摘　要

随着计算机网络技术的发展，信息安全问题日益突出，其核心技术基础之一的数字签名技术，被广泛地应用于军事、通信、电子商务和电子政务等领域，它在身份认证、数据完整性和抗否认等方面具有其它技术无法替代的作用，而且随着电子签名法的实施，这种应用将变得更加普遍。

本文比较系统地对数字签名理论、方法和应用进行了研究，重点研究了数字签名中的若干关键技术问题。

根据各种不同的签名方程的构造特点，比较完整地探讨了签名方案的构造及其参数选取的方法。包括：1）给出了 ElGamal 型数字签名方程参数选取的一般方法，推广了选择签名的方法和范围。2）提出了一种基于椭圆曲线的具有消息恢复的认证加密方案，并指出在单向函数为同态函数的情况下存在两种已知明文的伪造攻击，从而说明选取符合一定条件的签名方案可以有效地避免这样的攻击；结合消息链接恢复特性，提出了相应的认证加密方案，该方案较好地解决了消息加密认证、消息链接恢复及传输量较大等问题。3）提出了一种基于椭圆曲线的具有消息恢复的签名方案及其参数选取方法。

对于盲签名，考虑到信息拥有者是否被签名人追踪的问题，提出了广义弱盲签名方案的构造方法，该方案几乎包含了目前所有该类签名。结合代理签名和盲签名的特点，利用多元线性变换来刻画用户与代理签名人之间变量的传递关系，从而提出了一种基于椭圆曲线的代理盲签名方案。

利用椭圆曲线上的 Weil 配对的双线性性质，提出了基于 ID 的盲签名方案，该方案以 ID 为基础的公钥代替以数字证书为基础的公钥，节约了验证签名时的时间开销，减少了交互的次数并节省了存储空间。

基于公钥自证明的思想，提出了一种具有消息恢复的自认证加密方案。该方案实现了通信双方对彼此公钥的自证明和信息接收者可以从签名中恢复消息等功能，且具有第三层次的信任等级、较少的计算时间开销和较高的安全性等优点。

基于盲签名技术提出了一种匿名电子投票协议，该协议除满足电子投票的基本性质外，较好地解决了选票碰撞以及投票者的中途退出等问题，而且还可以有效地防止一人多票或一票多投现象的发生，即使管理机构和计票机构勾结，在计票前可同时保证选票的秘密性和公平性。还从实用的角度对电子投票系统原型进行了研究，对电子投票系统进行了设计，编程实现了其中的核心算法及部分功能。

关键词：数字签名　盲签名　消息恢复　椭圆曲线　电子投票

Abstract

The information security has become more and more crucial with the development of computer and network technologies. The digital signature is one of key techniques in information security, especially in the authentication, data integrity, and non-repudiation. It has been widely used in military, communication, e-commerce and e-government, etc., and will become more and more popular after the e-signature law is put in practice.

The main interest of this dissertation is on the theory and method of digital signature and its application. The research focuses on some key problems of digital signature.

Based on the characteristics of various signing equation, problems such as constructing signature scheme and chooing parameter of signing equation are fully investigated in this dissertation. Some significant results are obtained, including:1)a method of choosing the parmeters of signing equation to generate ElGamal signing equation, this method extends the available range of choosing signature. 2)a new elliptic curve authenticated encryption scheme with message recovery. It is pointed out that there are two forgery attacks with known plaintext under the one-way function is homostasis function, all of these indicate some signature schemes satisfying certain conditions can avoid the forgery attack. 3)a new elliptic curve authenticated encryption scheme with message linkage recovery, which solves the problems such as message encryption and authentication, message linkage recovery and load of transmitting data.4)an elliptic curve signature scheme with message recovery, and the generalized forms of constructing signing eqauation and methods of choosing parameteres of signing equation.

With the consideration of whether the owner of message is persuing by signer in blind signature, this dissertation proposes a method to generate ElGamal weakly-blind signature scheme, which contains almost all of the known type of weakly-blind signature scheme. Using multi-linear transform formula to describe the relationships among the variables held by user and proxy signer, this dissertation proposes a proxy blind signature based on elliptic curve cryptosystem.

Using the bilinear theory of Weil pairing defined on elliptic curve, a new ID-based blind signature scheme is proposed. In this scheme, ID-based public key is not the public key stored in certificate. This scheme can omit the process of getting public key from the system in verification phase, therefore decrease interaction time and reduce the store space.

Based on self-certificated public key, an authenticated encryption scheme with message recovery is proposed. In this scheme, both sides of communication can self verify

public key of opposite side, message receiver can recover the original message from the signature. The proposed scheme is in the credit of third level, and has less load in computational time and better security

In this dissertation, an anonymous e-voting protocol is proposed. In addition to the essential properties of e-voting, this protocol also satisfies some other properties such as vote collision and exit of voter, furthermore, it can effectively prevent more votes by one voter or more times voting by only one vote. When the manager colludes the counter of vote or they collude each other, this protocol can ensure the confidentiality of vote and justice. In order to develop a practical e-voting information system, this dissertation discusses the design of system and fulfills the main algorithms and partial functions of system.

Keywords: digital signature blind signature message recovery elliptic curve e-vote.

图表清单

声　明

本学位论文是我在导师的指导下取得的研究成果，尽我所知，在本学位论文中，除了加以标注和致谢的部分外，不包含其他人已经发表或公布过的研究成果，也不包含我为获得任何教育机构的学位或学历而使用过的材料。与我一同工作的同事对本学位论文做出的贡献均已在论文中作了明确的说明。

研究生签名：_____　　年　月　日

学位论文使用授权声明

南京理工大学有权保存本学位论文的电子和纸质文档，可以借阅或上网公布本学位论文的全部或部分内容，可以向有关部门或机构送交并授权其保存、借阅或上网公布本学位论文的全部或部分内容。对于保密论文，按保密的有关规定和程序处理。

研究生签名：_____　　年　月　日

1 绪论

1.1 研究问题的背景与意义

计算机网络的产生把我们带进一个信息化社会，在信息社会里，计算机网络已成为现代社会赖以生存的物质基础，大量传输和存储的信息的安全保密和防伪问题成为人们关注的一个重要课题。在当前，计算机网络的安全问题日益突出，有关网络安全威胁的事件频频在电视和网络等媒体报道，网络安全的形势不容乐观，已严重地威胁到人们正常的生活，甚至威胁到国家安全。

网络安全的实质是信息安全，信息安全的核心技术之一是密码技术。普遍认为现代密码是解决信息安全的最有效的方法，因此，密码学的研究成为当前国际上的一个研究热点。

1.1.1 信息安全的重要性

由于计算机网络技术的迅速发展，尤其是 Internet 的发展和广泛普及，如电子商务、电子政务、银行金融网络、网络游戏、聊天室和各类订票系统等等，这些应用已完全渗透到我们的日常生活之中，毫无疑问为生产力的发展起到了极大的推动作用。因此，网络技术及各种信息技术的应用将对社会生活产生革命性的影响，有人把因特网看作是信息革命的象征，并认为因特网不仅给我们的生活带来便利，更重要的是它将对传统产业和观念带来新的冲击，影响传统产业的运行模式和发展方向。

在信息技术的应用过程中，信息是最为宝贵的资源，因特网为信息的传播和获取提供了极大的便利，它可以使我们不受时间和空间的限制，和世界上任何一个角落的个人或组织进行信息交流，而且每天发生的各种政治事件较以往任何时候能以最快的速度、在最短的时间内向全世界传播，各种经济信息更是充斥网络让人应接不暇。

所谓信息安全，是指信息的五要素，即信息的保密性(Confidentiality)、完整性(Integrity)、可用性(Availability)、可控性(Controllability)与可审查性。保密性就是对抗对手的被动攻击，保证信息不泄漏给未经授权的人。完整性就是对抗对手主动攻击，防止信息被未经授权的篡改。可用性就是保证信息及信息系统确实为授权使用者所用。可控性就是对信息及信息系统实施安全监控。可审查性是指对出现的网络安全问题提供调查的依据和手段。

事物是一分为二的，网络也不例外。在网络给我们带来巨大的经济利益和便利的

同时，遍布全球的黑客，利用网络和系统漏洞，肆意攻击各种业务应用系统和网站，造成巨大的经济损失，搅得全球不安。机密信息在网络上被泄露、篡改和假冒，计算机病毒和垃圾邮件肆意传播，不良信息传播给青少年的成长带来负面影响，计算机犯罪呈上升趋势。网络信息安全问题不仅仅是一个技术问题，而且严重威胁到我国政治、军事、经济、文化等各方面的安全，还将使国家处于信息战和经济金融风险的威胁之中，网络信息安全已成为亟待解决的影响国家全局和长远利益的关键问题之一。

1.1.2 密码理论在信息安全中的重要作用

信息安全是一门涉及计算机技术、网络技术、信息论、密码学、应用数学、通信技术、法律和管理技术等众多学科交叉和融合的综合性学科。

密码学(Cryptology)是信息安全的基础之一。它包括两个分支：密码编码学(Cryptography)和密码分析学(Cryptanalysis)。密码编码学是对信息进行编码实现信息隐藏的一门学科，主要研究实现信息保密和认证的方法与技术。密码分析学是研究如何破译密码的一门学科，主要目的是研究密文的破译和消息的伪造。

历史上，密码学主要研究加密机制的设计和分析，为信息隐藏和保密通信提供方法和手段。中国古代秘密通信的手段是将信息隐藏在文本中，据《武经总要》记载，北宋前期，在作战中曾用一首五言诗的 40 个汉字，分别代表 40 种情况或要求。1871 年，由上海大北水线电报公司选用 6899 个汉字，代以四码数字，成为中国最早的商用明码本，同时设计了由明码本改编为密本及进行加乱码的方法，在此基础上逐步发展为各种比较复杂的密码。

在欧洲，公元前 405 年，斯巴达的将领来山得使用了原始的错乱密码；公元前一世纪，古罗马皇帝凯撒曾使用有序的单表代替密码；之后逐步发展为密本、多表代替等多种密码体制。

在公钥密码出现以前所用的密码体制的安全性都基于私钥和加密方法的保密，也就是说算法是不公开的。由于这种密码体制的代价昂贵，因此密码学主要应用于军事、政府和外交等机要部门。当时密码学几乎是国家安全机制独占的领域。

在传统密码中，用于加密的密钥和用于解密的密钥是相同的，因此通常使用的加密算法比较简单、高效，密钥简短，安全性高。但是，传送和保管密钥是一个严峻的问题。

1976 年，Diffie[1]发表了著名的论文《密码学的新方向》，提出了公钥密码体制的新思想，证明了在发方和收方之间不需要传递密钥的保密通信是可能的，它使密码学发生了一场变革，具有与传统密码不可取代的优势。

为了适应计算机通信和电子商务迅速发展的需要，密码学的研究领域逐步从消息

加密扩散到数字签名、消息认证、身份识别、防不可否认协议等新的课题。同时密码学不在局限于军事、政治和外交，而扩大到商务、金融和社会各个领域，特别是全球范围内的互联网的出现和发展，为人们提供了快速、高效和廉价的通信，大量敏感信息常常要通过互联网进行交换。由于互联网的开放性，任何人都可以接入互联网，使得有些人就有可能采用各种非法手段窃取、假冒、欺骗、篡改和破坏各种重要信息，甚至进行计算机犯罪。网络信息安全问题成为当前比较突出又急待解决的问题。

事实上，现在网络上应用的保护信息安全的技术，如数据加密技术、数字签名技术、消息认证与身份识别技术、防火墙技术以及反病毒技术等都是基于密码学来设计的，可以说密码学是信息安全技术的基础。由此可见，现代密码学的应用非常广泛。在任何企业、单位和个人都可以应用密码技术来保护自己的信息。由于在当今高度信息化的社会里，信息安全关系到国家全局和长远利益，各国政府都十分重视密码学的研究和应用。

美国国家标准局首先制定并于1977年向全世界公布了美国数据加密标准(DES)。1994 年又公布了美国国家标准技术研究所（NIST）提出的一个数字签名标准。1997年，美国国家标准技术研究所又在全世界公开征集高级加密标准（AES）活动，通过公布 15 个候选加密方案进行公开的评论和专家讨论，最后从中选出了一个方案作为AES。AES 将成为新的美国数据加密标准和一个供全球免费使用的数据加密标准。

最近欧洲委员会的信息社会技术（IST）规划中出资 33 亿欧元支持一项新的欧洲数字签名、信息完整性和加密方案（NESSIE）工程，目标是推出一套密码标准，包括分组密码、流密码、杂凑函数、消息认证码、数字签名和公钥密码等。所有这些密码标准的研究和公布，将极大为信息安全提供强大的理论基础和技术支持。

1.1.3 数字签名技术在网络通信中的重要作用

一般的书信或者重要文件（如签订合同、遗嘱、收养关系、夫妻财产关系等）是根据亲笔签名或印章来证明其真实性的。一些重要的证件，如护照、身份证、驾照、毕业证和技术等级证书等是通过权威部门颁发的。通常采用的防伪方法是：特殊材料制作或信息隐藏等。

在网络环境中，需要存储、传输大量信息。信息的接受方可以伪造一份报文，并声称是由发送方发送过来的，从而获得非法利益。比如，银行通过网络传送一张电子支票，接收方就可能改动支票的金额，并声称是银行发送过来的。同样地，信息的发送方也可以否认发送过报文，从而获得非法利益。比如，客户给委托人发送一份进行某项股票交易的报文，结果这项股票交易亏损了，客户为了逃避损失否认发送交易的报文。因此，需要新的信息安全技术来保证传输信息的真实性、解决通信双方的争端，

这种技术就是数字签名技术。

当通信双方发生了下列情况时，数字签名技术能够解决引发的争端。

●否认，发送方不承认自己发送过某一报文。

●伪造，接收方自己伪造一份报文，并声称它来自发送方。

●冒充，网络上的某个用户冒充另一个用户接收或发送报文。

●篡改，接收方对收到的信息进行篡改。

所谓数字签名就是由信息的发送者通过一个单向函数对要传送的报文进行处理产生别人无法伪造的一段数字串。这个数字串用以认证报文的来源并核实报文是否发生了变化。一般情况下，发送者用自己的私有密钥加密数据传给接收者，接收者用发送者的公钥解开数据后，就可确定消息来源，同时也是对发送者发送的信息的真实性的一个证明，发送者不能抵赖。

在传统的商业系统中，书面文件的亲笔签名或印章是用来规定契约性的责任的。签名或印章起到认证、核准、生效的作用。同样地，在电子商务活动中，传送的文件是通过数字签名来证明当事人身份与数据真实性的。数据加密是保护数据的最基本方法，但也只能防止第三者获得真实数据，它不能保证通信双方的相互欺骗。数字签名则可以解决否认、伪造、篡改及冒充等问题。使用数字签名技术使得：发送者事后不能否认发送的报文签名、接收者能够核实发送者发送的报文签名、接收者不能伪造发送者的报文签名、接收者不能对发送者的报文进行篡改、网络中的某一用户不能冒充另一用户。

数字签名技术的研究与使用，拓宽了密码学的研究范围和领域，在网络通信身份认证中占有独特的地位。

1.2 数字签名理论与应用研究现状

20 世纪 70 年代，公钥密码体制[1]的诞生是现代密码学形成的一个重要标志。不久，基于公钥密码体制的数字签名技术也随之产生[2]。1991 年 8 月美国国家标准局国家标准技术学会(National Institute of Standard and Technology，NIST)公布了数字签名标准(Digital Signature Standard，DSS)，此标准采用的算法称为 DSA。自数字签名概念提出之后，人们做了大量的研究工作，并取得了丰硕的成果[3~5]。

数字签名方案主要是基于公钥密码体制，实现公钥密码体制思想的主要方法是基于如下几个不同的数学难题[4]：

离散对数难题：这类应用特别广泛，现在的大部分方案如 ElGamal 型签名方案（1985 年）、广义 ElGamal 型签名方案（1994 年）、Schnorr 签名方案、DSA 方案、Neberg-Rueppel 签名方案、Okamoto 签名方案、Miyaji 签名方案、HMP 认证加密方案

和许多协议等都是基于这个问题进行设计的。

大素数因子分解难题：最著名的算法是 RSA（1978 年），还有 Rabin 签名方案、Fiat-Shamir 签名方案和 Guillou-Quisquater 签名方案等。

离散对数和素因子分解相结合难题：Harn 签名方案（1994）、Lai-Kuo 签名方案（1997）、He-Kieslolor 签名方案、Shao 签名方案和 Li 签名方案等。

二次剩余难题：Rabin 密码体制、Rabin 签名方案、He-W 签名方案和广义 Shimada 签名方案。

椭圆曲线离散对数问题：以椭圆曲线上的点构成的 Abel 群为背景结构构造公钥密码体制。自 80 年代中期引入这个概念以来，受到了密码学界的广泛关注和研究，取得了大量的成果.已成为密码学的重要的一个分支。

对于普通数字签名而言，解决的最基本问题是通过数字方式实现了通信双方的身份认证、通信的消息源真实性认证和消息的完整性认证等。由于各种不同的应用背景需要，人们基于不同的目的，研究了具有特殊用途的数字签名，对这些特殊的数字签名很难全面对其进行分类，因此大致可以分为如下几种特殊的数字签名[6]。

多重签名方案：一般的数字签名是由单个用户完成的，而由多人参与对同一文件进行签名的签名方案，称为多重签名方案（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）。多重签名方案的研究见参考文献[7~11]。

代理签名：Mambo[12]和 Kim[13]等人介绍了代理签名的概念。代理签名实现的功能是原始签名人把他的签名权授权给代理人，由代理人代表他对任何消息进行签名，消息接收者或签名验证者可以区分是普通签名还是代理签名。在 2000 年，Lee 和 Chang[14]提出了保护代理的代理签名方案。2003 年，吴克力[15~16]提出了签名接收方可查的时控代理签名方案和基于因子分解表述难题的代理签名方案，之后又于 2004 年提出了签名次数受限的代理签名方案[17]。代理签名与多重签名方案结合派生出代理多重签名[18~20]，它也是与其它签名技术结合较多的一种签名形式。

群签名方案[21]：1991 年,Chaum 和 Heyst 首先提出群签名（Group Signature）的概念,该方案允许合法用户以用户组的名义签名，即代表群体执行签名，验证者从签名不能判定签名者的真实身份，但能通过群管理员查出真实签名者。具有签名者匿名、只有权威才能辨认签名者等多种特点，在实际应用中有广泛应用。群签名研究重点在群公钥的更新、签名长度固定和群成员加入与撤消上[22~29]。最近，一种新的动态群签名模型由文献[30]给出。由于群签名方案中，群管理员具有特殊的身份，可以对群成员的签名进行跟踪，因此严格地说，不具有完全匿名性，在需要完全匿名性要求的情况下，无法满足。于是环签名[31]这一概念应运而生，它与群签名较为相似，最大的特

点是对签名者的身份是不可跟踪的，具有完全匿名性。自 2001 年提出这一签名后，渐渐成为研究的热点[32,33]。

盲签名方案：盲签名是一种特殊的数字签名，它与通常的数字签名的不同之处在于，签名者并不知道他所要签发文件的具体内容。正是这一特点，使得盲签名这种技术可广泛应用于许多领域，如电子投票系统和电子现金系统等。1982 年，D.Chaum[34]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）问题等相继提出各种盲签名方案。1983 年，Chaum[35]基于 RSA 公钥密码系统提出了第一种基于因子分解问题的盲签名方案,该方案可用于电子支付系统。Stadlerd 等[36]建议在匿名支付系统中应该建立一个可信的第三方。1992 年，Okamoto[37]基于 Schnorr 签名体制提出了一种基于离散对数问题的盲签名方案。1994 年，Camenisch 等[38]基于离散对数问题提出了两种盲签名方案。第一种方案来源于 DSA 的变形，第二种方案是以 Nyberg-Rueppel 签名体制为基础的。2000 年，姚亦峰等[39]提出了利用二元仿射变换，以 Harn 和 Xu 提出的 18 种安全广义 ElGamal 型数字签名方案为基础构造出 18 种相应的盲签名方案，进一步分析得到其中 12 种方案是强盲签名方案。Fan 等[40]于 1996 年提出一种盲签名方案，该方案的安全性是基于二次剩余方根的难解性。1998 年，Fan 等[41]提出一种盲签名方案以增强方案的计算效率。2000 年，Fan 等[42]又提出了一种盲签名方案以增强 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。在 2000 年，Lin 和 Jan[43]第一个提出了代理盲签名方案，Tan 等[44]人提出了一种基于 Schnorr 盲签名的代理盲签名方案，这种方案既具有盲签名的性质又具有代理签名的性质。Lai 和 Awasthi[45]于 2003 年提出了一种代理盲签名方案，该方案比 Tan 的方案的计算简单些。吴克力[46]于 2004 年提出了一种公平的群盲签名方案，该方案结合已有的公平盲签名和群签名思想，对一种群盲签名增添公平性而得到。

1998 年，Fan 等[47]提出一种部分盲签名方案，该方案能减少电子现金系统的计算量和数据库的大小。2001 年，Chien 等[48]基于 RSA 公钥密码系统提出一种部分盲签名方案，该方案可以减少数据库的大小以及避免电子现金的重复花费。2004 年，关于部分盲签名的最新研究见文献[49~51]。

自证明认证加密方案：Girault[52]于 1991 年首次介绍了基于公钥的自证明机制的思想,CA 不需要知道用户的私钥，公钥的产生是由用户和 CA 共同完成的,验证者可以验证公钥的真伪，相比基于 ID 的密码体制而言,自证明机制具有节省存储空间、用户自选私钥及 CA 不能冒充用户等优点,具有更高的安全性。Petersen 和 Horster[53]扩充了自证明机制的概念,提出了若干在不同可信等级下的具有自证明机制的公钥分发协议并将这些方法应用于授权签名、电子投票及会话密钥交换等领域。Chang Yuh-Shihng[54]等提出了 ElGamal 型自证明签名方案及群签名方案,这个方案从自证明机制简单地平

移到 ElGamal 型签名方案中来.Tseng Yuh-Min[55]等提出了具有消息恢复的基于自证明机制的签名方案及两个变形方案。其它关于自证明公钥认证的研究见文献[58~59]。

具有消息恢复的签名方案：这种类型的签名方案最早是由 Nyberg 和 Rueppel[65]在 1994 年首先提出的，其特点是消息可以从签名中被恢复出来。在 1996 年，文献[67]给出了所有基于离散对数问题的签名方案如何具有消息恢复功能的修正办法。IEEE 已将具有消息恢复的签名方案列为一个标准。围绕这个问题，Hwang[68]于 1996 年提出了一个基于 HMP 方案的具有消息链接功能的加密认证方案。在该方案中签名者把前一个消息块的信息加入到后一个消息块的签名中,从而使得消息链接的顺序被建立起来了。Lee 和 Chang[69]于 1997 年提出了一个基于 Lee-Chang 方案[70]的具有消息链接功能的方案,该方案比 Hwang 的方案具有较小的通信量且计算复杂性低。最近，Tseng 和 Jan[71]于 2002 年提出了一种基于 HMP 方案的具有消息链接功能和较低通信量的有效的认证加密方案。关于 ElGamal 型签名方案及其具有消息恢复的签名方案的研究见文献[72~75]。

此外，还有签名加密、门限共享、失败一停止签名、不可否认签名、零知识证明等其它不同形式的数字签名，吸引了学者们的广泛关注和研究，取得了大量的研究成果。

近年来，利用双线性配对技术来构造各种不同形式的数字签名方案，成为数字签名领域又一研究热点，它是利用超奇异椭圆曲线中 Weil 和 Tate 配对所具有的双线性性质，构造各种数字签名方案[60~61,76~78]。

在基础理论研究的同时，数字签名技术的应用研究也引起了学术界尤其是密码学界和计算机网络界的广泛重视。特别是随着电子通信和计算网络的应用，作为数据安全技术之一的数字签名技术的地位和作用，越来越显示出其优越性。

ISO(International Standardization Organization 国际标准化组织)于1984年9月专门为此立项，负责制定该标准。这表明了ISO对数字签名的重视。数字签名分为三类:带印章的数字签名、带影子的数字签名和使用Hash函数的数字签名;1988年5月提出了“数据加密技术:使用Hash函数的数字签名”的建议草案，即DP9796;1989年10月该草案提升为DIS9796。与此同时，各国的标准化组织对数字签名的标准化工作也紧锣密鼓地进行，尤其是美国，NIST在1991年推出了美国数字签名算法标准— DSA/DSS数字签名算法。2000年6月中旬，数字签名法案在美国众议院和参议院以压倒多数的赞成获得通过。6月30日，美国总统克林顿在费城以他爱犬的名字作为口令，用一张智能卡签署了数字签名法案。

2004年 8 月，我国正式颁布了《中华人民共和国电子签名法》，用于规范电子签名行为，确立电子签名的法律效力和地位。这部法律将为数字签名的应用和推广提供了最有力的保障和支持。

目前，数字签名技术已应用于商业、金融、军事等领域，特别是电子邮件(E-mail)、电子资金转账(EFT)、电子数据交换(EDI)、软件分发数据存储和数据完整性检验的应用，更使人们看到了数字签名的重要性。

最近，中科院研究生院信息安全国家重点实验室完成了“椭圆曲线公钥密码方案的设计与安全性分析”和“高安全弹性 CA 系统技术”两个国家“863 计划”课题。“椭圆曲线公钥密码方案的设计与安全性分析”研究了基于 Tate 配对的椭圆曲线系统的理论、椭圆曲线快速算法，实现了具有自主产权的 Tate 配对快速计算的软件系统，取得了创新性的理论成果。“高安全弹性 CA 系统技术”构建了具有自主知识产权的高安全弹性 CA 系统，设计了独有的双层秘密分享的入侵容忍方案，系统在安全性、可管理性、可扩充性和容错等方面具有创新。

2000 年 11 月 10 日，国家计委下达了由公安部主持开展的《计算机信息系统安全保护等级评估认证体系及互联网络电子身份认证管理与安全保护平台试点》项目建设的任务（简称“1110 工程”），“1110 工程”总投资 12975 万元。其中的两个子工程与数字签名技术密切相关，它们是“南海市网络电子身份认证示范工程”（电子政务环境下的身份认证）和“郑州粮食交易市场网络电子身份认证示范工程”（电子商务环境下的身份认证）。南海市网络电子身份认证示范工程是以中国电子政务应用示范工程和其它应用为背景，初步建设一个为电子政务、电子商务以及其它国民经济信息化应用提供自然人身份认证基础支持平台，并为社会信息化管理及公安机关打击网络犯罪提供基本技术支撑。目前工程正按预定计划稳步推进。郑州互联网电子身份认证示范工程以郑州粮食批发市场网上粮食交易业务为依托，建立网上身份认证系统，确保网上交易安全，探讨公安对重大网络交易的监管模式，并通过在粮食行业示范扩大影响，为将来全面推广电子身份认证积累经验。目前已完成了身份认证系统建设和安全保障系统（一期）建设，并通过了用户的验收。

广东省电子商务认证中心（网址：www.cnca.net）是经广东省人民政府批准成立的专业认证机构（CA:Certification Authority），创立于 1998 年，是中国成立最早的数字证书认证机构之一。该中心作为国家电子商务试点工程、广东省政府认可的认证机构、广东省"十五"规划重点建设项目，一直致力于推动数字证书认证事业的发展，成为数字证书认证技术与业务的领航者。该中心作为权威的认证机构，已签发超过 15 万张数字证书，建立了完善的数字证书登记、审批、发放、废止、查询、管理等运作规范，解决网上身份认证、密钥管理和信息安全等一系列问题。同时积极研发相关产品，提供信息安全整体解决方案及顾问咨询服务，以推动数字证书应用。目前该中心的数字证书及相关应用方案被广泛应用于网上报关、网上报税、网上报检、网上办公、网上招投标、网上采购、数字工商等大型电子政务和电子商务工程。

到目前为止，全国各省市几乎都建立了自己的 CA 认证中心，而且电子签名法的

培训工作正在抓紧地进行着，这些工作的开展将对电子商务、电子政务的推广和普及起到积极的作用。

每年在国际上召开的密码学学术会议和一些国际权威杂志（如 Proceedings of Crypto, Journal of Cryptology, Proceedings of IEEE International Conference on Advanced Information Networking and Applications, IEEE Journal of Transactions on Information Theory, Communications of the ACM 等）上都有大量的数字签名方面的学术论文发表。

中国科学院软件研究所信息安全国家重点实验室和中国科学院研究生院信息安全国家重点实验室是我国研究信息安全基础理论和应用系统的两个重要实验室，此外，西安电子科技大学综合业务国家重点实验室、北京邮电大学信息安全中心、山东大学网络信息安全研究所、上海交通大学、武汉大学和南京理工大学等高等院校都有相当的队伍在从事数字签名技术的研究。

1.3 选题的依据

随着各国电子签名相关法律的建立，电子签名将与手写签名或者盖章具有同等的法律效力。这为基于计算机网络技术的电子商务、电子政务等各种应用奠定法律基础和保障。我国将在国家计委项目—网络身份认证管理示范工程的基础上，逐步开展以公安户政信息和特征识别码为支持平台的网络身份管理工作，为电子签名法的实施提供技术上的保障。

从上一小节数字签名的研究现状就可以看出，在数字签名理论方面存在许多问题需要解决，而且这些问题的解决有助于为数字签名技术的应用打下坚实的基础。任何理论发展与技术的进步都是相对的，数字签名技术也不例外，一些原本认为是安全的方法和技术，随着时间的推移和技术的进步也逐渐暴露出其缺陷。例如，美国朗讯科技公司的贝尔实验室信息科学研究中心的 Daniel Bleichenbacher 研究员于 2000 年 2 月 5 日宣布在著名的数字签名算法 DSA 的随机数生成技术存在着重大缺陷。因为密钥的有效性依赖于数字产生的随机度，但 DSA 的随机数产生方法上存在偏重某些数字的现象。在概率上，从某个特定范围的数字中选择随机数的概率是从其它范围的数字中选择的 2 倍。正是这种偏重性大大减弱了 DSA 的安全性能，从而会加大整个系统的脆弱性。不过以目前性能还不足够发达的计算机而言，该缺陷还不至于立即构成威胁。但在不久的将来，因特网和企业/政府的内部网络业务的完整性就会面临危险。VPN(虚拟个人网络)、在线购物和金融交易等都有可能受到影响。

在最近的国际密码学会议（Crypto2004）上，研究人员宣布，他们发现了破解数种 Hash 算法的方法，其中包括 MD4、MD5、HAVAL-128、RIPEMD 以及 SHA-0，这些都是在数字签名中常用到的算法。分析表明，SHA-1 的减弱条件的变种算法可能

被破解，但完整的 SHA-1 并没有被破解，也没有找到 SHA-1 的碰撞。研究结果说明，SHA-1 的安全性暂时没有问题，但随着技术的进步，也面临着危险。

2004 年月 12 月(ASI2004,City Universtiy of HK,Dept.11~16),著名密码学家 Shamir 宣布 RAS 算法的安全性基础－大素数因子分解难题，将受到高速计算机的挑战，预测在未来 20 年内，其安全性将不复存在。

在军事上，敌我双方交战，不可避免地要打一场信息战，南联盟战争、海湾战争就是典型例证。这种新型作战模式决定胜负的因素不再仅仅是炸药、飞机和大炮，而是取决于双方掌握信息技术的攻击能力和防御能力等。这些都主要取决于计算机硬件、软件、网络通信技术的发展水平。数字签名技术由于其能有效地防止信息的伪造、确定信息的来源和判断信息是否完整等能力，使其在信息战中有着极其重要的作用。本论文研究内容是受国防科工委国防基础研究项目“信息安全与对抗技术研究－基于四层结构的战场信息安全性关键技术研究”（项目编号：J1300D004）资助，数字签名技术是其中关键技术之一。

1.4 本文的研究内容

本文主要围绕下面几个方面的问题来展开研究的：

1．在 ElGamal 数字签名方案中，通过参数选取的变化可以得到不同形式的签名方案，问题是：参数选取的原则是什么？有什么限制没有？在什么情况下选取需要的不同的参数？这些问题都需要回答。因此本文研究了签名方程的一般形式问题，在所有要考察的数字签名方案、具有消息恢复的签名方案、认证加密方案以及基于椭圆曲线密码体制的签名方案均对签名方程的一般形式做了推广和讨论。

2．研究了具有消息恢复的签名方案设计的特点和方法技巧，分析具有消息恢复签名方案的安全性特点，从而可以对具有消息恢复的数字签名进行推广和拓展。同时，在椭圆曲线密码体制中,相关问题虽然与基于离散对数难题处理的方法类似,但又不完全等同,因此需要对这些问题进行深入的研究并要做技术上的处理才能得到相应的结果。

3．分类总结盲签名方案的类型、满足的性质，包括各种不同类型的盲签名方案，比如：弱盲签名方案、强盲签名方案、代理盲签名方案等。探讨和研究新的不同类型的盲签名方案，并将这些盲签名方案应用于椭圆曲线密码体制之中，从而可以得到若干在椭圆曲线密码体制下的各种不同类型的盲签名方案。

4．在认证签名方案中,往往需要从认证机构(CA)处获取通信方的公开密钥,由此带来的问题是系统需要保存大量的公钥及公钥证书。Girault 在 1991 年首次提出基于公钥的自证明原理研究认证加密方案，这个领域的研究至今仍然比较活跃，因此结合公

钥自证明的原理、盲签名的思想和具有消息恢复的处理手段，可以构造新的认证方案。

5．建立在椭圆曲线上的双线性理论，是近几年来密码学界研究的热点，它为密码学的研究开辟了新的方向，存在许多问题需要进行深入的探讨和研究，因此，利用椭圆曲线的双线性性质把基于 ID 的加密方案和盲签名方案结合起来可以构造一些新的签名方案。

6．盲签名因其具有匿名性特点而倍受密码学家的重视和深入研究，它在电子投票领域具有独特的地位和作用，几乎没有任何其它方法可以取代。目前盲签名与各种其它特殊签名结合可以派生许多新的签名，而且方法五花八门。比如把代理签名和盲签名结合起来形成的代理盲签名如何避免安全性缺陷的问题、代理签名人与签名人之间是否可以追踪的问题、如何进行盲化及盲化的本质问题都需要深入研究。

7．到目前为止，有关盲签名应用的软件和应用系统比较少见，因此研究基于盲签名技术的电子投票协议、应用系统的设计，具有十分重要的意义。

1.5 本人的主要贡献和创新之处

数字签名技术是解决信息安全需求的关键技术之一，近几年来，数字签名的基础理论研究一直十分活跃，一些新概念、新签名方案、新密码体制不断地产生和发展。本文在前人工作的基础上，对数字签名技术及应用问题进行了研究，主要贡献和创新工作归纳如下：

1．根据各种不同的签名方程的构造特点，比较完整地探讨了签名方案的构造及其参数选取的方法。包括：

（1）给出了 ElGamal 型数字签名方程参数选取的原则，使得构造这种类型的签名方程并不局限于 Harn 的 18 种，推广了选择签名的方法和范围。

（2）提出了一种基于椭圆曲线的具有消息恢复的认证加密方案，且对这种方案进行了推广，并指出在单向函数为同态函数的情况下存在两种已知明文的伪造攻击，从而说明选取符合一定条件的方案可以有效地避免这样的攻击；结合消息链接恢复特性，提出了相应的认证加密方案，该方案较好地解决了消息加密认证、消息链接恢复及传输量较大等问题。

（3）提出了一种基于椭圆曲线的具有消息恢复的签名方案，同时讨论了所给出的方案的参数的一般形式及选取方法，从而弥补了在这个领域上的不足。

2．结合盲签名方案的协议过程和签名方程，给出了构造广义弱盲签名方案的一般方法，以此方法构造的弱盲签名方案几乎包含了目前所有该类弱盲签名方案。结合代理签名和盲签名的特点，通过多元线性变换的形式较好地刻画了签名过程中用户与代理签名人之间合作完成签名的关系，提出了一种基于椭圆曲线的代理盲签名方案，

以此方法构造的代理盲签名方案具有一般性。同时还结合消息恢复特性，提出了基于椭圆曲线的具有消息恢复的代理盲签名方案，就消息是否链接恢复和是否针对指定的接收者而言分别进行了相应的代理盲签名方案设计。总之，比较完整地阐述了如何构造弱盲签名和代理盲签名的问题。

3．利用椭圆曲线上 Weil 配对的双线性性质，提出了基于 ID 的盲签名方案，该方案以 ID 为基础的公钥取代了以数字证书为基础的公钥，这种技术上的处理省略了验证签名时从系统获取公钥的步骤，减少了交互的次数并节省了存储空间。

4．提出了一种基于公钥自证明的具有消息恢复的认证加密方案。该方案采用用户注册协议动态地完成用户向 CA 的匿名身份注册，通信双方使用公钥的自证明协议，动态地完成对彼此公钥的自证明；信息的接收者可以从签名中恢复原消息，这样，签名方案既具有身份鉴别作用，又具有信息保密性。其次，针对消息分块情况，进行了消息链接处理，这种方案具有第三层次信任等级的自证明认证、较少的计算时间开销和较高的安全性等优点。

5．基于盲签名技术提出了一种匿名电子投票协议，该协议除满足电子投票的基本性质外，较好地解决了选票碰撞以及投票者的中途退出等问题，而且还可以有效地防止一人多票或一票多投现象的发生，即使管理机构和计票机构勾结，在计票前可同时保证选票的秘密性和公平性。

1.6 论文的组织与结构

论文围绕着目前在数字签名领域最新的一些课题,阐述了作者所提出的一些新的数字签名方案设计和开发系统原型所做的探讨工作,较全面地概括了作者在四年多来所做的工作及取得的成绩。论文的组织结构如下：

第 1 章介绍了数字签名研究的背景和意义、数字签名理论和应用研究现状、选题的依据、本文的研究内容、作者的主要贡献和创新之处以及论文的组织结构。

第 2 章探讨了 ElGamal 型数字签名方程参数选取的方法问题，给出了 ElGamal 数字签名方程参数选取的一般方法。

第 3 章研究了具有消息恢复的签名方案的构造问题。提出了基于椭圆曲线的具有消息恢复的签名方案和一般签名方案，在此基础上签名方程的参数选取方法。

第 4 章给出了具有消息恢复的认证加密方案的一般签名方程的参数选取方法,提出了基于椭圆曲线的具有消息恢复的认证加密方案以及具有消息链接恢复的认证加密方案。

第 5 章提出了一种基于公钥自证明的认证加密方案、具有消息恢复及消息链接恢复的认证加密方案。

第 6 章提出了广义 ElGamal 型弱盲签名方案的构造方法、代理盲签名方案的构造方法、基于多元线性变换的代理盲签名方案、基于椭圆曲线的代理盲签名方案以及具有消息恢复的代理盲签名方案。

第 7 章利用椭圆曲线上 Weil 配对的双线性性质，提出了基于 ID 的盲签名方案。

第 8 章首先基于盲签名技术提出了一种匿名电子投票协议，在此基础上，探讨了系统原型的设计问题，编程实现了主要的核心算法和部分功能。

第 9 章概括了全文的结论，并对未来研究方向进行了展望。

2 ElGamal 型签名方案的推广

2.1 引言

ElGamal 签名方案[62]是由 ElGamal 在 1985 年首先提出的，它是基于离散对数问题为数字签名而设计的,之后,出现了许多关于 ElGamal 签名方案的改进方案和各种推广方案。1994 年，Harn 等人[63]对 ElGamal 及其类似方案进行了总结,给出了 18 个安全可行的方案,称之为广义 ElGamal 签名方案。在同一时期,Horster[64]也独立地给出了 " Meta-ElGamal 签名方案 ",它实质是 Harn 的 18 种签名方案的进一步推广。

虽然 ElGamal 型签名方程是在环或域上进行的二元运算，容易受到同态攻击和代换攻击，因此在实际应用 ElGamal 型签名方案时，需要将明文 m 进行处理，即利用 hash(m)来代替 m。本章主要讨论 ElGamal 型签名方程参数选取的一般方法，这种探讨对于其它签名方案可以提供方法上的借鉴和指导作用，即其它各种签名方程均可作类似的处理从而弥补签名方程参数选取方法上的不足。

2.2 ElGamal 型签名方案及安全性分析

2.2.1 ElGamal 型签名方案

ElGamal 型签名方案[62]包含系统初始化过程、签名过程和验证过程，叙述如下：

(1) 初始化过程：设 p 是一个大素数，q 是 p 的一个大素数因子，整数 $g \in Z_p$ 且阶为 q，即 $g^q \equiv 1 \bmod p$。系统用户中用户 A 的私钥为 $x(1<x<p-1)$，相应的公钥为 $y = g^x \bmod p$。

(2)签名过程：对于待签消息 m，签名者 A 任意选取一个随机数 $k(1<k<p-1)$，计算 $r = g^k \bmod p$ 和 $s = (m - xr)k^{-1} \bmod (p-1)$。$(r,s)$ 作为消息 m 的签名，将 m 和签名 (r,s) 一起发送给接收者。

(3)验证过程：接收方收到 m 和签名 (r,s) 后，验证 $g^m = y^r r^s \bmod p$ 是否成立?如果成立，则接收签名，否则，拒绝签名。

2.2.2 安全性分析

(1)整体性攻击[63]。如果一个攻击者试图伪造用户 A 对消息 m 的签名，他随机地

选取一个整数$s\in Z_{p-1}$，攻击成功的概率为$(p-1)^{-1}$，这对于大素数来讲几乎是不可能的.如果要从r中求出消息密钥k，将面临求解离散对数的难题。

(2)重复性攻击。如果对不同的消息使用相同的密钥,则面临消息密钥被暴露的危险。设$s_1=(m_1-xr)k^{-1}\bmod(p-1)$，$s_2=(m_2-xr)k^{-1}\bmod(p-1)$,则$(s_1-s_2)k=(m_1-m_2)\bmod(p-1)$.

若$s_1-s_2\neq 0\bmod(p-1)$，则$k=(m_1-m_2)(s_1-s_2)^{-1}\bmod(p-1)$，一旦得到$k$，就很容易求得$x$。

(3)任意性攻击。攻击者可以任意伪造签名,攻击者任意选取数对(u,v)且满足条件$\gcd(v,p-1)=1$，计算$r=g^u y^v=g^{u+xv}\bmod p$和$s=-rv^{-1}\bmod(p-1)$，则$(r,s)$就是消息$m=su\bmod p$的签名。因为$k=(m-xr)s^{-1}=(su-xr)s^{-1}=(u+xv)\bmod(p-1)$，所以$r=g^k=g^{u+xv}\bmod p$。

(4)代换攻击。设(r,s)是m的一个签名，若r可逆的话，设$k'=lk+n$,l,n为任意两个整数，且满足$k'\in Z_{p-1}$,$r'=r^l g^n\bmod p$，$s'=skr^{l-1}g^n(lk+n)^{-1}\bmod(p-1)$，则$(r',s')$是$m'$的签名，其中

$m'=r^{l-1}g^n m\bmod(p-1)$。因为$(r,s)$是m的一个签名，则有$m=(sk+xr)\bmod(p-1)$。若$r$可逆，又有$x=r^{-1}(m-sk)\bmod(p-1)$，由签名方程得$m'=s'k'+xr'\bmod(p-1)$，将$s',k',x,r'$代入上述方程得$m'=(r^{l-1}g^n m)\bmod(p-1)$。

(5)同态性攻击[74]。如果三个不同的签名所选取的消息密钥k_1,k_2,k_3满足条件：$k_3=k_1+k_2$，显然$r_3=r_1r_2$，则可以从中推出密钥$x=(m_1s_2s_3+m_2s_1s_3-m_3s_1s_2)(r_1s_2s_3+r_2s_1s_3-r_1r_2s_1s_2)^{-1}\bmod(p-1)$。

2.3 ElGamal 型签名方程的一般形式

在2.1节引言中提到，Harn等人[63]对ElGamal及其类似方案进行了总结，给出了18个安全可行的方案，称之为广义ElGamal签名方案。在本节中做进一步的探讨，ElGamal型签名方案的推广问题，本质上是签名方程的参数选取问题，因此方程的各参数选取更一般的形式为:$ax=bk+c\bmod(p-1)$。

当$(a,b,c)=(r,-s,m)$时，正好是2.3.1节中的情形。在一般形式下，验证方程为：$y^a=r^b g^c\bmod p$。在实际应用中，需要将签名方程中的明文m用h(m)来代替，以提高安全性，因此，下面的讨论均针对h(m)。考虑(a,b,c)选取$(h(m),r,s)$的任意一个置换，则可得到如下结论。

结论1：方程中的未知向量(a,b,c)可以是向量$(h(m),r,s)$的一个任意置换,再加上正负号的变化共有48种不同的签名方程,签名方程和验证方程如表2.3.1所示。

说明：不妨就未知向量(a,b,c)选取$(h(m),r,s)$作为置换的情况(

结论 1：方程中的未知向量 (a,b,c) 可以是向量 $(h(m),r,s)$ 的一个任意置换,再加上正负号的变化共有 48 种不同的签名方程,签名方程和验证方程如表 2.3.1 所示。

说明：不妨就未知向量 (a,b,c) 选取 $(h(m),r,s)$ 作为置换的情况(即表 2.3.1 中 S1 方程)来进行讨论.在方程中有 4 个参数变量，所有可能的符号变化共有 16 种，但方程两边的符号可以同时变化，即 2 种不同的符号本质上只能算 1 种，因此实际上只有 8 种不同的符号组合，这 8 种情况分别是：(+,++,+)、(+,+-,+)、(+,-+,+)、(+,--,+)、(+,++,-)、(+,+-,-)、(+,-+,-)、(+,--,-).未知向量可能的置换有 6 种。因此共有 48 种。

表 2.3.1　不同形式的签名方程和验证方程表

a	b	c	签名方程	验证方程	编号
$h(m)$	s	r	$s=k^{-1}(h(m)x-r)\bmod(p-1)$	$y^{h(m)}=r^s g^r \bmod p$?	S1
$h(m)$	r	s	$s=(h(m)x-kr)\bmod(p-1)$	$y^{h(m)}=r^r g^s \bmod p$?	S2
s	$h(m)$	r	$s=x^{-1}(h(m)k+r)\bmod(p-1)$	$y^s=r^{h(m)} g^r \bmod p$?	S3
s	r	$h(m)$	$s=x^{-1}(kr+h(m))\bmod(p-1)$	$y^s=r^r g^{h(m)} \bmod p$?	N4
r	$h(m)$	s	$s=(r\,x-h(m)k)\bmod(p-1)$	$y^r=r^{h(m)} g^s \bmod p$?	S5
r	s	$h(m)$	$s=k^{-1}(r\,x-h(m))\bmod(p-1)$	$y^r=r^s g^{h(m)} \bmod p$?	N6

结论 2：方程中的未知向量 (a,b,c) 可以是向量 $(r,s,h(m))$、$(1,rs,h(m))$、$(1,r,sh(m))$、$(1,rh(m),s)$ 等的一个任意置换，每一种情况有 6 种不同的置换，且每一种置换的参数前的不同的符号变化有 4 种情形，因此，对应一个向量的不同的置换和符号变化有 24 种。

方程中的未知向量 (a,b,c) 的选取方法除上述两个结论外，实际上还有其他很多种不同的选取方法。但不论何种方法必须满足下列原则：

(1)三个参数中必须至少有一个参数与消息 m 有关。否则的话，消息签名与消息无关，显然不能成为有效的签名。

(2)在这些参数中，签名中的一个关键分量 s 必须通过方程能够进行求解，且关于 s 的形式最好不要太复杂，一般选取比较简单的形式。

(3)签名方程中的参数 a，c 不能包含签名者的私有密钥 x 或消息密钥 k 或它们的乘积。一方面避免出现这些量的二次情形，如 x^2、k^2 项；另一方面避免出现两个秘密值的乘积项 xk。因为这两种情况一旦出现的话，接收者便不能借助于系统的公开参数

进行签名验证。

(4)尽管 k 是随机选取的，但从签名方程中解出 k 的表达式中不能含有形如 x^{-1} 的式子，因为验证签名方程时会碰到类似在(3)中的问题，无法进行验证。

2.4 本章小结

本章讨论了两个问题：1）ElGamal 型数字签名方案的安全性；2）ElGamal 型数字签名方案中签名方程参数选取的方法。

得到的主要结论如下：

（1）归纳总结了 ElGamal 型数字签名方案受到的各种不同类型的攻击方法，这说明这种类型的签名方案在实际应用中没有什么意义，但它所提供的获取签名的处理手段具有方法论的指导意义和作用，况且任何基于公钥密码的签名方案本质上属于这种基本框架。

（2）给出了 ElGamal 型数字签名方程参数选取的更一般的方法，并不局限于 Harn 的 18 种广义 ElGamal 型数字签名方案，结论 2 说明可以有其它的选择，推广了 ElGamal 型签名方案。

（3）本章的探讨说明沿着参数的不同组合去构造不同的签名方程是无法穷尽的，因此我们给出了构造有效的签名方程的参数选择原则。虽然除比较经典的签名方程外，其它形式的签名方程在计算效率上不可能提高，甚至可能降低，但这说明签名方程的选择是多种多样的。

3 具有消息恢复的签名方案

3.1 引言

自 Nyberg 和 Rueppel[65]在 1994 年提出的具有消息恢复的签名方案以来，相继提出很多种具有消息恢复特性的签名方案，而且针对消息量很大的情况，采用消息链接的方式进行处理取得了较好的效果。

椭圆曲线密码体制是利用有限域上的椭圆曲线上的点构成的有限群代替基于离散对数问题密码体制中的有限循环群而得到的一类密码体制。因其具有比在有限域上的密码体制更小的密钥量、更快的速度、更高的安全性等优点，因此倍受密码学界高度重视并进行了大量的研究。

然而基于椭圆曲线的具有消息恢复功能的签名方案问题的研究并不多，王晓明在文献[79]中给出了一种签名方案。本章根据 N-R 消息恢复签名方案的思想给出了一种基于椭圆曲线的具有消息恢复的签名方案，不能简单地把该方案看作是 N-R 消息恢复签名方案在椭圆曲线上的模拟，其安全性基于求解椭圆曲线上的离散对数问题，并由此给出了更一般的签名方案，还列举了 6 种不同形式的签名方程和验证方程。

3.2 Neberg-Rueppel 签名方案

Neberg-Rueppel 签名方案包含系统初始化过程、签名过程和验证过程，叙述如下：

(1)系统初始化过程

设 p 是一个大素数，q 也是一个大素数，且 $q|p-1$；整数 $g\in Z_p$ 且 $g^q\equiv 1 \bmod p$。用户 A 的私钥为 $x(1<x<p-1)$，公钥为 $y=g^x \bmod p$。

(2)签名过程

对于待签消息 m，签名者 A 计算出 $\overline{m}=R(m)$，其中 R 是一个单一映射，且容易求逆；任意选取一个随机数 k $(1<k<q)$，计算 $r=g^{-k} \bmod p$，计算 $e=\overline{m}r \bmod p$，$s=xe+k \bmod q$。则以 (e,s) 作为消息 m 的签名。

(3)验证过程

接收方在收到数字签名 (e,s) 后，进行如下计算：

验证 $0<e<p, 0\le s<q$；

计算 $v=g^{s}y^{-c} \bmod p$，$m'=ve \bmod p$；

验证 $m' \in R(M)$，其中 $R(M)$ 表示 R 的值域;

计算 $m=R^{-1}(m')$。

证明过程如下：

$m'=ve \bmod p=g^{s}y^{-c}e \bmod p=g^{xr+k-xc}e \bmod p=g^{k}e \bmod p=\overline{m}$。

3.3 基于椭圆曲线的具有消息恢复的签名方案

系统初始化过程

(1)选取定义在有限域 F_q 上的一条安全的椭圆曲线 E[80]，使得 E 上的 F_q-有理点群的阶被一个大素数 n 整除，保证椭圆曲线上有理点群上的离散对数问题是难解的。

(2)选取一个基点 $G=(x_G,y_G) \in E$，G 的阶为 n，即有 $nG=O$，O 表示一个无穷远点，基点 G 公开。

(3)设 Alice 和 Bob 为系统的两个用户，Alice 的私钥为 $k_A \in_R Z_n^*$，$P_A=k_AG \in E$，P_A 作为 Alice 的公钥。同样地 Bob 选择 $k_B \in_R Z_n^*$，$P_B=k_BG \in E$，P_B 作为 Bob 的公钥.它们的公钥 P_A 和 P_B 在系统内公开，并记 $P_A=(x_A,y_A)$，$P_B=(x_B,y_B)$。

签名过程

签名者 Alice 利用上面的域参数及用户 Bob 的公钥对消息 m 进行签名，做如下操作：

Step1：Alice 选取随机数或伪随机数 $k \in_R Z_n^*$，称 k 为消息密钥,要求保密；

Step2：计算 $R_1=kP_B=(x_1,y_1)$，$r_1=x_1 \bmod n$,若 $r_1=0$,则返回第一步；

Step3：计算 $R_2=kG=(x_2,y_2)$，$r_2=x_2m \bmod n$；

Step4：计算 $s=k+r_2k_A \bmod n$,此为签名方程,如果 $s=0$,则返回到第一步；

Step5：Alice 对消息 m 的签名是 (r_1,r_2,s)。

验证过程

消息接收者 Bob 收到 Alice 的签名 (r_1,r_2,s) 后，Bob 首先获取系统的域参数和 Alice 的公钥，然后 Bob 做以下的操作进行验证：

Step1：验证 r_1,r_2,s 是 $[1,n-1]$ 中的整数；

Step2：计算 $x=k_B^{-1}r_1 \bmod n$，$m=x^{-1}r_2=k_Br_1^{-1}r_2 \bmod n$，此为消息恢复方程，即可恢复原消息 m。

Step3：计算 $X=sG-r_2P_A=(x',y')$,如果 $X=O$,则拒绝这个签名。否则，计算 $v=k_Hx' \bmod n$。当且仅当 $v=r_1$ 时接受这个签名，且相信是 Alice 发送过来的。

签名验证工作的证明

先说明恢复消息的正确性。因为 $(x_1,y_1)=R_1=kP_B=k_BkG=k_BR_2=k_B(x_2,y_2)$，所以 $x_1=k_Bx_2 \bmod n$，又因为 $r_1=x_1 \bmod n$，$r_2=x_2m \bmod n$，于是有 $m=k_Br_1^{-1}r_2 \bmod n$。

如果 (r_1,r_2,s) 确实是 Alice 对消息 m 的签名，则 $s=k+r_2k_A \bmod n$。因为 $sG-r_2P_A=sG-r_2k_AG=(s-r_2k_A)G=kG$，记 $k_B(sG-r_2P_A)=(x',y')$，$v=x' \bmod n$，所以当 $v=r_1$ 时接受这个签名。

安全性分析

(1)攻击者截取签名 (r_1,r_2,s) 后，试图获取消息 m，但因不知道接收者的私有密钥 k_B，无法根据消息恢复方程求解得到 m，换句话说，只有消息接收者才可能求解。

(2)攻击者截取签名 (r_1,r_2,s) 后，试图从签名方程中获取签名者的私钥 k_A，因一个签名方程中含有两个未知数 k_A 和消息密钥 k，这是不可能的。

(3)消息密钥 k 不能重复使用，即不同的消息签名应使用不同的消息密钥。否则，私钥 k_A 将可能被恢复。例如，对于不同的消息 m_1、m_2，使用相同的消息密钥 k，产生两个消息签名 (r_{11},r_{12},s_1)，(r_{21},r_{22},s_2)。此时 $s_1=k+r_{12}k_A \bmod n$，$s_2=k+r_{22}k_A \bmod n$，因 $s_1-s_2\equiv(r_{12}-r_{22})k_A \bmod n$。如果 $r_{21}\neq r_{22}$，则有 $k_A\equiv(r_{12}-r_{22})^{-1}(s_1-s_2) \bmod n$，从而敌手可以恢复 k_A。

3.4 基于椭圆曲线的具有消息恢复的一般签名方案

在上述方案的第四步中，将签名方程改写为一般形式：$ak=b+ck_A \bmod n$，参数 a,b,c 可以有很多种选择，但一定要求能够从中解出 s 且保证 $s\neq 0$，如果 $s=0$，则返回到第一步重新选取消息密钥 k，从而得到签名为 (r_1,r_2,s)。

验证过程同上述基本一致，不同的是在第三步需计算 $X=a^{-1}bG+a^{-1}cP_A=(x',y')$，如果 $X=O$，则拒绝这个签名。否则，计算 $v=k_Hx' \bmod n$。当且仅当 $v=r_1 \bmod n$ 时接受这个签名。

签名方程的参数未知向量 (a,b,c) 可以是向量 $(1,s,r_2)$ 的一个任意置换，且参数前搭配不同的符号可以构成 4 种不同的签名方程，因此共有 24 种不同的签名方程，其中基本的 6 种签名方程列在表 3.4.1 中。

表 3.4.1　基于椭圆曲线的具有消息恢复的签名方程和验证方程表

编号	签名方程	验证方程
N1	$k=s+r_2k_A \bmod n$	$sG+r_2P_A=(x',y'),v=k_Bx' \bmod n,v=r_1?$
N2	$k=r_2+sk_A \bmod n$	$r_2G+sP_A=(x',y'),v=k_Bx' \bmod n,v=r_1?$
N3	$sk=1+r_2k_A \bmod n$	$s^{-1}G+r_2s^{-1}P_A=(x',y'),v=k_Hx' \bmod n,v=r_1?$
N4	$sk=r_2+k_A \bmod n$	$s^{-1}r_2G+s^{-1}P_A=(x',y'),v=k_Hx' \bmod n,v=r_1?$
N5	$r_2k=s+k_A \bmod n$	$r_2^{-1}sG+r_2^{-1}P_A=(x',y'),v=k_Bx' \bmod n,v=r_1?$
N6	$r_2k=1+sk_A \bmod n$	$r_2^{-1}G+r_2^{-1}sP_A=(x',y'),v=k_Bx' \bmod n,v=r_1?$

虽然签名方程中的参数 a,b,c 有上述许多种选择，但它们都有一个共同点，那就是能够从签名方程中解出签名时的一个变量 s，可以简单地表示为：$s=f(k_A,r_2,k)$.从理论上讲，只要符合这个条件，均可构造出签名方程.从实用的角度来看，签名方程不宜过分复杂，结果表明，表 3.4.1 中的各个签名方程都是比较简单、可行的签名方案。

3.5 本章小结

本章得到的主要结果如下：

（1）将签名方案中具有消息恢复的特性平移到椭圆曲线密码体制中来，得到了基于椭圆曲线密码的具有消息恢复的签名方案。

（2）与上一章类似，给出了所提出的方案的一般模型，讨论了不同的参数选取方法，列举出不同形式的各种签名方案，从而弥补在这个领域上的不足。

本章评注

虽然具有消息恢复的签名方案最早就由 Nyberg K.和 Rueppel R.A.在 1994 年提出来了，但方案的安全性是基于离散对数难题。消息恢复概念的提出，在数字签名领域开辟了一个新的研究方向，目前主要集中在两个方面：一是消息恢复的签名方案的创新，即要解决构造上的问题，不仅仅是形式上的推广；二是基于不同密码体制的的具有消息恢复的方案的延伸和拓展。前者的研究涉及到方案的构造问题，后者的研究是顺理成章的事情了。

4 具有消息恢复的认证加密方案

4.1 引言

与上一章不同的是，本章以 HMP 认证加密方案为基础来进行研究，尽管在签名过程中仍然使用了接收方的公钥和签名人的私钥，但最为突出的特点是根据恢复得来的消息 m 的冗余位进行认证，因此，我们不称之为签名方案，而称之为认证加密方案。

与上一章相同的是，我们仍然考虑在椭圆曲线密码体制下来进行研究，因此，首先首先提出了一种基于椭圆曲线的具有消息恢复的认证加密方案，对其安全性进行了分析，并由此给出了更一般的签名方案及其参数选取方法，还讨论了两种已知明文的伪造攻击方法。最后给出了一种基于椭圆曲线的具有消息链接恢复的认证加密方案，该方案较好地解决了消息加密认证、消息链接恢复及传输量较大等问题。并分类罗列不同的构造签名方程的方法，这些方案几乎包含了所有该类问题的签名方案。

4.2 HMP 方案介绍

HMP 方案[4,67]包含三个过程：系统初始化、签名并加密、认证并解密。

系统初始化

系统或认证中心(CA)选取一个大素数 p 满足条件:$q|p-1$，且 q 为一个大素数。设 $g\in Z_p^*$ 且 g 的阶为 q，即 $g^q=1 \mod p$，再选取一个单向函数 $h:Z_p^*\to Z_p^*$。公开系统参数 p,q,g 和单向函数 h。假设系统中两个用户分别为 A 和 B，每一用户 $i\in\{A,B\}$ 选取密钥 $x_i\in Z_q^*$，计算公钥 $y_i=g^{x_i} \mod p$，将公钥 y_i 存放在用户的公开文件中，秘密保存私钥 x_i。

签名并加密

假设 A 要发送消息 $m\in Z_p$ 给 B，A 从公开信息中获得 B 的公钥 y_B，随机选取 $k\in Z_q$，计算 $r=h(y_B^k)^{-1}m \mod p$，$r'=r \mod q$，$s=k-r'x_A \mod q$，则(r,s)就是 A 对消息 m 的签名(或称为密文)。A 将(r,s)传送给 B。

认证并解密

B 收到(r,s)后，从系统公开文件中获得系统的公开参数及 A 的公钥 y_A。计算

$r'=r \bmod q$，再计算 $m=h(y_B^s y_A^{r's_B})r \bmod p$，即从签名中恢复而得 A 发送的消息 m，检查 m 的冗余位可以进行认证。

4.3 一般签名方程的参数选取方法

设一般签名方程为：$ak=b+cx_A \bmod q$。在方程中的未知向量(a,b,c)有很多种选择，但一定要求能从签名方程中解出 s，得签名 (r,s).B 收到签名后，计算 $m=h(y_B^{a^{-1}b}y_A^{a^{-1}c\ s_B})r \bmod p$ 得到原消息，因为从方程中易得 $k=a^{-1}b+a^{-1}c\ x_A \bmod q$，将其代入消息恢复方程 $m=h(y_B^k)r \bmod p$ 即可。

签名方程的参数选择

结论：方程中的未知向量(a,b,c)可以是向量$(\pm r',\pm s,\pm 1)$、$(\pm 1,\pm 1,\pm sr')$、$(\pm 1,\pm s,\pm sr')$和$(\pm 1,\pm r',\pm sr')$的一个任意置换,分别有 24、12、24 和 24 种不同的选择，且都可以构成为具有消息恢复特性的认证加密方案，它们的签名方程和消息恢复方程如表 4.3.1 所示。

分析：Horster 等[4,67]给出了其方案的 9 种变形，但并不全面，上述结论包含了 HMP 方案在内的 84 种签名方案。所有结果列在表 4.3.1 中。就第一种情况而言，选择 $(r',s,1)$ 作为置换的基本方程有 6 个,且每一个基本方程又可以选取不同的符号，比如方案 S3，4 种选择分别是 $(1,s,r')$,$(1,s,-r')$,$(1,-s,r')$,$(1,-s,-r')$,故得上述结论。

4.3.1 签名方程参数选择的原则

从签名方程的特点来看，不可缺少的两个变量是用户选取的随机数 k 和其私钥 x_A，除签名中的一个分量 r 外，另一个分量 s 通过解签名方程而来，参数的选择主要基于以下几条原则：

(1)签名方程中的参数 a,b,c 可以分别选取 $r',s,1$ 中任何一个或它们的乘积，但最好不要重复选取，换句话说最多可选取 $r's$，乘积项的次数不要超过两次以免使得式子变得复杂而没有本质区别，上述四种不同的组合均出于这种考虑。

(2)签名方程中的参数 a,c 不能包含用户的私有密钥 x_A 或随机选取的秘密值 k 或它们的乘积，一方面避免出现这些量的二次情形，如 x_A^2,k^2 项；另一方面避免出现两个秘密值的乘积项 kx_A。因为这两种情况一旦出现的话，接收者不能借助于系统的公开参数换算成发送者的公钥，导致的结果是接收者无法恢复消息或验证签名，除非发送者自己，显然这是没有意义的。

(3)尽管 k 是随机选取的，但从签名方程中解出 k 的表达式中不能含有形如 x_A^{-1} 的式子，因为验证签名或恢复消息等计算过程必须用到它，一旦出现的话同上述第二条

原则结果一样。

表 4.3.1　基本签名方程和消息恢复方程表

	a	b	c	签名方程	消息恢复方程	编号[11]
1	1	s	r'	$k=s+r'x_A \mod q$	略	S3
	1	r'	s	$k=r'+sx_A \mod q$	略	S6
	r'	1	s	$r'k=1+sx_A \mod q$	略	S2
	r'	s	1	$r'k=s+x_A \mod q$	$m=h(y_B^{(r')^{-1}s}y_A^{(r')^{-1}x_B})r \bmod p$	N11
	s	r'	1	$sk=r'+x_A \mod q$	略	S4
	s	1	r'	$sk=1+r'x_A \mod q$	$m=h(y_B^{s^{-1}}y_A^{s^{-1}r'x_B})r \bmod p$	N12
2	1	1	sr'	$k=1+sr'x_A \mod q$	略	S8
	1	sr'	1	$k=sr'+x_A \mod q$	略	S7
	sr'	1	1	$sr'k=1+x_A \mod q$	$m=h(y_B^{(sr')^{-1}}y_A^{(sr')^{-1}x_B})r \bmod p$	N21
3	1	s	sr'	$k=s+sr'x_A \mod q$	略	S1
	1	sr'	s	$k=sr'+x_A \mod q$	$m=h(y_B^{sr'}y_A^{x_B})r \bmod p$	N31
	sr'	1	s	$sr'k=1+sx_A \mod q$	$m=h(y_B^{(sr')^{-1}}y_A^{(r')^{-1}x_B})r \bmod p$	N32
	sr'	s	1	$sr'k=s+x_A \mod q$	$m=h(y_B^{(r')^{-1}}y_A^{(sr')^{-1}x_B})r \bmod p$	N33
	s	1	sr'	$sk=1+sr'x_A \mod q$	$m=h(y_B^{s^{-1}}y_A^{r'x_B})r \bmod p$	N34
	s	sr'	1	$sk=sr'+x_A \mod q$	$m=h(y_B^{r'}y_A^{s^{-1}x_B})r \bmod p$	N35
4	1	r'	sr'	$k=r'+sr'x_A \mod q$	$m=h(y_B^{r'}y_A^{sr'x_B})r \bmod p$	N41
	1	sr'	r'	$k=sr'+r'x_A \mod q$	$m=h(y_B^{sr'}y_A^{r'x_B})r \bmod p$	N42
	sr'	1	r'	$sr'k=1+r'x_A \mod q$	$m=h(y_B^{(sr')^{-1}}y_A^{s^{-1}x_B})r \bmod p$	N43
	sr'	r'	1	$m=h(y_B^{s^{-1}}y_A^{(sr')^{-1}x_B})r \bmod p$	$m=h(y_B^{s^{-1}}y_A^{(sr')^{-1}x_B})r \bmod p$	N44
	r'	1	sr'	$r'k=1+sr'x_A \mod q$	$m=h(y_B^{(r')^{-1}}y_A^{sx_B})r \bmod p$	N45
	r'	sr'	1	$r'k=sr'+x_A \mod q$	$m=h(y_B^{s}y_A^{(r')^{-1}x_B})r \bmod p$	N46

(注:表中略去的部分可在文献[67]中查到)

4.3.2　已知明文的伪造攻击

引用文献[4]中关于同态函数的定义:设函数 $f:Z^*\to Z^*$，如果对 $\forall a,b\in Z_n^*$，有 $f(ab)=f(a)f(b)$，则称函数 f 为同态函数.

引理[4]:在 HMP 签名方案(S3)(S5)和(S7)中，假设单向函数 $h:Z^*\to Z^*$ 为同态函数，明文 m 的签名(密文)为 (r,s)，对于任意的整数 n，令 $\tilde{r}=r \bmod q$，$\tilde{s}=s+n \bmod q$

$$\tilde{m}=\begin{cases} mh^n(y_B) \bmod p & \text{对于S3} \\ mh(y_B)^{n(r')^{-1}} \bmod p & \text{对于S5} \\ m(h(y_B))^{n'} \bmod p & \text{对于S7} \end{cases}$$

则明文 $\tilde{m}$ 的签名为 $(\tilde{r},\tilde{s})$.

注:该引理引自文[4]中的推论 12，这个推论可能有印刷错误，这里已经更正.

推论:在签名方案(N42)(N46)中， 假设单向函数 $h:Z^*\to Z^*$ 为同态函数，明文 m 的签名(密文)为 (r,s)，对于任意的整数 n，令 $\tilde{r}=r \bmod q$，$\tilde{s}=s+n \bmod q$

$$\tilde{m}=\begin{cases} mh(y_B^{nr'}) \bmod p & \text{对于}N42 \\ mh(y_B^{n}) \bmod p & \text{对于}N46 \end{cases}$$

则明文 $\tilde{m}$ 的签名为 $(\tilde{r},\tilde{s})$.

证明:只证明方案 N42 的情况.因为 (r,s) 是消息 m 的签名(密文)，则

$m=h(y_B^{sr'}y_A^{r'x_B})r \bmod p$，于是有

$h(y_B^{\tilde{s}\tilde{r}}y_A^{\tilde{r}x_B})\tilde{r} \bmod p=h(y_B^{(s+n)r'}y_A^{r'x_B})r \bmod p=h(y_B^{nr'})h(y_B^{sr'}y_A^{r'x_B})r \bmod p$

$\therefore\ \tilde{m}=mh(y_B^{nr'}) \bmod p$，结论成立。

依此类推，在我们补充给出的签名方案中，签名方案(N11)(N31)同上述签名方案(N42)(N46)类似，攻击者可以假冒用户对消息 $\tilde{m}$ 产生有效的签名 $(\tilde{r},\tilde{s})$，从某种程度上来说，这些认证加密方案都是不安全的，但是，这种攻击对于其余的方案来说是无效的。

注：上述签名方案在单向函数为同态函数的情况下是否产生假冒攻击取决于恢复消息的表达式的构造特点。所谓假冒签名不外乎构造新的 r,s 使其符合消息恢复方程。从消息恢复方程的特点来看，r 可能的伪造只可能是它的倍数如 nr 的形式，这样涉及较多的指数处理，数学难度较大；s 可能的伪造只可能是 $s+n$ 的形式，因为 s 出现在指数中，这样利用函数的同态性可以进行分离，当然还必须要求在指数中不能出现 $sx_A,s^{-1}x_A$ 的式子，上述推论就是根据这个要求进行判断而得出结论的。

定理 4.3.2.1：在 HMP 签名方案(S1)(S2)(S4)(S6)(S8)(S9)中，假设单向函数 $h:Z^*\to Z^*$ 为同态函数，明文 m 的签名(密文)为 (r,s)，对于任意的整数 n，令 $\tilde{r}=r \bmod q$，$\tilde{s}=ns \bmod q$，则明文 $\tilde{m}$ 的签名为 $(\tilde{r},\tilde{s})$.其中

$$\tilde{m}=\begin{cases} m^n r^{1-n} & \text{对于}S1 \\ m^n h(y_B^{(r')^{-1}(1-n)})r^{1-n} & \text{对于}S2 \\ m^n r^{1-n^{-1}} & \text{对于}S4 \\ m^n h(y_B^{r'(1-n)})r^{1-n} & \text{对于}S6 \\ m^n h(y_B^{1-n})r^{1-n} & \text{对于}S8 \\ m^n r^{1-n^{-1}} & \text{对于}S9 \end{cases}$$

证明：只证明方案 S6 的情况。需要说明的是在文献[5]中方案 S6 的消息恢复方程可能是印刷错误，应改为 $m=h(y_B^{r'}y_A^{sx_B})r \bmod p$，于是有

$h(y_B^{\tilde{r}}y_A^{\tilde{s}x_B})\tilde{r} \bmod p=h(y_B^{r'}y_A^{nsx_B})r \bmod p=h(y_B^{(1-n)r'})h(y_B^{r'}y_A^{sx_B})^n r \bmod p$

$=h^n(y_B^{r'}y_A^{sx_B})r^n h(y_B^{(1-n)r'})r^{1-n} \bmod p=m^n h(y_B^{(1-n)r'})r^{1-n} \bmod p$ 证毕.

分析说明：在定理所设条件下，上述方案是不安全的，但对于方案(S1)(S3)(S5)来说则是安全的。巧的是这正好与推论中的结论相反，由此说明如果单向函数是同态

的，那么 HMP 方案的九个变形均是不安全的。同理本文中补充给出的其它方案也有类似缺陷。但要强调一点，上述的所有认证加密方案的安全性从本质上来说都是基于离散对数问题。

4.4 基于椭圆曲线的具有消息恢复的认证加密方案

在本节中，首先给出一种基于椭圆曲线的具有消息恢复的认证加密方案，然后对其推广，并列举其中 6 组参数的签名方程和消息恢复方程表，与 4.3.2 一样，还讨论了两种已知明文的伪造攻击。

4.4.1 方案描述

系统初始化过程除与第 3.3 节的初始化过程一样外，还需选取一个安全的 Hash 函数 $h(\cdot)$，并公开。

签名过程：签名者 Alice 利用上面的域参数及消息接收者 Bob 的公钥对消息 m 签名，步骤如下：

(1)Alice 选取随机数或伪随机数 $k\in_R Z_n^*$，称 k 为消息密钥，要求保密；

(2)计算 $R=kP_B=(x,y)$，$r=h(x)^{-1}m(\mathrm{mod}n)$，若 $r=0$，则返回第(1)步；

(3)计算 $s=k+rk_A \bmod n$，此为签名方程，如果 $s=0$，则返回到第(1)步；

(4)Alice 对消息 m 的签名是 (r,s).

消息恢复及验证过程：消息接收者 Bob 收到 Alice 的签名 (r,s) 后，Bob 首先获取系统的域参数和 Alice 的公钥，然后 Bob 做以下的操作进行验证：

(1)验证 r,s 是 $[1,n-1]$ 中的整数；

(2)计算 $X=sG-rP_A=(x',y')$，$m=h(k_Bx')r \bmod n$，此为消息恢复方程，即可恢复原消息 m.

(3)如果 X=O，则拒绝这个签名.否则，通过计算出的原消息 m，检查它的冗余位进行身份认证，若正确，则接受签名，否则拒绝接受签名。

增加冗余位的方法很多，比如，可以在末尾处增加发信人的身份 ID 或其它通信约定的字符串，因为接收者 Bob 的私钥是保密的，除 Bob 外，其他人不可能恢复原消息，也不可能判断是谁发送的，只有 Bob 才能求解得到原消息，从而达到对 Alice 的身份认证。

因为 $s=k+rk_A \bmod n$，$R=kP_B=k_BkG=k_B(sG-rP_A)=k_B(x',y')$，由签名过程中的第二步得 $m=h(k_Bx')r \bmod n$。

安全性分析

(1)攻击者截取签名(r,s)后，因不知道接收者的私有密钥k_B，无法恢复消息。

(2)攻击者截取签名(r,s)后，因在一个签名方程中含有私钥k_A和消息密钥k两个未知数，方程是不可解的，成功攻击的概率非常小。

(3)攻击者欲从签名者的公钥求解私钥，等价于求解椭圆曲线上的离散对数难题。

4.4.2 推广

在上述方案的第三步中，将签名方程改写为一般形式：$ak=b+ck_A \bmod n$，参数a，b，c可以有很多种选择，但一定要求能够从中解出s且保证$s\neq 0$，如果$s=0$，则返回到第一步重新选取消息密钥k，从而得到签名为(r,s)。

验证过程同上述基本一致，不同的是在第三步需计算$X=a^{-1}bG+a^{-1}cP_A=(x',y')$，如果$X=O$，则拒绝这个签名。否则，计算$m=h(k_Bx')r(\bmod n)$,此为消息恢复方程，即可恢复原消息 m。

定理 4.4.2.1：方程中的未知向量(a,b,c)可以是向量$(\pm r,\pm s,\pm 1)$、$(\pm 1,\pm 1,\pm sr)$、$(\pm 1,\pm s,\pm sr)$和$(\pm 1,\pm r,\pm sr)$的一个任意置换，分别有 24、12、24 和 24 种不同的选择，且都可以构成为具有消息恢复特性的基于椭圆曲线的认证加密方案。

分析：若(a,b,c)选取向量$(\pm r,\pm s,\pm 1)$的任意置换，基本方程有 6 个，这 6 个基本的签名方程和消息恢复方程列在表 4.4.2.1 中，其余情况略去。每一个基本方程又可以选取不同的符号，比如方案 N11，四种可能的选择分别是$(1,s,r)$、$(1,s,-r)$、$(1,-s,r)$、$(1,-s,-r)$，故有 24 种。

表 4.4.2.1 基于椭圆曲线的签名方程和消息恢复方程表

签名方程	消息恢复方程	编号
$k=s+rk_A \bmod n$	$sG+rP_A=(x',y')$，$m=h(k_Bx')r \bmod n$	N11
$k=r+sk_A \bmod n$	$rG+sP_A=(x',y')$，$m=h(k_Bx')r \bmod n$	N12
$rk=1+sk_A \bmod n$	$r^{-1}G+r^{-1}sP_A=(x',y')$，$m=h(k_Bx')r \bmod n$	N13
$rk=s+k_A \bmod n$	$r^{-1}sG+r^{-1}P_A=(x',y')$，$m=h(k_Bx')r \bmod n$	N14
$sk=r+k_A \bmod n$	$s^{-1}rG+s^{-1}P_A=(x',y')$，$m=h(k_Bx')r \bmod n$	N15
$sk=1+rk_A \bmod n$	$s^{-1}G+s^{-1}rP_A=(x',y')$，$m=h(k_Bx')r \bmod n$	N16

4.4.3 已知明文的攻击

定理 4.4.3.1：设单向函数 $h:Z^*\to Z^*$ 为指数型函数，明文 m 的签名(密文)为 (r,s)，对于任意的整数 t，令 $\tilde{r}=r \bmod n$，$\tilde{s}=s+t \bmod n$，

$$\tilde{m}=\begin{cases} mh(tx_B)\bmod n & \text{对于N11} \\ mh(r^{-1}tx_B)\bmod n & \text{对于N14} \end{cases}$$

则明文 $\tilde{m}$ 的签名为 $(\tilde{r},\tilde{s})$。

证明：只证明方案 N11。易知 $\tilde{s}G+\tilde{r}P_A=tG+sG+rP_A=(tx_G+x',ty_G+y')$，

$\tilde{m}=h(k_B(tx_G+x'))r=h(k_Bx')h(tk_Bx_G)r=mh(tx_B)\bmod n$，故 $(\tilde{r},\tilde{s})$ 为明文 $\tilde{m}$ 的签名(密文)。

由此可见，对于 N11，N14 方案，如果单向函数 h:Z*→Z*为指数型函数，且攻击者获得了一组明文和签名，那么攻击者就可以冒充用户对消息 $\tilde{m}$ 产生有效的签名，但是这种攻击对其余的方案是无效的。

定理 4.4.3.2：设单向函数 $h:Z^*\to Z^*$ 为同态函数，明文 m 的签名(密文)为 (r,s)，对于任意的整数 t，令 $\tilde{r}=r \bmod n$，$\tilde{s}=st^{-1} \bmod n$，$\tilde{m}=mh(t)\bmod n$，则有：对于方案 N15，N16 来讲，明文 $\tilde{m}$ 的签名为 $(\tilde{r},\tilde{s})$。

证明：只证明方案 N15。易知 $\tilde{s}^{-1}\tilde{r}G+\tilde{s}^{-1}P_A=t(s^{-1}rG+s^{-1}P_A)=(tx',ty')$，

$\tilde{m}=h(k_Btx')r=h(t)h(k_Bx')r=mh(t)\bmod n$，故 $(\tilde{r},\tilde{s})$ 为明文 $\tilde{m}$ 的签名(密文)。

4.5 基于椭圆曲线的具有消息链接恢复的认证加密方案

如果传输的消息量 m 超过大素数 n 时，需要对 m 分组，记为 $m=\{m_1,m_2,\cdots,m_t\}$，使得每一个子块 $m_i<n$，然后对每一个子块分别进行签名 (r_i,s_i)，并在每一个消息块上附加冗余位，使得接收者可以确定消息源的认证及排列顺序，从而正确地把消息链接起来，恢复原消息，但是采取这种方法却使得传输的信息量较大，且验证的工作量也较大。因此我们采用递推的方式构造消息分块的签名，把前一个参数作为后一个参数的输入，这样恢复消息时只需进行递推的运算就可以了一个一个地恢复全部消息了，从而大大地减少了通信传输量。

4.5.1 方案描述

签名过程

签名者 Alice 利用上面的域参数及信息接收者 Bob 的公钥对消息 $m=\{m_1,m_2,\cdots,m_t\}$ 进行签名，其中 $m_i\in_R Z_n^*$，步骤如下：

(1)选取随机数或伪随机数 $k\in_R Z_n^*$，令 $r_0=0$；

(2)计算 $R=kP_B=(x,y)$，$r_B=x \bmod n$，若 $r_B=0$，则返回到第(1)步；

(3)计算 $r_i=m_i h(r_{i-1}\oplus r_B)^{-1} \bmod n$，$i=1,2,\cdots,t$，$r=h(r_1\|r_2\|\cdots\|r_t)$；

(4)计算 $s=k+rk_A \bmod n$，如果 $s=0$，则返回到第(1)步；

(5)Alice 对消息 m 的签名是 $(r,s,r_1,r_2,\cdots,r_t)$。

消息恢复及验证过程

消息接收者 Bob 收到 Alice 的签名 $(r,s,r_1,r_2,\cdots,r_t)$ 后，Bob 首先获取系统的域参数和 Alice 的公钥，然后 Bob 做以下的操作进行验证:

(1)验证 $r,s,r_1,r_2,\cdots,r_t$ 是 $[1,n-1]$ 中的整数;

(2)计算 $r'=h(r_1\|r_2\|\cdots\|r_t)$，$r'\neq r$，则签名不成立;

(3)计算 $X=sG-rP_A=(x',y')$，$r_B'=k_B x' \bmod n$，$m_i=r_i h(r_{i-1}\oplus r_B')\bmod n$，即恢复原消息串 $m=\{m_1,m_2,\cdots,m_t\}$.若 $x'=0$，则拒绝这个签名. 否则，通过计算出的消息串的冗余位进行身份认证，若正确，接受签名，否则拒绝接受。

签名验证工作的证明

因为 $s=k+rk_A \bmod n$，$R=kP_B=k_B kG=k_B(sG-rP_A)=k_B(x',y')$，所以 $r_B'=k_B x' \bmod n$，从而 $m_i=r_i h(r_{i-1}\oplus r_B')\bmod n$，$i=1,2,\cdots,t$。

4.5.2 信息传输量和计算时间效率对比分析

在这一小节中，我们对消息链接恢复的方案与分组签名恢复的方案进行对比分析。

(1)传输信息量大小对比

对于 m 分组的情况，$m=\{m_1,m_2,\cdots,m_t\}$，得 t 组签名 $(r_i,s_i),i=1,2,\cdots,t$，共需传输的信息量为 $2tn$;对于链接的情况，签名为 $(r,s,r_1,r_2,\cdots,r_t)$，则需要传输的信息量为 $(t+2)n$。当 $t>1$ 时,显然有 $2tn>(t+2)n$,因此，后者传输的信息量较小。若分组较多时，传输的效率会更高。

(2)计算时间效率分析

为计算方便，不妨设 Tpmul 表示椭圆曲线上点的数乘的计算时间，Tmul 表示在模意义下两个整数相乘的计算时间，Tinv 表示在模意义下计算某个整数的逆的时间，Th 表示计算一次 hash 函数所划的时间。在两种情况下签名阶段和验证阶段的计算时间复杂度情况列于表 4.5.2.1 中。

表 4.5.2.1 计算时间复杂度对比表

方案	签名阶段	验证阶段	总计
分组签名	t(Tpmul+3Tmul+ Th+Tinv)	t(2Tpmul+2Tmul+ Th)	3tTpmul+5tTmul+2t(Th+tTinv
链接签名	Tpmul+(t+1)Tmul+(t+1)Th+tTinv	2Tpmul+(t+1)Tmul+(t+1)Th	3Tpmul+(2t+2)Tmul+(2t+2)Th+tTinv

从表 4.5.2.1 中不难看出，我们没有考虑椭圆曲线上点的加法和在模意义下两个整数相加的计算时间，具有消息链接恢复的认证加密方案的计算时间优于分组的情况。因此，采用链接恢复不失为一种好的处理办法。

4.5.3 安全性分析

(1)攻击者从用户的公钥 P_A 获取其私钥 k_A 是不可能的，因为他面临求解椭圆曲线离散对数难题.同样从签名方程 $s=k+rk_A \bmod n$ 中获取私钥也是不可能的，因为在签名方程中含有另一个未知数 k 。

(2)攻击者截取签名 $(r,s,r_1,r_2,\cdots,r_l)$ 后，因不知道接收者的私有密钥 k_B ，虽然可以计算 $X=sG-rP_A=(x',y')$ ，但是无法计算 $r'_B=k_Bx' \bmod n$ ，从而不可能计算 $m_i=r_ih(r_{i-1}\oplus r'_B) \bmod n$.因此他无法恢复消息。在本方案中，只有消息接收者 Bob 才可能恢复消息。

(3) 若攻击者获取了明文 $m=\{m_1,m_2,\cdots,m_l\}$ 的签名 $(r,s,r_1,r_2,\cdots,r_l)$ ，因为 $h(r_{i-1}\oplus r'_B)=m_ir_i^{-1} \bmod n$ ，hash 函数 $h(\cdot)$ 是一个安全的函数，使用 160 位的 hash 值，保证了已知明文的攻击是困难的，也就是说不可能从中求得 r'_B 。

(4)消息密钥 k 不能重复使用，即不同的消息签名应使用不同的消息密钥.否则，私钥 k_A 将可能被恢复.例如，对不同的消息 m_1，m_2，若使用相同的消息密钥 k，产生两个消息签名 $(r_1,s_1,r_{11},r_{12},\cdots,r_{1l})$ ，$(r_2,s_2,r_{21},r_{22},\cdots,r_{2l})$.此时 $s_1=k+r_1k_A \bmod n$ ，$s_2=k+r_2k_A \bmod n$ ，因 $s_1-s_2=(r_1-r_2)k_A \bmod n$.如果 $r_1\neq r_2$ ，则有 $k_A=(r_1-r_2)^{-1}(s_1-s_2) \bmod n$ ，从而攻击者可以恢复 k_A 。

4.6 本章小结

本章主要探讨了在不同密码体制下具有消息恢复的认证加密方案的构造问题，获得的主要结果如下：

（1）给出了 HMP 认证加密方案中签名方程的参数选取的一般原则，并由此列举了不同参数组合下相应的签名方程和消息恢复方程表。

（2）指出在 HMP 认证加密方案中存在两种已知明文的伪造攻击，从而说明何种方案可以避免这种攻击。

（3）提出了一种基于椭圆曲线的具有消息恢复的认证加密方案，对其安全性进行了分析；同时，对这种方案进行了推广，并指出与 HMP 认证加密方案一样，存在两种已知明文的伪造攻击。

（4）考虑到消息链接恢复特性，给出了相应的认证加密方案，并进行了信息传输量和计算复杂度的对比分析，该方案较好地解决了消息加密认证、消息链接恢复及

传输量较大等问题。

5 基于公钥自证明的认证加密方案

5.1 引言

具有消息恢复的认证签名方案在签名时必须从系统公共文件中获取通信方的公开密钥，签名者还要随机地选取一个秘密密钥并计算相应的公钥，经认证机构(CA，以下统称)认证后，颁发用户的公钥证书。由此带来的一个问题是系统需要保存大量的公钥及公钥证书。Shamir[81]于 1984 年首次提出了基于标识(ID)的密码体制的思想，在这个密码体制中，用户的标识被用作公钥，由于用户的标识是公开的，不需要保存，也就不需要保存用户公钥的证书了。但是，用户的私钥不是自己选择的，而由系统产生提供的，这样系统可以冒充用户，因此系统的安全性极大地依赖于系统的公正和权威。Girault[52]于 1991 年首次介绍了基于公钥的自证明机制的思想，CA 使用系统的私钥对用户的标识签名，任何用户都可以从签名中获取其公钥，公钥的产生是由用户和 CA 共同完成的，且 CA 不知道用户的私钥，验证者在验证签名时就能验证公钥的真伪了。相比基于 ID 的密码体制而言，自证明机制具有节省存储空间、用户自选私钥及 CA 不能冒充用户等优点，具有更高的安全性。Petersen 和 Horster[53]扩充了自证明机制的概念，提出了若干在不同可信等级下的具有自证明机制的公钥分发协议并将这些方法应用于授权签名、电子投票及会话密钥交换等领域。在 2000 年，Chang Yuh Shihng[54]等提出了 ElGamal 型自证明签名方案及群签名方案，这个方案从自证明机制简单地平移到 ElGamal 型签名方案中来。在 2003 年，Tseng Yuh-Min[55]等提出了具有消息恢复的基于自证明机制的签名方案及两个变形方案。

本章主要基于 Girault 自证明原理并结合上述具有消息恢复的签名方案和盲签名的思想方法，提出了一种基于公钥自证明的认证加密方案，同时还考虑了当消息量很大需要分组的情况，提出了具有消息链接恢复的基于公钥自证明的认证加密方案。

5.2 基于公钥自认证的认证加密方案

首先说明关于公钥认证的几个概念，关于公钥认证大体上可以分为三个层次的信任等级。

第一层次：基于 ID 模式的公钥认证.公钥代表了用户的身份，不需要存取用户的

公钥，因此不存在用户的公钥认证问题，但 CA 可以计算出用户的私钥.因此，这一模式安全的前提条件是 CA 是高度值得信任的。CA 掌握所有用户的私钥，可以假冒任一用户。这种模式相当于基于口令的用户登录系统，系统好比一个可信任中心，系统中存有用户的口令(相当于私钥)，只要口令对，就通过了身份认证。

第二层次：基于数字证书的公钥认证.CA 通过发布数字证书的形式向用户分发公钥，私钥由用户保存.私钥既可以由用户自己产生，也可以由 CA 产生，并安全地传送给用户。数字证书中主要存放公钥和 CA 利用自己的私钥对用户公钥的签名等信息.任何用户都可以使用 CA 的公钥对数字证书中的签名进行验证，判断数字证书的有效性，也就证明了公钥的有效性，从而达到对身份认证的最终目的。这种模式依赖于 CA 签名的正确性验证，仍然存在 CA 假冒用户的可能。

第三层次：基于自证明的公钥认证。公钥由用户和 CA 在公钥分发协议下共同产生，CA 不知道用户的私钥，但 CA 可产生一个公钥的证明，同样地用户也不知道 CA 的私钥，各自私钥对彼此双方都是保密的，这样 CA 就不可能假冒用户，用户也不能怀疑 CA 作弊.任何用户可以通过公钥的证明、用户的身份标识和 CA 的公开密钥计算他的公钥。相比前两种模式而言，这种模式具有更高的安全性。

下面给出的签名方案是在公钥认证的第三层次上进行的，因为用户和 CA 各自的私钥对彼此双方是保密的，所以用户注册获取 CA 对公钥的证明和通信双方身份的相互确认均是在一个交互协议下完成的。

系统初始化阶段

设 CA 选取两个相同大小的大素数 p,q（保密），计算 $n=pq$（公开），$\phi(n)=(p-1)(q-1)$（保密），随机选取一个整数 e（公开），满足 $\gcd(e,\phi(n))=1$，$1\le e\le\phi(n)$，计算 d，满足 $ed=1\bmod\phi(n)$，d 保密，从 Z_n^* 中选取一个与 n 互素的整数 g（公开），选取一个安全的单向的哈希函数 h。

CA 的公开参数：n,e,g,h；CA 的秘密参数：p,q,d。

用户注册阶段

为了使得向 CA 注册的用户获取的公钥具有第三层次的信任等级，因此公钥的分发不能简单地由 CA 产生颁布，同时也为了用户身份的匿名要求，对 CA 也不能暴露，因此公钥的产生由用户与 CA 共同完成一个会话过程动态地产生，把这个注册过程称之为用户注册协议。

Step1：Alice 计算 $h_A=h(ID_A)$，其中 ID_A 代表 Alice 的身份标识，且对 CA 保密，Alice 以匿名 h_A 向 CA 提出注册申请；

Step2：CA 检查、核实用户 h_A 的身份，若通过检查，则 CA 为用户提供服务.CA 任选一个随机数 $k_{CA}\in_R Z_n^*$，计算 $\tilde{r}_A=g^{-k_{CA}}\bmod n$，随即将 $\tilde{r}_A$ 传送给 Alice；

Step3：Alice 收到后，任选一个随机数 $x_A\in_R Z_n^*$ 作为私钥，计算 $v_A=g^{-x_A}\tilde{r}_A^{-1}\bmod n$，

将v_A发给 CA；

Step4：CA 计算$C_A=(v_A\tilde{r}_A-h_A)^d \bmod n$，称 C_A 为 CA 颁发给 Alice 的公钥的证明，并传给他；

Step5：Alice 收到 C_A 后，计算出证明、匿名标识及 CA 的公钥导出的自己的公钥$y_A=C_A^e+h_A$，同时验证等式$C_A^e+h_A=g^{-x_A} \bmod n$是否成立，若成立，则说明证明在传输过程中未被篡改，由 CA 签发的公钥的证明 C_A 是有效的，否则是无效的。

显然只有 CA 才能颁发 Alice 的公钥的证明，因为在注册过程中，CA 使用私钥对 Alice 在协议交互过程中产生的一些特定信息及匿名信息进行签名，任何人是无法伪造的，其安全性程度高。如果攻击者企图获取 Alice 的私钥，那么他将面临求解离散对数的困难，如果攻击者企图伪造 CA 的公钥的证明，那么他将面临求大素数的因子分解的困难。

公钥的验证阶段

假设 Alice 欲与 Bob 通信，他们从 CA 处获得各自公钥的证明分别为C_A和C_B. Bob 对 Alice 的公钥进行自证明需要执行如下过程才能完成，与 2.2 节一样，称这个过程为公钥的自证明协议。

Step1：Alice 任选一个随机数$r_A\in_R Z_n^*$，计算$t_A=g^{r_A} \bmod n$，将(h_A,C_A,t_A)传给 Bob；

Step2：Bob 收到后，计算$p_A=C_A^e+h_A$，再任选一个随机数$k\in_R Z_n^*$传给 Alice；

Step3：Alice 计算$s_A=r_A-x_Ak \bmod n$，将s_A传给 Bob；

Step4：Bob 收到s_A后，验证等式$g^{s_A}=p_A^k t_A(\bmod n)$是否成立，若成立，则说明 Alice 的公钥是由 CA 签发的证明导出的，是有效的，因此他相信与他通信的正是 Alice，此时$p_A=y_A$。

定理 5.2.1：Alice 的公钥经验证阶段的协议过程完成验证后，可以正确地验证 Alice 的证明是由 CA 颁发的，同时也验证了 Alice 的公钥是有效的。

证明：因为$p_A=C_A^e+h_A=v_A\tilde{r}_A=g^{-x_A} \bmod n$，$s_A=r_A-x_Ak \bmod n$，则有$g^{s_A}=g^{r_A}(g^{-x_A})^k=p_A^k t_A(\bmod n)$.这个等式成立说明了前面的条件$p_A=g^{-x_A} \bmod n$是正确的，而这个条件隐含了只可能是 CA 的 RSA 签名才能产生这个结果，正好说明 Alice 的证明是由 CA 颁发的。

最后等式中含有 Alice 的私钥，而私钥是代表个人身份的，其他任何攻击者要想获取私钥将面临求解离散对数的难题，只有 Alice 才能完成协议过程产生签名，由此说明与之通信的正是 Alice。

签名阶段

假设 Alice 欲向 Bob 发送消息 m，在完成通信双方对对方身份的相互确认后，发送方已经获得接收方的公钥 y_B，Alice 任意选取随机整数$k\in_R Z_n^*$，称为消息密钥，计算$r=h(y_B^k)^{-1}m(\bmod n)$，$s=k-x_Ar \bmod n$，则$(r,s)$为 Alice 对消息 m 的签名。

消息恢复阶段

Bob 收到签名 (r,s) 后，采用发送方的公钥恢复原消息：$m = rh(y_B^s y_A^{sr}) \bmod n$。验证是非常容易的.因为 $s = k - x_A r$，所以 $y_B^k = y_B^s y_B^{x_A r} = y_B^s g^{-x_B x_A r} = y_B^s g^{-x_A s r} = y_B^s y_A^{sr} \bmod n$，从而 $m = rh(y_B^k) = rh(y_B^s y_A^{sr}) \bmod n$。

安全性分析

(1)用户 Alice 的公钥的证明 C_A 是由 CA 颁发的，任何攻击者不可能伪造 CA 的证明.因为 $C_A = (v_A \tilde{r}_A - h_A)^d \bmod n$，只有 CA 拥有私钥 d，其他任何人不可能计算，攻击者将面临大素数的因子分解困难.同时用户的注册过程是在交互对话协议中完成的，属于第三层次的信任等级，具有很高的安全性。

(2)攻击者仿造签名人 Alice 的概率很小，可以忽略不计.假设一个攻击者试图仿造 Alice 对一个任意的消息 m_1 的一个有效的签名，他首先任意地选取一个固定的 r，然后再选取 s，他虽然不知道 Alice 的私钥 x_A，但他猜对的概率为 $1/n$，因此他伪造一个有效签名的概率为 $1/n^2$，由于这个概率非常小，可以忽略不计。

(3)攻击者截取签名 (r,s) 后，试图破解它，但因不知道接收者的私有密钥 x_B，无法根据消息恢复方程求解得到 m，只有消息接收者才可能求解，而且消息接收者是一个特定的接收者，他与消息发送者之间的相互确认是通过用户公钥的自认证协议实现的。

(4)消息密钥 k 只能使用一次，不能重复使用，否则，私钥 x_A 将可能被恢复.对于不同的消息 m_1, m_2，使用相同的消息密钥 k，产生两个消息签名 (r_1,s_1)，(r_2,s_2)。此时 $s_1 = k - r_1 x_A \bmod n$，$s_2 = k - r_2 x_A \bmod n$，因 $s_1 - s_2 = (r_2 - r_1) x_A \bmod n$。如果 $r_1 \neq r_2$，则有 $x_A \equiv (r_2 - r_1)^{-1}(s_1 - s_2) \bmod n$，从而攻击者可以恢复 x_A。

5.3 具有消息链接恢复的自认证签名方案

上述方案在信息量 m 较大且超过大素数 n 时，就不适用了.虽然可以采取分块的办法将消息分为若干块，表为 $m = \{m_1, m_2, \cdots, m_t\}$，使得每一个子块 $m_i < n$，然后对每一个子块分别进行签名 (r_i,s_i).但是消息接收者无法确定消息在传输过程中是否被重排、重发或删除，而且传输的信息量太大.因此一个自然的想法是如何降低通信量，同时又能把消息按正确的顺序恢复，于是采用递推形式对分块消息签名，使得恢复消息时也只能进行递推运算才可能一个一个地恢复，从而大大地减少了通信传输量。

假设系统参数和上述方案一致，通信各方已经向 CA 完成注册会话协议，获得了相应的公钥的证明。

签名阶段

Alice 向 Bob 发送信息 $m=\{m_1,m_2,\cdots,m_t\}$，与上述方案一样在完成通信双方的公钥自证明协议后，Alice 获得了 Bob 的证明 C_B 和身份匿名标识 h_B，然后进行签名操作，步骤如下：

Step1：任意选取某一随机数或伪随机数 $k\in_R Z_n^*$，令 $r_0=0$；

Step2：计算 $b=y_B^k=(C_B^v+h_B)^k \bmod n$，若 $b=\vec{0}$，则返回到 Step1；

Step3：计算 $r_i=m_i h(r_{i-1}\|b)^{-1} \bmod n$，$i=1,2,\cdots,t$，$r=h(r_1\|r_2\|\cdots\|r_t)$，其中符号“‖”表示连接；

Step4：计算 $s=k-x_A r \bmod n$，如果 $s=0$，则返回到 Step1；

Step5：Alice 对消息 m 的签名为 $(r,s,r_1,r_2,\cdots,r_t)$。

消息恢复阶段

Bob 收到签名 $(r,s,r_1,r_2,\cdots,r_t)$ 后，采取如下步骤恢复消息：

Step1：验证 $r,s,r_1,r_2,\cdots,r_t$ 是 $[1,n-1]$ 中的整数；

Step2：计算 $r'=h(r_1\|r_2\|\cdots\|r_t)$，若 $r'\neq r$，则签名不成立；

Step3：计算 $b=y_B^s y_A^{sr'} \bmod n$；

Step4：计算 $m_i=r_i h(r_{i-1}\|b) \bmod n$，其中 $r_0=0$，连接起来即为原消息串 $m=\{m_1,m_2,\cdots,m_t\}$。

事实上，可以验证上述消息恢复过程.因为 $s=k-x_A r \bmod n$，$r=h(r_1\|r_2\|\cdots\|r_t)$，则有 $y_B^k=y_B^s y_B^{sr'}=y_B^s(g^{-x_A})^{sr'}=y_B^s(g^{-x_A})^{sr'}=y_B^s y_A^{sr'} \bmod n$。

又因为消息发送者 Alice 的公钥为 $y_A=C_A^v+h_A \bmod n$，所以 Bob 得到签名后，计算 $b=y_B^k=y_B^s y_A^{sr'} \bmod n$，再根据 $r_i=m_i h(r_{i-1}\|b)^{-1} \bmod n$，得 $m_i=r_i h(r_{i-1}\|b) \bmod n$，从而恢复原消息 $m=\{m_1,m_2,\cdots,m_t\}$。

安全性分析

(1)攻击者从用户的公钥的证明 C_A 可以计算得到用户的公钥 y_A，但由于 $y_A=g^{-x_A} \bmod n$，从中获取用户的私钥 x_A 是不可能的，这将面临求解离散对数的难题。

(2)攻击者截取签名 $(r,s,r_1,r_2,\cdots,r_t)$ 后，试图获取消息 m_i，但因不知道接收者的私有密钥 x_B，从而无法计算 b，因而不可能计算 $m_i=r_i h(r_{i-1}\|b) \bmod n$.换句话说，只有特定的消息接收者 Bob 才可能恢复消息。

(3)若攻击者获取了明文 $m=\{m_1,m_2,\cdots,m_t\}$ 的签名 $(r,s,r_1,r_2,\cdots,r_t)$，因为 $h(r_{i-1}\|b)=m_i r_i^{-1} \bmod n$，hash 函数 $h(\cdot)$ 是安全的，保证了已知明文的攻击是困难的，也就是说不可能从中求得 b。

(4)消息密钥 k 不能重复使用，即不同的消息签名应使用不同的消息密钥.否则，私钥 x_A 将可能被恢复。

计算时间效率的比较

本文所提出的具有消息恢复的公钥自证明的认证加密方案是在 Girault 的自证明

公钥理论基础上进行设计的，因此，系统的基本参数仍然采用 Girault 所提出的建议：认证机构 CA 选取的秘密参数 p,q 应在 350 位(指二进制位)以上，用户选取的私钥应在 160 位以上。为便于比较各方案的计算时间复杂性，仍然采用文献[55]的表示符号：Th 表示执行一次 hash 函数的时间开销，Tmul 表示两个数相乘的时间开销，Tmmul 表示在整数模的意义下两个数乘积的时间开销，Texp 表示整数模的意义计算指数的时间开销，Tinv 表示在整数模的意义下计算逆的时间开销.但需要说明三点：1）本文使用的签名方程是 $s_A = r_A - x_A k \bmod n$，变量的计算是在整数模的意义下进行的，主要的好处是可以求整数的逆元，从而可以将签名方程进行推广，而在文献[55]中却不能进行逆运算。2）为便于和文[55]进行对比，对本文的方案而言，Tmul 特指在签名方程中的两个整数的乘积的时间开销(它实际上和 Tmmul 是相等的)。3）本文消息分块数记为 t，文[55]中记为 n，这里统一记为 t，各方案在签名阶段和验证阶段的计算时间对比如表 5.3.1 所示。

表 5.3.1　各方案计算时间对比表

	方案	签名阶段	验证阶段	总的时间
No.1	Tseng[55]的消息恢复签名方案	Texp+Th+Tinv +Tmmul+Tmul	3Texp+2Th +2Tmmul	4Texp+3Th+Tinv +3Tmmul+Tmul
No.2	Tseng[55]的认证加密方案	2Texp+Th+Tinv +Tmmul+Tmul	4Texp+2Th +2Tmmul	6Texp+3Th+Tinv +3Tmmul+Tmul
No.3	Tseng[55]的具有消息链接恢复的认证加密方案	2Texp+(t+2)Th+Tinv +tTmmul+Tmul	4Texp+(t+2)Th +(tInv+(t+1)Tmmul	6Texp+2(t+2)Th+(t+1)Tinv +(2t+1)Tmmul+Tmul
No.4	本文的具有消息恢复的认证加密方案	Texp+Th+Tinv +Tmmul+Tmul	2Texp+Th +Tmul+Tmmul	3Texp+2Th+Tinv +2Tmul+2Tmmul
No.5	本文的具有消息链接恢复的认证加密方案	2Texp+(t+1)Th+tTinv +tTmmul+Tmul	2Texp+(t+1)Th +(t+1)Tmmul+Tmul	4Texp+2(t+1)Th+tTinv +(2t+1)Tmmul+2Tmul

从表 5.3.1 中可以看出，方案 No.4 在签名产生阶段，时间开销为 Texp+Th+Tinv+Tmmul+Tmul，验证阶段的时间开销为 2Texp+Th+Tmul+Tmmul，总的时间开销为 3Texp+2Th+Tinv+2Tmul+2Tmmul，比方案 No.1 的时间开销少 Texp+Th，比 No.2 的时间开销少 3Texp+Th，从这个角度来讲，方案 No.4 优于方案 No.2 和 No.3. 同样的道理，方案 No.5 也优于方案 No.3。

安全性的比较

（1）方案 No.1 和 No.2 不能算做第三层次的公钥自证明的认证加密方案

这两个方案系统初始化阶段是相同的。一方面，攻击者一旦得到了用户的标识 ID_i 后，完全可以象用户一样，做相同的操作，可以获得由 CA 颁发的自证明公钥，从而可以冒充用户。另一方面，攻击者截获 (p_i, ID_i) 后，可以冒充 CA 产生用户 U_i 的公钥 y_i，且完全能够经得起用户的自验证.因为验证方程 $y_i^{h(ID_i)} + ID_i = g^{x_i} \bmod n$ 中没有包含 CA 的任何私有信息，显然任何人都可以冒充.这样一来，CA 的公钥的权威受到挑战，其

后果是 CA 可以对发布的公钥抵赖，不承担任何责任;用户也可以避开 CA，自己计算公钥.这和用户的某种标识 ID 一样，显然不能作为代表用户身份的公钥。如果 CA 颁发的公钥附带 CA 的权威标识或者某种验证方法的话，这相当于第二层次的信任等级--基于数字证书的公钥认证，不能作这第三层次的自证明公钥认证。

（2）方案 No.4 是建立在第三层次的公钥自证明的认证加密方案

①CA 和用户双方对各自的私钥都是保密的，从而不存在冒充对方的问题.在用户注册阶段，用户公钥的产生是根据 RSA 算法进行设计实现的.只有 CA 才能颁发用户的公钥的证明，用户根据 CA 颁发的证明得到一个自证明的公钥。

②CA 可以在系统内公开公钥，但公钥代表谁呢?通信双方只有完成公钥的相互认证后才能确信对方，通信双方可以对公钥进行互证明，并用到了 CA 的公钥.因此这是可以自验证的公钥。

③虽然通信双方可以通过 Differ-Hallman 交互协议进行通信双方的认论，但限于通信双方的相互信任基础上.如果一旦发生纠纷，没有第三方做证，也没有承担风险责任的第三方.公钥的互认证过程使用了 CA 颁发的公钥的证明及 CA 的公钥 e，这些都可以用来作为凭证，保证通信双方的安全。

（3）方案 No.1 不具有消息的保密性，方案 No.2 和方案 No.4 具有消息的保密性

任何攻击者获取签名后，都可以根据发送者的公钥 y_i 和身份标识 ID_i 计算恢复原消息，因此，该方案不具有消息的保密性.方案 No.2 和方案 No.4 指定了特定的接收者，任何其他人都无法恢复原消息，因此，具有消息保密性.上述三个签名方案都是通过增加消息冗余位来判断消息的发送者，显然均具有身份认证性。

（4）方案 No.4 和 No.5 具有匿名性

用户向 CA 注册时，是用 $h_A = h(ID_A)$ 进行注册登记的，CA 不知道 h_A 代表的究竟是谁，但对颁发过的公钥的证明 C_A 予以承认和证实，这样保护了用户的隐私，也保障了用户的权益.当出现纠纷时，CA 可以作为第三方进行仲裁。文[54]中的方案，存在的一个问题是 CA 可以冒充用户进行签名.这必须建立在 CA 高度信任的基础上.这不符合自证明公钥密码体制的思想。

5.4 本章小结

本章主要基于 Girault 的公钥自证明思想展开研究，主要做了以下的工作:

1.概要地介绍了公钥自证明的思想和公钥自证的三个信任等级，我们研究的方案是在公钥自证明的基础上进行的，属于第三层次的信任等级。

2.提出了一种基于公钥自证明的认证加密方案，该方案主要针对原方案所做的改

进在于:在用户注册阶段通过公钥自证明原理进行用户自验证，在消息恢复阶段，通过技术处理，用户不需要发送原消息，只需要发送签名，限于特定的接收者能接收签名恢复消息。这种方案体现公钥自证明的思想和实现手段更完备，对用户而言进行匿名身份注册，保证了用户的匿名要求,而且该方案相比 Tseng[55]的方案具有通信量小、抗攻击性强等优点。

3.当消息量很大需要分组的情况，在上述方案的基础上提出了具有消息链接恢复的处理办法，并进行了计算时间复杂性和安全性的分析比较。表明链接恢复比分块签名的计算效率高。

本章评注

评注 5.1 本章探讨在通信过程中，如何通过公钥进行身份的自证明，这种思想有效地满足了用户对身份的匿名性要求，这是公钥自证明方案的最大特点。

评注 5.2 在本章提出的方案中,由于用户进行匿名身份注册的协议过程比较复杂，实际上等于增加了计算时间，比基于数字证书的身份认证在计算时间上明显慢，正因为如此，使得公钥自证明方案在应用中遇到了障碍，这也是目前较少有这方面的实际应用系统的原因。

评注 5.3 在数字签名过程中，作为用户的匿名性身份认证要求是合情合理的，继续探讨这一课题具有实际意义，把公钥自证明方法和盲签名技术结合起来，有可能设计出具有较好完备性的具有匿名要求的身份认证方案。

6　盲签名方案

6.1　引言

盲签名是一种特殊的数字签名，它与通常的数字签名的不同之处在于，签名者并不知道他所要签发文件的具体内容。正是这一特点，使得盲签名这种技术可广泛应用于许多领域，如电子投票系统和电子现金系统等。自 1982 年 Chaum 首次提出盲签名概念以来，取得了丰硕的成果，学者们提出了许多新的签名方案，如强盲签名、弱盲签名、部分盲签名、代理盲签名等。

本章首先对盲签名进行分类，然后提出构造广义 ElGamal 型弱盲签名的方法。关于代理盲签名，分别提出了一种构造方法、基于多元线性变换的代理盲签名、基于椭圆曲线的代理盲签名、具有消息恢复的代理盲签名等。

6.2　盲签名的分类及联系

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[82]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，仍然沿着祁明的思路进行如下的分类：

(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 $sig(m')$ 进行了盲化。若签名者保留 $sig(m')$ 及有关数据，待 $sig(m)$ 公开后，签名者可以找出 $sig(m')$ 和 $sig(m)$ 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 $sig(m')$ 进行了盲化。即使签名者保留 $sig(m')$ 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。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。

6.3 广义 ElGamal 型弱盲签名的构造方法

6.3.1 引言

在盲签名概念提出以后，人们致力于构造各种各样的盲签名方案[38,79]。祁明[82]将盲签名方案分为四类：盲消息签名、盲参数签名、弱盲签名和强盲签名。姚小峰[39]在广义 ElGamal 型签名方案[63]的基础上基于二元仿射变换构造了强盲签名方案和弱盲签名。杜伟章[84]提出的构造弱盲签名方案的方法实际上是文献[39]的特例。这一节着重从签名方程的特点出发，分类总结了包含 ElGamal 型签名方案在内的更为广泛的签名方案，以这些签名方案为基础，构造相应的弱盲签名方案，它们几乎包含了所有该类弱盲签名方案。

6.3.2 CPS 弱盲签名

CPS 弱盲签名方案[38]包含系统初始化、签名过程和验证过程，具体叙述如下。

系统初始化过程

p是一个大素数，q是$p-1$的一个大素数因子，整数$g\in(1,p-1)$且阶为q，即$g^q\equiv 1 \bmod p$。设A为消息m的拥有者，B为签名者，它的私钥为x，$1<x<p-1$，公钥为$y=g^x \bmod p$。

签名过程

Step1：A向B发出请求，希望他为自己的消息签名；

Step2：B接到请求后，若同意的话，他任意选取一个随机数$k'(1<k'<p-1)$，计算$r'=g^{k'} \bmod p$，将r'传送给A；

Step3：A收到后，随机地选取两个整数α,β，计算$r=(r')^{\alpha}g^{\beta} \bmod p$，$m'=\alpha r'r^{-1}m \bmod q$，将$m'$传送给B；

Step4：B收到盲消息m'后，计算$s'=k'm'+r'x \bmod q$，并将s'传送给A；

Step5：A计算$s=s'r(r')^{-1}+m\beta \bmod q$，这样A得到了消息m的签名$sig(m)=(r,s)$。

验证过程

消息接收者或签名验证者容易验证签名的正确性.若m和(r,s)满足方程$g^s=y^r r^m \bmod p$，则接受签名，否则拒绝接受。

当A公开$sig(m)=(r,s)$后，B已保留(r',s')，B计算$\alpha'=m'm^{-1}(r')^{-1}r \bmod q$，

$\beta'=m^{-1}(s-s'r(r')^{-1}) \bmod q$，若$r=(r')^{\alpha'}g^{\beta'} \bmod p$成立，则可确认$sig(r',s')$与$sig(r,s)$相联系。

6.3.3 ElGamal型弱盲签名方案的构造

假定系统参数和符号约定同上，在构造弱盲签名方案时必须满足的条件是盲消息的签名方程与原消息的签名方程在形式上必须相同。设签名人B对盲消息的签名方程为$a'k'=b'+c'x \bmod q$，其中向量(a',b',c')是参数$(\pm r',\pm m',\pm s')$的某一置换或线性组合，原始签名人A通过变量转换所得的签名变量s和r也必须满足相应的签名方程$ak=b+cx \bmod q$，且向量(a,b,c)是参数$(\pm r,\pm m,\pm s)$的对应的某一置换或线性组合。

比如，盲消息签名方程为$s'=r'x-k'm' \bmod q$，要求原消息的签名方程也应为$s=rx-km \bmod q$，又因为$r=(r')^{\alpha}g^{\beta} \bmod p=g^{\alpha k'+\beta} \bmod p$，即有$k=\alpha k'+\beta \bmod q$，从而得方程组：

$$\begin{cases} s'=r'x-k'm' & (1) \\ s=rx-km & (2) \\ k=\alpha k'+\beta & (3) \end{cases}$$

解此方程组，从(2)中得$x=r^{-1}(s+km)$　(4)，将(4)代入(1)得

$r'r^{-1}(s+km)-k'm'-s'=0$　(5)，又将(3)代入(5)并化简得

$(\alpha r'r^{-1}m-m')k'+r'r^{-1}s+r'r^{-1}\beta m-s'=0$，该方程是一个关于任意变量$k'$的恒等式，所

以有

$\alpha r' r^{-1} m - m' = 0$，$r' r^{-1} s + r' r^{-1} \beta m - s' = 0$，故得 $m' = \alpha r' r^{-1} m \bmod q$，$s = r(r')^{-1} s' - \beta m \bmod q$。

根据上面的推导，得到了盲消息与原消息的关系式，以及签名变量与盲签名变量的关系式，据此可以仿照上面的协议过程得到盲签名方案.在以广义 ElGamal 型[63]18 个安全的签名方案为基础构造的弱盲签名方案中不同的签名方程、消息盲化方程和签名变量方程列在表 6.3.3.1 中，签名正确性的验证式也有相应的变化，在此略去。

表 6.3.3.1　签名方程、消息盲化方程和签名变量方程表

分类		签名方程	消息盲化方程	签名变量方程
S1	(1)	$mx = rk + s \bmod p-1$	$m' = \alpha^{-1} r^{-1} r' m \bmod p-1$	$s = m(m')^{-1} s' - \beta r \bmod p-1$
	(2)	$mx = sk + r \bmod p-1$	$m' = r^{-1} r' m \bmod p-1$	$s = \alpha^{-1} m (m')^{-1} s' \bmod p-1$
	(3)	$rx = mk + s \bmod p-1$	$m' = \alpha r^{-1} r' m \bmod p-1$	$s = r(r')^{-1} s' - \beta m \bmod p-1$
	(4)	$rx = sk + m \bmod p-1$	$m' = r^{-1} r' m \bmod p-1$	$s = \alpha^{-1} r (r')^{-1} s' \bmod p-1$
	(5)	$sx = rk + m \bmod p-1$	$m' = \alpha^{-1} r^{-1} r' (m + \beta r) \bmod p-1$	$s = \alpha r (r')^{-1} s' \bmod p-1$
	(6)	$sx = mk + r \bmod p-1$	$m' = \alpha r' (\beta m + r)^{-1} m \bmod p-1$	$s = \alpha m (m')^{-1} s' \bmod p-1$
S2	(7)	$mrx = k + s \bmod p-1$	$m' = \alpha^{-1} r (r')^{-1} m \bmod p-1$	$s = m(m')^{-1} r (r')^{-1} s' - \beta \bmod p-1$
	(8)	$x = mrk + s \bmod p-1$	$m' = \alpha r (r')^{-1} m \bmod p-1$	$s = s' - \beta r m \bmod p-1$
	(9)	$sx = k + mr \bmod p-1$	$m' = \alpha^{-1} (r')^{-1} (mr + \beta) \bmod p-1$	$s = \alpha s' \bmod p-1$
	(10)	$x = sk + rm \bmod p-1$	$m' = r (r')^{-1} m \bmod p-1$	$s = \alpha^{-1} s' \bmod p-1$
	(11)	$rmx = sk + 1 \bmod p-1$	$m' = r (r')^{-1} m \bmod p-1$	$s = \alpha^{-1} mr (m'r')^{-1} s' \bmod p-1$
	(12)	$sx = mrk + 1 \bmod p-1$	$m' = \alpha mr (r')^{-1} (mr\beta + 1)^{-1} \bmod p-1$	$s = \alpha mr (m'r')^{-1} s' \bmod p-1$
S3	(13)	$(r+m)x = k + s \bmod p-1$	$m' = \alpha^{-1} (m + r) - r' \bmod p-1$	$s = \alpha s' - \beta \bmod p-1$
	(14)	$x = (m+r)k + s \bmod p-1$	$m' = \alpha (m + r) - r' \bmod p-1$	$s = s' - \beta (m + r) \bmod p-1$
	(15)	$sx = k + (m+r) \bmod p-1$	$m' = \alpha^{-1} (m + r + b) - r' \bmod p-1$	$s = \alpha s' \bmod p-1$
	(16)	$x = sk + (r+m) \bmod p-1$	$m' = (m + r - r') \bmod p-1$	$s = \alpha^{-1} s' \bmod p-1$
	(17)	$(r+m)x = sk + 1 \bmod p-1$	$m' = (m + r - r') \bmod p-1$	$s = \alpha^{-1} (r+m)(r'+m')^{-1} s' \bmod p-1$
	(18)	$sx = (m+r)k + 1 \bmod p-1$	$m' = \alpha (m+r)[\alpha (m+r) + b]^{-1} - r' \bmod p-1$	$s = \alpha (m+r)(m'+r')^{-1} \bmod p-1$

两点说明：

(1)上述所有 18 个广义的盲签名方案均为弱盲签名方案，即当消息拥有者公布签名后，签名者可以找出它们之间的内在联系，从而达到对消息拥有者的追踪。

(2)表 1 的方案 2、4、10、11、16 和 17，它们的签名过程的 Step2 应做相应的修改，以方案 2 为例进行说明.当 A 收到 r' 后，随机地选取一个整数 α，计算 $r = (r')^{\alpha} \bmod p$，$m' = r' r^{-1} m \bmod q$，将 m' 传送给 B;另外，签名的验证过程也应做修改.仍以方案 2 进行说明，当 A 公开签名 (r,s) 后，签名者 B 可求得 $\alpha' = m(m')^{-1} s' s^{-1} \bmod q$，若 $r = (r')^{\alpha'} \bmod p$ 成立，则可确认而确认 $sig(r',s')$ 与 $sig(r,s)$ 相联系。

6.3.4 ElGamal 型弱盲签名方案的推广

除 18 种广义 ElGamal 型签名方案外，实际上签名方程的参数选取远不止这些，下面将要给出的两个结论表明，在这些签名方案的基础上借助于上面的方法照样可以构造盲签名方案。

结论 1：签名方程中的未知向量 (a,b,c) 可以是向量 $(1,m,rs)$、$(1,r,ms)$、$(m+s,1,r)$ 和 $(r+s,1,m)$ 的一个任意置换，且参数前搭配不同的符号可以构成若干种不同的签名方程，在这些签名方案的基础上可以构造相应的盲签名方案。

结论 2：签名方程中的未知向量 (a,b,c) 可以取自集合 $\{m,1,r,mr,ms,sr,rs\}$ 中的三个有效元素的一个任意置换或线性组合，但所选取的元素中必须含有 m，这些不同组合可以构成若干种盲签名方程。

不妨以签名方程 $srx=k+m \bmod p-1$ 为例进行说明。系统参数和签名阶段的第一步是相同的，从第二步开始做相应的修改就可以了。

Step2：A 收到后，随机地选取两个整数 α,β，计算 $r=(r')^{\alpha}g^{\beta} \bmod p$，$m'=\alpha^{-1}(\beta+m) \bmod q$，将 m' 传送给 B；

Step3：B 收到盲消息 m' 后，计算 $s'=(r'x)^{-1}(k'+m') \bmod q$，并将 s' 传送给 A；

Step4：A 计算 $s=\alpha r^{-1}r's' \bmod q$，这样 A 得到了消息 m 的签名方案 $sig(m)=(r,s)$。

验证过程：容易验证消息 m 及其签名(r，s)应满足验证方程 $y^{sr}=rg^{m} \bmod p$，否则，拒绝接受签名。当消息拥有者 A 公开 m 的签名(r，s)后，签名者 B 可求得 $\alpha'=r(r')^{-1}s(s')^{-1} \bmod q$，$\beta'=(r(r')^{-1}s(s')^{-1}m'-m) \bmod q$，若满足 $r=(r')^{\alpha'}g^{\beta'} \bmod p$，则可确认 $\alpha'=\alpha$，$\beta'=\beta$，从而确认 $sig(r',s')$ 与 $sig(r,s)$ 相联系。

6.4 代理盲签名方案的构造方法

6.4.1 引言

盲签名概念的提出是为了保护消息拥有者隐私的问题，而 Mambo 等[12]人提出的代理签名的概念是为了把签名人的签名权授权给代理人、由代理人代表原始签名人行使签名的权利而进行设计的，消息接收者或签名验证者可以区分是普通签名还是代理签名。之后，Lee 和 Chang[14]提出了保护代理的代理签名方案，同年，Lin 和 Jan[85]第一个提出了代理盲签名方案。最近，Tan 等[44,86]人提出了一种基于 Schnorr 盲签名的代理盲签名方案，这种方案既具有盲签名的性质又具有代理签名的性质。Lai 和 Awasthi[45]于 2003 年提出了一种代理盲签名方案，该方案以 Mambo[12]的方案为基础，

比 Tan 的方案计算简单。

本节分析了代理签名方案的特点，以 Lai 和 Awasthi 的方案为基础，提出了构造代理盲签名方案的一般方法，并以 4 个 ElGamal 型签名方案为基础构造了相应的代理盲签名方案，并对其安全性进行了分析。

6.4.2 ElGamal 型代理盲签名方案

系统参数及符号约定

p 是一个大素数，q 是 $p-1$ 的一个大素数因子，整数 $g\in(1,p-1)$ 且阶为 q，即 $g^q\equiv 1 \bmod p$。系统中 A 为原始签名人。私钥为 x_A。公钥为 $y_A=g^{x_A} \bmod p$，B 为代理签名人，私钥为 x_B，公钥为 $y_B=g^{x_B} \bmod p$，C 为消息 m 的拥有者。

委托阶段

Step1：(代理产生阶段)A 随机地选取整数 $k_A\in Z_q^*$，$k_A\neq 1$，计算 $r_A=g^{k_A} \bmod p$，$\tilde{a}k_A=\tilde{b}+\tilde{c}x_A \bmod q$，其中向量 $(\tilde{a},\tilde{b},\tilde{c})$ 可以是 $(\pm r_A,\pm\sigma,\pm 1)$ 的某一个置换。从中解出 $\sigma=\sigma(k_A,x_A,r_A)$，计算 $y_p=g^{\sigma}y_B \bmod p$，称 y_p 为 A 授权给特定代理签名人 B 的授权签名公钥，在系统内公开。

Step2：(代理传递阶段)A 安全地将 (σ,r_A) 传递给代理签名人 B。

Step3：(代理验证阶段)B 收到 (σ,r_A) 后，验证是否成立 $y_p=g^{\sigma}y_B \bmod p$，如果成立，则 B 接受 A 的委托，代表 A 签名，并计算 $s_p=\sigma+x_B \bmod q$，称 s_p 为 A 授权给 B 的授权签名密钥；否则，拒绝接受 A 的委托。

代理签名阶段

Step1：B 随机地选取整数 $k_B\in Z_q^*$，$k_B\neq 1$，计算 $r_B=g^{k_B} \bmod p$，将 r_B 传递给 C；

Step2：C 随机地选取两个整数 $\alpha,\beta\in Z_q^*$，计算 $r_{t'}=r_Bg^{\beta}y_p^{\alpha} \bmod p$，如果 $r_{t'}=0$，他重新选取 α,β。否则计算 $e=h(r_{t'}\|m)$，“$\|$”表示字符串或整数的二进制表示的连接，计算 $e'=e'(e,\alpha,\beta) \bmod q$，其中 e' 出下面的注释推导导出。C 将 e' 传递给 B；

Step3：B 收到 e' 后，计算 $ak_B=b+cs_p \bmod q$，其中向量 (a,b,c) 可以是 $(\pm s',\pm e',\pm 1)$ 的某一个置换.从中解出 s' 并传送给 C，B 保留盲签名 (s',e')；

Step4：C 计算 $s=s(s',\alpha,\beta,e) \bmod q$，其中 s 也出下面的注释推导导出.则 (m,s,e) 就是 B 代表 A 对消息 m 的代理盲签名。

代理签名的验证阶段

代理盲签名的接收者或验证者收到 (m,s,e) 后，计算 $\tilde{e}=(h(g^{a^{-1}b+\beta}y_p^{a^{-1}c+\alpha} \bmod p)\|m) \bmod q$，如果 $\tilde{e}=e$ 成立，则 (m,s,e) 就是消息 m 的有效的代理盲签名。否则，拒绝接受该签名。

在消息拥有者 C 公布签名(m,s,e)后，B 计算$\alpha=\alpha(s,s',e,e')$和$\beta=\beta(s,s',e,e')$，其中α,β由上面的关系式推出，如果满足$e=(h(g^{a^{-1}b+\beta}y_p^{a^{-1}c+\alpha} \bmod p)\| m) \bmod q$，则他可以从中推断 C 的签名就是由他自己的代理签名产生的。

注释：因为 B 关于签名密钥s_p的签名方程为$ak_B=b+cs_p \bmod q$，其中向量(a,b,c)是$(s',e',1)$的某一置换，原始信息拥有者 C 的签名方程也应为$a'k_{t'}=b'+c's_p \bmod q$，所以要求向量$(a',b',c')$选取的参数与向量$(a,b,c)$选取的参数在形式上是相同的，只不过是$(s,e,1)$的对应的置换。比如$(a,b,c)=(1,e',s')$，那么$(a',b',c')=(1,e,s)$。同时，记$k_{t'}=k_B+\beta+\alpha s_p \bmod q$，则$r_{t'}=g^{k_{t'}} \bmod p$，显然$k_{t'}=(a^{-1}b+\beta)+(a^{-1}c+\alpha)s_p \bmod q$，这样得方程组：

$$\begin{cases} a^{-1}b+\beta=(a')^{-1}b' \\ a^{-1}c+\alpha=(a')^{-1}c' \end{cases}$$

不妨将方程组中的变量e',s设为未知变量，其余变量为已知变量，从中解出e',s，记$e'=e'(e,\alpha,\beta) \bmod q$，$s=s(s',\alpha,\beta,e) \bmod q$。

定理 6.4.2.1：在上述代理盲签名方案中，设系统参数及协议过程不变，代理签名阶段 Step3 的签名方程可供选择的形式有$(1,s',e')$、$(1,e',s')$、$(e',1,s')$、$(e',s',1)$等，加上符号变化，各有 4 种不同的形式，共有 16 种不同的代理盲签名方案，而且均是代理盲签名方案，其中 4 种方案的变量替换、签名方程和验证关系式如表 6.4.2.1 所示。

表 6.4.2.1　代理签名方案变量替换、签名方程和验证关系式表

N	$e'=e'(e,\alpha,\beta) \bmod q$	$ak_B=b+cs_p \bmod q$	$s=s(s',\alpha,\beta,e) \bmod q$	$\tilde{e}=(h(g^{a^{-1}b+\beta}y_p^{a^{-1}c+\alpha} \bmod p)\| m)$
1	$e'=e-\alpha \bmod q$	$k_B=s'+e's_p \bmod q$	$s=s'+\beta \bmod q$	$\tilde{e}=(h(g^{s'}y_p^{e'} \bmod p)\| m)$
2	$e'=e-\beta \bmod q$	$k_B=e'+s's_p \bmod q$	$s=s'+\alpha \bmod q$	$\tilde{e}=(h(g^{e'}y_p^{s'} \bmod p)\| m)$
3	$e'=e(1-e\beta)^{-1} \bmod q$	$e'k_B=1+s's_p \bmod q$	$s=e\alpha+(1-e\beta)s' \bmod q$	$\tilde{e}=(h(g^{e'^{-1}}y_p^{e'^{-1}s'} \bmod p)\| m)$
4	$e'=e(1-e\alpha)^{-1} \bmod q$	$e'k_B=s'+s_p \bmod q$	$s=(e^{-1}-\alpha)\beta+(1-e\alpha)s' \bmod q$	$\tilde{e}=(h(g^{e'^{-1}s'}y_p^{e'^{-1}} \bmod p)\| m)$

从下面的两个具体方案可以看出，当原始签名人公布原消息m和签名(s,e)后，代理签名人可以根据自己保留的签名(s',e')，从中导出与它的联系，从而说明原消息m的签名是由他的代理签名产生的。

6.4.3　代理盲签名方案举例

代理盲签名方案一

系统参数及符号约定同上，对应表 6.4.2.1 中的方案 2。

委托阶段

Step1：A 随机地选取整数$k_A \in Z_q^*$，$k_A \neq 1$，计算$r_A=g^{k_A} \bmod p$，$\sigma=k_A+r_Ax_A \bmod q$，

$y_p = g^{\sigma} y_B \bmod p$， y_p作为 A 签名授权的验证公钥在系统内公开.

Step2：A 将(σ, r_A)安全地传递给代理签名人 B.

Step3：B 收到(σ, r_A)后，验证是否成立$y_p = r_A y_B y_A^{r_A} \bmod p$，如果成立，则 B 接受 A 的委托，代表 A 签名，并计算$s_p = \sigma + x_B \bmod q$，$s_p$将作为签名授权的秘密密钥;否则，拒绝接受.

代理签名阶段

Step1：B 随机地选取整数$k_B \in Z_q^*$，$k_B \neq 1$，计算$r_B = g^{k_B} \bmod p$，将r_B传递给 C.

Step2：C 随机地选取两个整数$\alpha, \beta \in Z_q^*$，计算$r_{C'} = r_B g^{\beta} y_p^{\alpha} \bmod p$，如果$r_{C'} = 0$，他重新选取$\alpha, \beta$.否则计算$e = h(r_{C'} \| m)$，$e' = e - \beta \bmod q$，C 将$e'$传递给 B.

Step3：B 收到e'后，对s_p签名，$s' = s_p^{-1}(k_B - e') \bmod q$，并将$s'$传给 C，B 保留盲签名$(s', e')$.

Step4:C 计算$s = s' + \alpha \bmod q$，则(m, s, e)就是 B 代表 A 对消息 m 的代理盲签名.

代理签名的验证阶段

代理盲签名的接收者或验证者收到(m, s, e)后，计算$\tilde{e} = (h(g^e y_p^s \bmod p) \| m)$，则$\tilde{e} = e$成立，当且仅当$(m, s, e)$是消息 m 的有效的代理盲签名.

在消息拥有者 C 公布签名(m, s, e)后，B 计算$\alpha = s - s' \bmod q$，$\beta = e - e' \bmod q$，若α, β满足$e = (h(r_B g^{\beta} y_p^{\alpha} \bmod p) \| m)$，则他可以判断 C 的签名就是由他的代理签名产生的.

代理盲签名方案二

系统参数及符号约定同上，对应表 6.3.3.1 中的方案 3。代理委托阶段及代理签名阶段第一步与方案一相同，不同的是在代理签名阶段签名人 B 对s_p的签名方程设为$s' = s_p^{-1}(e' k_B - 1) \bmod q$，这样$k_B = (e')^{-1}(1 + s' s_p) \bmod q$，

$k_{C'} = k_B + \beta + \alpha s_p = [(e')^{-1} + \beta] + [(e')^{-1} s' + \alpha] s_p \bmod q$，又设$k_{C'} = (e)^{-1}(1 + s s_p) \bmod q$，因此得:

$e' = e(1 - e\beta)^{-1} \bmod q$，$s = e\alpha + (1 - e\beta) s' \bmod q$。

代理签名阶段

Step2：C 随机地选取两个整数$\alpha, \beta \in Z_q^*$，计算$r_{C'} = r_B g^{\beta} y_p^{\alpha} \bmod p$，如果$r_{C'} = 0$，他重新选取$\alpha, \beta$.否则计算$e = h(r_{C'} \| m)$，$e' = e(1 - e\beta)^{-1} \bmod q$，C 将$e'$传递给 B.

Step3：B 收到e'后，对s_p签名，$s' = s_p^{-1}(e' k_B - 1) \bmod q$，并将$s'$传给 C，B 保留盲签名$(s', e')$.

Step4：C 计算$s = e\alpha + (1 - e\beta) s' \bmod q$，则$(m, s, e)$就是 B 代表 A 对消息 m 的代理盲签名.

代理签名的验证阶段

代理盲签名的接收者或验证者收到(m, s, e)后，计算$\tilde{e} = (h(g^{e^{-1}} y_p^{e^{-1} s} \bmod p) \| m)$，则$\tilde{e} = e$成立，当且仅当$(m, s, e)$是消息 m 的有效的代理盲签名.

若消息拥有者 C 公布签名(m, s, e)后，B 计算$\alpha = e^{-1} s - s' e (e')^{-1} \bmod q$，

$\beta=(e'-e)e^{-1}(e')^{-1} \bmod q$，若$\alpha,\beta$满足$e=(h(r_B g^{\beta} y_p{}^{\alpha} \bmod p)\| m)$，则他可以判断C的签名就是由他的代理签名产生的.

代理盲签名方案三

系统参数、代理委托阶段及代理签名阶段前两步与方案一完全相同，在代理签名阶段Step3签名人B对s_p的签名方程设为$s'=k_B^{-1}(1+e's_p) \bmod q$，这样$k_t=k_B+\beta+\alpha s_p=[(s')^{-1}+\beta]+[(s')^{-1}e'+\alpha]s_p \bmod q$，从而可得到下面的代理签名方案。

Step3：B收到e'后，对s_p签名，计算$s'=k_B^{-1}(1+e's_p) \bmod q$，并将$s'$传给C，B保留盲签名$(s',e')$.

Step4：C计算$s=\alpha+s' \bmod q$，$u=g^{\beta+\alpha s^{-1}(s-\alpha)^{-1}} y_p{}^{\alpha+(e\alpha-\beta)s^{-1}(s-\alpha)^{-1}} \bmod q$，则$(m,s,u,e)$就是B代表A对消息m的代理盲签名.

代理签名的验证阶段

代理盲签名的接收者或验证者收到(m,s,u,e)后，计算$\tilde{e}=(h(g^{s^{-1}} y_p{}^{s^{-1}e} u \bmod p)\| m)$，如果$\tilde{e}=e$成立，则接受签名，否则，拒绝接受签名。

代理盲签名方案四

系统参数、符号约定、代理委托阶段及代理签名阶段前两步与方案一完全相同。

Step3:B收到e'后，对s_p签名，计算$s'=k_B^{-1}(e'+s_p) \bmod q$，并将$s'$传给C，B保留盲签名$(s',e')$；

Step4：C计算$s=\alpha+s' \bmod q$，$u=g^{\beta+e\alpha s^{-1}(s-\alpha)^{-1}} y_p{}^{\alpha+\alpha s^{-1}(s-\alpha)^{-1}} \bmod q$，则$(m,s,u,e)$就是B代表A对消息m的代理盲签名。

代理签名的验证阶段

代理盲签名的接收者或验证者收到(m,s,u,e)后，计算$\tilde{e}=(h(g^{s^{-1}e} y_p{}^{s^{-1}} u \bmod p)\| m)$，如果$\tilde{e}=e$成立，则接受签名，否则，拒绝接受签名.

6.4.4 安全性分析

在这些签名方案中，所有的验证关系式均含有原始签名人的签名授权的验证公钥y_p，这说明最终签名(m,s,e)或(m,s,u,e)是由代理签名方和消息拥有者共同完成的，同时也可以把y_p看作是代理盲签名的验证公钥。这些方案具有共同的基本性质：

(1)基本签名的不可伪造性

在这些代理盲签名方案中，B难以根据他所得到的(σ,r_A)计算出A的私钥x_A，从而不能伪造A的普通数字签名。其安全性是基于离散对数问题的难解性，由此也说明任何其他攻击者都难以伪造A的普通数字签名。

(2)代理签名的不可伪造性

出签名授权的秘密密钥 $s_p = \sigma + x_B \bmod q$ 可以看出，由于只有 B 才能生成 s_p，因此除了 B 以外，任何其他人(包括 A 在内)都难以伪造一个有效的代理签名。

(3)代理签名的可区分性

代理签名接收人或验证人在验证代理盲签名的有效性时，需要原始签名人 A 公布的验证公钥 y_A，所以很容易将代理盲签名和原始签名区分开。

(4)不可抵赖性

由于任何人都不能伪造原始签名人 A 的普通数字签名，所以 A 不能否认他的一个有效的普通数字签名。同样由性质 1 可以得到，由于除了代理签名人 B 以外，任何人都不能伪造 B 的代理签名，所以 B 也不能否认一个有效的代理签名。

(5)可注销性

如果 A 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，那么他就可以在系统内公布消息，宣布验证公钥 y_p 无效。从而，B 生成的所有代理签名随之失效。

(6)代理签名和原签名之间的联系性

若 B 在签名时保留 (s',e')，待 C 公开签名 (m,s,e) 后，就表 6.4.1 给出的 4 个签名方案而言，B 可以确认它们之间是有联系的，从而可以确定 C 的签名就是由他自己的代理签名产生的。这 4 个签名方案可以认为是代理弱盲签名方案。但对方案三和方案四来说，B 无法确认它们之间是有联系的，可以认为这两个方案是一个代理强盲签名方案。

6.5 基于多元线性变换的代理盲签名方案

系统参数和符号为：p 是一个大素数，q 是 $p-1$ 的一个大素数因子，整数 $g \in (1, p-1)$ 且阶为 q，即 $g^q \equiv 1 \bmod p$。设 A 为原始签名人，B 为代理签名人，A 的私钥为 x_A，公钥为 y_A，且 $y_A = g^{x_A} \bmod p$，B 的私钥为 x_B，公钥为 y_B，且 $y_B = g^{x_B} \bmod p$。$h(\cdot)$ 为一个安全的单向的 hash 函数。C 为消息拥有者。

代理盲签名方案包含三个阶段。

代理阶段

Step1：(代理产生)签名人 A 随机地选取 $k_A \in Z_q^*$，使 $k_A \neq 1$，然后计算 $r_A = g^{k_A} \bmod p$。

令 $\tilde{a}k_A = \tilde{b} + \tilde{c}x_A \bmod q$，此处向量 $(\tilde{a},\tilde{b},\tilde{c})$ 表示向量 $(\pm r_A, \pm\sigma, \pm 1)$ 的某一置换。A 从这个方程中求出 σ，显然可以表示为 $\sigma = \sigma(k_A, x_A, r_A)$。然后 A 计算 $y_p = g^{\sigma} y_B \bmod p$，这里 y_p 被称作签名权授权的验证公钥并在系统内公开。

Step2：(代理传递)A 将 (r_A,σ) 安全地传递给 B。

Step3：(代理验证)A 接收到σ后，代理签名人 B 检验一下验证公钥的有效性，计算$y_p = g^{\sigma} y_B \bmod p$。如果$\sigma$满足这个方程，B 接受代理，并使用这个代理权代表 A 进行签名，然后计算$s_p = \sigma + x_B \bmod q$，$s_p$作为 A 授权的私钥。否则，B 拒绝接受代理。

签名阶段

Step1：B 任意选取一个随机数$k_B \in Z_q^*(k_B \neq 1)$，计算$r_B = g^{k_B} \bmod p$，并将$r_B$传递给 C。

Step2：C 随机地选取 4 个随机数$\alpha, \beta, \gamma, \tau \in Z_q^*$，令$r_{t'} = r_B^{\alpha} y_p^{\beta} y_B^{\gamma} g^{\tau} \bmod p$.如果$r_{t'} = 0$，C 重新选取另一组$\alpha, \beta, \gamma, \tau$，C 计算$e = h(r_{t'} \| m)$，此处符号“||”表示字符串的连接，从下面介绍的方程中计算$e' = e'(e, \alpha, \beta, \tau) \bmod q$，并将$e'$传送给 B。

Step3：B 接收到e'后，计算$ak_B = b + cs_p \bmod q$，这时向量(a,b,c)表示向量$(\pm s', \pm e', \pm 1)$的某一置换，B 从签名方程中求得s'，并传递给 C，同时 B 保存盲签名(s', e')。

Step4：C 计算$s = s(s', \alpha, \beta, e, \tau) \bmod q$，这时 s 表示从下面的方程组中求得的一组解，令$u = y_B^{\gamma} \bmod p$。这样$(m, s, u, e)$就是 B 代表 A 的代理盲签名。

验证阶段

接收(m, s, u, e)后，验证者计算$\tilde{e} = (h(g^{\alpha a^{-1} b + \tau} y_p^{\alpha a^{-1} c + \beta} u \bmod p) \| m) \bmod q$.如果$\tilde{e} = e$，则$(m, s, u, e)$就是有效的代理盲签名.否则拒绝接受签名。

当消息拥有者 C 公开签名(m, s, u, e)后，如果 B 能求得$\alpha = \alpha(s, s', e, e')$，$\beta = \beta(s, s', e, e')$，$\gamma = \gamma(s, s', e, e')$，$\tau = \tau(s, s', e, e')$，并满足方程：$e = (h(g^{\alpha a^{-1} b + \tau} y_p^{\alpha a^{-1} c + \beta} u \bmod p) \| m) \bmod q$，其中$u = y_B^{\gamma} \bmod p$，然后 B 就可以确定 C 的签名就是由他的代理签名产生的，称这种方案为代理弱盲签名方案.否则称为代理强盲签名方案。

注：B 的验证私钥为s_p，满足$ak_B = b + cs_p \bmod q$，这里向量(a,b,c)表示$(s', e', 1)$的某一置换，消息拥有者 C 的签名方程是$a' k_{t'} = b' + c' s_p \bmod q$，此处的参数$(a', b', c')$必须与$(a,b,c)$在形式上一致。例如：若$(a,b,c) = (1, e', s')$，则取$(a', b', c') = (1, e, s)$。

令$k_{t'} = \alpha k_B + \beta s_p + \gamma x_B + \tau \bmod q$，称$k_{t'}$为变量的多元线性转换关系式，计算$r_{t'} = g^{k_{t'}} \bmod p$。显然得$k_{t'} = (\alpha a^{-1} b + \tau) + (\alpha a^{-1} c + \beta) s_p + \gamma x_B \bmod q$，从而得方程组如下：

$$\begin{cases} \alpha a^{-1} b + \tau = (a')^{-1} b' \\ \alpha a^{-1} c + \beta = (a')^{-1} c' \end{cases}$$

设e'和 s 是未知变量，其它变量是已知的，从上面的方程组中可以求出e'和 s，并记为：

$e' = e'(e, \alpha, \beta, \gamma, \tau) \bmod q$，$s = s(s', e, \alpha, \beta, \gamma, \tau) \bmod q$。

定理 6.5.1：在上述代理盲签名方案中，设系统参数及协议过程不变，代理签名阶段 Step3 的签名方程可供选择的形式有$(1, s', e')$、$(1, e', s')$、$(e', 1, s')$、$(e', s', 1)$等，加上符号变化，各有 4 种不同的形式，共有 16 种不同的代理盲签名方案，而且均是代理盲签名方案，其中 4 种方案的变量替换、签名方程和验证关系式如下页中表 6.5.1 所示.

表 6.5.1　变量置换、签名方程和验证方程表

	变量置换	签名方程	变量方程	验证方程
	$e'=e'(e,\alpha,\beta,\tau) \bmod q$	$ak_B=b+cs_p \bmod q$	$s=s(s',\alpha,\beta,e,\tau) \bmod q$	$\tilde{e}=(h(g^{a^{-1}b+\beta}y_p^{a^{-1}c+\tau}u \bmod p)\|m)$
No.1	$e'=\alpha^{-1}(e-\beta) \bmod q$	$k_B=s'+e's_p \bmod q$	$s=\alpha s'+\tau \bmod q$	$\tilde{e}=(h(g^{s}y_p^{e}u \bmod p)\|m)$
No.2	$e'=\alpha^{-1}(e-\tau) \bmod q$	$k_B=e'+s's_p \bmod q$	$s=\alpha s'+\beta \bmod q$	$\tilde{e}=(h(g^{e}y_p^{s}u \bmod p)\|m)$
No.3	$e'=\alpha(e^{-1}-\tau)^{-1} \bmod q$	$e'k_B=1+s's_p \bmod q$	$s=\alpha e(e')^{-1}s'+e\beta \bmod q$	$\tilde{e}=(h(g^{e^{-1}}y_p^{e^{-1}s}u \bmod p)\|m)$
No.4	$e'=\alpha(e^{-1}-\beta)^{-1} \bmod q$	$e'k_B=s'+s_p \bmod q$	$s=\alpha e(e')^{-1}s'+e\tau \bmod q$	$\tilde{e}=(h(g^{e^{-1}s}y_p^{e^{-1}}u \bmod p)\|m)$

从下面的两个具体方案可以看出，当原始签名人公布原消息 m 和签名(s，e)后，代理签名人不能找出代理签名和原始签名的联系，这样任何人都不能从中发现它们之间的联系，称这样的签名方案为代理强盲签名方案。

代理盲签名举例

系统参数和符号与上面的一样，下面介绍的方案对应于表 6.5.1 中的方案 1 此时 $k_{C'}=\alpha k_B+\beta s_p+\gamma x_B+\tau \bmod q$。

代理阶段

Step1：原始签名人 A 任意地选取一个整数 $k_A\in Z_q^*$，$k_A\neq 1$，计算 $r_A=g^{k_A} \bmod p$，$\sigma=x_A+r_Ak_A \bmod q$，$y_p=g^{\sigma}y_B \bmod p$，并在系统内公开 y_p，y_p 作为代理签名的验证公钥。

Step2：A 传递 (r_A,σ) 给代理签名人 B。

Step3：B 接收到 (r_A,σ) 后，验证 $y_p=g^{\sigma}y_B \bmod p$ 是否成立？如果 σ 满足，则 B 接收 A 的代理委托，并行使 A 的签名授权，然后计算 $s_p=\sigma+x_B \bmod q$，s_p 作为 A 的代理授权的验证私钥.否则 B 拒绝接受委托。

签名阶段

Step1：B 随机地选取一个整数 $k_B\in Z_q^*$，$k_B\neq 1$，并计算 $r_B=g^{k_B} \bmod p$，然后将 r_B 传递给 C.

Step2：C 随机地选取 4 个整数 $\alpha,\beta,\gamma,\tau\in Z_q^*$，并计算 $r_{C'}=r_B^{\alpha}y_p^{\beta}y_B^{\gamma}g^{\tau} \bmod p$.如果 $r_{C'}=0$，C 重新选取另一组参数。计算 $e=h(r_{C'}\|m)$，$e'=\alpha^{-1}(e-\beta) \bmod q$.将 e' 送给 B.

Step3：收到 e' 后，B 计算 $s'=k_B-e's_p \bmod q$，并将 s' 送给 C，B 保存盲签名 (s',e').

Step4：C 计算 $s=\alpha s'+\tau \bmod q$ 和 $u=y_B^{\gamma} \bmod p$.则 (m,s,u,e) 即为 B 代表 A 作的代理盲签名。

验证阶段

接收到代理盲签名(m,s,u,e)后，接收者或验证者计算$\tilde{e}=(h(g^s y_p{}^e u \bmod p)\| m)$，方程$\tilde{e}=e$成立当且仅当$(m,s,u,e)$是有效的代理盲签名。

C 公开签名(m,s,u,e)后，B 不能从上面的方程组中获得α,β,γ,τ.他不能判断一个有效的签名是否是由他的代理签名所产生，因此这个签名方案是一种强盲签名方案。

多元线性变换的退化情况

考虑$\gamma=0$，此时$r_{C'}=r_B^{\alpha} y_p{}^{\beta} g^{\tau} \bmod p$，$k_{C'}=\alpha k_B+\beta s_p+\tau \bmod q$。

在代理签名阶段 Step2 之前的操作与上一节的一样，余下的步骤如下：

Step2：C 随机地选取 3 个整数$\alpha,\beta,\tau\in Z_q^*$，令$r_{C'}=r_B^{\alpha} y_p{}^{\beta} g^{\tau}\neq 0 \bmod p$，计算$e=h(r_{C'}\| m)$。此时$e'=\alpha^{-1}(e-\beta)\bmod q$，C 将$e'$传送给 B。

Step3：接收到e'后，B 计算$s'=k_B-e's_p \bmod q$。然后将其传送给 C，并保存盲签名(s',e')。

Step4：C 计算$s=\alpha s'+\tau \bmod q$，这样(m,s,e)即为代理盲签名。

验证阶段

收到盲签名(m,s,e)后，接收者或验证者计算$\tilde{e}=(h(g^s y_p{}^e \bmod p)\| m)$，则方程$\tilde{e}=e$成立当且仅当$(m,s,e)$是一个有效的代理盲签名。

如果消息拥有者 C 公开签名(m,s,e)，B 不能从方程组中$\begin{cases}\alpha e'+\beta=e\\ \alpha s'+\tau=s\end{cases}$求得$\alpha,\beta,\tau$.因此，他不能判断这个签名是否是由他的代理签名所产生，因此这个签名方案是一种强盲签名方案。

考虑特例$\alpha=1$、$\gamma=0$，此时$r_{C'}=r_B y_p{}^{\beta} g^{\tau} \bmod p$，$k_{C'}=k_B+\beta s_p+\tau \bmod q$。

从下面的步骤开始有所区别，之前的步骤是一致的。

Step2：C 选取 2 个整数$\beta,\tau\in Z_q^*$，计算$r_{C'}=r_B y_p{}^{\beta} g^{\tau} \bmod p$。如果$r_{C'}=0$，则重新选取。然后计算$e=h(r_{C'}\| m)$，$e'=e-\beta \bmod q$，并将$e'$传送给 B。

Step3：接收到e'后，B 计算$s'=k_B-e's_p \bmod q$，并传递给 C，B 保存盲签名(s',e')。

Step4：C 计算$s=s'+\tau \bmod q$，则(m,s,e)即为 B 所作的代表 A 对消息 m 的代理盲签名。

验证阶段

收到代理盲签名(m,s,e)后，接收者或验证者计算$\tilde{e}=(h(g^s y_p{}^e \bmod p)\| m)$.这样方程$\tilde{e}=e$成立，当且仅当$(m,s,e)$是消息 m 的有效的代理盲签名。

当 C 公开(m,s,e)后，B 能从方程$\begin{cases}e'+\beta=e \bmod q\\ s'+\tau=s \bmod q\end{cases}$求出$\beta,\tau$。这样他就能确定 C 的签名就是由他的代理签名产生的.所以说这种情况下的签名是代理弱盲签名。

6.6 基于椭圆曲线的代理盲签名方案

本节在分析文献[44~45]的基础上，着重对协议过程中的变量进行了更加一般性的转化和处理，通过线性变换的形式较好地刻画了协议过程中各种变量之间的转化关系，从而提出了一种基于线性变换的代理盲签名方案，以此方法构造的代理盲签名方案包括文献[44~45]中的方案.我们将这种方法平移到椭圆曲线密码体制中来，从而得到了在椭圆曲线密码体制下的基于线性变换的代理盲签名方案.并总结了以 4 个 ElGamal 型[63]签名方案为基础构造的 4 种相应的代理盲签名方案，还考虑了协议过程中的变量的线性变换的退化情况.

6.6.1 系统参数

(1)选取定义在有限域 F_q 上的一条安全的椭圆曲线 E，使得 E 上的 F_q-有理点群的阶被一个大素数 n 整除，保证椭圆曲线上有理点群上的离散对数问题是难解的。

(2)选取一个基点 $G \in E$，G 的阶为 n，即有 $nG = O$，O 表示一个无穷远点.基点 G 公开。

(3)设 A 为系统的原始签名人，B 为 A 授权的代理签名人， A 的私钥为 $x_A \in_R Z_n^*$，$P_A = x_A G \in E$，P_A 作为 A 的公钥.B 的私钥为 $x_B \in_R Z_n^*$，$P_B = x_B G \in E$，P_B 作为 B 的公钥.它们的公钥 P_A 和 P_B 均在系统内公开。

(4)设 C 为信息拥有者，D 为信息的接收者.D 的私钥为 $x_D \in_R Z_n^*$，$P_D = x_D G \in E$，P_D 作为 D 的公钥，在系统内公开。

(5)选取一个安全的 Hash 函数 h，在系统内公开。

6.6.2 基于多元线性变换的代理盲签名方案

方案由签名权委托过程、代理签名过程和签名验证过程共同组成，各个过程的具体操作步骤如下：

委托过程

Step1：委托产生阶段。A 任意地选取一个随机数 $k_A \in_R Z_n^*$ 且 $k_A \neq 1$，计算 $R_A = k_A G$，令 $r_A = x(R_A) \bmod n$，其中 $x(R_A)$ 表示椭圆曲线上点 R_A 的 x 坐标，然后计算 $\sigma = k_A + r_A x_A \bmod n$，称这个方程为 A 的授权签名方程。又令 $R_p = \sigma G + P_H$，R_p 被称为原始签名人将签名权委托给代理签名人的签名的验证公钥，在系统内公开。

Step2：委托传递阶段。A 将委托签名 (σ, r_A) 安全地传递给 B。

Step3：委托验证阶段。B 收到委托签名 (σ, r_A) 后，计算 $\tilde{R}=\sigma G-r_A P_A$，检验是否成立 $x(\tilde{R})=r_A \bmod n$？如果成立，则说明 (σ, r_A) 是 A 发送过来的，B 接受 A 的委托，并代表 A 行使签名的权力。否则，拒绝接受 A 的委托.同时计算 $s_p=\sigma+x_B \bmod n$，s_p 被称为签名权委托的验证私钥(保密)，满足关系 $R_p=s_p G$。

事实上，$\tilde{R}=\sigma G-r_A P_A=(\sigma-r_A x_A)G=k_A G$，所以成立 $x(\tilde{R})=r_A \bmod n$.因此 B 接受 A 的委托，代表 A 进行签名。

代理签名过程

Step1：B 接受 A 的委托后，任意地选取一个随机数 $k_B \in_R Z_n^*$，且 $k_B \neq 1$，计算 $R_B=k_B G$，并将 R_B 传给 C。

Step2：C 得到 R_B 后，任意地选取四个随机数 $\alpha, \beta, \gamma, \tau \in_R Z_n^*$，计算 $R_{t'}=\alpha R_B+\beta R_p+\gamma P_B+\tau G$（称这个关系式为变量的多元线性变换）。如果 $r_{t'}=x(R_{t'})=0 \bmod n$，则需要重新选取这组参数并使 $r_{t'} \neq 0$，然后计算 $e=h(r_{t'} \| m)$，其中符号“‖”表示字符串或整数的连接，令 $e'=\alpha^{-1}(e-\beta) \bmod n$，C 将 e' 传递给 B。

Step3：B 收到 e' 后，计算 $s'=k_B-e' s_p \bmod n$，并将 s' 传给 C，B 保留盲签名 (e', s')。

Step4：C 收到 s' 后，计算 $s=\alpha s'+\tau \bmod n$，$U=\gamma P_B$，则 (e, s, U) 就是 B 代表 A 对消息 m 的代理盲签名。

签名验证过程

消息的接收者 C 或验证者接收到消息 m 和签名 (e, s, U) 后，计算 $\tilde{r}_{t'}=x(sG+eR_p+U) \bmod n$，判断 $e=h(\tilde{r}_{t'} \| m)$ 是否成立？如果成立，则说明 (e, s, U) 就是消息 m 的有效的代理盲签名。否则，拒绝接收这个签名。事实上

$sG+eR_p+U=(\alpha s'+\tau)G+eR_p+U=(\alpha k_B-\alpha e' s_p+\tau)G+eR_p+U=\alpha P_B+\beta R_p+\gamma P_B+\tau G$，因此，上述结论成立。

定理 6.6.2.1：若将上述方案的代理签名过程中的 Step3 的签名方程改为一般式 $ak_B=b+cs_p \bmod n$，其中参数 (a, b, c) 表示向量 $(\pm s', \pm e', \pm 1)$ 的某一个置换，则有 4 种不同形式的代理盲签名方案.在这些方案中协议的整个过程都不变，产生变化的只是相应的两个变量替换式、签名方程和验证方程等，把这 4 种方案列在表 6.6.2.1 中.如果还考虑到参数前面的符号的变化，那么可以得到 16 种不同的方案。

表 6.6.2.1　代理盲签名方案的变量替换式、代理签名方程和验证方程表

编号	变量关系式 1	签名方程	变量关系式 2	验证方程
一般式	$e'=e'(e, \alpha, \beta, \tau) \bmod q$	$ak_B=b+cs_p \bmod n$	$s=s(s', \alpha, \beta, e, \tau) \bmod q$	$\tilde{e}=h(x((a^{-1}b+\beta)G+(a^{-1}c+\alpha)R_p+U) \| m)$
N31	$e'=\alpha^{-1}(e-\beta) \bmod n$	$k_B=s'+e' s_p \bmod n$	$s=\alpha s'+\tau \bmod n$	$\tilde{e}=h(x(sG+eR_p+U) \| m)$
N32	$e'=\alpha^{-1}(e-\tau) \bmod n$	$k_B=e'+s' s_p \bmod n$	$s=\alpha s'+\beta \bmod n$	$\tilde{e}=h(x(eG+sR_p+U) \| m)$
N33	$e'=\alpha(e^{-1}-\tau)^{-1} \bmod n$	$e'k_B=1+s' s_p \bmod n$	$s=\alpha c(e')^{-1}s'+c\beta \bmod n$	$\tilde{e}=h(x(e^{-1}G+e^{-1}sR_p+U) \| m)$

N34	$e'=\alpha(e^{-1}-\beta)^{-1} \bmod n$	$e'k_B = s' + s_p \bmod n$	$s=\alpha e(e')^{-1}s'+e\tau \bmod n$	$\tilde{e}=h(x(e^{-1}sG+e^{-1}R_p+U)\|\|m)$

定理 6.6.2.2：在表 6.6.2.1 中列举的代理盲签名方案是代理强盲签名方案的概率为$(1-1/n^2)$。

注：代理强盲签名指代理签名人不能根据签名判断这个签名是由他的代理签名所产生，即签名人不能对原消息的拥有者进行追踪。反之，称为代理弱盲签名方案。

证明：以表 6.6.2.1 中的方案 N31 为例进行说明。在消息拥有者 C 公布签名(e,s,U)后，B 保留了盲签名(s',e')，但不能从方程组

$$\begin{cases} s=\alpha s'+\tau \bmod n & (1) \\ e'=\alpha^{-1}(e-\beta) \bmod n & (2) \end{cases}$$

中解出求知参数α,β,τ，因为两个方程中含有 3 个未知数。

又由于$U=\gamma P_B$，虽然已知U和P_B，但仍然不能求出γ，因为这将面临求解椭圆曲线 E 的离散对数难题。

但值得注意的是：在上述方程组中，猜对其中一个参数的概率为$1/n$，如果一个参数猜对的话，那么其余的两个参数也就可以从中解出。同样的道理，猜对γ的概率也为$1/n$，这样同时猜对的概率为$1/n^2$。当求得这 4 个参数时，B 就可以计算$R'_{C'}=\alpha R_B+\beta R_{P'}+\gamma P_B+\tau G$，$r'_{C'}=x(R'_{C'}) \bmod n$，如果满足$e=(r'_{C'}\|m)$，则他可以判断 C 的签名就是由他的代理签名产生的。因此，定理的结论成立。

由于产生这种可能性的概率非常小，按照小概率原理，对这种情况几乎可以忽略不计，所以认为这些方案均是代理强盲签名方案。

考虑当$\gamma=0$，即$R_{C'}=\alpha R_B+\beta R_{P'}+\tau G$时的情况

系统参数、委托过程和代理签名过程中的 Step1 都与上述方案完全相同，从 Step2 开始，依照如下步骤进行：

Step2：C 随机地选取三个数$\alpha,\beta,\tau\in_R Z_n^*$，计算$R_{C'}=\alpha R_B+\beta R_{P'}+\tau G$，如果$r_{C'}=x(R_{C'}) \bmod n=0$，那么他重新选取这些参数.否则计算$e=h(r_{C'}\|m)$，$e'=\alpha^{-1}(e-\beta) \bmod n$，并将$e'$传递给 B。

Step3：B 收到e'后，对s_p签名，计算$s'=k_B-e's_p \bmod n$，并将s'传给 C，同时，B 保留盲签名(s',e')。

Step4：C 计算$s=\alpha s'+\tau \bmod n$，则(e,s)就是 B 代表 A 对消息 m 的代理盲签名。

签名验证过程。代理盲签名的接收者或验证者收到(e,s)后，计算$\tilde{r}_{C'}=x(sG+eR_p) \bmod n$，判断$e=h(\tilde{r}_{C'}\|m)$是否成立？如果成立，则说明$(e,s)$就是消息 m 的有效的代理盲签名。否则，拒绝接收签名。

定理 6.6.2.3：当$R_{C'}=\alpha R_B+\beta R_{P'}+\tau G$时，上述代理盲签名方案是代理强盲签名方案的概率为$(1-1/n)$。

证明：当$\gamma=0$时，与定理 6.6.2 一样，当 C 公布签名(e,s)后，B 能判断 C 的签

名就是由他的代理签名产生的概率为 $1/n$，因此结论成立。

考虑当 $\alpha=1,\gamma=0$，即 $R_{C'}=R_B+\beta R_{P'}+\tau G$ 时的情况

Step2：C 随机地选取两个整数 $\beta,\tau\in_R Z_n^*$，计算 $R_{C'}=R_B+\beta R_{P'}+\tau G$，如果 $r_{C'}=x(R_{C'})\bmod n=0$，那么他重新选取这组参数.否则计算 $e=h(r_{C'}\|m)$，$e'=e-\beta \bmod n$，并将 e' 传递给 B。

Step3：B 收到 e' 后，对 s_p 签名，计算 $s'=k_B-e's_p \bmod n$，并将 s' 传给 C，B 保留盲签名 (s',e')。

Step4：C 计算 $s=s'+\tau \bmod n$，则 (e,s) 就是 B 代表 A 对消息 m 的代理盲签名。

签名验证过程。代理盲签名的接收者或验证者收到 (e,s) 后，计算 $\tilde{r}_{C'}=x(sG+eR_p)\bmod n$，判断 $e=h(\tilde{r}_{C'}\|m)$ 是否成立？如果成立，则说明 (e,s) 就是消息 m 的有效的代理盲签名。否则，拒绝接收签名。

定理 6.6.2.4：当 $R_{C'}=R_B+\beta R_{P'}+\tau G$ 时，上述代理盲签名方案是代理弱盲签名方案。

证明：在消息拥有者 C 公布签名 (e,s) 后，B 保留了盲签名 (s',e')。因此，他可以求出参数 $\beta=e-e' \bmod n$，$\tau=s-s' \bmod n$，从而据此计算 $R'_{C'}=R_B+\beta R_{P'}+\tau G$，$r'_{C'}=x(R'_{C'})\bmod n$。如果满足 $e=(r'_{C'}\|m)$，则他可以据此判断 C 的签名就是由他的代理盲签名产生的，从而可以对消息拥有者进行追踪。故我们认为在这种情况下的代理盲签名方案是代理弱盲签名方案。

6.6.3 方案的安全性及应用分析

在这些签名方案中，所有的验证过程均使用了原始签名人的签名授权的验证公钥，这说明最终签名是通过原始签名人的授权由代理签名人和信息拥有者共同完成的，同时也可以把 R_p 看成是代理盲签名的验证公钥之一。虽然各个方案的形式和特点不一样，但它们具有如下一些共同的性质。

(1)签名授权人的签名的不可伪造性。在这些代理盲签名方案中，代理签名人 B 不能根据 (σ,r_A) 计算出签名授权人 A 的私钥 x_A，从而不能伪造 A 的签名，其安全性基于椭圆曲线的离散对数问题的难解性。也不能从签名方程 $\sigma=k_A+r_Ax_A \bmod n$ 中获取 A 的私钥，因为签名方程中含有两个未知数 x_A 和 k_A，由此说明任何攻击者都难以伪造 A 的签名。

(2)代理盲签名的不可伪造性。因为代理签名密钥 $s_p=\sigma+x_B \bmod n$，其中含有 B 的私钥，所以只有 B 才能生成 s_p，尽管 $R_p=s_pG$，R_p 公开，但不能从中得到 s_p，因为这面临椭圆曲线的离散对数难题。因此除了 B 以外，其他任何人(包括 A 在内)都难以伪造一个有效的代理签名。

(3)代理盲签名的可区分性。在验证代理盲签名的有效性时，要用到签名授权人公布的签名验证公钥 R_p，所以很容易将代理盲签名和原始签名区分开。

(4)代理盲签名的不可抵赖性。由于任何人都不能伪造原始签名人 A 的普通数字签名，所以 A 不能否认他的一个有效的普通数字签名.同样由性质(2)可以得到，由于除了代理签名人 B 以外，任何人都不能伪造 B 的代理签名，所以 B 也不能否认一个有效的代理盲签名。

(5)代理盲签名的可注销性。如果 A 想收回 B 的代理签名权，那么他就可以在系统内公布消息，宣布验证公钥 R_p 无效，从而 B 生成的所有代理盲签名随之失效。

(6)代理签名和原签名之间的联系性。根据上述分析，这些方案要么是代理强盲签名方案，要么是代理弱盲签名方案.如果是代理强盲签名方案，说明代理签名人 B 无法确认和原始签名人 A 之间的联系，这种方案比较适合于有匿名性要求、同时又不能对签名追踪的领域，如电子货币支付系统、电子选举等领域.如果是代理弱盲签名方案，这时方案比较适合于有匿名性要求、且又能对签名进行追踪的情况。

本节比较完整地给出了在椭圆曲线密码体制下如何运用线性变换来构造代理盲签名方案的方法，这种方法可以任意地选取不同的参数组合，从而使得产生代理盲签名方案具有较大的选择空间，再加上这种方案同时具备代理签名和盲签名的特点，因此可广泛应用于有匿名性要求的领域，如匿名电子选举和电子货币匿名支付系统等，具有广阔的应用前景。

6.7 具有消息恢复的代理盲签名方案

6.7.1 方案描述

方案由签名权委托过程、代理签名过程和签名验证过程共同组成，各个过程的具体操作步骤如下：

委托过程

Step1：委托产生阶段。A 任意地选取一个随机数 $k_A \in_R Z_n^*$ 且 $k_A \neq 1$，计算 $R_A = k_A G$，令 $r_A = x(R_A) \bmod n$，其中 $x(R_A)$ 表示椭圆曲线上点 R_A 的 x 坐标，然后计算 $\sigma = k_A + r_A x_A \bmod n$，称这个方程为 A 的授权签名方程.又令 $R_p = \sigma G + P_B$，R_p 被称为原始签名人将签名权委托给代理签名人的签名的验证公钥，在系统内公开。

Step2：委托传递阶段。A 将委托签名 (σ, r_A) 安全地传递给 B。

Step3：委托验证阶段。B 收到委托签名 (σ, r_A) 后，计算 $\tilde{R} = \sigma G - r_A P_A$，检验是否成立 $x(\tilde{R}) = r_A \bmod n$?如果成立，则说明 (σ, r_A) 是 A 发送过来的，B 接受 A 的委托，并代表

A 行使签名的权力。否则，拒绝接受 A 的委托.同时计算 $s_p=\sigma+x_B \bmod n$，s_p 被称为签名权委托的验证私钥(保密)，满足关系 $R_p=s_pG$。

事实上，$\tilde{R}=\sigma G-r_A P_A=(\sigma-r_A x_A)G=k_A G$，所以成立 $x(\tilde{R})=r_A \bmod n$.因此 B 接受 A 的委托，代表 A 进行签名。

代理签名过程

Step1：B 接受 A 的委托后，任意地选取一个随机数 $k_B \in_R Z_n^*$，且 $k_B \neq 1$，计算 $R_B=k_B G$，并将 R_B 传给 C。

Step2：C 任意地选取 3 个整数 $\alpha,\beta,\gamma \in_R Z_n^*$，计算 $R_{C'}=\alpha R_B+\beta R_P+\gamma G$，使得 $r_{C'}=x(R_{C'}) \neq 0 \bmod n$。计算 $m'=mr_{C'}^{-1} \bmod n$，并将盲消息 m' 传递给 B。

Step3：B 收到 m' 后，计算 $s'=k_B-m's_p \bmod n$，并将 s' 传递给 C，B 保留盲签名(m'，s')。

Step4：C 收到 s' 后，先验证 $R_B=sG+m'R_P$ 是否成立？若不成立，则拒绝接受 B 的代理签名。反之，则说明是代理签名人发送过来的，然后计算 $s=\alpha s'+\gamma \bmod n$ 和 $m''=\alpha m'+\beta \bmod n$，则 (m'',m',s) 就是消息 m 的代理盲签名。

签名验证过程。消息的接收者接收到 (m'',m',s) 后，先计算 $r_{C'}=x(sG+m''R_P) \bmod n$，然后通过计算 $m=m'r_{C'} \bmod n$ 就可以恢复原消息了。我们可以在原消息的末尾处增加一些冗余信息，用以说明 C 的身份，这样当恢复原消息后，实际上签名的验证工作也就随之完成。否则，拒绝接收签名。

事实上，

$sG+m''R_P=(\alpha s'+\gamma)G+(\alpha m'+\beta)R_P=\alpha(k_B-m's_P)G+\gamma G+\alpha m'R_P+\beta R_P=\alpha R_B+\beta R_P+\gamma G$，显然有 $r_{C'}=x(sG+m''R_P) \bmod n$ 成立。

注：在这个方案中，任何人收到消息的签名后，都可以恢复原消息，包括代理签名人 B 在内，因此这个签名的作用不在于信息的机密性要求，而在于信息的完整性要求等，不过对于 B 来讲，他的代理签名是针对盲消息的，因此仍然称这个方案为代理盲签名方案。下面提出的具有指定接收者的代理盲签名方案较好地解决了这个问题。

6.7.2 针对指定接收者

系统参数同前，并设消息及签名的接收者为 D。方案的委托过程和签名过程中的 Step1 都与第 6.7.1 节的方案完全相同，从 Step2 开始，照如下步骤进行：

Step2：C 随机地选取三个整数 $\alpha,\beta,\gamma \in_R Z_n^*$，计算 $R_{C'}=\alpha R_B+\beta R_P+\gamma G$，$r_{C'}=x(R_{C'}) \bmod n$，并要求 $r_{C'} \neq 0$。然后计算 $m'=mr_{C'}^{-1} \bmod n$。C 欲将消息发送给指定的接

收者 D，因此，他将(m', P_D)传递给 B。

Step3：B 收到(m', P_D)后，计算$s' = k_B - m's_p \bmod n$，$r_1 = x(k_B P_D) \bmod n$，$\tilde{r} = m' r_1^{-1} \bmod n$，$\tilde{s} = k_B + \tilde{r}x_B \bmod n$，并将$(s', \tilde{r}, \tilde{s})$传递给 C。B 保留盲消息$m'$及其签名$(s', \tilde{r}, \tilde{s})$。

Step4：C 计算$s = \alpha s' + \gamma \bmod n$，$m'' = \alpha m' + \beta \bmod n$，则$(m'', s, \tilde{r}, \tilde{s})$就是 B 代表 A 对消息 m 的代理盲签名。

签名验证过程。代理盲签名的接收者 D 接收到$(m'', s, \tilde{r}, \tilde{s})$后，首先获取签名者 B 的公钥，计算$\tilde{r}_C = x(sG + m''R_p) \bmod n$，$\tilde{m}' = \tilde{r}x(\tilde{s}P_D - \tilde{r}x_D P_B) \bmod n$，然后再计算$m = \tilde{r}_C \cdot \tilde{m}' \bmod n$，这样就可以恢复原消息了。同上面的处理方法一样，可以在消息的末尾处添加冗余位，在冗余位中包含一些信息拥有者的信息，从而就可以验证发送者的身份。否则，拒绝接收签名。

与上一节的情况类似，显然成立$r_C = x(sG + m''R_p) \bmod n$，又因为

$m' = \tilde{r}x(\tilde{s}P_D - \tilde{r}x_D P_B) = \tilde{r}x(k_B P_D) \bmod n$，所以有$m = m' r_C \bmod n$。

注：如果需要传输的消息量较大，超过大素数n时，这时该方法就不适用了，于是我们借鉴文献[71]的处理办法，先把消息分为若干块，表示为$m = \{m_1, m_2, \cdots, m_t\}$，使得每一个子块$m_i < n$，然后运用递推的方式把前一个参数作为后一个参数的输入，使得在恢复消息时只需进行递推运算就可以一个一个地恢复全部消息了，从而大大地减少了通信传输量，于是得到下一节的方案。

6.7.3 具有消息链接恢复特性

在进行签名阶段的 Step2 之前，系统参数及操作均与第 6.7.1 小节中的方案完全相同，从 Step2 开始，按照如下步骤进行：

Step2：这一步与第 6 节相应步骤基本相同，仅不同的是 C 将盲消息串$(m_1', m_2', \cdots, m_t')$和 D 的公钥$P_D$一起传递给 B。

Step3：B 接收到$(m_1', m_2', \cdots, m_t')$和$P_D$后，计算$s_1' = k_B - m_1' s_p \bmod n$，$\tilde{r}_1 = x(k_B P_D) \bmod n$，记$r_0 = 0$，分别计算下面各式：

$r_i = m_i' h(r_{i-1} + \tilde{r}_1)^{-1} \bmod n$，$i = 1, 2, \cdots, t$

$\tilde{r} = h(r_1 \oplus r_2 \oplus \cdots \oplus r_t)$，其中符号“$\oplus$”表示异或运算。

$\tilde{s} = k_B + \tilde{r}x_B \bmod n$

将$(s_1', \tilde{s}, \tilde{r}, r_1, r_2, \cdots, r_t)$传递给 C。B 保留盲消息串$(m_1', m_2', \cdots, m_t')$及其签名$(s_1', \tilde{s}, \tilde{r}, r_1, r_2, \cdots, r_t)$。

Step4：C 计算$s_1 = \alpha s_1' + \gamma \bmod n$，$m_1'' = \alpha m_1' + \beta \bmod n$，则$(m_1'', s_1, \tilde{r}, \tilde{s}, r_1, r_2, \cdots, r_t)$就是 B 代表 A 对消息 m 的签名。

原消息的恢复过程

D 接收到 C 发送过来的签名 $(m_1'', s_1, \tilde{r}, \tilde{s}, r_1, r_2, \cdots, r_t)$ 后，他首先获取系统的域参数和代理签名者 B 的公钥，然后做如下的操作:

Step1：验证 $m_1'', s_1, \tilde{r}, \tilde{s}, r_1, r_2, \cdots, r_t$ 是 $[1, n-1]$ 中的整数。

Step2：D 分别计算: $\tilde{r}_1' = x(\tilde{s}P_D - \tilde{r}x_D P_B) \bmod n$，$\tilde{m}_i' = r_i h(r_{i-1} + \tilde{r}_1') \bmod n$，$i = 1,2,\cdots,t$，

$\tilde{r}_C' = x(s_1 G + m_1'' R_p) \bmod n$，$m_i = \tilde{m}_i' \tilde{r}_C' \bmod n$，这样就可以恢复消息串 $\{m_1, m_2, \cdots, m_t\}$ 了。

若通过计算恢复出的消息能确认发送者的身份，那么接受其签名，否则拒绝接受。

签名验证的正确性证明：因为 $\tilde{s}P_D - \tilde{r}x_D P_B = k_B P_D + \tilde{r}x_B P_D - \tilde{r}x_D P_B = k_B P_D$，所以 $\tilde{r}_1' = \tilde{r}_1 \bmod n$，从而有 $\tilde{m}_i' = r_i h(r_{i-1} + \tilde{r}_1') = m_i' \bmod n$。

又 $s_1 G + m_1'' R_p = (\alpha s_1' + \gamma)G + (\alpha m_1' + \beta)R_p = \alpha(k_B - m_1' s_p)G + \gamma G + \beta R_p - \alpha m_1' s_p G = \alpha R_B + \beta R_p + \gamma G$

则 $\tilde{r}_C' = x(s_1 G + m_1'' R_p) = r_C' \bmod n$。

故 $m_i = \tilde{m}_i' \tilde{r}_C' = m_i r_C' \bmod n$，$1 \le i \le t$。

6.8 本章小结

本章围绕代理签名、盲签名和代理盲签名问题进行了研究，获得的一些结果如下：

（1）对各种各样的盲签名进行了较系统的分类，对研究现状及存在的问题进行了总结。

（2）探讨了代理签名方案中委托人和代理签名人之间的联系问题，即是否可以对代理签名人进行追踪的问题，提出了构造 ElGamal 型弱盲签名方案的方法，用此种方法构造的弱盲签名方案几乎包含了目前所有该类签名方案。

（3）给出了基于离散对数的代理盲签名方案的构造方法，列举了由此种方法导出的 4 种不同形式的代理盲签名方案。

（4）给出了基于多元线性变换的代理盲签名方案，这种方法较好地刻画了委托人和代理签名人以及代理签名人与信息拥有者之间的联系；同时给出了在椭圆曲线密码体制下的相应的代理盲签名方案，并进行了安全性的分析。

（5）把这种签名方案与消息的恢复特性结合起来，给出了具有消息恢复的代理盲签名方案。

本章评注

评注 **6.1** 盲签名的概念是由 Chaum 在 1982 年提出的，直到 2000 年左右，关于盲签名的研究非常活跃，各种各样的盲签名方案相继提出，最近比较热门的一个研究

课题是部分盲签名方案[47~50]，这些方案可广泛应用于电子商务的交易活动中。

评注 6.2 代理盲签名的概念最早是由 Lin 和 Jan[85]在 2000 年提出的，之后，学者们提出了各种各样的代理盲签名方案，影响比较大的一种代理盲签名方案当数 Lal 和 Awasthi[45]在 2003 年提出的，该方案以 Mambo[12]的方案为基础，比 Tan[44]的方案在计算上简单些。作者在本章的工作主要是基于这种思想进行构造的。

评注 6.3 值得注意和研究的问题是在代理盲签名方案的研究中，Sun 和 Hsieh[110]指出 Tan[44]的方案并不满足不可伪造性和不可追踪性，Lal 和 Awasthi[45]的方案也不满足不可追踪性，由此可见，关于代理盲签名的基础研究还需要进行深入探讨并改进。

7　基于双线性理论的签名方案

在传统的公钥密码体制中，通常私钥是由一个可信的 CA 产生的，由用户自己保存并使用，而公钥是以数字证书的形式保存，在加密或数字签名时使用。1984 年，Shamir[81]首次提出了基于 ID（identity-based）的加密和签名方案，该方案的公钥使用用户的身份（identity），如邮箱地址、身份证号等，目的是为了简化密钥的管理。在对密钥的管理和安全性有更高要求时，这种以 ID 为基础的公钥密码系统优于以数字证书为基础的公钥密码系统。

2001 年,Boneh 和 Franklin[92]明确给出了基于身份加密的定义，利用椭圆曲线上的双线性性质，提出了一种基于 ID 的加密方案，文中指出基于 ID 的加密方案可以将有效时间加入到身份中，这样得到的公钥和私钥只能在规定的时间有效。Hess[93]于 2002 年总结了一般的基于离散对数的签名方案，并提出了将基于离散对数签名方案转换到利用双线性映射的基于 ID 签名方案的一般方法。Zhang 和 Kim[94]提出了一种基于 ID 的盲签名和一种基于 ID 的环签名方案，其中的盲签名方案是根据 Schorr 盲签名思想转换而来。

由于盲签名的性质很好地满足了人们对个人隐私的要求，所以被广泛地应用于电子商务和在线投票中。因此,本文把基于 ID 的签名方案和盲签名方案结合起来，提出了一种新型的基于 ID 的盲签名方案。

由于这一章的内容涉及椭圆曲线的有关基础知识，虽然这些知识在前面的章节中已多次用到，但考虑到本章内容是在椭圆曲线基础之上的深入研究和探讨，因此在本章 7.1 节专门介绍有关基本理论和一些特殊的符号。

7.1　准备工作

7.1.1　椭圆曲线

Miller[88]与 Koblitz[89]分别于 1985 和 1987 年提出将椭圆曲线用于公钥密码体制，但并没有给出在有限域上使用椭圆曲线的密码算法，而是建议在现有的加密系统中使用椭圆曲线。

所谓椭圆曲线是指由韦尔斯特拉（Weierstrass）方程：

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

所确定的平面曲线 E。密码学中使用的椭圆曲线是定义在有限域这样的有限代数结构上。$P=(x,y)\in E$ 是椭圆曲线上的一点，引入一个特殊的被称为无穷远点的点 $O=(x,\infty)$，在椭圆曲线上可利用弦切运算（用“+”标记）构建一个阿贝尔（Abel）群。常用域 F_p 和 F_{2^m} 上的椭圆曲线。

弦切运算的几何表示。设 $P=(x_1,y_1)$，$Q=(x_2,y_2)$ 是 E 上任意两点，l 是 PQ 连线。若 P 和 Q 重合于一点，则 l 为过 P 点的切线。l 和曲线相交于另一点 R，l' 是 R 点和无穷远点 O 的连线（过 R 点与 y 轴平行的直线），l' 和曲线交于一点，该交点为 $P+Q$ 的值，参见示意图 7.1.1。若 P 和 Q 关于 x 轴对称或重合于 x 轴，则 PQ 垂直于 x 轴，此时 l 和椭圆曲线交于无穷远点 O。

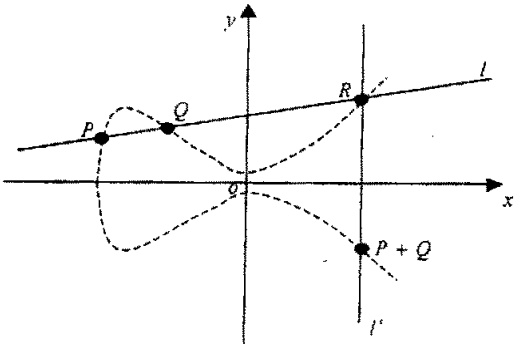

图 7.1.1　椭圆曲线上“+”运算的几何表示

椭圆曲线上的点关于运算“+”有如下性质：

若直线 l 和 E 相交于 P，Q，R 三点，则 $(P+Q)+R=O$。

对任一 $P\in E$，有 $P+O=P$。

对任意 P，$Q\in E$，有 $P+Q=Q+P$。

对任一 $P\in E$，存在 E 上一点，记为 $-P$，使 $P+(-P)=O$。

设 P，Q，$R\in E$，则 $(P+Q)+R=P+(Q+R)$。

如果记 $2P=P+P$，$3P=P+P+P$，…，$mP=\overbrace{P+\cdots+P}^{m\text{个}}$，则称 mP 为椭圆曲线 E 上的点乘运算。如果存在最小的正整数 n，使得 $nP=O$，则称 n 是点 P 的阶。

对给定的 P 和 mP，求整数 m。这个问题是与有限域上的离散对数问题类似的一个问题，当点 P 有大的素数阶时，被称为椭圆曲线离散对数问题。

7.1.2　有限域上的椭圆曲线公钥密码体制

系统参数的选取与前面章节中的类似，但有些符号已略作修改，叙述如下：

1）选取定义在有限域 F_q 上的一条安全的椭圆曲线 E，使得 E 上的 F_q-有理点群的

阶被一个大素数 n 整除，保证椭圆曲线上有理点群上的离散对数问题是难解的。

2）选取一个基点 $P=(x_P,y_P)\in E$，P 的阶为 n，即有 $nP=O$，O 表示一个无穷远点，基点 P 公开。

3）设 Alice 和 Bob 为系统的两个用户，Alice 的私钥为 $k_A\in_R Z_n^*$，$P_A=k_AP\in E$，P_A 作为 Alice 的公钥。同样地 Bob 选择 $k_B\in_R Z_n^*$，$P_B=k_BP\in E$，P_B 作为 Bob 的公钥。它们的公钥 P_A 和 P_B 在系统内公开，并记 $P_A=(x_A,y_A)$，$P_B=(x_B,y_B)$。

椭圆曲线上的密码体制通常有两种用法：一是用于加密，二是用于签名。用于加密时，需使用接收方的公钥，而用于签名时，要使用自己的私钥。不论加密还是签名，第一个任务是要把发送的明文编码成椭圆曲线上的点 P_m，进行编码的方法在此不作介绍了。

有限域上的椭圆曲线加密算法描述如下：

Alice 要将明文 P_m 发送给 Bob，他首先选取一个随机整数 $k\in_R Z_n^*$，计算 $R=kP$，$S=P_m+kP_B$，然后将密文 (R,S) 发送过去。

Bob 收到后，计算 $S-k_BP$ 即可得明文 P_m。

显然 $S-k_BR=P_m+kP_B-k_BkP=P_m+kk_BP-k_BkP=P_m$ 成立。

有限域上的椭圆曲线签名算法描述如下：

签名者 Alice 利用系统参数、自己的私钥对消息 m 进行签名。

签名过程

1）Alice 选取随机整数 $k\in_R Z_n^*$，称 k 为消息密钥,要求保密；

2）计算 $R_1=kP=(x_1,y_1)$，$r=x_1 \bmod n$，若 $r=0$，则返回第一步；

3）计算消息 m 的 hash 值，并转化为整数 e；

4）计算 $s=k^{-1}(e+rk_A)\bmod n$，如果 $s=0$，则返回第一步；

5）Alice 对消息 m 的签名是 (r,s)。

验证过程

消息接收者 Bob 收到 Alice 的签名 (r,s) 后，首先从系统中获取域参数及 Alice 的公钥 P_A，然后做以下的操作进行验证：

1）验证 r,s 是 $[1,n-1]$ 中的整数，对消息 m 与签名过程一样做相同的处理得 e；

2）计算 $w=s^{-1}\bmod n$、$u_1=ew\bmod n$ 和 $u_2=rw\bmod n$；

3）计算 $X=u_1P+u_2P_A=(x',y')$，如果 $X=O$，则拒绝这个签名。否则，计算 $v=x'\bmod n$。当且仅当 $v=r$ 时接受这个签名。

事实上，$k=s^{-1}(e+rk_A)=ew+rwk_A=(u_1+u_2k_A)\bmod n$，所以 $u_1P+u_2P_A=kP$，即 $v=r_1$ 必须成立。

7.1.3 双线性映射的基本概念

在椭圆曲线中，有一类被称为超奇异曲线的椭圆曲线，该类曲线被认为是“弱”椭圆曲线。Menezes, Okamota 和 Vanstones 的工作[90]指出了这些椭圆曲线上利用椭圆曲线离散对数问题构建密码体制较标准的离散对数问题可使用较小的有限域的优势将消失。把超奇异椭圆曲线排除在密码应用之外已成为一个普遍接收的约定。

Joux 在文献[91]中首先利用椭圆曲线中的 Weil 配对构造了一个一轮三方密钥交换协议，Boneh 和 Franklin 用 Weil 配对构造了一个基于身份的加密体制[92]。从此以 Weil 配对技术为基础的各种密码学算法层出不穷，成为近年来的一个研究热点。

双线性对内容的简要介绍，详见文献[92]。

定义：设 G 是由 P 生成的循环加群，其阶为素数 q，V 是一个阶为 q 的循环乘群。双线性对是指具有下面性质的映射 $e: G\times G\to V$：

1．双线性：对所有的 $P,Q\in G$ 和 $a,b\in Z_q^*$，

$e(aP,bQ)=e(abP,Q)=e(P,abQ)=e(P,Q)^{ab}$。

2．非退化：存在一个 $P\in G$，满足 $e(P,P)\neq 1$。

3．可计算：对 $P,Q\in G$，存在一个有效的算法计算 $e(P,Q)$。

注：超奇异椭圆曲线中的 Weil 和 Tate 配对具有上述双线性性质。

假设 G 是一个加法群，在 G 上的四个数学难题分别为：

离散对数难题（Discrete Logarithm Problem，简记为 DLP）：设 P 和 G 是群中的两个元素，要找到某一个正整数 $n\in Z_q^*$，使之满足 $Q=nP$ 是困难的。

判定 Diffie-Hellman 难题（Decision Diffie-Hellman Problem，简记为 DDHP）：给定 $P,aP,bP,cP\in G$，其中 $a,b,c\in Z_q^*$，要判定 $c\equiv ab \bmod q$ 是否成立是困难的。

计算 Diffie-Hellman 难题（Computational Diffie-Hellman Problem，简记为 CDHP）：对 $a,b\in Z_q^*$ 给定 P,aP,bP，计算 abP 是困难的。

间隙 Diffie-Hellman 难题（Gap Diffie-Hellman problem，简记为 GDHP）：是指这样一类问题，在群 G 上，给定 $P,aP,bP,cP\in G$，容易判定 $c\equiv ab \bmod q$ 是成立的，但是计算 abP 是困难的，换句话说，在群 G 上，DDHP 易于解决而 CDHP 难以解决，则我们称此群为间隙 Diffie-Hellman 群，简记为 GDH 群。

这里我们假设 CDHP 和 DLP 是困难问题，即对该问题不存在具有不可忽略概率值的多项式时间算法。在群 G 上，若 DDHP 不是困难问题而 CDHP 是困难问题，即群 G 为间隙 Diffie-Hellman 群。这类群存在于超奇异椭圆曲线上。在 G 上，求双线性配对的逆是困难问题，即给出 $P\in G$ 和 $e(P,Q)\in V$，找 $Q\in G$ 还不存在有效的算法。

7.1.4 基于 ID 的密码体制

Boneh－Franklin 的基于 ID 的密码体制描述如下[92]。

系统参数的建立：

生成两个阶为素数 p 的群 G 和 V（同前），e 是一个双线性映射，任意选择一个生成元 $P \in G$。

选取 $s \in_R Z_p^*$，并计算出 $P_{pub} = sP$，s 作为主密钥。

选择一密码 Hash 函数 $h:\{0,1\}^* \mapsto G$，该杂凑函数把用户的身份 ID 映射到 G 中的一个元素。

选择一密码 Hash 函数 $h_1 : V \mapsto \{0,1\}^n$，该杂凑函数决定明文空间是 $\{0,1\}^n$。

公开的系统参数是 $(G, V, e, n, P, P_{pub}, h, h_1)$。

用户密码生成：

设用户 A 的惟一可识别身份标识是 ID，计算 $Q_{ID} = h(ID)$，这是 G 中的一个元素，是 A 的基于身份的公钥。可信中心根据申请人的身份 ID 计算对应的私钥，A 的私钥 $S_{ID} = sQ_{ID}$。

加密：

对消息 $m \in \{0,1\}^n$，加密人 B 选取 $r \in_R Z_p^*$，并计算 $g_{ID} = e(Q_{ID}, P_{pub})$、$U = rP$ 和 $V = m \oplus h(g_{ID}^r)$，以 $C = (U, V)$ 为消息 m 的签名。

解密：

用户 A 的私钥 S_{ID} 通过计算下式进行解密。

$$V \oplus h(e(S_{ID}, U))$$

算法成立的推导：

因为　$e(S_{ID}, U) = e(sQ_{ID}, rP) = e(Q_{ID}, P)^{sr} = e(Q_{ID}, P_{pub})^r = g_{ID}^r$

所以由异或运算的性质得

$$V \oplus h(e(S_{ID}, U)) = V \oplus h(g_{ID}^r) = m \oplus h(g_{ID}^r) \oplus h(g_{ID}^r) = m$$

7.2 基于 ID 的盲签名方案

本方案是基于 GDH 群而提出来的，包括四个步骤：初始化过程、密钥提取过程、签名过程和验证过程。

设 G 是阶为 q 的 GDH 群，其中 q 是素数，V 是阶为 q 的加法群，e 是 $G \times G$ 到 V 的双线性映射。

[初始化过程]：

初始化过程由可信中心（TA）完成。P 是 G 的一个生成元。随机选择一个数 $s \in_R Z_q^*$，计算 $P_{pub} = sP$。选择两个公开的加密用的哈希函数 $h:\{0,1\}^* \to G$ 和 $h_1:\{0,1\}^* \to Z/q$。则系统的公开参数为 $(G, V, q, P, P_{pub}, h, h_1)$，系统主密钥为 s。

[密钥提取过程]：

设用户 A 的惟一可识别身份标识是 ID，计算 $Q_{ID} = h(ID)$，这是 G 中的一个元素，是 A 的基于身份的公钥。可信中心根据申请人的身份 ID 计算对应的私钥，A 的私钥 $S_{ID} = sQ_{ID}$。

[签名过程]：

m 是一条待签名的消息。签名过程如图 7.2.1 所示：

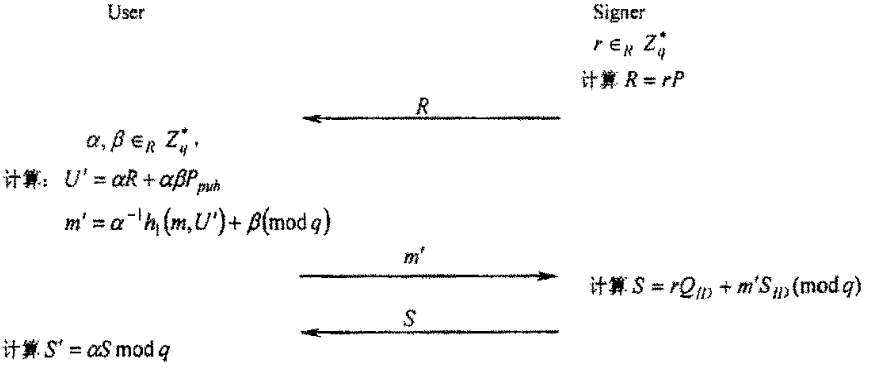

图 7.2.1　盲签名过程图

Step1：签名人随机地选择一个整数 $r \in_R Z_q^*$，计算 $R = rP$，然后将 R 发送给用户。

Step2：（盲化）用户随机选择两个整数 $\alpha, \beta \in_R Z_q^*$ 作为盲化因子，计算 $m' = \alpha^{-1} h_1(m, U') + \beta \pmod q$，然后将 m' 发送给签名人。

Step3：（签名）签名人计算 $S = rQ_{ID} + m'S_{ID}$。

Step4：（去盲）用户计算 $S' = \alpha S$，输出 (m, U', S')，即 (U', S') 为消息 m 的盲签名。

[验证过程]：

要验证盲签名的正确性，需要判断 $e(S', P)$ 与 $e(h_1(m, U')P_{pub} + U', Q_{ID})$ 是否相等，如果相等，则说明签名是正确的，否则，拒绝接受签名。

方案分析

(1)正确性分析

由双线性的定义及性质，以及上述盲签名方案中使用的变量和符号定义，得到下列等式：

$$\begin{aligned} & e(S', P) \\ &= e(\alpha(rQ_{ID} + m'S_{ID}), P) \\ &= e(\alpha(rQ_{ID} + (\alpha^{-1} h_1(m, U') + \beta)S_{ID}), P) \\ &= e(h_1(m, U')Q_{ID}, sP)e(\alpha r Q_{ID} + \alpha\beta s Q_{ID}, P) \\ &= e(h_1(m, U')Q_{ID}, sP)e((\alpha r + \alpha\beta s)P, Q_{ID}) \end{aligned}$$

$$= e(h_1(m,U')Q_{ID}, P_{pub})e(U', Q_{ID})$$
$$= e(h_1(m,U')P_{pub} + U', Q_{ID})$$

上述等式成立说明,基于 ID 的盲签名方案是正确的。

(2)安全性分析

• 盲性(blindness)：指签名人对所签的消息 m 一无所知,换句话说,只有消息所有者才知道消息的内容,这样很好地保护了消息拥有者的隐私。

因为在签名方程中用户引入了两个盲化因子 $\alpha,\beta \in_R Z_q^*$，签名人对盲化消息 m' 进行签名，他不可能知道所签消息的内容是什么，从而满足盲性的要求。

• 不可追踪性(untraceability)：指签名人在签名后，不能根据其保留的中间计算结果把签名和盲消息对应起来。也就是说签名人不能根据他所掌握的中间结果来判断一个盲签名是否是他签的,我们把这种性质称为不可追踪性。

给定一个合法的签名 (m,U',S')，对于任何一组签名人可得到的中间结果 (R,m',S)，总存在特定的一对盲因子 $\alpha,\beta \in_R Z_q^*$ 与之对应，这说明中间结果可以对应任何一个签名，签名人由此不能推断这个签名是否是自己签过的，即他不能把中间结果和原始签名 (R,S) 对应起来，即他不能根据中间结果追踪签名。下面给出其证明过程。

给定签名 (m,U',S') 和中间结果 (R,m',S)，由签名过程得知以下等式成立：

$$m' = \alpha^{-1}h_1(m,U') + \beta \pmod q \qquad (1)$$

$$S' = \alpha S \bmod q \qquad (2)$$

由(2)得 $\alpha = (S')^{-1}S \bmod q, \alpha \in_R Z_q^*$，不妨仍记为 α，再由(1)得 $\beta = m' - \alpha^{-1}h_1(m,U')$。这样任何一对签名和中间结果均可以求得一组参数 α,β。

还需证明求得的这组参数 α,β 满足 $U' = \alpha R + \alpha\beta P_{pub}$，根据双线性配对的非退化性，只须证明 $e(U', Q_{ID}) = e(\alpha R + \alpha\beta P_{pub}, Q_{ID})$。

因为 (m,U',S') 是合法的盲签名，所以满足验证方程 $e(S',P) = e(h_1(m,U')P_{pub} + U', Q_{ID})$。从而有

$$e(\alpha R + \alpha\beta P_{pub}, Q_{ID}) = e(\alpha R + \alpha(m' - \alpha^{-1}h_1(m,U'))P_{pub}, Q_{ID})$$
$$= e(\alpha rP + \alpha m'P_{pub}, Q_{ID})e(h_1(m,U')P_{pub}, Q_{ID})^{-1}$$
$$= e(\alpha rQ_{ID} + \alpha m'S_{ID}, P)e(S',P)^{-1}e(U', Q_{ID})$$
$$= e(\alpha S, P)e(-S',P)e(U', Q_{ID})$$
$$= e(U', Q_{ID})$$

上述证明说明了由签名和中间结果均可以求得一组符合条件的参数 α,β，但是这个签名未必是中间结果对应的签名，据此不能断定和原始签名的联系，即证明了盲签名的不可追踪性。

• 不可伪造性(unforgeability)：签名持有人不能根据已有的合法签名，私自构造出其它的有效签名。盲签名可以应用于电子货币系统的货币认证，较好地满足了用户私

有信息的保密要求,它的不可伪造性更是必不可少的。用户(user)不能根据银行(signer)提供的签名伪造出更多的合法签名，即不能私自捏造出货币来。

不可伪造性是指攻击者包括用户或第三方不可以伪造签名(m,U',S')。任何攻击者可以获得的信息包括：系统的公开信息(G,V,q,P,P_{pub},h,h_1)和所要伪造的签名人的公钥Q_{ID}。攻击者试图伪造签名可以通过三种途径实现，这三种攻击方法都建立在一定的假设之上，实际中这些假设可能并不会得到满足，因此我们假定攻击者可以获得最有利攻击的条件。第一个假设指将密钥产生机构看作一个问答机，不需要身份验证，对任何人的询问都予以回答。第二个假设指将签名人看作一个问答机，对任何人的签名要求都予以满足。

第一种攻击方法是攻击者要求密钥产生机构产生自己所选的$ID_i(i=1,\cdots,q)$(其中 q 为攻击者可以询问密钥产生机构的次数，$q>0$；$ID_i \neq ID$，ID为攻击对象的身份) 对应密钥S_{ID_i}；第二种攻击方法是攻击者要求签名人对自己所选信息进行签名，以便攻击人通过签名过程的交互获得(R,m',S)，再推导出私钥S_{ID}；第三种攻击方法是攻击人任意构造出一个(m,U',S')使其满足验证方程。这三种攻击方法对于本方案都是不适用的。

（3）计算时间效率分析

为了比较本方案与其它方案的计算时间效率，不妨设T_e表示计算一次$e(P,Q)$所需的时间，T_{p_mul}表示一次G上的点乘所需时间，T'_{p_mul}表示一次V上的点乘所需时间，T_{p_add}表示一次G上任意两点相加所需时间，T_{n_mul}表示一次任意两个整数在模意义下的数乘所需的时间，T_{n_div}表示一次求Z_q^*上数的逆元所需的时间。

比较本方案与文献[94]、[95]中提出的基于 ID 的盲签名方案，得到了这三种方案在不同阶段的计算时间的情况如表 7.2.1 所示。从表 7.2.1 中得知，本方案的计算时间效率与方案[95]相当，但比方案[94]有所提高。

而且本方案在验证时还可以运用批验证方法[96]来进行验证，以提高验证的效率。例如，银行系统中验证电子现金的数据量就比较大，这对系统的效率要求非常高。不妨假设$(U_1',S_1'),(U_2',S_2'),\cdots,(U_n',S_n')$是一串消息$m_1,m_2,\cdots,m_n$的基于某签名人 ID 的盲签名，应用批验证的方法，如果验证式$e\left(\sum_{i=1}^{n}V_i',P\right)=e\left(\sum_{i=1}^{n}\left(H(m,U_i')P_{pub}+U_i'\right),Q_{ID}\right)$成立，那么就可以一次完成验证工作；但是，如果该等式不成立，那么就需要分组再进行处理。一般情况下，前者成立的可能性较大，总的说来，本方案在计算效率方面优于方案[94]。

表 7.2.1　不同方案计算时间对照表

本方案	方案[94]	方案[95]

盲化	签名	验证	盲化	签名	验证	盲化	签名	验证
		$2T_e$			$2\ T_e$	T_e		$2\ T_e$
$3T_{p\_mul}$	$3T_{p\_mul}$	T_{p_mul}	$3\ T_{p\_mul}$	$2\ T_{p\_mul}$	T_{p_mul}	$3\ T_{p\_mul}$	$3\ T_{p\_mul}$	T_{p_mul}
T_{p_add}	T_{p_add}	T_{p_add}	T_{p_add}		T_{p_add}	$3\ T_{p\_add}$	T_{p_add}	
$2T_{n\_mul}$			T_{n_mul}			$2T_{n\_mul}$		
T_{n_div}			T_{n_div}					
								T_{p_mul}
$2T_e+7\ T_{p\_mul}+3\ T_{p\_add}+2T_{n\_mul}+T_{n\_div}$			$2T_e+6\ T_{p\_mul}+2\ T_{p\_add}+T_{n\_mul}+T_{n\_div}$			$3T_e+7\ T_{p\_mul}+4\ T_{p\_add}+2T_{n\_mul}+T_{p\_mul}$		

7.3 本章小结

本章利用双线性映射理论，在盲签名的基础上构造了基于 ID 的盲签名，该方案以 ID 为基础的公钥取代了以数字证书为基础的公钥，省略了验证签名时从系统中获取公钥的步骤，减少了交互的次数并节省了存储空间。这种方案可以应用于电子现金系统和在线投票系统等。

本章评注

虽然利用双线性映射理论来构造盲签名，不失为一种较好的建立盲签名方案的途径，但还需要进行基础理论的深入探讨和研究，尤其是对于安全性的分析，缺乏安全理论模型的支持，其理论的完备性研究甚少，而且到目前为止，由于基于椭圆曲线上的 weil 配对的算法及编程实现尚未完全解决，这些都需要进一步研究。

8 匿名电子投票协议设计及系统实现

8.1 引言

近年来电子投票问题受到人们越来越广泛的关注和研究，它与传统的实物选票形式相比较，其显著特点是投票者不需要到一个指定的投票箱投票，具有很高的效率和灵活性。具体体现在两方面：首先，组织者利用电子投票可以省去在组织工作、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，投票人可以不到有关管理部门指定的投票处投票，通过网络投票快捷方便。

电子投票的探讨和实践由来已久。1884 年，发明天才爱迪生发明了一种电子投票装置，主要功能是能自动地进行会场投票计数。不幸的是这个很实用的装置，竟被国会拒绝采用，因为计数太准确了。虽然电子计票失败了，但人们对电子投票方式的研究和憧憬一直未改。随着计算机的出现，人们开始利用计算机进行电子选举的尝试。1958 年，哥伦比亚广播公司（Columbia Broadcasting System）选举总部开始利用计算机对投票结果进行预测。1964 年，美国有 5 个县在选举中使用了计算机。在 1992 年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，并在站内设立相应的电子投票装置，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。在 2004 年美国总统大选中，一些州政府积极试用新的电子投票系统。但许多安全问题专家警告称，使用这些计算机投票系统极有可能导致投票欺诈行为，也可能因为黑客攻击而出现投票数据错误。其他一些专家也认为，如果使用电子投票系统，一旦在选举中出现选票争论，重新计票几乎不可能。不过，支持使用电子投票系统的人则表示，利用计算机技术将可以更加明确地记录选民的投票意向，其精确度肯定高于手写选票。通过 Internet 进行投票选举仍然处于摸索、实验阶段。

电子投票作为消息认证系统的重要课题之一，必须要从理论上进行关键技术的研

究和论证，也就是说要设计基于数字签名理论的安全的电子投票协议，保证投票人身份的匿名性、选票的秘密性和公平性，以及方案的高效性。Benaloh[97]和 Iverson[98]利用高度剩余加密技术提出了一些电子投票方案。然而，当选举人数较多时，这些方案中数据的通讯量和计算量就无法忍受，所以这些方案都不适合大群体的选举。

Chaum[99]和 Ohta[100]利用匿名通讯信道分别给出了一种适合于大群体选举的投票方案，而且保证了投票者的匿名性，然而这两个方案都没有解决选票的秘密性和公平性。当投票者发现自己的选票没有被正确计入时，他必须通过公开选票来要求计票机构加入自己的选票，这样就泄露了自己的选票；而且，管理者可以知道选举的一些中间结果，所以他能通过泄露这些信息影响选举的最终结果，从而破坏了选票的公平性。Asano[101]提出的方案解决了公平性的问题，但该方案要求管理者是公正的，一旦管理者作弊，仍是不安全的。Sako[102]随后提出的方案虽然解决了秘密性问题，但是又没有解决公平性的问题。Fujioka[103]利用比特承诺协议和盲签名技术提出了一个实用的、秘密的，适合于大群体选举的电子投票方案。该方案同时保证了选票的秘密性和公平性，而且也解决了投票者身份的匿名性问题。但是，它仍然有一些缺点：首先，它没有解决“选票碰撞”的问题。如果两个投票者使用相同的随机密钥及以相同的方式投票，那么选票及其签名就完全一样。于是计票机构去掉一些重复的选票而伪造另一些“合法的”的选票，但是投票者无法察觉。其次，使用比特承诺协议虽然保证了选票的公平性，但是在计票时需要投票者提供自己的随机密钥 k。如果投票者提供一个非法的密钥，则对应的选票无法打开。为了区分不诚实的投票者和不诚实的计票机构，Fujioka 建议将该密钥发送给几个相互独立的机构(如不勾结的候选人)，这不仅增加了选举中数据的通讯量和计算量，而且如果投票者中途退出，即不发送随机密钥，则对应的选票无法打开。计票机构就可能与管理机构相勾结来影响投票结果(剔除该选票而加入其它结果)。最后，Fujioka 的方案要求弃权者提交一张空白选票来防止选举中的腐败行为(管理者就有可能代替这些选举者投票)，但实际上如果选举者决定放弃选举，他就不愿花费时间来提交一张空白选票。

国内也开展了这方面的研究[104~109].汪保友等[106]利用盲知识签名提出了一种在线选举方案,但实现起来具有一定的难度。周怡丹等[107]提出了一种基于盲签名的电子选举方案,但没有解决当某人重复投票时如何进行追踪以剔除不诚实投票者的问题或者有人假冒投票如何进行鉴别等问题。陈晓峰等人[109]利用群签名协议和时限承诺协议，给出了一种新的基于匿名通讯信道的安全电子投票方案。诚实的投票者可以无条件保持身份匿名，然而不诚实的投票者则一定能被可信赖的注册机构追踪到。而且可证明即使管理机构和计票机构勾结，在计票前可同时保证选票的秘密性和公平性。除此之外，该方案还解决了选票碰撞以及投票者的中途退出等问题。

本章研究了目前电子投票的研究现状，本着从实用的角度出发，试图制定一个比

较实用的电子投票协议，研制有实用价值的系统原型。为此，基于电子投票系统应当满足的性质，设计了一种匿名电子投票协议，并基于该协议进行了系统的软件设计，给出了部分核心算法的实现过程。

8.2 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.一个安全的电子投票协议应满足下列基本性质:

(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。

8.3 匿名电子投票协议设计及安全性分析

一般来说，匿名电子投票系统由四部分构成，包括认证中心（Certificate Authority，简称 CA）、管理机构(Administration Organization，简记为 A)、投票人(Votor，简记为 V)和计票机构(Counting Organization，简记为 C)。认证中心负责向管理机构、计票机构和所有投票人颁发数字证书，数字证书中存放参与方的身份信息及公钥等信

息；管理机构负责对投票人的身份进行审核，确认后颁发正式选票；计票机构负责对选票的有效性进行验证、计票,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。

8.3.1 匿名电子投票协议设计

由于公钥密码体制既可用于加密，也可用于签名，因此，匿名电子投票协议是基于公钥密码体制基础而进行设计的，具体描述如下：

(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。不妨记 A 的公钥为 PKa，私钥为 SKa；同样 C 的公钥记为 PKc，C 的私钥记为 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 $SIG_{SKv}(IDv||Rv)$，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(·)为一哈希函数。A 用自己的私钥进行签名 $SIG_{SKa}(Nv||MACv)$，并将 $SID_{SKa}(Nv||MACv)$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 的公钥进行解密，解密后得(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 $Rv||SID_{SKa}(Nv||MACv)$，以此证明自己是经认证过的合法的投票人。

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 $SID_{SKa}(Nv||MACv)$发送给计票中心 C，同时公布所有的$(Nv, SID_{SKa}(Nv||MACv))$，并宣布在某一时刻开始投票。

(3)投票协议

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 C 发给选票 M，选票中包含 Nv 及 C 的签名 $SIG_{SKc}(Nv)$。

Step2：V 根据自己的意愿填上选票内容，对 M||Nv 进行盲化处理得 M'，并用 A 的公钥加密得 $SID_{PKa}(Nv||SIG_{SKc}(Nv)||M')$，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：$Nv||SIG_{SKc}(Nv)||M'$，然后用 C 的公钥 PKc 验证 $Nv=D_{PKc}(SIG_{SKc}(Nv))$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 $SIG_{SKa}(M')$，然后传送给 V。

Step4：V 进行去盲处理后，得到 A 的签名 $SIG_{SKa}(M||Nv)$，这时 V 用 C 的公钥 PKc 加密得 $SIG_{PKc}(M||Nv||SIG_{SKa}(M||Nv))$并传递给 C。

Step5：C 收到后，用私钥解密得 $M||SIG_{SKa}(M||Nv)||Nv$，首先验证 $M||Nv=D_{PKa}(SIG_{SKa}(M||Nv))$是否成立？如果成立，则说明是经 A 签名过的投票，这些 C 对 $S_f=SIG_{SKc}(Nv||T)$进行签名并发给 V,V 保留 S_f,用以证明自己投过票.同时 C 还需要检查是否存在 Nv 或是否是第二次计票，以保证正确计票，并宣布在某一时刻结束投票,在这一阶段,未投票的人视为弃权处理。投票结束后,C 将所有参加投票的 Nv 公布，进入复查投票阶段。

(4)复查投票协议

计票中心宣布第一阶段投票结束后，将所有正式投票的人的编号予以公布。在这一阶段,投票人检查自己的选票是否被公布,如果没有发现自己的编号，则可以在规定的一段时间内向计票中心提交 S_f 以示抗议,并进行重新投票,充分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)计票协议

在某一时刻,C 宣布终止复查,进行统一计票.之前不能透露任何投票信息，以保证对任何被选举人是公平的，不能因为前面的投票情况而影响后面投票人的投票倾向。计票结束后，公布统计结果。

8.3.2 协议的安全性分析

(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。但是在注册协议阶段，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 $SIG_{SKv}(IDv||Rv)$，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。在投票阶段，投票人对 M||Nv

进行了盲化处理得 M'，并用 A 的公钥加密得到 $SIG_{PKa}(Nv||SIG_{SKc}(Nv)||M')$，将其发给 A。管理机构解密后并不知道选票的具体内容，只是验证投票人的选票是否有效，然后再签名，使其合法化。

(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。

注 1：选票碰撞问题。这个问题在 Fujioka 的方案中没有提到，是指如果两个投票者如果投票的内容相同，而且 A 和 C 勾结，只公布一张有效选票，那么他们就可以伪造一张选票而不被察觉。在我们的方案中，计票机构必须公布所有投票人选举的统一编号，并进行计票，这项工作不由人工操作，由计票服务器自动完成，我们认为可以解决选票碰撞的问题。

注 2：管理机构的信赖问题。在投票人向管理机构申请选票编号时，要提供身份证号码和公钥，而且管理要保留这些信息，这样做的一个前提是管理机构是高度信任的。如果管理机构把这些信息透露给计票机构，计票机构是可以知道投票人的选举结果的。

注 3：有限匿名问题。在投票人向管理机构和计票机构通信过程中，我们通过消息认证和签名手段等技术上的处理，即使攻击者获得通信信息也无法得知投票人的真实情况，而且计票机构也不能把选票编号和投票人联系起来，因此，我们说这个方案具有匿名性。当然，这不是绝对的，正如上段分析的那样，如果管理机构不信任的话，再和计票机构勾结就可能透露选举情况，这对投票人是非常不利的。如果对投票人做到绝对匿名的话，带来的一个新问题是组织者无法追踪不诚实的投票人。

总之，我们给出的方案符合电子投票具有的基本性质，而且还可以有效地防止一人多票或一票多投现象的发生。

8.4 系统设计与实现

在协议中已指出，一个电子投票系统由四部分组成：认证中心、管理机构、投票人和计票机构。系统的数据流程图如图 8.4.1 所示。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、选票签名模块和计票模块。

1．系统初始化模块设计

本模块实现的功能有：CA 为用户（管理机构、计票机构和投票人等）颁发数字证书，且私钥秘密传递给用户、用户将私钥加密后自己保存。

采用 RSA 公钥密码体制，要求公钥密钥的长度达到二进制 1024 位，其中私钥由 DES 加密保存在用户的专门文件中，公钥则存放在经过 CA 中心签名的数字证书中。CA 初始化参数包括：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。CA 通过这种机制管理机构 A 颁发公钥，记为 PKa=(n,e)，私钥记为 SKa=d（公钥和私钥的二进制位为 1024 位）。

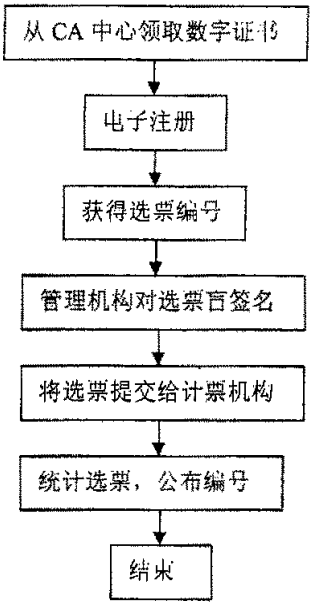

图 8.4.1　匿名电子投票系统流程图

RSA 算法中要用到大素数，虽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。

反过来，我们考虑先生成一个随机数，然后再测试它是否为素数，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。拉宾-米勒测法的的流程图如图 8.4.2 所示。

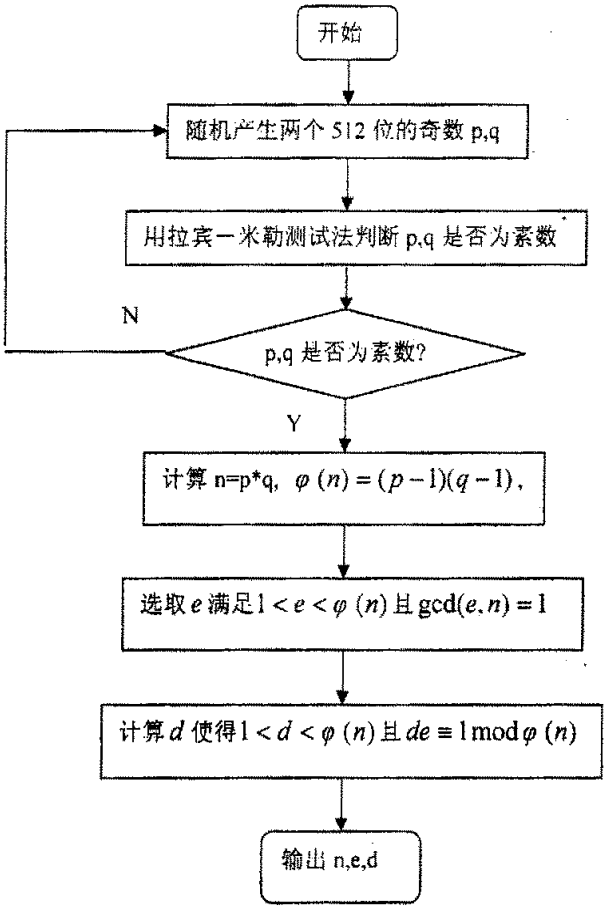

图 8.4.2 拉宾-米勒测法的的流程图

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。

系统公钥是可以公开的，无保密性的要求，可以存放在 CA 中心的数据库中，供用户查询使用。再看一下系统私钥，由持有人妥善保管，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。

2．注册模块设计

注册模块实现的主要功能是：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 $SIG_{SKv}(IDv||Rv)$，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。注册模块的数据流程图如图 8.4.3 所示。

3．选票签名模块设计

选票签名模块的设计是本系统设计的核心内容，它实现的功能主要是：管理机构对提交的盲化电子选票进行盲签名使其合法化，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。

具体描述：投票人 V 将选票编号 Nv 和 A 的签名 $SIG_{SKa}(Nv||MACv)$提交计票机构服务器，计票机构服务器对 $SIG_{SKa}(Nv||MACv)$进行验证，若签名正确则用私钥签名然后将 $SIG_{SKc}(Nv)$ 发送给 V。投票人 V 根据自己的意愿填上选票内容 M，对 M||Nv 进行盲化处理得 M'，并用 A 的公钥加密 $Nv||SIG_{SKc}(Nv)||M'$后将其提交管理机构服务器。管理机构服务器对提交的盲化电子选票进行盲签名使其合法化，然后发送给投票人 V，但无法知道其选票的真实内容。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。

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。

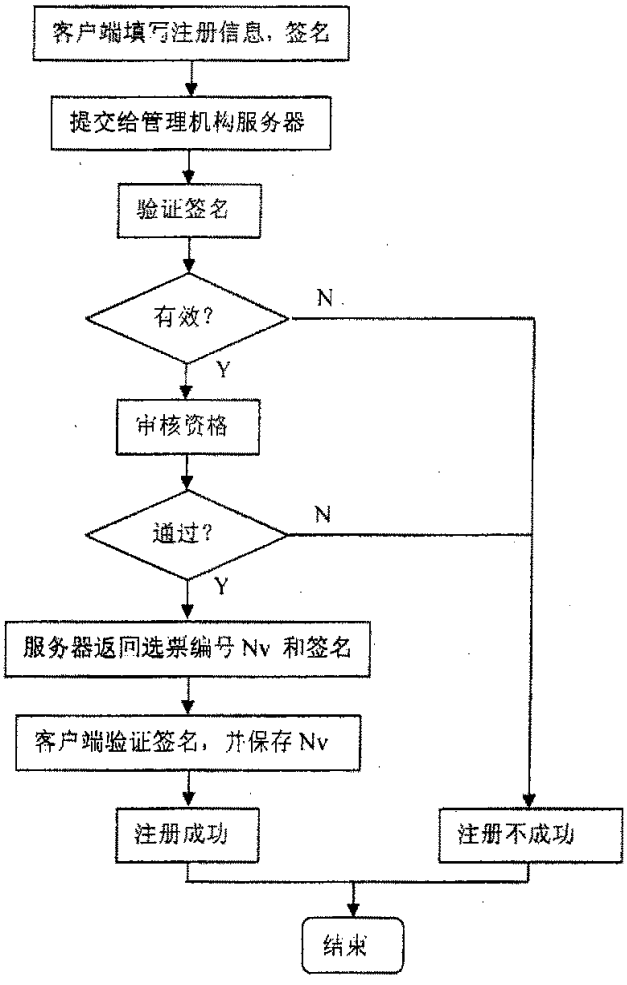

图 8.4.3 注册模块的流程图

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。

先定义大整数类 CBigInteger 及相应的模幂运算、模逆运算、模乘运算等函数，

实现盲签名协议的功能。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 $S_m=(M')^d \bmod n$，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 $S_m=k^{-1}S_{m'}=k^{-1}(M')^d \bmod n=(h(M||Nv))^d \bmod n$，这时 V 用 C 的公钥签名得 $Se=(M||Nv||S_m)^{e'} \bmod n'$。并传递给 C。

```
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
    ……
}
```

4. 计票模块设计

本模块实现的主要功能是：验证投票人的选票的真伪，并进行计票。投票人 V 用计票机构 C 的公钥加密电子选票及签名，并提交计票机构服务器。计票机构服务器收到后用自己的私钥解密得到选票及签名，首先验证签名是否正确，如果正确则说明是经 A 签名过的选票，然后通过检查数据库判断是否是第二次计票，以保证正确计票。

第一阶段投票结束后，计票机构 C 将所有选票的 Nv 公布，使得投票人知道自己的选票是否被计入。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，以保证所有的选票都能被有效地接收。

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 $M||Nv=(S_m)^e \bmod n$ 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。

8.5 本章小结

本章分析了目前电子投票的研究现状，主要做了以下工作：

（1）提出了一种匿名电子投票协议，该协议除满足电子投票的基本性质外，较好地解决了选票碰撞以及投票者的中途退出等问题，而且还可以有效地防止一人多票或一票多投现象的发生，即使管理机构和计票机构勾结，在计票前可同时保证选票的秘密性和公平性。

（2）从实用的角度对电子投票系统进行了系统设计，对各功能模块进行了详细设计，编程实现了其中的核心算法及部分功能。

本章评注：

评注 8.1 将盲签名用于电子投票系统，虽然可以较好地满足匿名性和安全性等要求，但运算较繁琐，计算比较复杂。

评注 8.2 本章给出的协议是基于公钥的数字证书来证明投票人身份，因而依赖于公钥基础设施的建立，目前还不普遍。如果采用基于指纹识别系统对身份进行确认，操作起来比较直观，但指纹取样的成本不容忽视。

评注 8.3 电子投票问题仍然是一个需要在理论和实际应用中值得继续研究的问题，只有当在理论上比较完善，应用上比较方便才可能得到较好的应用。

评注 8.4 关于大数的运算,目前有许多网站提供了技术支持比较好的网站有：

Crypto++：http://www.eskimo.com/~weidai/cryptlib.html（C++）

MIRACL：http://indigo.ie/~mscott/（C/C++）

GNU MP：http://www.swox.com/gmp/ （C）

cryptlib：http://www.cs.auckland.ac.nz/~pgut001/cryptlib/

RSARef：http://download.gale.org/rsaref20.tar.Z

9 结论与展望

全文比较系统地对数字签名理论、方法和应用进行了研究和探讨，重点研究了数字签名中的若干关键技术问题，得到了如下一些结论：

（1）给出了 ElGamal 型数字签名方程参数选取的一般方法，使得这种类型的签名方程并不局限于 Harn 的 18 种，这说明沿着参数的不同组合去构造不同的签名方程是无法穷尽的，因此我们给出了构造有效的签名方程的参数选择原则和方法。

（2）将基于 DLP 的签名方案的具有消息恢复特性平移到椭圆曲线密码体制中来，得到了基于椭圆曲线密码的具有消息恢复的签名方案，这项工作不能简单地等同于基于 DLP 的方案，且本方案只能限于指定的接收者接收，因此除具有签名作用外，还具有消息的保密性作用。同时讨论了所给出的方案的参数的一般形式及选取方法，列举出不同形式的各种签名方案，从而弥补在这个领域上的不足。

（3）给出了 HMP 认证加密方案中签名方程的参数选取的一般原则和方法，并由此列举了不同参数组合下相应的签名方程和消息恢复方程表；指出在 HMP 认证加密方案中存在两种已知明文的伪造攻击方法，从而说明符合一定条件的签名方案可以避免这样的攻击；提出了一种基于椭圆曲线的具有消息恢复的认证加密方案，对其安全性进行了分析，同时对这种方案进行了推广，并指出与 HMP 认证加密方案一样，在映射为同态函数的情况下存在已知明文的攻击问题；考虑到消息链接恢复特性，给出了相应的认证加密方案，并进行了信息传输量和计算复杂度的对比分析，该方案较好地解决了消息加密认证、消息链接恢复及传输量较大等问题。

（4）提出了一种基于公钥自证明的认证加密方案，采用用户注册协议动态地完成用户向 CA 的匿名身份注册，并获取由 CA 和用户共同产生的公钥的证明，据此可以计算用户的公开密钥；通信双方使用公钥的自证明协议，动态地完成对彼此公钥的自证明；信息的接收者可以从签名中恢复原消息。这种方案体现公钥自证明的思想和实现手段更完备，对用户而言进行匿名身份注册，保证了用户的匿名要求。针对消息分块情况，给出了一种具有消息链接恢复的基于公钥自证明的认证加密方案。该方案具有第三层次的信任等级、较少的计算时间开销和较高的安全性等优点。

（5）提出了构造 ElGamal 型弱盲签名方案的方法，用此种方法构造的弱盲签名方案几乎包含了目前所有该类签名方案；分别给出了基于离散对数和椭圆曲线的多元线性变换的代理盲签名方案的构造方法，该方法较好地刻画了委托人和代理签名人以

及代理签名人与信息拥有者之间的联系；把这种签名方案与消息的恢复特性结合起来，分别给出了具有消息恢复、消息链接恢复的代理盲签名方案。

（6）基于椭圆曲线上 Weil 配对的双线性理论，提出了基于 ID 的盲签名方案，该方案以 ID 为基础的公钥取代了以数字证书为基础的公钥，省略了验证签名时从系统中获取公钥的步骤，减少了交互的次数并节省了存储空间。

（7）基于盲签名技术提出了一种匿名电子投票协议，该协议除满足电子投票的基本性质外，较好地解决了选票碰撞以及投票者的中途退出等问题，而且还可以有效地防止一人多票或一票多投现象的发生，即使管理机构和计票机构勾结，在计票前可同时保证选票的秘密性和公平性；从实用的角度对电子投票系统进行了系统设计，对各功能模块进行了详细设计，编程实现了其中的核心算法及部分功能。

以上是作者近几年来开展研究工作所取得的一些成绩，但有些研究工作才刚刚起步，还需要不断地深入下去。限于掌握的资料和研究水平所限，还存在许多问题需要继续研究。下面列出的问题是目前研究的一些热点问题。

安全形式化证明问题。虽然我们探讨了许多不同形式的签名方案，并进行了安全性分析，但没有从理论上对签名方案的安全性给出形式化的证明。因此，安全协议的形式化分析方法、可证明安全性理论、安全多方计算理论和应用协议的设计与分析等问题是密码学界研究的难点问题，也是目前国际上研究的一个热点问题。

轻量密码研究问题。由于无线通信技术的飞速发展，无线保密通信和签名成为无线通信领域新的研究热点。无线保密通信的最大特点是：密钥短、计算时间少、传输信息量小等，因此适用于这个领域的密码体制是人们热盼的目标。

新型数字签名方案问题。随着全球信息化进程的加快，在现实生活中的许多工作都将由各种各样的信息系统完成，要适合各种不同的应用，必须要有相应的技术手段做支撑。因此，各种各样的符合特殊需要的数字签名方案应运而生。多重签名、群签名、代理签名、盲签名、部分盲签名、环签名等签名方式在一些应用环境中有其独特的作用，然而这些特殊数字签名技术远没有到尽善尽美的地步，还需要进行深入的研究，有许多问题还没有很好地解决，其中部分问题具有相当的挑战性。将这些技术很好地应用于实际还有一段路要走。

网络身份认证综合技术问题。建立在 PKI 之上的公钥数字证书在近几年得到了较快的推广和应用，但基于生物特征的网络身份认证比如指纹认证技术比数字证书用起来更加方便，因此在计算机网络环境下，为了保障安全通信，综合运用各种身份认证技术将是未来发展的趋势。

总而言之，随着计算机网络技术、信息处理技术和网络安全技术的发展，网络通信将变得更加安全可靠，与此同时，现实生活中的许多工作将逐步转移到网络上开展是一个大潮流，电子投票、电子拍卖、电子政务、移动安全计算等各种应用又反过来

促进网络安全技术、信息安全技术的发展,作为这些技术的基础研究之一数字签名技术将会更加丰富和实用。

致 谢

本文的完成，自始自终得到了我的导师刘凤玉教授的关心、指导和帮助，没有老师的热情鼓励和精心培养，本文是不可能完成的，离开了老师的亲切关怀和教育，作者也不可能在学术领域取得现在的成绩。在四年的研究学习期间，是刘老师给予我耐心的指导、严格的要求和及时的帮助，使我渐渐地在学术方面得到了较快的成长；是刘老师正直的为人、乐观的人生态度和崇高的师德给了我克服困难、勇于探索的信心和力量，这将使我终身受益，在此，谨向恩师表示最诚挚的感谢，道一声：刘老师您辛苦了。

在攻读学位期间，作者得到了南京大学计算机系许满武教授、南京理工大学计算机系的张宏教授、王宗月老师的关心和帮助，也得到了作者所在计算机系和研究生院领导的关心和支持，在此向他们表示深深的谢意。向作者攻读硕士学位期间的导师中南大学关家骥教授的鼓励和关心表示感谢。

作者向所在教研室的严悍博士、张琨博士、李千目博士和袁宜硕士等给予的关心和帮助表示感谢。向同窗学习好友孙向军、徐慧、刘春庆、陈才扣、宋枫溪、王元全、石澄贤、马建伟等同学的关心和帮助表示感谢。向淮阴师范学院吴克力博士、扬州大学杨云博士、江苏大学周莲英博士和朱小龙博士也一并表示感谢。

在此，还要向师兄中南大学武坤教授的关心和帮助表示感谢。

特别要感谢的是作者所在单位河海大学计算机及信息工程学院(常州)的领导和同事们，是他们的关心、理解和支持，为作者创造了良好的学习、工作和研究条件。

最后，作者十分感谢数十年来节衣缩食的父母和精心照顾年迈父母的哥哥姐姐们，是他们全力的支持和关心使作者免除后顾之忧来完成学业。特别要感谢的是我的妻子李然琼，十多年来在生活上的关心和精神上的理解与支持。还要感谢我的女儿赵明璐，在繁忙的生活中给我们家带来的欢乐和笑声。

谨以此文献给所有爱我和关心我的人们!

参考文献:

1 Diffie W,Hellman M E. New directions in cryptography[J]. IEEE Transactions on Information Theory.1976,IT-22(6):644~654.

2 Revist R L,Shamir A,Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J].Communications of the ACM. 1978,21(2):120~126.

3 冯登国,卿斯汉.信息安全－核心理论与实践.北京:国防工业出版社,2000.

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

5 Mao W 著,王继林等译.现代密码学理论与实践.北京:电子工业出版社,2004.

6 吴克力.数字签名理论与算法研究[D]. 博士学位论文. 南京：南京理工大学，2004.

7 张键红,韦永壮,王育民.基于 RSA 的多重数字签名[J].通信学报,2003,24(8)：150~154.

8 王庆梅,吴克力,刘凤玉.具有消息认证功能的多重数字签名方案.计算机工程,2003,29(19):13~15.

9 Harn I，Keisler T. New scheme for Digital Multisignature[J]. Electronic Letters，1989，25(15):1002~1003.

10 Mitomi S,Miyaji A.A general model of multisignature schemes with message flexibility,order flexibility,and order verifiability[J]. IEICE Trans.，Fundamentals. 2001,E84-A(10):2488~2499.

11 Lin C Y,Wu T C,Hwang J J.ID-based Structured Multisignature Schemes[A]. Advances in Network and Distributed systems Security[C]. Boston,2001,45~59.

12 Mambo M,Usuda K,Okamoto E.Proxy signature for delegating signing operation[A].Proc.3rd ACM Conference on computer and communication security[C].1996,48~57.

13 Kim S，Park S，Won D．Proxy signatures:Revisited[A]．ICICS'97，LNCS #1334[C]．Springer-Verlag，223~232.

14 W B Lee，C Y Chang．Efficient proxy-protected proxy signature scheme based on discrete logarithm[A]．Proceedings of 10th Conference on information security[C]．Hualien，Taiwan，ROC，2000，4~7.

15 吴克力，郝鹃，刘凤玉.签名接收方可查的时控代理签名方案.计算机应用，

2003,23(6),38~39,42.

16 吴克力，刘以安.基于因子分解表述难题的代理签名方案.华东船舶工业学院学报（自然科学版），2003,17（5）：66~69.

17 吴克力，刘凤玉.签名次数受限的代理签名方案.兵工学报，2004 年 10 月已录用，编号：A4073.

18 李继国，曹珍富等．代理签名的现状与进展[J]．通信学报，2003，24(10):114~124.

19 伊丽江，白国强，肖国镇．代理多重签名[J]．计算机研究与发展， 2001，38 (2)：204~206.

20 李继国，曹珍富等．代理多重签名方案的密码分析与修改[J]．高技术通讯，2003，13(4):1~5.

21 Chaum D，Heyst E.V.Group signatures[A].Advances in Cryptology-Eurocrypto'91，LNCS 547[C].Berlin:Springer-Verlag，1991: 257~65.

22 Camenish J， Stadler M. Efficient Group Signature Schemes for Large Groups[A]. Advances in Cryptology-CRPTO'97， LNCS 1294[C]. Berlin: Springer-Verlag，1997， 410~424.

23 Bresson E， Stern J. Efficient revocation in group signature[A]. PKC 2001， LNCS 1992[C]. Berlin: Springer-Verlag， 1999: 190~206.

24 王尚平，王育民等．群签名中成员删除问题的更新算子解决方案[J]．软件学报，2003，14(11)：1911~1917.

25 张福泰等．群签名及其应用[J]．通信学报，2001，22(1)：77~85.

26 Ateniese G， Camenisch J， Joye M， Tsudik G. A practical and provably secure coalition-resistant group signature scheme[A]. In Advances in CRYPTO'00， LNCS 1880[C]. Springer-Verlag， 2000. 255~270.

27 Ateniese G， Tsudik G. Some open issues and directions in group signature[A]. In Financial Crypto'99， LNCS 1648[C]. Springer -Verlag， 1999. 196~211.

28 Camenisch J. Efficient and generalized group signature[A]. In Eurocrypt'97， LNCS 1233[C]. Springer -Verlag， 1997. 465~479.

29 Chen L， Pedersen T P. New group signature schemes[A]. In Eurocrypt'94， LNCS 950[C]. Springer -Verlag， 1994. 171~181.

30 Bellare M，Shi H，Zhang C. Foundations of Group Signatures:The Case of Dynamic Groups[J/OL]. http://eprint.iacr.org/2004/077.

31 Rivest R L， Shamir A， Tauman Y. How to Leak a Secret[A]. Cryptology-Asiacrypt 2001， LNCS 2248[C]. Berlin: Springer-Verlag， 2001:552~565.

32 Zhang F，Kim K. ID-Based Blind Signature and Ring Signature from pairings[A].

Cryptology-Asiacrypt 2002, LNCS 2501[C]. Berlin: Springer-Verlag, 2002: 533~547.

33 CY Lin, TC Wu. An Identity-based Ring Signature Scheme from Bilinear Pairings[A]. 18th International Conference on Advanced Information Networking and Applications (AINA'04) Volume 2[C]. 2004:182~186.

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

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

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

37 Okamoto T. Provable secure and practical identification schemes and corresponding digital signature schemes[A]. CRYPTO'92[C]. New York : Springer-Verlag, 1992:31~52.

38 Camenisch J, Piveteau J, Stadler M. Blind signatures based on discrete logarithm problem[A]. EUROCRYPT'94[C]. Heidelberg: Springer-Verlag, 1994: 428~432.

39 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.

40 Fan C I, Lei C L. Efficient blind signature scheme based on quadratic residues[J]. IEE Electronic Letters, 1996.32(9): 811~813.

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

42 Fan C I, Chen W K, Yeh Y S. Randomization enhanced Chaum's blind signature scheme[J]. Computer Communications, 2000, 23(13): 1677~1680.

43 Lin W D, Jan J K. A security personal learning tools using a proxy blind signature scheme[A]. Proceedings of International Conference on Chinese Language Computing[C]. USA:Chinese Language Computer Society Knowledge Systems Institute, 2000:273~277.

44 Tan Z, Liu Z, Tang C. Digital proxy blind signature schemes based on DLP and ECDLP[J]. MM Research Preprints, 2002, 21(7): 212~217.

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

46 吴克力，朱保平，刘凤玉. 公平的群盲签名方案.南京理工大学学报(自然科学版)，

2004, 28(1), 90~94.

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

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

49 Fuw-Yi Yang， Jinn-Ke Jan. A provably secure scheme for restrictive partially blind signatures[J/OL]. http://eprint.iacr.org/2004/037/.

50 Fuw-Yi Yang， Jinn-Ke Jan. A Provable Secure Scheme for Partially Blind Signatures[J/OL]. http://eprint.iacr.org/2004/230/

51 Sherman S.M. Chow，Lucas C.K. Hui，S.M. Yiu，K.P. Chow. Two Improved Partially Blind Signature Schemes from Bilinear Pairings[J/OL]. http://eprint.iacr.org/2004/108/.

52 Girault M. Self-certified public keys[A]， Advances in cryptology， Proc. Eurocrypt'91，LNCS 434[C]，Springer，490~497.

53 Petersen H.， Horster P. Self-certified keys--concepts and applications[A]. In Proc. 3rd Int. Conference on Communications and Multimedia Security'97[C]， Chapman & Hall， September， 102~116.

54 Chang， Yuh-Shihng，Wu， Tzong-Chen; Huang， Shih-Chan.ElGamal-like digital signature and multisignature schemes using self-certified public keys[J]. Journal of Systems and Software， 2000， 50(2):99~105

55 Tseng, Yuh-Min Jan, Jinn-Ke, Chien,Hung-Yu. Digital signature with message recovery using self-certified public keys and its variants[J]. Applied Mathematics and Computation 2003， 136(2-3): 203~214

56 李子臣，杨义先.具有消息恢复的数字签名方案[J].电子学报，2000，28(1):125~126.

57 李子臣，李中献.具有消息恢复签名方案的伪造攻击[J].通信学报，2000，21(5):84~87.

58 何柱萍.基于离散对数加密系统的密钥认证模式[J].计算机工程与设计，2000，21(5):26~29.

59 张爱新 杨明福.基于自证明公钥认证的数字签名方案[J].计算机应用与软件，2001，18(8):63~65.

60 Boneh D，Shacham H，Lynn B. Short signatures from the Weil pairing[A]. In proceedings of Asiacrypt '01， LNCS 2139[C]. Berlin: Springer-Verlag，

2001:514~532.

61 王泽成等. 一种基于 Weil 配对的数字签名方案的安全性分析与改进[J]. 计算机工程，2003，29(16):60~61.

62 ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transaction on information theory，1985，31(4):469~472.

63 Harn，L.，Xu Y. Design of generalized ElGamal type digital scheme based on discrete logarithm[J]. Electronics letters，1994，31(24):2025~2026.

64 Horster P., Michels M.and Petersen H. Meta-ElGamal signature schemes[A].Proc.2nd conference computer communication security[C]，Fairfax，Virginia，1994，Nov.2~4，96~107.

65 Nyberg K.，Rueppel R.A. Message recovery for signature schemes based on the discrete logarithm[A]. Advances in Cryptology –Eurocrypt'94[C]. Springer-Verlag，1994，175~190.

66 Nyberg K.，Rueppel R.A. Message recovery for signature schemes based on the discrete logarithm[J]. Designs，Codes and Cryptography，Vol.7，1996，61~81.

67 Horster P.， Michels M.，Petersen H.. Authenticated encryption schemes with low communication costs[J]. Electronics Letters，1994，30(15):1230~1231.

68 S.J.Hwang， C.C.Chang ，W.P.Yang. Authenticated encryption schemes with message linkages[J]. Information Processing Letters .1996，Vol.58，189~194.

69 W.B.Lee，C.C.Chang. Authenticated encryption schemes with linkage between message blocks[J]. Information Processing Letters，1997，63:247~250.

70 W.B.Lee，C.C.Chang. Authenticated encryption schemes without using a one-way hash function[J]. Electronics Letters，1995，31:1656~1657.

71 Y.M.Tseng J.K.Jan. An efficient authenticated encryption schemes with message linkages and low communication costs[J]. Journal of information and engineering.2002，Vol.18，41~46.

72 李继红 肖国镇. 广义 ElGamal 签名的一种安全性分类[J]. 西安电子科技大学学报，1998，25(5)：654~658.

73 李继红 谷大武 肖国镇. ElGamal 型签名方案与相应型方案的安全性关系研究[J]. 通信学报，2000，21(4)：58~61.

74 He J, Kiesler T. Enhancing the security of ElGamal's signature scheme.IEE Pro.digit.Tech.，1994，141(4):249~252.

75 卢建株，陈火炎. 具有消息恢复的数字签名方案及其安全性[J]. 小型微型计算机系统，2003，24(4)：695~697.

76 Nguyen L. A Trapdoor-free and Efficient Group Signature Scheme from Bilinear Pairings. http:// eprint.iacr.org/2004/104/.

77 Chen X, Zhang F, Kim K. A New ID-based Group Signature Scheme from Bilinear Pairing. Proceedings of WISA'2003, Jeju Island(KR), August 2003, 585~592.

78 Libert B, Quisquater J J. New identity based signcryption schemes from pairings. http://eprint.iacr.org/2003/023/.

79 王晓明. 基于椭圆曲线的若干密码方案[J]. 计算机工程与设计, 2002, 23(7): 18~19.

80 ANSI X9.62.Public key cryptography for the financial services industry: The elliptic curve digital signature (ECDSA)[S]. 1999

81 Shamir. identity-based cryptosystem based on the discrete logarithm problem[A]. In: Advances in cryptology-Eurocrypt'84[C], Springer, Berlin, 1985, 47~53.

82 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.

83 Harn L.Cryptanalysis of blind signature based on the discrete logarithm problem.Electronic Letters, 1995, 31(14):1136

84 杜伟章, 陈克非. 基于线性变换构造弱盲签名方案[J]. 计算机工程与应用, 2003, 39(17): 38~40.

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

86 谭作文等. 基于离散对数的代理盲签名[J]. 软件学报, 2003, 14(11): 1931~1935.

87 Zhao Zemao, Liu Fengyu. Construction of Proxy Blind Signature Scheme Based on Multi-Linear Transform. Journal of Electronics(China), 2004, 21(6): 505~510.

88 Miller V. Use of elliptic curves in cryptography. Advances in Cryptology-Proceedings of CRYPTO'85, LNCS 218. Berlin: Springer-Verlag, 1985, 410~424.

89 Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation. 1987,48(5):203~209.

90 MenezesA J, Okamota T, Vanstones S A. Reducing elliptic curve logarithms to a finite field. IEEE Transactions on Information Theory. 1993, 39:1639~1646.

91 Joux A. A one round protocol for tripartite Diffie-Hellman, In Proceedings of the 4th International Symposium on Algorithmic Number Theory, LNCS 1838. Springer-Verlag, 2000, 385~394.

92 Boneh D, Franklin M. Identity-Based Encryption from the Weil Paring. Advances in Cryptology-Proceedings of CRYPTO'01, LNCS 2139. Berlin: Springer-Verlag, 2001,

213~229.

93 Hess F. Exponent group signature schemes and efficient identity based signature schemes based on pairings[EB/OL]. Cryptology ePrint Archive, Report 2002/012, available at http://eprint. iacr. org/2002/012/.

94 Fangguo Zhang，Kwangjo Kim. ID-Based Blind Signature and Ring Signature from Pairings[A]. Proc of Asiacrpt, 2002 LNCS, 533~547, Springer-Verlag, 2002.

95 Fangguo Zhang and Kwangjo Kim. Efficient ID-Based Blind Signature and Proxy Signature from bilinear pairings[A]. In:Advances in Cryptology- Crypto'2003[C], volume 2727 of Lecture notes in Computer Science, 312-323, Springer-Verlag. 2003.

96 Jung Hee Cheon, Yongdae Kim and Hyo Jin Yoon. A New ID-based Signature with Batch Verification[EB/OL]. Cryptology ePrint Archive, Report 2004/131,available at http://eprint. iacr. org/2004/131/.

97 Benaloh J，Yung M. Distributing the power of a government to enhance the privacy of votes[A]. Proc of the 5th ACM of distributed computing[C]. Calgary，1986. 52~62.

98 Iverson K R . A Cryptographic Scheme for Computerized General Elections[A]. Proceedings of Crypto'91，LNCS576[C]. Berlin：Springer-verlag，1991，405~419.

99 Chaum D. Elections with unconditionally secret balllots and disruption equivalent breaking RSA[A]. Eurocrypt'88，LNCS330[C]. Berlin：Springer-verlag，1988，177~182.

100 Ohta K. An electrical voting scheme using a single administrator[A]. 1988 Spring National Convention Record[C]. Berlin：IEICE，1988，A-294.

101 Asano T，Matsumoto T，Imai H. A study on some schemes for fair election secret voting[A] . Proc. of the 1991 symposium on cryptography and information security[C]. Japan，1991：SCIS91-12A.

102 Sako K. Electronic voting system with objection to the center[A]. Proc. of the 1992 symposium on cryptography and information security[C]. 1992：SCIS92-13C.

103 Fujioka A，Okamoto T，Ohta K. A practical secret voting scheme for large scale elections[A].Auscrypt'92，LNCS718[C]. Berlin：Springer-verlag，1993，244~251.

104 孟江涛,冯登国,胡振宇.电子选举中的安全协议[J].中国科学院研究生院,2002,19(3):295~305.

105 郑燕飞,陈克非.电子选举:理论实践与未来.计算机科学[J].计算机科学,2002,29(4):12~14.

106 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，

2003，24（3）：588~591.

107 周怡丹，张曙光，付志峰．一个基于盲签名的电于选举方案[J]．计算机工程与应用，2003，15(4)：171~172.

108 王文龙，王泽成，李志斌．基于椭圆曲线的电子选举协议[J]．计算机工程，2003，29(22)：144~145.

109 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.

110 Sun H.-M. and Hsieh B.-T. On the security of some proxy blind signature schemes[J/OL] . http://eprint.iacr.org/2003/068. AISW2004[C]. New Zealand: Dunedin，2004.

攻读博士学位期间发表的论文

1 Zhao Zemao，Liu Fengyu．Method of Constructing Elliptic Curve Authenticated Encryption Scheme，Accepted in Applied Mathematics and Computation 录用.(SCI, Ei 源).

2 赵泽茂，刘凤玉，徐慧．基于椭圆曲线密码体制的签名方程的构造方法．计算机工程，2004，30(19)：96~97(Ei：0447840787).

3 Zhao Zemao，Liu Fengyu．Construction of Proxy Blind Signature Scheme Based on Multi-Linear Transform．Journal of Electronics(China)，2004，21(6)：505~510.

4 赵泽茂，徐慧，刘凤玉．具有消息恢复的认证加密方案的改进．小型微型计算机系统，2005，26(3)：431~433.

5 赵泽茂，徐慧，刘凤玉．具有消息链接恢复的椭圆曲线认证加密方案．南京理工大学学报，2005，29(1)：81~84.

6 赵泽茂，吴远高，刘凤玉．基于椭圆曲线的具有消息恢复的签名方案．计算机工程与科学，2005，21(2):3~4.

7 赵泽茂，刘凤玉．广义 ElGamal 型弱盲签名的构造方法．计算机工程与设计，2004，25(12)：2168~2169.

8 Zhao Zemao，Liu Fengyu．Constructing Method of Proxy Blind Signature Scheme and Its Extension，应用科学学报，2005(3)：

9 赵泽茂，刘凤玉．基于公钥自证明的认证加密方案．计算机工程与应用，将于 2005 年 10 月发表.

10 Zhao Zemao，Liu Fengyu．A new signature scheme based on ElGamal signature and its extension．ACA'04，2004 年全国计算机体系结构学术会议论文集，《高技术通讯》增刊，2004 年 8 月，443~446.

参加科研项目情况：

项目名称：基于四层结构的战场信息安全性关键技术研究

来源：国防科学工业委员会国防基础科研项目

经费数：65 万元人民币，　项目编号：J1300D004。

本人在该项目中，承担了数字签名方案的研究与设计，现已完成预定的任务。