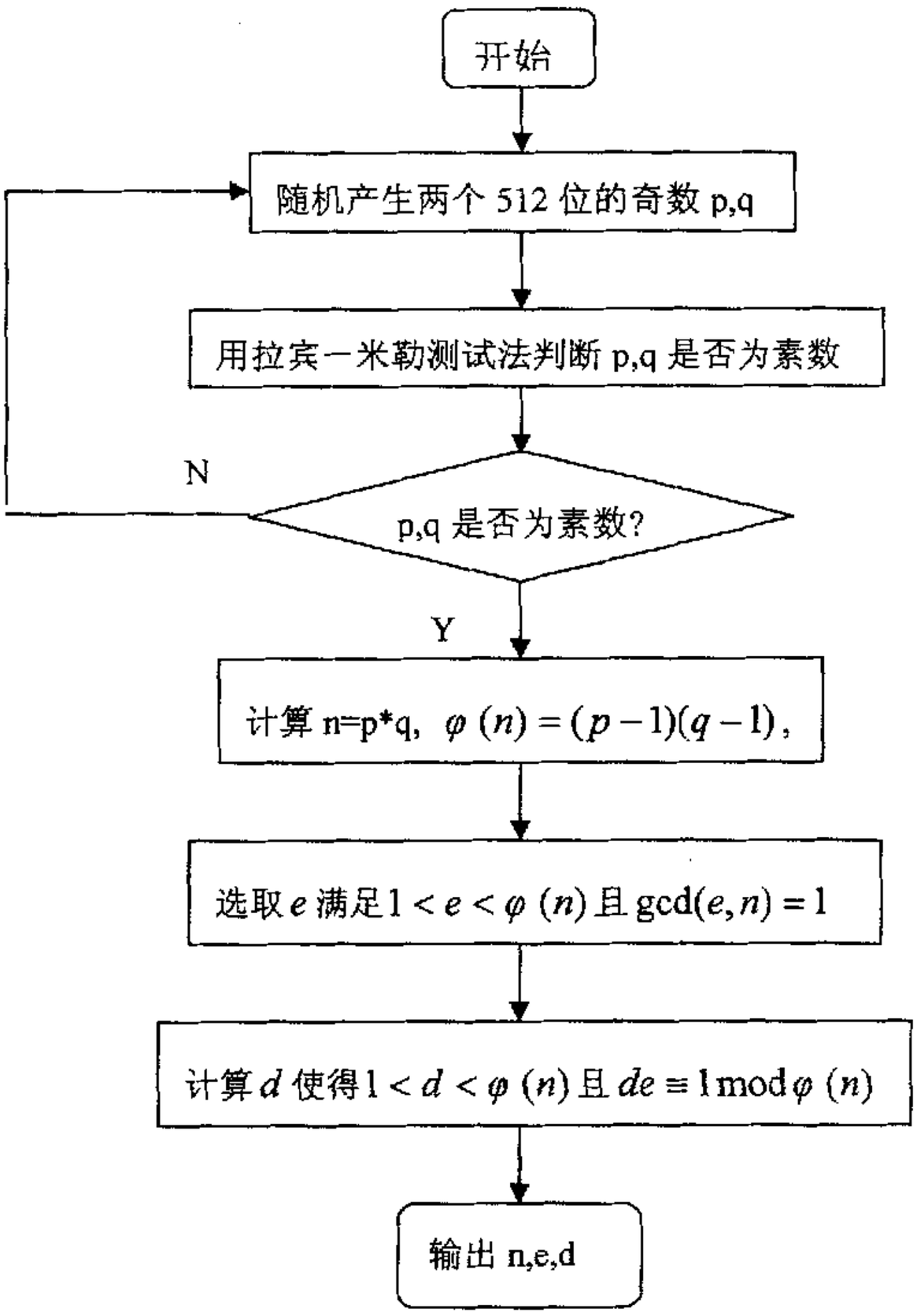


图 6.4 系统初始化流程图

系统公钥是可以公开的，无保密性的要求，可以存放在中心数据库中，供用户查询使用。再看一下系统私钥，持有人必须妥善保管，千万不可泄漏。一旦泄漏，应立即吊销。系统私钥由各参与方自己产生，自己使用，不存在分发

的问题。从理论上讲，应将私钥记忆在头脑中，这是最安全的，但这种方法不可行。一方面私钥难于记忆，另一方面每次签名都要输入私钥很麻烦。还是要将用户私钥存储在数据库中。但直接把私钥存入数据库中，会降低系统的安全性，为此我们考虑以密文形式存储私钥。这样既免去了记忆私钥的麻烦，也使私钥的安全性得到了保证。私钥的加解密都是由私钥拥有者自行完成，不存在密钥的传送问题，而且在一段时间内密钥是唯一的，只要记在用户的脑子里就可以了，不必再对私钥加密密钥进行管理，因此我们可以采用加密速度快些的对称钥加密算法—DES 算法对私钥加密。

5.4.2 注册模块的设计

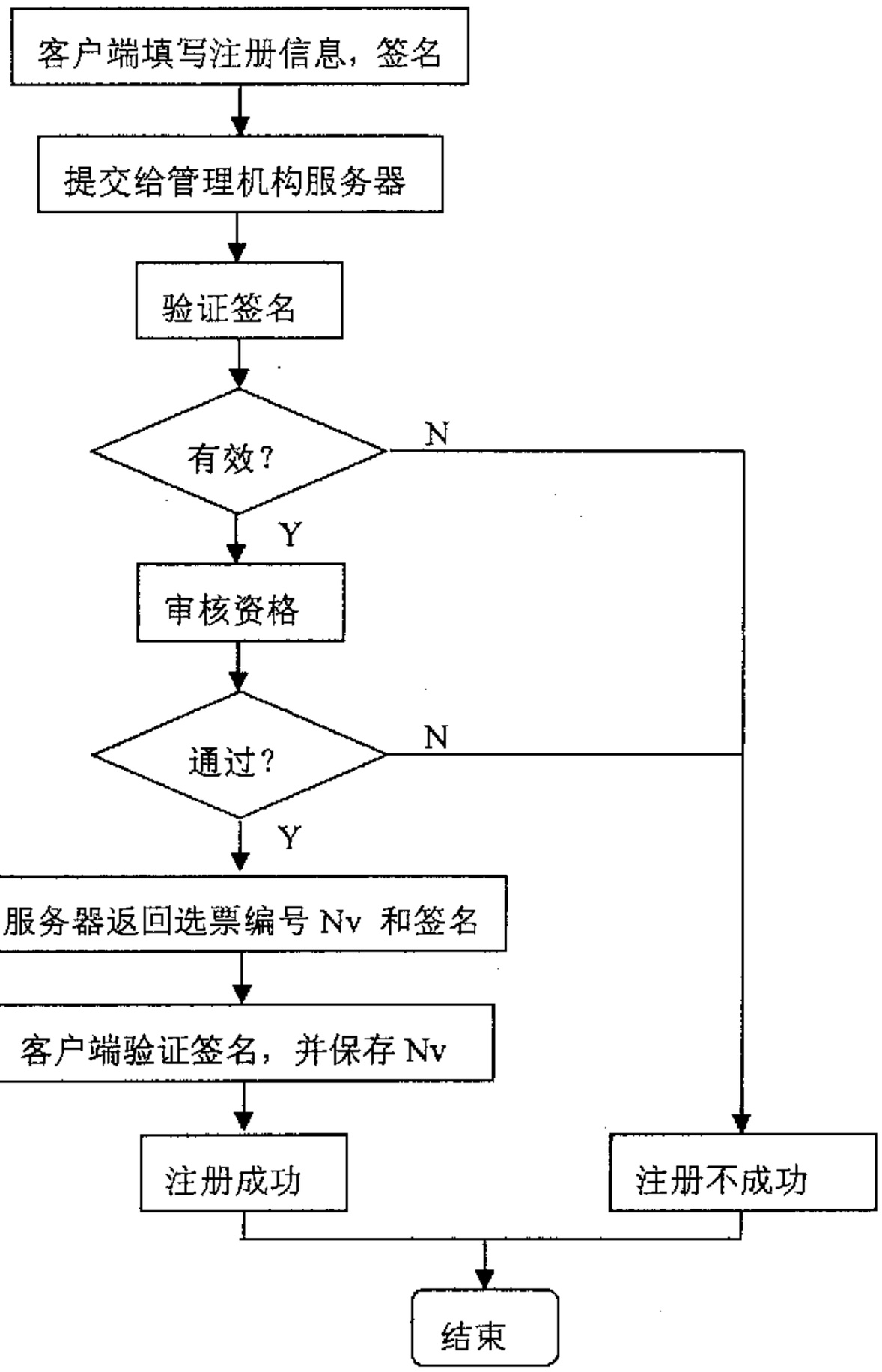


图 6.5 注册模块流程图

注册模块主要负责的工作是：投票人 V 填写注册信息，如身份证号码 IDv 和一个随机数 Rv，并用私钥对信息进行签名然后提交给管理机构服务器。管理

机构服务器验证提交的数字签名是否正确，对每一位注册的投票人的资格进行审核，若资格审核通过，则管理机构服务器为每一位投票人自动生成一个唯一的选票编号 Nv，并计算相应的认证码 MACv，用私钥对其签名后发送给投票人 V。其具体过程如下：

投票人 V 到投票管理机构 A 处进行注册，填上身份证号码 IDv 和一个随机数 Rv，并用私钥对信息进行签名 $SIG_V(IDv||Rv)$，然后发送给 A。A 首先用 V 的公钥验证签名的正确性，然后判断 V 是否具有选举资格，如果 V 通过验证，则 A 向他颁发一个统一的投票编号 Nv(该号具有唯一性,只有合法的投票人才能领取这样一个编号)，并计算编号 Nv 的认证码 MACv=H(IDv||Rv||Nv)，H(·)为哈希函数。A 用自己的私钥进行签名 $SIG_{SKa}(Nv||MACv)$，并将 $SIG_{SKa}(Nv||MACv)$ 发送给 V，同时保留投票人的身份信息(IDv,Nv,MACv)，以便将来发生纠纷时对不诚实的投票人进行追踪。

V 收到 A 的签名后，用 A 的公钥计算得到(Nv)'||(MACv)'。如果(MACv)'=H(IDv||Rv||(Nv)')成立，则说明 A 的签名有效，而且只有 V 才能进行验证，因为任何人不知道 V 选取的随机数 Rv。V 保留 $Rv||SIG_{SKa}(Nv||MACv)$，以此证明自己是经过认证的合法的投票人。

5.4.3 选票签名模块的设计

选票签名模块的设计是本系统设计的核心内容，它主要负责的工作是：管理机构对提交的盲化的电子选票进行签名使其合法化，但并不知道其选票的内容。投票人通过去盲得到管理机构对原始电子选票的合法签名。这样计票机构可以通过验证提交的选票的签名，来判断选票的合法性，其流程图如图 6.6 所示。

在方案的设计中，我们选用 RSA 盲签名对电子选票进行盲签名。在具有代表性的 RSA 盲签名，Schnorr 盲签名和 ElGamal 盲签名中，从安全性方面比较，RSA 盲签名基于因子分解问题的难解性,Schnorr 盲签名和 ElGamal 盲签名基于离散对数的难解性。从速度方面比较，RSA 速度最快，Schnorr 盲签名次之，ElGamal 盲签名最慢，并且 RSA 盲签名也易于理解和操作。因此，本方案选择 RSA 盲签名对电子选票进行盲签名。

从前面对电子投票协议的详细描述可以看出，在选票签名协议 Step2～Step4 中需要使用到盲签名技术。其过程如下：投票人 V 填上选票， 随机选取与 n 互素的 k，然后计算 $M'=h(M||Nv)k^e \bmod n$，并用 A 的公钥加密得到 $Sa=(Nv||Sc||M')^e \bmod n$，将其发给 A。A 收到 Sa 后，验证 V 的选票是否合法？A 首先用私钥 SKa 解密得：Nv|| Sc||M'，然后用 C 的公钥 PKc 验证 $Nv=(Sc)^{e'}=\bmod n'$是否成立？ 如果成立，则说明 V 的选票有效，同时对 M'进行签名 $S_{m'}=(M')^d \bmod$

n，然后传送给 V。V 得到 $S_{m'}$后，计算 $S_m=k^{-1}S_{m'}= k^{-1}(M')^d \bmod n=(h(M||Nv))^d \bmod n$，这时 V 用 C 的公钥签名得 $Se=(M||Nv||S_m)^e \bmod n'$。并传递给 C。

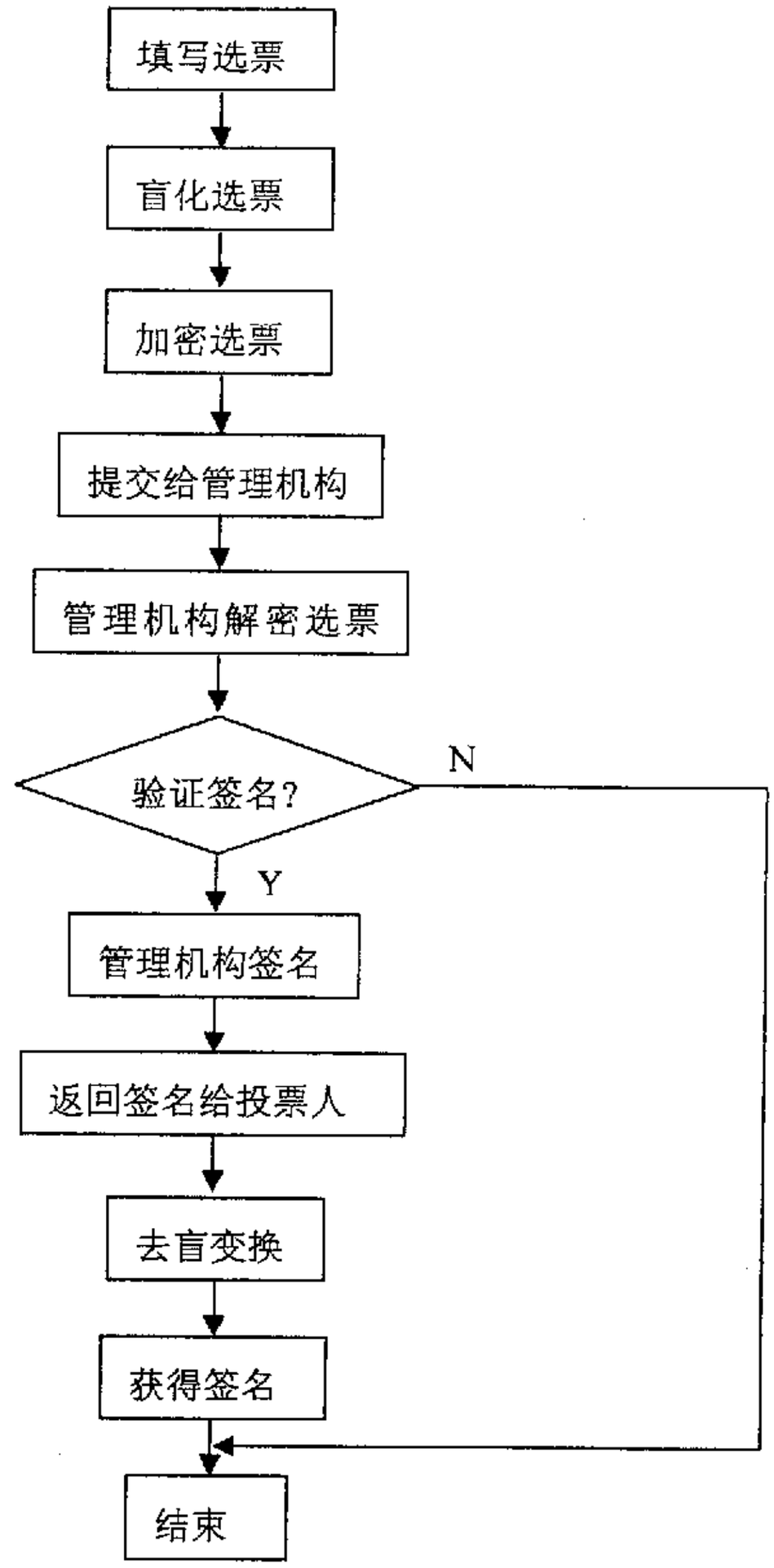


图 6.6 选票签名模块流程图

本节借助于前面设计的大整数类 CBigInteger 中提供的模幂运算、模逆运算等函数实现了盲签名协议的基本过程。其中哈希函数属于一个预处理模块，是为签名及验证模块做准备的。通过对消息提取哈希值，将输入的不定长的信息变换成定长的信息串输出，而且此过程不可逆。该模块应具有以下三个特点：

（1）为了提高签名及验证过程的速度，该模块应能够对输入的信息进行压缩，减少原始数据量；

（2）该模块应具有单向性，即由该模块的输入很容易得到输出结果，但由一个已知的输出结果却很难推测出原始的输入信息；

（3）通过该模块处理后得到的信息与原始信息应该密切相关，对原始信息

的任何一个比特的改动，都能够引起变换后数据的激烈变动，以便能够检测出对原始信息的任何细微改动，这样一方面可以充分防止对原始信息的破坏，另一方面也避免了当原始信息发生较少变化时，相同签名结果的出现，提高了系统的抗碰撞性。

现对盲签名的实现过程详细说明如下：

Step2：投票人 V 填上选票， 随机选取与 n 互素的 k，并计算选票 M 的哈希值 h(M)，然后对原始消息进行盲化，计算 $M'=h(M||Nv)k^e \bmod n$，并用 A 的公钥加密得到 $Sa=(Nv||Sc||M')^e \bmod n$，将其发给 A。其中选票内容分为“同意”、“不同意”两种情况，分别用字符‘0’和‘1’来表示。

```
BOOL CEvoteDlg::OnGeneratevote()
{
        ……                          //系统参数初始化
         int squencelen=m_squence.GetWindowTextLength ();//获取序列号的长度
        char message[squencelen]={0};
        char temp[256]={0};
        m_squence.GetWindowText (message,squencelen+1);  //获取序列号
        if(option==TRUE)
           message[squencelen]='1';
        else
           message[squencelen]='0';
        char HashMessage[32]={0};
        BOOL result = SHAEncrypt(message,HashMessage, squencelen+1);
        if(!result)
        {
           MessageBox("SHA Error! ");
           return FALSE;
        }
        bytes_to_big(32,HashMessage,m);//将字符数组消息 m 转化为大数
        //计算 mm=m*k^e mod n
        modexp (m,1,n,result1);
        modexp (k,e,n,result2);
        modmul (result1,result2,n,mm);
        //发送 mm 至服务器
        big_to_bytes(256,mm,temp,FALSE);//将 mm 转换成数组写入 temp
```

```
        CString str;
        str.Format("%s",temp);
        SendMsg(str);
        return TRUE;
}
```

Step3：A 收到 Sa 后，验证 V 的选票是否合法？A 首先用私钥 SKa 解密得：Nv‖ Sc‖M'，然后用 C 的公钥 PKc 验证 $Nv=(Sc)^{e'}$=mod n'是否成立？如果成立，则说明 V 的选票有效，同时对 M'进行签名 $S_{m'}=(M')^{d}$mod n，然后传送给 V。

```
void CServerDlg::ProcessPendingRead(CClientSocket* pSocket)
{
    ……                    //系统参数初始化
    //定义缓冲区
    char buffer[BUFFER_SIZE];
    //接收数据
    int nReceived = pSocket->Receive(buffer,BUFFER_SIZE,0);
    buffer[nReceived] = 0;
    bytes_to_big(nReceived,buffer,mm);//将字符数组消息 m 转化为大数
    modexp (mm,d,n,ss);//计算 ss=mm^d mod n
    //将 ss 发送至客户端
    char temp[256]={0}; //建立临时数组
    big_to_bytes(256,ss,temp,FALSE);//将 ss 转换成数组写入 temp
    CString str;
    str.Format("%s",temp);
    pSocket->Send(str.GetBuffer(0),str.GetLength(),0);//发送数据到客
户端
    ……
}
```

Step4：V 得到 $S_{m'}$后，计算 $S_m=k^{-1}S_{m'}= k^{-1}(M')^{d}$mod n=($h(M||Nv))^{d}$mod n，这时 V 用 C 的公钥签名得 $Se=(M||Nv||S_m)^{e'}$mod n'。并传递给 C。

```
void CEvoteDlg::ProcessPendingRead()
{
    ……                    //系统参数初始化
    //定义缓冲区
    char buffer[BUFFER_SIZE];
    //接收数据
```

```
int nReceived = m_pSocket->Receive(buffer,BUFFER_SIZE,0);
buffer[nReceived] = 0;
bytes_to_big(nReceived,buffer,ss);//将字符数组消息 m 转化为大数
//计算 s=1/k *ss mod n
modinv(1,k,n,result3);
modexp (ss,1,n,result4);
modmul (result3,result4,n,s);
char signature[256]={0};
    cotstr(s,signature);                    //将 m 以 16 进制串写入 signature
    m_sn.SetWindowText (signature); //输出 16 进制 signature
    ......
}
```

5.4.4 计票模块的设计

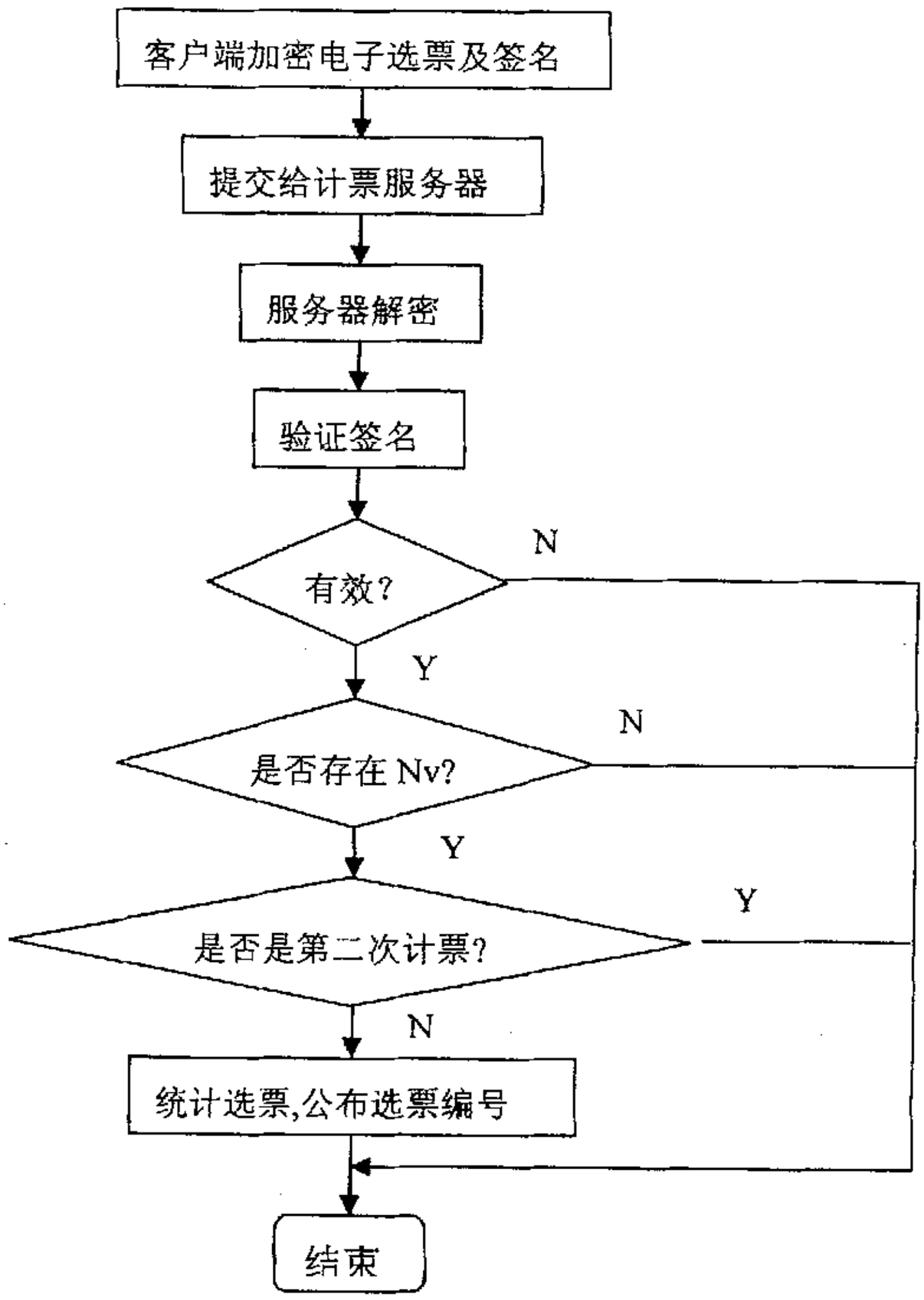


图 6.7 计票模块流程图

计票模块采用了普通的 RSA 算法，用公钥对选票进行加密用私钥对选票进行解密。计票模块主要负责的工作是：V 用 C 的公钥加密电子选票及签名得 $Se=(M||Nv||S_m)^{e'} \bmod n'$，并传递给 C。C 收到后，用私钥解密得 $M||Nv||S_m$，首先验证 $M||Nv= (S_m)^{c} \bmod n$ 是否成立？如果成立，则说明是经 A 签名过的投票，同时判断是否存在 Nv 或是否是第二次计票，以保证正确计票，这时将所有参加投票的 Nv 公布，使得投票人知道自己的选票是否被计入。

第一阶段投票结束后，C 应将投票人的编号予以公布，如果投票人没有发现自己的编号 Nv，则可以在规定的一段时间进行重新投票，以保证所有的投票都能被有效地接收，而不漏掉任何一个人。计票模块的流程图如图 6.7 所示。

5.4.5 数据库的设计

数据库是网络的核心部分，用来存储所有用户的登记信息、公钥和私钥等有价值的数据资源，这些共享的数据资源既要面对必需的可用性需求，又要面对被篡改、毁坏和被窃取的威胁。

表 6.1 投票者表结构

字段名称	类型	长度(Byte)	说明
ID_Votor	CHAR	18	身份证号码
Vote_Number	CHAR	18	投票人统一编号
Mac_Votor	CHAR	40	认证码
Apply_No	BOOL	1	是否申请

表 6.2 选票表结构

字段名称	类型	长度(Byte)	说明
Vote_Number	CHAR	18	投票人统一编号
Sig_A_Votor	CHAR	256	A 对投票人的签名
Sig_A_Ticket	CHAR	256	A 对选票的签名
Voting_No	BOOL	1	是否投票
Voting_Result	CHAR	1	投票结果
Voting_Repeat	BOOL	1	是否第二次投票

要实现匿名电子投票功能，需要用到数据库管理系统作为后台支撑，由于涉及到的数据关系简单，因而数据库的设计非常简单，只需 2 张关系表就可以满足要求。需要说明的是由系统随机生成的公钥和私钥，其类型是自定义的大整数类型，需要先将其进行加密保存,需要使用时须解密后再使用，以保证签名的有效性。管理认证机构 A 负责对投票人的身份进行验证，投票人的数据结构如表 6.1 所示。

计票机构C首先从A处获得所有选民的统一编号Nv和A的签名Sv,然后还需要验证选票并签名，最后将合法选票的信息存入选票表中，选票表的结构如表6.2所示。

本系统开发的软硬件环境配置如下：

(1)软件环境配置

操作系统：Windows 2000 Professional

开发工具：Visual C++6.0, SQL Server2000

通信协议：TCP/IP

(2)硬件环境配置

CPU Type: PENTIUN IV

CPU Clock: 2.0GHZ

内存:256MHz

硬盘:60G

5.5 本章小结

本章基于盲签名技术构造了一种匿名电子投票协议，该协议借助盲签名技术可以实现投票者身份的匿名性，并且有效的防止了一人多票或一票多投现象的发生。然后基于该协议构造了一个匿名电子投票系统，对该系统进行了详细设计，并给出了部分算法的实现。

第六章 结论与展望

盲签名是一种特殊的数字签名，盲签名所具有的匿名性使得这种技术可广泛用于许多领域。本文对盲签名理论进行了系统地、深入地研究，对各种典型的盲签名方案及代理盲签名方案进行了分析及改进，并探讨了盲签名技术的广泛应用。在这期间的研究成果总结如下：

(1)对谭作文等人提出的代理盲签名方案进行了改进，基于Schnorr盲签名设计了一种代理盲签名方案，并对其进行了理论证明和试验分析。结果表明，该方案在满足了代理盲签名基本安全性要求的前提下，缩短了计算时间，提高了计算效率；

(2)对祁明提出的多重盲签名方案进行了分析，指出了方案中存在的不足，然后基于 ElGamal 强盲签名设计了一种多重盲签名方案，该方案可以实现多人同时对消息进行盲签名，并且在安全性上具有强盲性，即可以同时满足盲性和不可追踪性。

(3)本文基于盲签名技术提出了一种匿名电子投票协议，能够满足电子投票系统的基本安全性要求。然后基于该协议设计了一个匿名电子投票系统，对该系统进行了详细设计，并给出了部分算法的实现。

鉴于盲签名的发展趋势和重要性，本文综述了有关盲签名研究的若干结果并进行了相应的分析。国内外学者对其进行了深入的探讨与研究并取得了丰富的研究成果。作者认为以下问题值得进一步研究：

(1)目前很多盲签名方案还存在隐患，各种盲签名方案的安全性还有待进一步的检验；

(2)目前大部分盲签名方案的计算复杂度高，通信量大，计算效率低，因此如何设计简单有效的盲签名方案还有待进一步的研究；

(3)随着公钥基础设施（PKI）的出现，越来越多的电子商务方面的应用可以架构其上。因此，如何基于现有的基础公钥设施（PKI），利用盲签名技术构造各种安全高效的电子商务应用将是研究的热点。

经过一年多的学习和研究，本论文已经告一段落，本人深感在此领域的研究还不够深入，论文中一定会有许多不足之处，欢迎各位老师和同学批评指正，在以后的学习和工作中，我将继续密切关注这一领域的发展和动向，争取为这个领域的发展做出更大的贡献。

致 谢

本文是在导师赵泽茂副教授的悉心指导和热情关怀下完成的，导师为人正直的品质、严谨的治学态度、勤奋的工作态度和深厚的学术造诣令我敬佩至深。三年学习期间导师为作者提供了极好的学习和工作条件，认真耐心地解答了作者在工作学习中遇到的问题，值此论文完成之际，首先向导师表示衷心的感谢和深深的敬意。

感谢胡钢教授、王萍副教授、张金波副教授的帮助和指导，作者从中得到了很多有益的指导和启发。

感谢李文辉、谢大权、郭建甲、江金龙、陈佑健、张伯约、江富椿、周炳忠、卢家凰、李斌等 2002、2003、2004 级硕士在学习和生活上给予的帮助和支持。

特别感谢我的父母、家人，是他们多年来无私的奉献、鼓励和支持才能使作者顺利完成学业。

最后向所有帮助和鼓励过我的人表示最真诚的谢意！

作者：龚少麟

2005 年 6 月

参考文献

[1] 卢开澄. 计算机密码学（第二版）[M]. 北京：清华大学出版社, 1998.

[2] 赖溪松，韩亮，张真诚. 计算机密码学及其应用[M]. 北京：国防工业出版社, 2001.

[3] Oded Goldreich. 密码学基础[M]. 北京：人民邮电出版社, 2003.

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

[5] 卿斯汉. 密码学与计算机网络安全[M]. 北京：清华大学出版社, 2001.

[6] 杨义先，孙伟，钮心. 现代密码新理论[M]. 北京：科学出版社, 2002.

[7] Chaum. D. Blind signature for untraceable payments[C]. Proc. Crypto' 82. New York: Plenum Press, 1983:199-203.

[8] Chaum. D. Blind signatures system[C]. CRYPTO' 83. New York: Plenum Press, 1983:153-158.

[9] Solms S V, Naccache D. On blind signature and perfect crime[J]. Computer and Security, 1992, 11: 581 - 583.

[10] Stadler M A, Piveteau J M, Camenisch J L. A blind signatures scheme based on ElGamal signature[C]. EUROCRYPT' 95. 1995:209 - 219.

[11] Coron J S, Naccache D, Stern J P. On the security of RSA cryptosystem padding[C]. CRYPTO' 99. 1999:1 - 18.

[12] Fan C I, Chen W K, Yeh Y S. Randomization enhanced Chaum' s blind signature scheme[J]. Computer Communications, 2000, 23: 1677 - 1680.

[13] Chien H Y, Jan J K, and Tseng Y M. RSA-Based partially blind signature with low computation[C]. IEEE 8th International Conference on Parallel and Distributed Systems. Kyongju: Institute of Electrical and Electronics Engineers Computer Society, 2001: 385 - 389.

[14] Okamoto T. Provable secure and practical identification schemes and corresponding digital signature schemes[C]. CRYPTO' 92. 1992:31-52.

[15] Camenisch J, Piveteau J, Stadler M. Blind signatures based on discrete logarithm problem[C]. EUROCRYPT' 94. 1994: 428 - 432.

[16] Harn L. Cryptanalysis of the blind signatures based on the discrete logarithm problem[J]. IEE Electronic Letters, 1995, 31(14): 1136 - 1137.

[17] Mohammed E, Emarah A E, Shennawy K E. A blind signatures scheme based on ElGamal signature[C]. IEEE/AFCEA EUROCOMM 2000 Information Systems for Enhanced Public Safety and Security, 2000:51 - 53.

[18] Fan C I, Lei C L. Efficient blind signature scheme based on quadratic residues[J]. IEE Electronic Letters, 1996, 32(9): 811 - 813.

[19] Fan C I, Lei C L. Low-computation partially blind signatures for electronic cash[J]. IEICE Transactions on Fundamentals, 1998, 81(5): 818 - 824.

[20] Hwang M S, Lee C C, Lai Y C. Traceability on low-computation partially blind signatures for electronic cash[J]. IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, 2002, 85(5): 1181 - 1182.

[21] Fan C I, Lei C L. User efficient blind signatures[J]. IEE Electronics Letters, 1998, 34(6):544 - 546.

[22] Lysyanskays A, Ramzan Z. Group blind signatures: A scalable solution to electronic cash[C]. Financial Cryptography '98. Springer-Verlag, 1998:184-197.

[23] Lin W D, Jan J K. A security personal learning tools using a proxy blind signature scheme[C]. Proceedings of International Conference on Chinese Language Computing. USA, 2000:273-277.

[24] Tan Z, Liu Z, Tang C. Digital proxy blind signature schemes based on DLP and ECDLP[J]. MM Research Preprints, 2002, 21: 212-217.

[25] Lal S, Awasthi A K. Proxy blind signature scheme[EB/OL]. http://eprint.iacr.org/2003/072/. 2003.

[26] 祁明,史国庆.多重盲签名方案及其应用[J]. 计算机工程与应用,2001,37(3):91-92.

[27] 黄少寅,刘岩,高传善. 一种基于Schnorr体制的同时型多盲签名方案[J]. 计算机应用与软件,2002,19(11):27-28.

[28] 陈晋大，郑纪姣.用数字签名来保护网络通信安全[J].计算机应用研究,2000,17(9):43-44.

[29] 蒋艳凰.数字签名技术及其发展动态[J].计算机应用研究,2000,17(9):1-3.

[30] 祁明,林卓声. 若干盲签名方案及其在电了商务中的应用[J]. 计算机工程与设计, 2000,21(4):39-41,49.

[31] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation[C]. Proc.3rd ACM Conference on Computer and Communication Security, 1996:48-57.

[32] 姚亦峰，朱华飞，陈抗生. 基于二元仿射变换的广义 ElGamal 型盲签名方案[J]. 电子学报, 2000,28(7):128-129,134.

[33] Mambo M, Usuda K and Okamoto E. Proxy signatures: Delegation of the power to sign messages[J]. IEICE Trans. Fundamentals, 1996(9):1338-1354.

[34] Zhang K. Threshold Proxy signature schemes[C]. Japan: Information Security Workshop, 1997:191-197.

[35] A.Fujioka, T.Okatoma and K.Ohta. A Practical Secret Voting Scheme for Large Scale Elections[C]. Proceedings of Auscrypt92, 1992:244—256.

[36] K R Iverson. A Cryptographic Scheme for Computerized General Elections [C]. Proceedings of Crypto91, 1991:405-419.

[37] K Sako J Kilian. Secure Voting Using Partially Compatible homomorphism[C]. Proceedings of Crypto94, 1994:411-424.

[38] V Niemi, A Renvall. How to Prevent Buying of Votes in computer elections[C]. ASIACRYPT94, 1994:141-148.

[39] 汪保友,杨风,胡运发.基于盲签名的在线选举方案[J]. 小型微型计算机系统, 2003, 249(3):588—591.

[40] 陈晓峰,王育民.基于匿名通讯信道的安全电子投票方案[J]. 电子学报, 2003,31(3): 390-393.

[41] 周伯丹,张曙光,付志峰. 一个基于盲签名的电子选举方案[J].计算机工程与应用, 2003, 15(4):171-172.

附录 A 作者在攻读硕士学位期间发表的论文

[1] 龚少麟，赵泽茂. 一个新的代理盲签名方案，计算机工程与设计，已录用.

[2] 龚少麟，赵泽茂，周炳忠，卢家凰，李斌. RSA 盲签名在电子竞标系统中的应用，计算机应用研究，已录用.

[3] 赵泽茂，龚少麟. 盲签名理论研究进展，河海大学常州分校学报，2004, 18(4):1-5.

[4] 李斌，龚少麟，赵泽茂. 基于 Schnorr 体制的多重数字签名方案，河海大学常州分校学报，2005, 19(2):12-15.

[5] 李斌，赵泽茂，龚少麟. 一种新的有序多重数字签名方案，计算机工程与设计，已录用.

[6] 卢家凰，赵泽茂，龚少麟，周炳忠. 一种新型的基于 ID 的盲签名，计算机工程与设计，已录用.

盲签名理论研究及应用

作者：龚少麟
学位授予单位：河海大学
被引用次数：2次

参考文献(42条)

1. 参考文献

2. 卢开澄 计算机密码学 1998

3. 赖溪松.韩亮.张真诚 计算机密码学及其应用 2001

4. Oded Goldreich 密码学基础 2003

5. Wade Trappe.Lawrence C Washington.邹红霞 密码学概论 2004

6. 卿斯汉 密码学与计算机网络安全 2001

7. 杨义先.孙伟.钮心 现代密码新理论 2002

8. Chaum D Blind signature for untraceable payments 1983

9. Chaum D Blind signatures system 1983

10. Solms S V.Naccache D On blind signature and perfect crime 1992

11. Stadler M A.Piveteau J M.Camenisch J L A blind signatures scheme based on ElGamal signature 1995

12. Coron J S.Naccache D.Stern J P On the security of RSA cryptosystem padding 1999

13. Fan C I.Chen W K.Yeh Y S Randomization enhanced Chaum' s blind signature scheme 2000

14. Chien H Y.Jan J K.Tseng Y M RSA-Based partially blind signature with low computation 2001

15. Okamoto T Provable secure and practical identification schemes and corresponding digital signature schemes 1992

16. Camenisch J.Piveteau J.Stadler M Blind signatures based on discrete logarithm problem 1994

17. Harn L Cryptanalysis of the blind signatures based on the discrete logarithm problem 1995(14)

18. Mohammed E.Emarah A E.Shennawy K E A blind signatures scheme based on ElGamal signature 2000

19. Fan C I.Lei C L Efficient blind signature scheme based on quadratic residues 1996(09)

20. Fan C I.Lei C L Low-computation partially blind signatures for electronic cash 1998(05)

21. Hwang M S.Lee C C.Lai Y C Traceability on low-computation partially blind signatures for electronic cash 2002(05)

22. FanC I.Lei CL User efficient blind signatures 1998(06)

23. Lysyanskays A.Ramzan Z Group blind signatures:A scalable solution to electronic cash 1998

24. Lin W D.Jan J K A security personal learning tools using a proxy blind signature scheme 2000

25. Tan Z.Liu Z.Tang C Digital proxy blind signature schemes based on DLP and ECDLP 2002

26. Lal S.Awasthi A K Proxy blind signature scheme 2003

27. 祁明.史国庆 多重盲签名方案及其应用[期刊论文]-计算机工程与应用 2001(3)

28. 黄少寅.刘岩.高传善 一种基于Schnorr体制的同时型多盲签名方案[期刊论文]-计算机应用与软件 2002(11)

29. 陈晋大.郑纪蛟 用数字签名来保护网络通信安全[期刊论文]-计算机应用研究 2000(9)

30. 蒋艳凰.白晓敏.杨学军 数字签名技术及其发展动态[期刊论文]-计算机应用研究 2000(9)

31. 祁明.林卓声 若干盲签名方案及其在电子商务中的应用[期刊论文]-计算机工程与设计 2000(4)

32. Mambo M.Usuda K.Okamoto E Proxy signatures for delegating signing operation 1996

33. 姚亦峰.朱华飞.陈抗生 基于二元仿射变换的广义ELGamal型盲签名方案[期刊论文]-电子学报 2000(7)

34. Mambo M.Usuda K.Okamoto E Proxy signatures:Delegation of the power to sign messages 1996(09)

35. Zhang K Threshold Proxy signature schemes 1997

36. A Fujioka.T Okatoma.K Ohta A Practical Secret Voting Scheme for Large Scale Elections 1992

37. K R Iverson A Cryptographic Scheme for Computerized General Elections 1991

38. K Sako J Kilian Secure Voting Using Partially Compatible homomorphism 1994

39. V Niemi.A Renvall Howto Prevent Buying of Votes in computer elections 1994

40. 汪保友.杨凤.胡运发 基于盲签名的在线选举方案[期刊论文]-小型微型计算机系统 2003(3)

41. 陈晓峰.王育民 基于匿名通讯信道的安全电子投票方案[期刊论文]-电子学报 2003(3)

42. 周怡丹.张曙光.付志峰 一个基于盲签名的电子选举方案[期刊论文]-计算机工程与应用 2003(15)

本文读者也读过(10条)

1. 徐光宝 盲签名方案及其应用研究[学位论文]2005

2. 陈华 盲签名理论研究与设计[学位论文]2007

3. 刘敏 代理盲签名分析及一种改进[学位论文]2008

4. 付春宝 盲签名理论研究及其应用[学位论文]2007

5. 吴勇 盲签名研究及其在电子选举中的应用[学位论文]2006

6. 程征 盲签名方案研究及其应用[学位论文]2008

7. 李方伟.谭利平.邱成刚.LI Fang-wei.TAN Li-ping.QIU Cheng-gang 基于离散对数的代理盲签名[期刊论文]-电子科技大学学报2008,37(2)

8. 许静 盲签名技术在电子商务中的研究与应用[学位论文]2007

9. 李云龙 盲签名的理论研究与应用[学位论文]2008

10. 王静然 盲签名的研究与应用[学位论文]2009

引证文献(2条)

1. 陈明.葛永亮 浅谈盲签名[期刊论文]-科技信息（科学·教研） 2007(31)

2. 柳菊霞 强代理签名的研究与应用[学位论文]硕士 2006