基于椭圆曲线的数字签名研究与仿真

学　　院　　信息工程学院

年级专业　　信息安全 111 班

学生姓名　　江 林 伟

指导教师　　巫光福

日　　期　　2014 年 1 月 5 日

摘 要

随着信息技术的不断发展和应用，信息的安全性变得越来越重要，数字签名技术是当前网络安全领域的研究热点。自从N.Koblitz和Miller提出将椭圆曲线应用于密码算法以来，椭圆曲线密码体制已得到了很大的发展，已经成为密码学的重要研究热点之一。

目前国内对于椭圆曲线公钥的快速实现、智能卡应用等研究较多。由于它本身的优点也特别适用于无线Modem、Web服务器、集成电路卡等方面，随着网上交易的频繁，这将成为今后研究的热点。然而，在现有的研究中它在进行大型安全交易的电子商务领域中研究比较有限。

本文主要是对椭圆曲线密码体制的研究，并在此基础上实现了一种基于椭圆曲线的数字签名体制，主要完成了以下几个方面的工作:

在查阅大量文献资料的基础上，分析了密码学领域里的对称加密体制和非对称体制, 并对二者进行了对比，指出了公钥加密体制的优点所在；深入分析ECDSA椭圆曲线数字签名算法的理论基础及算法原理，研究了随机生成有限域上的椭圆曲线方程算法；研究了基于椭圆曲线的数字签名方案，探讨了椭圆曲线密码算法的优点及其特别适用的领域；并简单了解了下椭圆曲线密码体制中的一些基本算法，如快速取模算法、快速模加算法、快速模逆算法等；同时设计了一种基于ECDSA算法的数字签名系统，分析了其系统架构，并对ECDSA数字签名进行了成功的仿真。

关键词 椭圆曲线密码体制；数字签名；仿真；ECDSA

Abstract

Along with the continuous development and application of Information Technology, the security of information has become

Currently, there is much research on rapid realization and smart card application of elliptical curve public key. Because of its own advantages, it also can be applied to Wireless Modem, Web Services, and integrated circuit cards and so on. However, in Ongoing study, there search of mass security transactions in the area of e- business is so limited. With the online transactions become more frequent, this research filed will become hot spots in future.

Access to a large number of literatures, the symmetric and a symmetric encryption system has been analyzed in cryptography field structure. And a comparison that the public key encryption system has the advantage between them has been proposed. On this basis, commonly digital signatures algorithm systems have been advanced.

In-depth analysis of ECDSA elliptical curve digital signature algorithm theoretical basis and algorithm theory, a random on the limited jurisdiction of the elliptical curve equation algorithms has been generated, and its validity has been analyzed. On the basis of previous research, a system based on elliptical curve proxy signature and the signature threshold agent system has been proposed, and an analysis of their safety certification of its safety performance is reliable. Meanwhile this paper designed a digital signature system based on the ECDSA algorithms, an analysis of its system. And the digital signature system based on the ECDSA has been successfully simulated.

Keywords Elliptical Curve Encryption System digital signatures simulation ECDSA

目 录

第 1 章 绪论

1.1 课题背景

当今社会是信息化社会，电子计算机和通信网络已经广泛的应用于社会的各个领域，以此为基础建立起来的各种信息系统，给人们的生活、工作带来了巨大变革。大型信息系统将众多的计算机和只能化设备连在一个四通八达的通信网络中，共享丰富的数据库信息和计算机资源，储存大量的数据文件，完成异地之间的数据交换与通信。信息系统的应用，加速了社会自动化的进程，减轻了日常繁杂的重复劳动，同时也提高了生产率，创造了经济效益。

信息安全技术在信息化迅速发展的今天已进入了高速发展的新时期，形成了密码技术、可信计算技术、电磁辐射泄露防护技术、系统入侵检测技术和计算机病毒检测消除技术等多个安全防护技术门类。

数字签名又称之为数字签字、电子签名、电子签章等。其提出的初衷就是在网络环境中模拟日常生活中的手工签名或印章；而要使数字签名具有与传统手工签名一样的法律效力，又催生了数字签名法律的出现。数字签名具有许多传统签名所不具备的优点，如签名因消息而异，同一个人对不同的消息其签名结果是不同的，原有文件的修改必然会反映为签名结果的改变，原文件与签名结果两者是一个混合不可分割的整体等。所以，数字签名比传统签名更具可靠性。

1.1.1 研究现状

目前，密码理论与技术主要包括两部分，即基于数学的密码理论与技术(其中包括公钥密码、分组密码、流密码、认证码、数字签名、Hash M数、身份识别、密钥管理、PKI技术等卿非数学的密码理论与技术(包括信息隐形、量子密码、基于生物特征的识别理论与技术)。

实现数字签名有很多方法，目前数字签名采用较多的是公钥加密技术[1]，如基TRSA Data Security中的PKCS(Public Key Cryptography Standards)，DSA (Digital Signature Algorithm), x.509, POP (Pretty Good

Privacy)。1994年美国标准与技术协会公布了数字签名标准(DSS)而使公钥加密技术广泛应用。同时应用散列算法(Hash)也是实现数字签名的一种方法。而关于椭圆曲线数字签名的研究正处于开始状态，所以很多问题都没能有效解决。在个别领域，我国开始尝试采用新的椭圆曲线数字签名算法(包括192位椭圆曲线算法、224位椭圆曲线算法和256位椭圆曲线算法)。

目前影响最大的三类公钥密码是 RSA 公钥密码、ElGamal 公钥密码、椭圆曲线公钥密码。其中 RSA 公钥密码的安全性依赖于数学中大整数因子分解问题的难度，而 ElGamal 公钥密码与椭圆曲线公钥密码分别基于一般有限域离散对数问题（DLP）和椭圆曲线离散对数问题（ECDLP）。在以上三类公钥系统中，椭圆曲线公钥系统最具有优势。因为：

(1) 在有限域 F_q 上的椭圆曲线很多，为我们用椭圆曲线构造密码系统提供了丰富的资源。

(2) 椭圆曲线公钥密码系统中的主要计算量是计算 Q= kg，且 Q 很容易求出[1],而知道 Q、 g ，求 k 十分困难。

(3) 要获得同样安全强度，比 RSA 用的参数规模小得多[2]，开销较少且速度快。

(4) 椭圆曲线离散对数问题（ECDLP）比有限域离散对数问题（DLP）困难得多。

基于具有无可比拟的优势，椭圆曲线公钥密码系统被认为是新一代公钥密码系统。无论在数据加密和数字签名上，椭圆曲线公钥密码系统已成为人们非常感兴趣的研究方向之一，从而在这方面涌出了很多有价值的成果。

目前国内对于椭圆曲线公钥的快速实现、智能卡应用等研究较多。由于它本身的优点也特别适用于无线Modem, Web服务器、集成电路卡等方面。但是综合浏览后，发现关于在要进行大量安全交易的电子商务领域中研究比较有限。随着网上交易的频繁，这将成为今后研究的热点。

1.1.2 数字签名技术选题依据和意义

信息时代虽然给我们带来了无限商机与方便，但同时也充斥着隐患与危险。由于网络很容易受到攻击，导致机密信息的泄漏，引起重大损失。由于信息技术已经成为综合国力的一个重要组成部分，因此信息安全已成

为保证国民经济信息化建设健康有序发展的保障。

网络安全技术众多，目前在电子商务、电子政务、电子邮件系统、电子银行等方面必备的关键技术就是数字签名。数字签名又称为数字签字，电子签章等。“数字签名”用来保证信息传输过程中信息的完整和提供信息发送者的身份认证和不可抵赖性，数字签名技术的实现基础是公开密钥加密技术，是用某人的私钥加密的消息摘要用于确认消息的来源和内容。

目前普遍采用的数字签名算法，都是基于下面三个数学难题的基础之上[2]：

(1)难题1　整数的因式分解(Integer Factorization)问题，如RSA算法；

(2)难题2　离散对数(Discrete Logarithm)问题，如ElGamal，DSA，等算法；

(3)难题3　椭圆曲线(Elliptic Curve)问题，如ECDSA算法；

而在众多算法中，椭圆曲线密码体制由于具有密钥长度短、数字签名快、计算数据量小、运算速度快、灵活性好等特点，已经广泛地被应用。由于ECC能实AIR高的安全性，只需要较小的开销和延迟，较小的开销体现在如计算量、存储量、带宽、软硬件实现的规模等;延迟体现在加密或签名认证的速度方面。所以ECC特别使用于计算能力和集成电路空间受限(如工C智能卡)、带宽受限(如高速计算机网络通信)等情况。

1.1.3 论文结构与内容

本文在阅读了国内外大量的参考文献资料的基础上，进行了如下布局结构:

首先对密码学技术的发展现状及其发展趋势进行了分析和综述。

其次，介绍了密码学的基本理论及基本概念，并详细介绍了公钥密码算法，给出了一些典型的公钥加密体制的简要分析。

第三，探讨了椭圆曲线密码算法的基本概念及理论基础，包括群和域、散列函数及SHA算法、椭圆曲线的基本概念、有限域椭圆曲线的运算等，同时分析了有限域上安全椭圆曲线的生成。

第四，研究了基于ECDSA数字签名算法，并对其安全性作了分析，简要介绍了椭圆曲线密码算法的优点及适用的领域。

最后，深入探讨了基于椭圆曲线的数字签名体制，同时设计了一种基

于 ECDSA 算法的数字签名系统，分析了其系统架构，并对 ECDSA 数字签名进行了成功的仿真。

第 2 章 密码学基本理论及基本概念

密码学是网络信息安全的基础，公钥密码体制是密码学的只要组成部分，数字签名的基础就是公钥密码体制。网络信息安全是密码学的重要应用领域，公钥密码体制的主要应用之一就是数字签名。

2.1 密码学基本概念

1949年，Shannon发表了著名论文《保密系统的通信理论》[3]，把古老的密码学置于坚实的数学基础之上。1977年，美国联邦政府正式颁布了数据加密标准(DES)，这是密码学历史上的一个创举，由此，过去神秘的密码学逐步走向公开的学识殿堂。1976年，Whitfield Dife与Martin Hellman的开创性论文《密码学新方向》，首次提出了公钥密码的概念，建立了公钥密码体制基础。

密码学包括两个方面：密码编码学和密码分析学。密码编码学就是研究对数据进行变换的原理、手段和方法的技术和科学。密码分析学是为了取得秘密的消息，而对密码系统及其流动数据进行分析，是对密码原理、手段和方法进行分析、攻击的技术和科学[7]。

密码学的理论基础是数学，其基本思想是隐藏、伪装信息，使未经授权者不能得到消息的真正含义[4,8]。伪装(变换)之前的信息是原始信息，成为明文(plaintext)； 伪装之后的消息，看起来是一串无意义的乱码，称为密文(cipher text)。把明文伪装成密文的过程称为(encryption)，该过程使用的数学变换就是加密算法。把密文还原成明文的过程称为解密(decryption)，该过程使用的数学变换，通常是加密时数学变换的逆变换，就是解密算法。加密与解密通常需要参数控制，我们把该参数称为密钥，有时也称为密码。加密时使用的为加密密码(加密密钥)，解密时使用的为解密密码(解密密钥)。加密密钥与解密密钥可能相同也可能不同。相同时称为对称型或单钥的，不相同时称为非对成型或双钥的。

那么一个密码系统或称其为密码体制，是由明文空间、密文空间、密

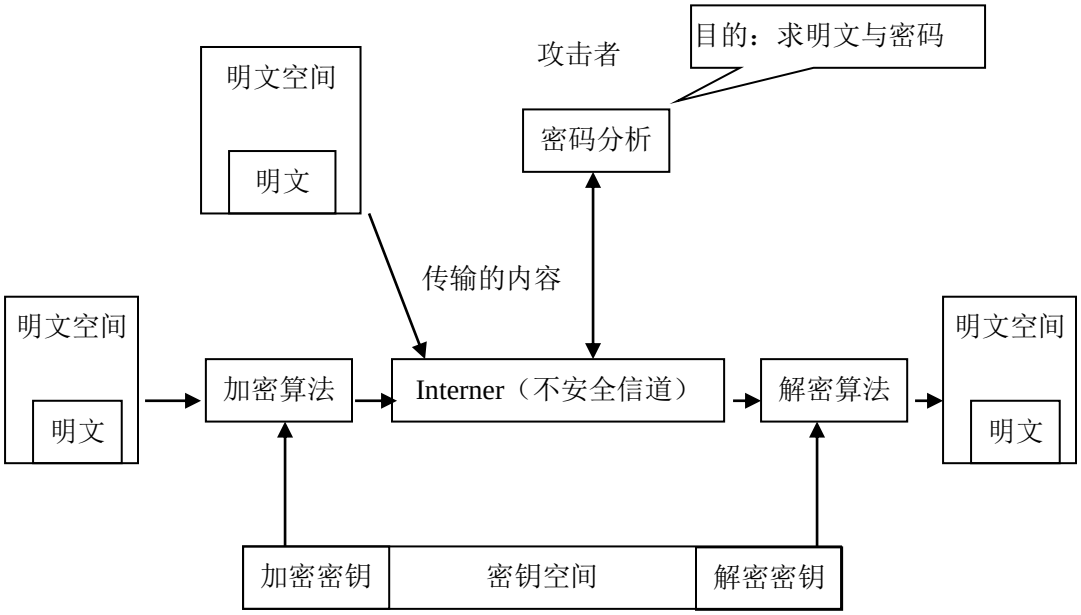
钥空间、加密算法与解密算法五个部分组成。明文、密文、密钥空间分别表示全体明文、全体密文、全体密钥的集合；加密与解密算法通常是一些公式、法则或程序，规定了明文与密文之间的数学变换规则。

下面用字母分别表示这个概念，密钥K=<Ke,Kd>，Ke表示加密密钥，Kd表示解密密钥，设明文M，密文c，加密算法E，解密算法D。

把明文加密为密文：C=E(M,Ke)

把密文解密为明文：M=D(C,Kd)=D(E(M,Ke),Kd)

上述的讲解可用图2-1表示



（用安全信道传输密钥）

图2-1 加密过程与密码分析

2.2 公钥加密体制

2.2.1 公钥密码基本概念

公钥密码概念是由Whitfield Diffie和MartinH ellma于1976年提出的，它是密码学历史上的一个重大成就。公钥密码与以前所有的密码方法都大相径庭:一是以前的密码算法都基于代换与置换操作，而公钥密码使用数学函

数进行变换；二是公钥密码体制使用非对称的方式，使用两个密钥(加密密钥与解密密钥)，而传统密码算法仅仅使用一个密钥。公钥密码体制的提出首先是为了解决利用传统密码体制进行密钥分发时遇到的问题，数字签名也是其重要应用之一。

从1976年起，学者们提出了许多种公钥加密方法，它们的安全性都是基于复杂的数学难题。根据所基于的数学难题来分类，有以下三类系统目前被认为是安全和有效的：

(1) 基于大整数因子分解的：RSA和Rabin-Williams。

(2) 基于离散对数问题的：DSA和EIGamal。

(3) 基 于椭圆曲线离散对数问题的：椭圆曲线密码系统。

公开密钥加密算法与对称密钥加密算法相比来说，安全性能更好，密钥管理、分配都容易实现，其中有些加密算法还能应用在数字签名上，但是它们相对于对称密钥加密算法运行速度要慢得多，所以不能加密大量的数据。

2.2.2 公钥密码原理

公开密钥密码理论是1976年美国发表的RSAl41算法，它是以三个发明人的名字命名的，后来又有椭圆算法ECC，但常用的、成熟的公钥算法是RSA。它与传统的对称密钥算法有本质的区别，对称密钥算法常用的是DES算法，加/解密时用的是同一个密钥。而公钥算法利用的是非对称的密钥，即利用两个足够大的质数与被加密原文相乘生产的积来加/解密。这两个质数无论是用哪一个与被加密的原文相乘(模乘)，即对原文件加密，均可由另一个质数再相乘来进行解密。但是，若想用这个乘积来求出另一个质数，就要进行对大数分解质因子，分解一个大数的质因子是十分困难的，若选用的质数足够大，这种求解几乎是不可能的。因此，将这两个质数称密钥对，其中一个采用私密的安全介质保密存储起来，应不对任何外人泄露，简称为“私钥”；一个密钥可以公开发表，用数字证书的方式发布在称之为“上黄页”的目录服务器上，用LDAP协议进行查询，也可在网上请对方发送信息时主动将该公钥证书传送给对方，这个密钥称之为“私钥”。

公、密钥对的用法是，当发方向收方通信时发方用收方的公钥对原文进行加密，收方收到发方的密文后，用自己的私钥进行解密，其中他人是

无法解密的，因为他人不拥有自己的私钥，这就是用公钥加密，私钥解密用于通信;而用私钥加密文件公钥解密则是用于签名，即发方向收方签发文件时，发方用自己的私钥加密文件传送给收方，收方用发方的公钥进行解密。

但是，在实际应用操作中发出的文件签名并非是对原文本身进行加密，而是要对原文进行所谓的“哈希”(Hash)运算，即对原文作数字摘要。该密码算法也称单向散列运算，其运算结果称为哈希值，或称数字摘要，也有人将其称为“数字指纹”。哈希值有固定的长度，运算是不可逆的，不同的明文其哈希值是不同的，而同样的明文其哈希值是相同并且是唯一的，原文的任何改动，其哈希值就要发生变化。数字签名是用私钥对数字摘要进行加密，用公钥进行解密和验证。

公钥证书和私钥是用加密文件存放在证书介质中，证书是由认证服务机构CA所签发的权威电子文档，CA与数字证书等是公钥基础设施PKI的主要组成机构和元素。

公钥密码算法使用两个密钥，其中一个用于加密(加密密钥)，另外一个用于解密(解密密钥)。公钥密码算法具有如下特征：加密密钥与解密密钥时本质上不通的，也就是说如果仅仅知道密码算法和加密密钥，而要确定解密密钥，在计算上是不可行的；大多数公钥密码算法的加密密钥与解密密钥具有互换的性质。如RSA算法，密钥对中的一个用于加密，另一个用于解密。

2.2.3 利用公钥密码体制进行数字签名

下面举例简单介绍用户i把消息x签名，然后传送给用户j的过程。

用户i首先产生签名 $x''=D_i(x)$；然后把(x, x'')送给用户j即可。

用户j接受到(x, x'')后，验证是否为用户i的签名：首先计 $r=E_i(x'')$；然后通过比较，r=x表示是用户i数字签名，否则不是。因为 $E_i(x'')=E_i(D_i(x))=x$，所以可以通过比较r与x来判断签名的有效性。

因为 D_i 是保密的，所以除了用户i之外，他人不能产生x对应的正确的

x''；也就是说，他人不能假冒用户i进行数字签名。

2.2.4 公钥密码体制的数学基础

通观公钥密码算法，它们的数学基础是比较狭窄的。大多数公钥密码算法都是基于以下三种数学难题之一的：

一是背包问题：给定一个互不相同的数组成的集合，要找出一个子集，其和为N。

二是离散对数问题：如果P是素数，9和M是整数，找出x，使得 $g^x = M(\text{mod } p)$；还有一种方法，就是基于椭圆曲线的离散对数问题。

三是因数分解问题：设N是两个素数的乘积，则：

（1） 分解N；

（2） 给定整数M（明文）和C（密文），寻找d满足 $M^d \equiv C(\text{mod } N)$；

（3） 给定整数e和C，寻找M满足 $M^e \equiv C(\text{mod } N)$；

（4） 给定整数 x，判定是否存在整数 y 满足 $x \equiv y^2(\text{mod } N)$；

2.3 对称加密体制

对称加密算法，又称私钥加密算法，就是加密密钥能够从解密密钥中推出来，反过来也成立，在大多数对称算法中，加密解密密钥是相同的。对称算法的加密和解密表示为:

$$E_k(M) = C, D_k(C) = M \qquad (2\text{-}1)$$

对称加密算法的典型代表有:DES，AES，3DES，RC2，RC4，RCS，RC6，IDEA等。以DES为代表的对称密钥加密算法的设计原则主要基于信息论的混乱和扩散。混乱指的是密钥和明文及密文之间的依赖关系应该尽量复杂，以破坏分组间的统计规律，通常依靠多轮迭代来实现；扩散则应使密钥和明文的每一位影响密文中尽可能多的位数，这样可以防止逐段破译，并通过S盒的非线性变换来实现。实际上，所有的对称密钥加密算法都采用Feistel网、S盒及多次迭代等思想。

对称加密有速度上的优点，用软件实现，对称密钥比非对称密钥快100-1000倍。然而，如果一个消息想以密文的形式传到接收者，我们应该找到一个方法安全传输密钥。对称加密系统用键长来衡量加密强度，40比特的键长被认为比较脆弱，128比特比较健壮。

对称加密算法的缺点则是密钥分发困难，密钥管理难，无法实现数字签名。

2.4 常用数字签名算法

早在1979年，GJ.Simmons就将数字签名讨论应用于美苏两国的禁止核试验条约的验证工作中。在1991年，美国NIST公布了其数字签名标准，DSS(Digital Signature Standard)，于1994年正式采用为美国联邦信息处理标准；DSS标准中采用的签名算法称为DSA。随后其他一些国家也颁布了自己的数字签名标准，如俄罗斯1994年颁布的GOST R34.10-94标准等。较早出现的数字签名算法，如1978年前后提出的RSA，Rabin等数字签名算法，至今还在使用。

第 3 章 椭圆曲线密码算法的研究

3.1 群（Groups）

抽象代数[9,10,11]不但是数学的一个重要分之，同时在其他学科如量子力学、结晶学、原子物理学等中都已经称为研究者的有力武器；群论因为是研究对称性问题的基础，例如其在物理学中在诸如时间和空间的对称性研究、乃至超对称性问题等研究中都有应用。在密码学中，抽象代数也已经扮演重要角色，如在椭圆曲线密码体制中，群以及域上的多项式理论等都是其理论基础。

设有一个由任意元素a，b，c. . . 组成的非空集合G，即$G=\{g_i\}$。在G上有一个针对其中元素进行组合操作的二元运算规则*，同时满足下列四个条件，则G对于运算*称为群，并称二元运算*为群的运算。

(1) 封闭性　对于任意a、$b\in G$，有$ab\in G$。

(2) 结合律成立　对于任意$a,b,c\in G$，有(ab)c=a(bc)。

(3) 有单位元e　对任意$a\in G$，有$e\in G$，使得ae=ea=a。

(4) 存在逆元　对任意$a\in G$，有$a^{-1}\in G$，使$a*a^{-1}=a^{-1}*a=e$；称a^{-1},a互为逆元。

上述四个条件是构成群的充分必要条件，通常被称为群的公理。若仅满足条件(1)和(2)，则被称为半群(Semigroup)；满足条件(1)，(2)和(3)者，称么半群(Monoid)、弱群或类群。

若群G对运算还满足交换律，即对于任意的g_i，$g_i\in G$，都有$g_i\ g_i=g_i\ g_i$成立，则称群G为交换群或阿贝尔群(Abel Groups)。此时，通常用符号“+”来代替“•”称群运算“+”为“加法”，称a+b为a与b的和，称单位元素。为零元素0，称逆元素a^{-1}为元素a的负元素，并一记作-a。相应的，称群运算“•”为“乘法”，称a•b为a与b的积，简写为ab。

例如：全体整数的集合在通常的加法运算下构成一个阿贝尔交换群。设n为任意正整数，对于任意的$a \in G$，定义：

$$a^n = \underbrace{a \cdot a \ldots a}_{n个}, a^0 = e, a^{-n} = (a^{-1})^n$$

则对于任意整数m，有$(a^m)^n = a^{mn}, a^m a^n = a^{m+n}$。定义<a>表示所有的$a^m$的集合，则<a>也构成一个有限群。特别的，若G中一个元素a，得<a>=G成立，则称G为循环群。显然，循环群G都是阿贝尔群。

例如：由集合{1，-1}对于乘法运算所构成的群就是二阶循环群。

设n为任意正整数，对于任意的$a \in G$，称满足$a^n = E$的最小正整数n为群元a的阶数。显然，对于有限群G而言，其每一群元的阶都是有限正整数。

例如：在由集合{1，-1}对于乘法运算所构成的群中，群元一1的阶数为2。

自19世纪中叶由拉格朗日、阿贝尔、伽罗瓦等人引入群的概念以来，经过一百多年的发展，群论已经成为现代代数学的重要分支，其内容非常丰富。下面介绍一些与椭圆曲线密码学有关的群的重要性质：

（1）广义结合律：对群中的任意n个元素g1，g2，g3，..gn，其积g1g2...gn唯一确定。由自然归纳法和结合律很容易得到此结论。

（2）单位元e都是唯一的。用反证法。若e1和e2都是群G的单位元，则根据群的公有：$e_1 e_2 = e_1$，$e_1 e_2 = e_2$，则$e_1 = e_2$。

（3）存在a，b，$c \in G$，若ab=ac，则b=c；若ab=cb，则a=c。先证明第一条。若ab=ac，用a^{-1}互乘等式两端得: $a^{-1}(ab) = a^{-1}(ac)$

根据结合律，可知 $a^{-1}(ab) = (a^{-1}a)b = (a^{-1}a)c$, 所以，b=c

（4）每一元素的逆元是唯一的。用反证法。若不然，设群元G存在两个逆元$b, c \in G$，则依据群的公理，有ab=ac=e

由上述的性质(3)可知 b=c，所以群元的逆元唯一。

3.2 有限域（Finite Field）

只含有有限多个元素的域叫有限域。由于它首先由E. 伽罗瓦所发现，因而又被称为伽罗瓦域(Galois Field)。在同构意义下，对任一素数P和正整数n，存在且仅存在一个含厂个元素的有限域，记作$GF(p^n)$。有限域$GF(p^n)$的特征为P，其阶为域中元素的个数，即p^n。另一方面，对q>1整数而言，q阶有限域GF(q)存在的充要条件是q是某一素数的整次幂(以下简称素数幂)。

设有限域GF(q)上的多项式为：

$$f(x) = f_n x^n + f_{n-1} x^{n-1} + \ldots f_1 x + f_0, f_i \in GF(p) \qquad i = 0,1,2,\ldots,n,$$

用$F_p[x]$表示系数取自域GF(p)的一切多项式的集合。$F_p[x]$中的任何多项式不一定有乘法逆元，所以$F_p[x]$只能组成一个有单位元的无零因子环，这与整数环Z完全相似。与Z环上的素数相对应，在域$F_p[x]$上有既约多项式。设f(x)是次数大于0的多项式，若除了常数、常数与本身的乘积以外，不能再被域GF(p)上的其他多项式除尽，则称f(x)为域GF(p)上的既约多项式。

所以，一个常数总是多项式的因子，f(x)是否既约与讨论的域有很大关系。

3.3 数据完整性与散列函数

散列(Hash)函数，又称为哈希函数、杂凑函数。其运算结果就像数字式的指纹，即用一小段数据来识别大的数据对象。散列函数是密码学，也是认证理论研究的主要内容之一。

数据完整性服务确保：接收到的信息如同发送的消息一样，其在传输过程中没有被攻击或者插入、篡改、重排等。破坏数据完整性是一种主动攻击；而加密可以保护信息的机密性，是为了抵御被动攻击。散列函数是目前保护数据完整性的主要技术手段。

常见的散列函数攻击方法有：生日攻击、中途相遇攻击和穷举攻击等。

一个安全的散列函数应该对这些已知的攻击法有很好的抗攻击性。

3.3.1 散列函数原理

散列函数H(M)，就是把任意长度的消息M，通过函数H，将其变换为一个固定长度的散列值h: h=H(M)。消息M的散列值h，就像该消息的数字指纹，可以用来保证数据的完整性，我们在前面称其为数据摘要。散列函数是公开的，一般不涉及保密密钥。少量有密钥的散列函数，可以作为计算消息的认证码等其他用途，因其有密钥而具有一定的身份鉴别功能。

目前我们指的散列函数都是单向散列函数h=H(M)，即函数H是单向函数。它有弱单向散列函数和强单向散列函数之分。单向散列函数是建立在压缩函数(compression function)的想法之上的：给一个输入n位长消息，得到一个较短的散列值。

单向散列函数的性质：

（1）函数H适用于任何大小的数据分组；

（2）函数H产生一定长度输出；

（3）对于任何数据M，计算H(M)是容易实现的；

（4）对于任何给定的散列值h，要计算出M使H(M)=h，这在计算上是不可行的；

（5）对于任意给定的数据x，要计算出另外一个数据Y，使H(x)=H(y)，这在计算上是不可行的；

（6）要寻找任何一对数据（x，y），使H(x)=H(y)，这在计算上也是不可行的；

其中前面3个性质是散列函数应用于报文（数据）鉴别的基本要求；性质4是单向函数性质；性质5也可称其为弱抗冲突（weak collision resistance），就是在给定x之后，考察与本特定的x相冲突的情况：性质6也可称其为强抗冲突（strong collision resistance），是考察任意两个元素x，y相冲突的情况。

3.3.2 散列函数的一般结构

散列函数是建立在压缩函数的基础之上的，它通过对消息分组的反复迭代压缩，生成一个长度固定的散列值。一般在迭代的最后一个分组中，还包含有消息的长度，从而在散列值中引入消息长度的影响。

下面介绍的散列函数结构是Merkie提出的，如图3-1所示。

本结构符合大多数散列函数的结构，如MD5，SHA-1，RIPEMD-160等。它接受一个消息，并把消息分为L个分组，每个分组长度为b比特。如果最后一个分组长度不足b比特，可以强制将其填充为长b比特；并且包含消息a的总长度值，从上面讲述可知，添加消息的总长度值，可以提高散列函数的安全强度。

由图3-1可知，散列函数重复使用相同的压缩函数f重复处理分组。f有两个输入:一个是前一步的n比特输出，称为链接变量；另一个是b比特的分组数据Y。在算法开始时，链接变量是一个初始化向量IV。最后的链接变量就是散列值。一般情况是b>n, 所以称f为压缩函数。（注释） IV = 初始向量

CV_i = 链接变量　Y_i = 第i个输入分组　f = 压缩函数　L = 输入的分组数

n = 散列值长度　b = 输入分组长度

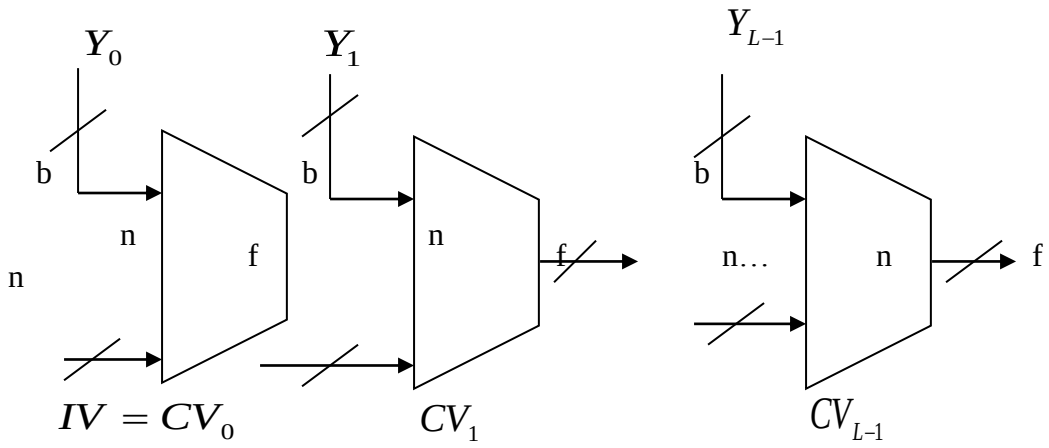


图3-1 散列函数总体结构

可以把散列函数总结如下：

$$CV_0 = IV = \text{初始} n-bit \text{值} \qquad (3\text{-}1)$$

$$CV_i = f(CV_{i-1}, Y_{i-1}), 1 \le i \le L;$$

$$H(M) = CV_L$$

其中散列函数的输出是CV_L；输入是消息M的分组$Y_0, Y_1, \ldots, Y_{L-1}$。

如果压缩函数是抗冲突的，那么迭代函数的合成值也是抗冲突的，也就是说散列函数也是抗冲突的。所以设计安全的散列函数的关键就是设计安全的、抗冲突的压缩函数。散列函数的密码分析的着重点在于压缩函数f的内部结构，并基于这种尝试来寻找对f单次运行后就能产生冲突的高效技术。

总的说来，任何散列函数必定存在冲突，因为将长度至少等于分组长度b的数据映射为长度n的散列值，其中b>n，所以冲突是肯定存在的。而需要做的是要把寻找冲突在计算上变为不可能。

3.4 SHA 算法

安全散列算法(SHA：Secure Hash Algorithm)是美国NIST和NSA共同设计的一个标准，用于作为数字签名标准(DSS)的散列函数，产生数据摘要。当然也可以用到其他需要散列函数的场合。该算法于1993年公布为联邦信息处理标准FIPS PUB 180;于1995年又颁布了一个修订版FIPS PUB 180-1，常记作SHA-1。

SHA的要求是消息长度小于2^{64} bit, 输出的散列值长度为160bit，分组长度是512bit。该算法是基于MIT的Ronald.L .Rivest教授设计的MD4算法原理，并模仿了该算法。

下面介绍一下该算法的主要步骤。

(1)附加填充比特　对于末尾分组，要求其是512bit长度，并且包含64bit的消息长度值。所以要求填充，填充比特串为100...0，即填充的最高位为I，后续各位是0。填充串的长度满足:末尾分组剩余的剩余比特长度+填充串比特长度=512-64=448，也就是在分组的最后，预留了64bit填写消息长度。

此外，如果消息的最后分组刚好512bit，此时由于需要加入64bit的消息长度，所以还是要再新增加一个分组，前面填充100...0共448bit；如果消息最后分组数据长度大于448bit,此时用100...0填满512bit,再新增加一个分组；在新分组前面填充000...0共448bit，最后填写消息长度。

(2)附加长度值　由上面一步知道，末尾分组在最后64bit还没有填写，它就是用来填写消息长度的，所以要求消息长度小于2^{64}比特。填写的64bit长度被看作无符号整数，高字节优先。

(3)设置初始化向量　压缩函数f产生160bit的结果，可以用五个32bit的缓存寄存器A,B,C,D,E来保存这些中间结果和最终结果。初始化向量IV也装入这五个机器存，它们的值是:

A=67452301，

B=EFCDAB89，

C=98BADCFE，

D=10325476，

E=C3D2EIF0。

(4)处理报文分组　处理一个512bit的报文分组比较复杂。它的输入是512bit的分组数据和上一此的输出160bit(在A,B,C,D,E五个寄存器中)；产生的输出是160bit(保存在A,B,C,D,E五个寄存器中)。总的说来，其包含了四个循环的模块，每个循环模块由20个处理步骤。四个循环体的结构是相似的，但是使用不同的原始逻辑，创门分别是fl,f2 ,S ,f4 。

每一个循环模块的输入是:A,B,C,D,E五个寄存器共160bit;从当前512bit分组数据产生的20个32bit字W[i,⋯,i+ 19]。每一个循环模块的输出是160bit,也保存在A,B,CD,E五个寄存器中。

每一个循环模块还使用一个常数值K，其中四个模块分别使用 $K_1 = 5A827999, K_2 = 6ED9EBA1, K_3 = 8F1BBCDC, K_4 = CA62C1D6$ 。其实 K_1 是 $\sqrt{2} \times 2^{30}$ 次方取整， K_2 是 $\sqrt{3} \times 2^{30}$ 次方取整， K_3 是 $\sqrt{5} \times 2^{30}$ 次方取整， K_4 是 $\sqrt{10} \times 2^{30}$ 次方取整。

所有的L个分组处理完毕之后，第L阶段产生的输出便是最终的160bit散列值。

SHA 算法操作:

$$CV_0 = IV;\ CV_{q+1} = SUM_{32}(CV_q, (ABCDE)_q);\ MD = CV_L$$

其中：IV是初始化向量，$(ABCDE)_q$ 是第q个分组的最后一次循环体的输出，L是报文的分组数目， SUM_{32} 是 $\bmod 2^{32}$ 的加法，MD是最终的散列值。

3.5 椭圆曲线密码体制数学原理

3.51 椭圆曲线的数学定义

椭圆曲线的研究来源于椭圆积分：

$$\int \frac{d_x}{\sqrt{E(x)}} \qquad (3\text{-}2)$$

这里的E(x)是x的三次多项式或四次多项式。这样的积分不能用初等函数来表示，为此引进了所谓椭圆函数。所谓椭圆曲线是指由Weierstrass方程描述:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (3\text{-}3)$$

所确定的曲线，是该方程的解及无穷远点0的集合，其中 $a_i \in F,(i=1,2,\ldots,6)$，F可以是有理数域、复数域、还可以为有限域G(p)（素数p>3）或 $G(2^m)(m \in Z^+)$

椭圆曲线通常用 E 表示，若令 $x = X/Z, y = Y/Z$，代入（3-3）得

$$(Y/Z)^2 + a_1(XY/Z^2) + a_3(Y/Z) = (X/Z)^3 + a_2(X/Z)^2 + a_4(X/Z)^2 + a_6 \qquad (3\text{-}4)$$

当 $Z \neq 0$ 时整理得：

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4X^2Z + a_6Z^3 \qquad (3\text{-}5)$$

定义如下参数：

$$b_2 = a_1^2 + 4a_2, b_4 = a_1a_3 + 2a_4, b_6 = a_3^2 + 4a_6$$
$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

其中Δ为Weierstrass方程的判别式，当满足 $\Delta \neq 0$ 时，该椭圆曲线为非奇异曲线，即满足曲线上任意一点的偏导数不能同时为0，也就是曲线上的任意一点都有切线存在，则上面的实数点可以构成加法群，而当Δ=0时，此时

的椭圆曲线上的点就不宜构造群。因为若 Δ=0，方程就存在两相等的根，也就是有两个相重合的曲线点，求这两点之间的加之和就是一个困难，一般情况下要去除重根的点，才可能构成群，在密码学中一般不使用此种情形。

设K是一个域(可以是有理数域、实数域或者有限域)，$\overline{K}$ 和 K^+，分别为其代数闭域和乘法群，椭圆曲线E(K)定义为 $\overline{K}\times\overline{K}$ 上满足Weierstrass方程的点加上所谓的无穷远点的集合。

$Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4X^2Z+a_6Z^3$，其中 $a_i\in K$ 。

椭圆曲线的图象实例，如图 3-2 所示。

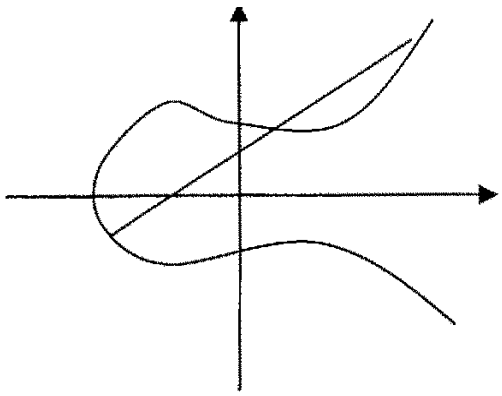


图 3-2 椭圆曲线图象实例

3.5.2 椭圆曲线上的离散对数问题

离散对数问题1201是很多密码体制的安全基础，而椭圆曲线密码体制的安全性也是基于椭圆曲线离散对数问题(ECDI，P：Elliptic Curve Discrete Logarithm Problem[16])。根据前面介绍的椭圆曲线加法运算，假设椭圆曲线E上有点P，Q有：kP=Q，此时ECDLP就可以描述为:已知E上的点P，Q，求k使kP=Q，显然E上不是任意两个点都有离散对数解k的。在实际的密码系统中的Fp，模p可以达到上百比特，要计算k是非常困难的。

3.5.3 有限域上安全椭圆曲线的选取

安全椭圆曲线的选取需要满足前面所描述的安全准则，下面基于这些

准则，来介绍选取安全椭圆曲线的方法。

获取安全的椭圆曲线主要有以下四种办法:

⑴方法一　有限域GF(q)上随机生成一椭圆曲线，直接计算其阶，判断阶是否为大素数或含大素数因子，若是即确定，否则继续选取曲线，直至符合条件。

⑵方法二　取具有一定特殊性椭圆曲线的系数，计算该椭圆曲线的阶，对该阶进行判断，直至找到所需要的安全曲线。

⑶方法三　如果$q = 2^m$，其中m能被一个比较小的整数d整除，我们首先在有限域$GF(q_1)(q_1 = 2d)$上选择椭圆曲线E’并计算其阶，根据此值，利用Weil定理计算该曲线在其扩域GF(q)上的阶，若此阶符合安全标准，我们再找曲线E'在域GF(q)上的嵌入E，则E即为所需的安全椭圆曲线。

⑷方法四　首先给出具有安全条件的曲线阶，然后构造具有此阶的椭圆曲线。

第 4 章 基于椭圆曲线数字签名的实现

4.1 数字签名

数字签名能够实现电子文档的辨认和验证。数字签名是传统文件手写签名的模拟，能够实现用户对电子形式存放的消息认证。

数字签名的目的是什么呢?签名者要留下证据来证明他办了这件事，所谓“白纸黑字”，亲手写下的名字就是一个最好的依据。在政治、军事、外交等活动中签署文件，商业活动中鉴定契约、合同，以及日常生活中写信等，都是采用手写签名或盖印章的方式来起到认证和鉴别的作用。几百年来，用这种方式解决了许多复杂的问题。随着信息时代的到来，电子商务、办公自动化等数字化业务的兴起，文件将不再是实实在在的物理实体，而是以电子形式进行存储和传输，传统的手写签名和印章方式已经很难再适用，需要一种能够对电子文件进行认证的新的手段。

所谓数字签名, 是以电子化形式, 使用密码方法, 在数字消息中嵌入一个秘密信息, 以验证这个秘密信息是否正确来达到识别的目的。它的实质是一种密码变换。数字签名是认证理论和密码学研究的一个新课题, 现在已经是网络安全中最流行的一个话题[12,15]。数字签名，要能起到认证和识别的目的，至少要达到以下要求:

⑴ 要求一　不可否认性。签名者事后不能否认自己的签名。

⑵ 要求二　可验证性。接收者能验证签名，而任何其他人都不能伪造签名。

⑶ 要求三　可仲裁性。当双方发生争执时，可以由一个公正的第三方出面解决争端。

数字签名方案一般包括三个过程:系统的初始化过程、签名产生过程和签名验证过程。在系统的初始化过程中要产生的数字签名方案中用到的一切参数，有公开的，也有秘密的。在签名产生的过程中用户利用给定的算法对消息产生签名，这种签名过程可以公开，也可以不公开。在签名验证过程中，验证者利用公开验证算法对给定签名的消息进行验证，得出签名的有效性。

数字签名一般的工作流程是：信息的发送方首先通过运行一个哈希函

数(hash function[17])，对要发送的报文生成消息摘要，然后用自己的私钥对这个消息摘要生成数字签名，将这个数字签名和报文一起发送给接收方。接收方在收到后，对数字签名和报文进行一定的运算，通过判断运算结果就可以确认发送方和报文的真实性。

4.2 椭圆曲线代理签名体制

4.2.1 主要参数的选择

选取一个基域F_q，一个定义在F_q上的椭圆曲线 E 和 E 上一个为素数阶 p 的 G 点，G 可以公开。全局参数组为（q，FR，a，b，G，n，h）。

4.2.2 密钥的生成

（1）步骤一　选择一个随即整数$d_i, d_i \in [1, n-1]$；

（2）步骤二　计算$Q_i = d_i G$，若Q_i的横坐标为 0，则返回（1）；

（3）步骤三　实体的公钥为Q_i，私钥为d_i；

这里，记原始签名 A 和代理签名 B 的公钥和私钥对为$(Q_1, d_1)(Q_2, d_2)$，其中$Q_1 = d_1 G, Q_2 = d_2 G$。

4.2.3 代理签名协议

（1） 委托过程

步骤一：A 随即选取一个整数$k \in [1, n-1]$；

步骤二：计算$K = kG \bmod n(d_1, d_2), r = d_1 \bmod n$;

步骤三：A 计算$\sigma_1 = d_1 + kK$,并将（σ_1, K）秘密的发给B；

步骤四：B 验证等式

$$\begin{aligned}&\sigma_1 G = (d_1 + kK)G \bmod n\\&= d_1 G + kKG \bmod n\\&= Q_1 + K * K \bmod n\end{aligned}$$

步骤五：B 计算 $\sigma = \sigma_1 + d_2 Q_2$

（2） 签名过程

步骤一：B 随即选取一个整数 $k \in [1, n-1]$；

步骤二：计算 $K_1 = kG \bmod n = (d_1, G_1); r = d_1 \bmod n$；

步骤三：B 计算 $e = SHA1(m)$；

步骤四：计算 $s = k^{-1}(e + d_1 r) \bmod n$，如果 s=0，则返回（*）；式中（r，s，K）就是 B 对消息 m 的签名。

（3） 签名过程

$$v = Q_2 + K \bullet K + Q_2 \bullet Q_2$$

计算 $X = e^{-1}(sG - rv) = (d_1, d_2)$；若 X=0，则拒绝这个签名；否则计算 $v = d_1 \bmod n$，当且仅当 $v^1 = r$ 时接受这个签名。

其正确性可由下面算式证明：

$$\begin{aligned}&v = Q_2 + K \bullet K + Q_2 \bullet Q_2\\&= d_2 G + K \bullet kG + d_2 G_2 \bullet d_2 G_2\\&= G(d_2 + K \bullet k + d_2 G_2 = G\sigma\\&e^{-1}(sG - rv) = e^{-1}(sG - r\sigma G)\\&e^{-1}((k_1 e + r\sigma)G - r\sigma G)\\&= e^{-1}(k_1 eG) = k_1 G = (d_1, d_2) = r\end{aligned}$$

安全性分析[13]：

（1)基本的不可伪造性　在该代理签名协议[12]中,B虽然得到K和σ_1，但是他不能推算出d_1，这是由于从K不能得到k，因此不能获得d_1，从而无法伪造A的签名。

（2）代理签名的不可伪造性　由于只有B知道（σ，K)，因为只有B能生成有效的代理签名，甚至A都不能伪造该代理签名。

（3）代理签名的可区分性　代理签名是由(r，s，K)三部分组成，因此很容易将代理签名和原始签名区分开。同时由于在签名过程中用到了各自的公钥，很容易与他人的代理签名区分开。

（4）不可抵赖性　由于任何人都无法伪造A的普通数字签名，所以不能否认他的有效的普通数字签名。同样，除了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数字签名。

（5）可识别性　在本协议中，如果A在向B发送(σ_1K)时候，将K和B的身份保存在一起，那么当A看到一个有效的代理签名(r，s，K)的时候，就可以通过K确认B的身份。

（6）密码依赖性　在该协议中，σ_1是A密钥d_1的函数，σ是A的密钥d_1和B的密钥d_2的函数，即它依赖于d_1和d_2。

（7）可注销性　A如果想注销B拥有的代理签名σ，那么A可以公布K不再有效，从而B所生成的所有代理签名随之失效。

4.3 椭圆曲线数字签名的计算机实现

4.3.1 椭圆曲线数字签名方案的建立

A为签名方，即为发送方，B为验证方，即为接收方：

(1)步骤一　用户A选定一个Hash函数。

(2)步骤二　用户A建立椭圆曲线域参数T=(p，a，b，Qn，h)，根据情况选择适当安全强度的密钥数据长度；

(3)步骤三　用户B通过可靠的方式获得A所选择的Hash函数和建立的椭圆曲线域参数T。

4.3.2 椭圆曲线数字签名算法

Input：待签名消息m；

Output：对待签名消息M的数字签名S为整数对(r,s)；

Actions：选择一临时FCC密钥对(k,R)，其中 $R=(x_R,y_R)$ 与域参数T相关；令 $r=x_R(\mathrm{mod}\,n)$，*if* r=0, return to step 1；计算待签名的hash值H=Hash(M)；将H换成整数e；计算： $s=k^{-1}(e+rd_A)(\mathrm{mod}\,n)$；

If s=0,return to step 1。

Output：S=(r,s)为数字签名。

4.3.3 椭圆曲线验证算法

验证方B验证从签名方A发来的数字签名是否正确，从而判断接收到的消息是否真实或对方是否为真实的实体。

Input:首先输入待验证的数字消息M，然后，A对消息M产生的数字签名S=(r，s)。

Output：如果判断签名为U对数字消息M的签名，则output=“valid”，否则output=“invalid”

Actions:

步骤一 If $r,s\notin[1,n-1]$, output=invalid，stop；

步骤二 计算待签名的hash值，H=Hash(M)；

步骤三 将H换成整数e；

步骤四 计算 $u_1=es^{-1}(\mathrm{mod}\,n)$ $u_2=rs^{-1}(\mathrm{mod}\,n)$；

步骤五 计算 $R=(x_R,y_R)=u_1G+u_2QA$，If R=0，output “invalid”and stop；

步骤六 另 $v=x_R(\mathrm{mod}\,n)$；

步骤七 比较v和r，if v=r,output=“valid”；if $v\neq r$,output=“invalid”。

4.3.4 椭圆曲线数字签名方案及仿真实现

根据 ECDSA 的原理[14]，我们用 C 语言开发了二元域上的应用程序。下面给出了 ECDSA 方案的签名流程图（图 4-1）和验证流程图（图 4-2）。

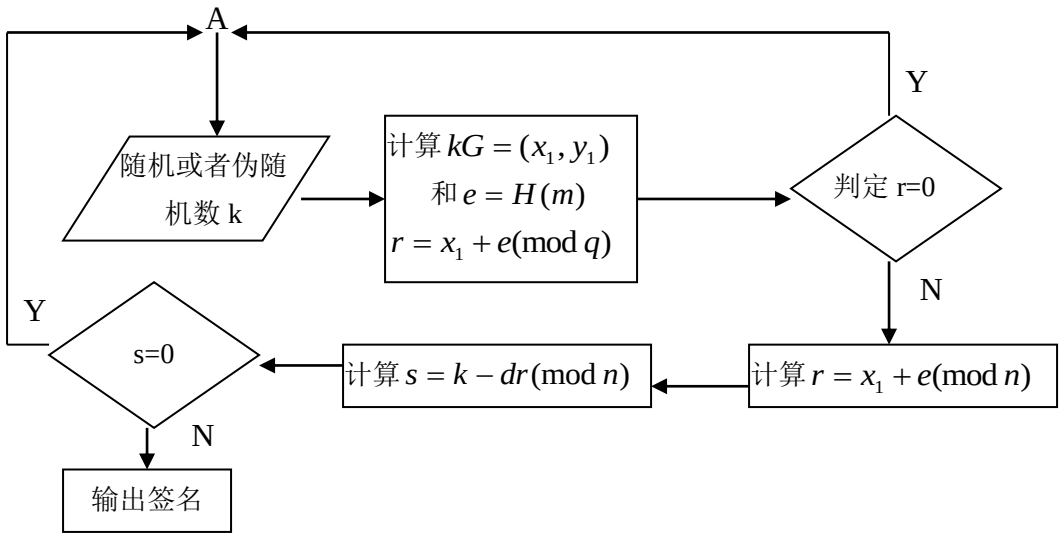


图 4-1 ECDSA 算法签名流程图

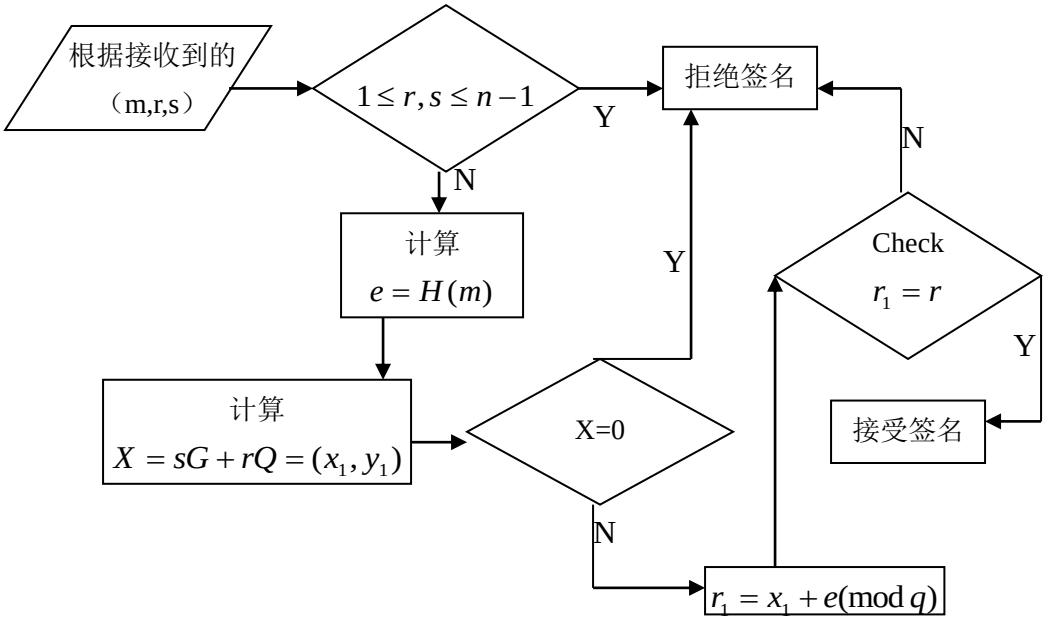


图 4-2 ECDSA 算法验证签名流程图

根据流程图，我们以 NIST 推荐的椭圆曲线为例，编程实现 ECDSA 的

签名算法及验证过程。由于篇幅有限，这里只列出重要的参数和结果。

主要参数如下。

（密文）m：163 位有限域；

FR：Gaussion Normal Basis,T=4；

A：0x00 00000000 00000000 00000000 00000000 00000001；

B：0x00 00000000 00000000 00000000 00000000 00000001；

XG：0x02 FE13C053 7BBCl1AC AA07D793 DE4E6D5E 5C94EEE8；

YG：0x02 89070FB0 5D38FF58 321F2E8O 0536D538 CCDAA3D9；

N：0x04 00000000 00000000 000201O8 A2EOCCOD 99F8A5EF；

H：2；

其中A，B，XG，YG，N，H为ECC签名系统参数, 可以根据情况设置。

FR2约简多项式为：$f(x) = x^{163} + x^7 + x^6 + x^3 + 1$

私钥：Ox00x5584d4bf0x7562818e 0x97eda7b0x85626bde 0x5689e56c；

公钥：0x3 0x4c6750fd 0xa319d548 0x89ae53d2 0x9ae4a5bl 0x898c949d0x7 0x3c409530 0xld297132 0x5la04080 0xb6ffe820 0xlca09450；

签名:

437352739857664o0635793O435496927561584355920663235825943lO21O8548792244141942078832449299231590 93。

椭圆曲线数字签名密钥对生成、对消息文件签名以及验证签名的过程(见图 4-1 和图 4-2)该程序都采用 163 位推荐椭圆曲线,目前可按受的安全强度为 112 位,所以它的安全性是足够的。

4.4 椭圆曲线加密体制的安全性分析

基于模数运算的整数因式分解问题和离散对数问题都存在亚指数时间复杂度的通用算法。目前采用最快的算法计算这两类问题所需的时间复杂度为：

$$O(\exp\{1+O(1)\sqrt{\ln p \ln(\ln p)}\}) \qquad (4\text{-}1)$$

其中P为模的大小。对于椭圆曲线离散对数问题，虽然也可以使用对一般群都有效的baby—step—gi—ant—step算法来求解，但是该方法对椭圆曲线离散对数的时间复杂度是完全指数级的，仅当椭圆曲线上的点加群的阶不含大素数因子时才是有效的。另外指数计算法也不能有效地用来攻击椭圆曲线密码体制。到目前为止取椭圆曲线离散对数的最快的技术是Pollald rho方法，根据最新资料公布的数据，Pollard rho方法的时间复杂度是指数级的，利用Pollard rho方法求解椭圆曲线离散对数问题的最好时间复杂度是，其中 $O(\sqrt{\frac{\pi l}{4n}})$ l为$\#E(F_q^n)$中的最大因子。但当椭圆曲线上的阶含有较大素因子时这两种方法也是无效的。

为了保证RSA密码体制的安全性，它的密钥长度需要一再增大，使得它的运算负担越来越大。相比之下，椭圆曲线加密体制(ECC)可以用短得多的密钥获得同样的安全性，因此具有广泛的应用前景。实现椭圆曲线密码时有许多关键性的问题需要解决，其中主要包括2个方面：第一方面：如何选取合适的符合安全条件的随机椭圆曲线；第二方面：如何快速实现椭圆曲线密码。密算法的安全性能一般通过该算法的抗攻击强度来反映。要保证RSA密码体制使用的安全性，就要相应地增加其密钥的位数，目前一般认为RSA密码体制需要1024位以上的字长才有安全保障。但是，密钥长度的增加导致了其加解密的速度大大降低，硬件实现也比较困难，这对RSA密码体制的应用带来了很重的负担，从而使得其应用范围越来越受到制约。而椭圆曲线则具有较短的密钥长度，例如160位ECC与1024位RSA，DSA(数字签名算法)具有相同的安全强度，210位ECC则与2048位RSA，DSA具有相同的安全强度。ECC与其他公钥加密系统相比，能提供更好的加密强度、更快的执行速度和更小的密钥长度，因此ECC可用较小的开销(所需的计算量、存储量、带宽、软件和硬件实现的规模等)和时延(加密和签字速度高)实现较高的安全性。特别适合用于计算能力和集成电路空间受限(如IC卡)、带宽受限(如无线通信和某些计算机网络)或要求高速实现的情况。

结 论

信息时代虽然给我们带来了无限商机与方便，但同时也充斥着隐患与危险。由于网络很容易受到攻击，导致机密信息的泄漏，引起重大损失。由于信息技术已经成为综合国力的一个重要组成部分，因此信息安全已成为保证国民经济信息化建设健康有序发展的保障。

椭圆曲线密码体制由于具有密钥长度短、数字签名快、计算数据量小、运算速度快、灵活性好等特点，已经广泛地被应用。由于ECC能实现较高的安全性，只需要较小的开销和延迟，在如计算量、存储量、带宽、软硬件实现的规模等；延迟体现在加密或签名认证的速度方面。所以ECC特别使用于计算能力和集成电路空间受限(如IC智能卡)、带宽受限(如高速计算机网络通信)等情况。

通过对椭圆曲线密码系统的学习和研究，本文主要完成了以下几个方面的工作：

(1) 研究学习了ECDSA椭圆曲线数字签名算法的理论基础及算法原理，研究了随机生成有限域上的椭圆曲线方程算法。

(2) 设计了一种基于ECDSA算法的数字签名系统，分析了其系统架构，并对ECDSA数字签名进行了成功的仿真。

2000年10月2日新的高级加密标准(AES：Advanced Encryption Standard)算法被确定。数字加密标准(DES ，Data Encryption Standard)将被具有更高强度和效率的新的高级加密标准所替代。随着计算机性能和密码分析水平的不断提高，数字签名技术今后可能的研究与发展方向为：

(1) 高效、强安全的数字签名研究。数字签名是信息安全技术中一个基础性关键技术，寻找基于新的计算困难问题上的单向函数是数学家、密码学家不断努力的重要目标，也是数字签名算法的基础。设计短密钥、短签名、强安全和抗攻击的数字签名是数字签名技术研究的一个重点。

(2) 新型安全体制下的数字签名技术研究。近几年，量子密码、DNA密码、混沌理论等新型的安全体制的理论研究十分活跃。在此基础上的数字签名技术是一个值得研究的新问题。

(3) 安全协议研究。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是当前国际上研究的一个热

点，其中的许多方法都能应用到数字签名理论和应用的研究上。

(4) 特殊数字签名技术研究。多重签名、群签名、代理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。有许多问题值得进一步研究，其中部分问题具有相当的挑战性。将这些技术能很好地应用于实际还有一段路要走。

(5) 网络应用刺激着数字签名技术研究。现实中的许多工作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都离不开数字签名技术。利用数字签名技术设计安全的应用协议是未来数字签名应用和理论所不能回避的问题。

参考文献

1 杨明，肯光辉，齐望东. 密码编码学与网络安全:原理与实践. 北京：电子工业出版社，2001，59~60

2 卢开澄. 计算机密码学. 北京：清华大学出版社，1998，102~103

3 冯登国. 密码分析学，北京：清华大学出版社，2000，66~67

4 SalommaA，公钥密码学. 北京：国防工业出版社，1998，32~33

5 张先红. 数字签名原理及技术. 北京：机械工业出版社，2004，87~88

6 白国强. 椭圆曲线密码及其算法研究：（博士学位论文）. 西安:西安电子科技大，2003，10~11

7 卿斯汉. 密码学与计算机网络安全. 北京：清华大学出版社，2001， 55~56

8 朱文余，孙琦. 计算机密码应用基础. 北京：科学出版社，2000，132~133

9 陈景润. 初等数论I. 北京：科学出版社，1978，154~156

10 谢邦杰. 抽象代数学. 上海：上海科学技术出版社，1982，187~188

11 潘承洞，潘承彪. 简明数论北京：北京大学出版社，1998，197~198

12 吴克力. 数字签名理论与算法研究：（博士学位论文）. 南京理工大学，2005，77~78

13 李继国，曹珍富，李建中，张亦辰. 代理签名的现状与进展通信学报加密与解密，2003，203~204

14 伍忠东，谢维信，喻建平. 一种安全增强的基于椭圆曲线可验证门限签名方案计算机研究与发展，2005，705~710

15 秦晓东，辛运怀，卢桂章基于椭圆曲线的数字签名系统的设计与实现计算机工程与应用，2003，302~303

16 杨义先，孙伟，钮心忻，现代密码新理论, 北京：科学出版社，2002

17 Koblitz N.Elliptic curve cryptosystems. Mathematics of Computation,1987，203~209

18 B. Preneel. Cryptographic Hash Functions. Mathematics of Computation,1990，31~45

19 V Miller.Uses of elliptic curves in cryptography .Advances in Cryptology-CRYPTO'85 ,LC NS 218, 1986 ,417~426

附录 1 开题报告

燕山大学
本科毕业设计（论文）开题报告

课题名称：基于椭圆曲线的
数字签名研究与仿真

课题性质：模拟

课题来源：自选

学院（系）：里仁学院

专　　业：电子信息工程

年　　级：03 级电信

学生姓名：李哲

指导教师：田澈

2007 年 4 月 1 日

一、综述本课题国内外研究动态，说明选题的依据和意义

当今社会是信息化社会，电子计算机和通信网络已经广泛的应用于社会的各个领域，以此为基础建立起来的各种信息系统，给人们的生活、工作带来了巨大变革。大型信息系统将众多的计算机和只能化设备连在一个四通八达的通信网络中，共享丰富的数据库信息和计算机资源，储存大量的数据文件，完成异地之间的数据交换与通信。信息系统的应用，加速了社会自动化的进程，减轻了日常繁杂的重复劳动，同时也提高了生产率，创造了经济效益。

信息安全技术在信息化迅速发展的今天已进入了高速发展的新时期，形成了密码技术、可信计算技术、电磁辐射泄露防护技术、系统入侵检测技术和计算机病毒检测消除技术等多个安全防护技术门类。

数字签名又称之为数字签字、电子签名、电子签章等。其提出的初衷就是在网络环境中模拟日常生活中的手工签名或印章;而要使数字签名具有与传统手工签名一样的法律效力，又催生了数字签名法律的出现。数字签名具有许多传统签名所不具备的优点，如签名因消息而异，同一个人对不同的消息其签名结果是不同的，原有文件的修改必然会反映为签名结果的改变，原文件与签名结果两者是一个混合不可分割的整体等。所以，数字签名比传统签名更具可靠性。

信息时代虽然给我们带来了无限商机与方便，但同时也充斥着隐患与危险。由于网络很容易受到攻击，导致机密信息的泄漏，引起重大损失。由于信息技术已经成为综合国力的一个重要组成部分，因此信息安全已成为保证国民经济信息化建设健康有序发展的保障。

网络安全技术众多，目前在电子商务、电子政务、电子邮件系统、电子银行等方面必备的关键技术就是数字签名。数字签名又称为数字签字，电子签章等。“数字签名”用来保证信息传输过程中信息的完整和提供信息发送者的身份认证和不可抵赖性，数字签名技术的实现基础是公开密钥加密技术，是用某人的私钥加密的消息摘要用于确认消息的来源和内容。

二、研究的基本内容，拟解决的主要问题：

大量搜集、阅读有关数字签名技术的资料、专著，了解、掌握数字签名技术的发展趋势及现状。研究数字签名的产生、工作原理、各类典型算法的特点及其在保密通信领域的应用。自学 MATLAB 仿真语言，并用 MATLAB 对某种典型的数字签名进行仿真，对其安全性能指标进行分析

三、研究步骤、方法及措施：

搜集、查阅资料，掌握数字签名的产生、工作原理、各类典型算法的特点及其在保密通信领域的应用。自学 MATLAB 仿真语言的一种版本。用 MATLAB 仿真数字签名，分析安全性能指标。

四、研究工作进度：

查阅资料读专著分析原理过程。确定仿真方案，自学语言，设计编程。编程，仿真分析。仿真调试。仿真写论文答辩。

五、主要参考文献：

［1］William Stalling. 密码编码学与网络安全:原理与实践. 杨明，肯光辉，齐望东等译. 北京：电子工业出版社，2001

［2］卢开澄. 计算机密码学. 北京：清华大学出版社，1998

［3］冯登国. 密码分析学，北京：清华大学出版社，2000

［4］SalommaA，公钥密码学. 北京：国防工业出版社，1998

［5］张先红. 数字签名原理及技术. 北京：机械工业出版社，2004

［6］白国强. 椭圆曲线密码及其算法研究：［博士学位论文］. 西安:西安电子科技大

［7］卿斯汉. 密码学与计算机网络安全. 北京：清华大学出版社，2001

［8］朱文余，孙琦. 计算机密码应用基础. 北京：科学出版社，2000

［9］陈景润. 初等数论I. 北京：科学出版社，1978

［10］谢邦杰. 抽象代数学. 上海：上海科学技术出版社，1982

［11］潘承洞，潘承彪. 简明数论北京：北京大学出版社，1998

［12］吴克力. 数字签名理论与算法研究：［博士学位论文］南京理工大学，2005

［13］李继国，曹珍富，李建中，张亦辰. 代理签名的现状与进展通信学报，2003,Vo1.24 No.10

［14］伍忠东，谢维信，喻建平. 一种安全增强的基于椭圆曲线可验证门限签名方案计算机研究与发展，2005,42(4)：705—710

［15］秦晓东，辛运怀，卢桂章基于椭圆曲线的数字签名系统的设计与实现计算机工程与应用，2003.2

［16］杨义先，孙伟，钮心忻，现代密码新理论, 北京：科学出版社，2002

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

［18］B. Preneel. Cryptographic Hash Functions.ETT Vol.5, N o.4, 17 /431-31/45

六、导师意见：

指导教师（签字）_____

____年 ____月 ____日

七、审核意见：

审查结果： 1、通过； 2、完善后通过； 3、未通过

负责人（签字）：_____

____年____月____日

附录 2 文献综述

燕 山 大 学
本科毕业设计（论文）文献综述

课题名称：基于椭圆曲线的
数字签名研究与仿真

课题性质：模拟

课题来源：自选

学院（系）：里仁学院

专　　业：电子信息工程

年　　级：03 级电信

学生姓名：李哲

指导教师：田澈

2007 年 6 月 1 日

一、课题国内外现状：

目前，密码理论与技术主要包括两部分，即基于数学的密码理论与技术(其中包括公钥密码、分组密码、流密码、认证码、数字签名、Hash M数、身份识别、密钥管理、PKI技术等卿非数学的密码理论与技术(包括信息隐形、量子密码、基于生物特征的识别理论与技术)。

实现数字签名有很多方法，目前数字签名采用较多的是公钥加密技术，如基TRSA Data Security中的PKCS(Public Key Cryptography Standards)，DSA (Digital Signature Algorithm), x.509, POP (Pretty Good Privacy)。1994年美国标准与技术协会公布了数字签名标准(DSS)而使公钥加密技术广泛应用。同时应用散列算法(Hash)也是实现数字签名的一种方法。而关于椭圆曲线数字签名的研究正处于伊始状态，所以很多问题都没能有效解决。在个别领域，我国开始尝试采用新的椭圆曲线数字签名算法(包括192位椭圆曲线算法、224位椭圆曲线算法和256位椭圆曲线算法)。

目前国内对于椭圆曲线公钥的快速实现、智能卡应用等研究较多。由于它本身的优点也特别适用于无线Modem, Web服务器、集成电路卡等方面。但是综合浏览后，发现关于在要进行大量安全交易的电子商务领域中研究比较有限。随着网上交易的频繁，这将成为今后研究的热点。

二、研究主要成果：

椭圆曲线密码体制由于具有密钥长度短、数字签名快、计算数据量小、运算速度快、灵活性好等特点，已经广泛地被应用。由于 ECC 能实 AIR 高的安全性，只需要较小的开销和延迟，较小的开销体现在如计算量、存储量、带宽、软硬件实现的规模等;延迟体现在加密或签名认证的速度方面。所以 ECC 特别使用于计算能力和集成电路空间受限(如工 C 智能卡)、带宽受限(如高速计算机网络通信)等情况。

三、发展趋势：

当今社会是信息化社会，电子计算机和通信网络已经广泛的应用于社会的各个领域，以此为基础建立起来的各种信息系统，给人们的生活、工作带来了巨大变革。大型信息系统将众多的计算机和只能化设备连在一个四通八达的通信网络中，共享丰富的数据库信息和计算机资源，储存大量的数据文件，完成异地之间的数据交换与通信。信息系统的应用，加速了

社会自动化的进程，减轻了日常繁杂的重复劳动，同时也提高了生产率，创造了经济效益。

信息安全技术在信息化迅速发展的今天已进入了高速发展的新时期，形成了密码技术、可信计算技术、电磁辐射泄露防护技术、系统入侵检测技术和计算机病毒检测消除技术等多个安全防护技术门类。

四、存在问题：

目前普遍采用的数字签名算法，都是基于下面三个数学难题的基础之上：(1)整数的因式分解(Integer Factorization)问题，如RSA算法。(2)离散对数(Discrete Logarithm)问题，如 ElGamal,DSA,Schnorr等算法；(3)椭圆曲线(Elliptic Curve)问题，如ECDSA算法。

五、主要参考文献：

［1］William Stalling. 密码编码学与网络安全:原理与实践. 杨明，肯光辉，齐望东等译. 北京：电子工业出版社，2001

［2］卢开澄. 计算机密码学. 北京：清华大学出版社，1998

［3］冯登国. 密码分析学，北京：清华大学出版社，2000

［4］SalommaA，公钥密码学. 北京：国防工业出版社，1998

［5］张先红. 数字签名原理及技术. 北京：机械工业出版社，2004

［6］白国强. 椭圆曲线密码及其算法研究：［博士学位论文］. 西安:西安电子科技大

［7］卿斯汉. 密码学与计算机网络安全. 北京：清华大学出版社，2001

［8］朱文余，孙琦. 计算机密码应用基础. 北京：科学出版社，2000

［9］陈景润. 初等数论I. 北京：科学出版社，1978

［10］谢邦杰. 抽象代数学. 上海：上海科学技术出版社，1982

［11］潘承洞，潘承彪. 简明数论北京：北京大学出版社，1998

［12］吴克力. 数字签名理论与算法研究：［博士学位论文］南京理工大学，2005

［13］李继国，曹珍富，李建中，张亦辰. 代理签名的现状与进展通信学报，2003,Vo1.24 No.10

［14］伍忠东，谢维信，喻建平. 一种安全增强的基于椭圆曲线可验证门限签名方案计算机研究与发展，2005,42(4)：705—710

［15］秦晓东，辛运怀，卢桂章基于椭圆曲线的数字签名系统的设计与实现计算

机工程与应用，2003.2

［16］杨义先，孙伟，钮心忻，现代密码新理论, 北京：科学出版社，2002

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

［18］B. Preneel. Cryptographic Hash Functions.ETT Vol.5, N o.4, 17 /431-31/45

附录 3 英文翻译

燕 山 大 学
本科毕业设计（论文）英文翻译

课题名称：基于椭圆曲线的
数字签名研究与仿真

课题性质：模拟

课题来源：自选

学院（系）：里仁学院

专　　业：电子信息工程

年　　级：03 级电信

学生姓名：李哲

指导教师：田澈

ECC 是基于有限域上，椭圆曲线点集 E 所构成的群上定义的离散对数系统.有限域上椭圆曲线的选择，应避免使用超奇异曲线,以保证足够的安全性.椭圆曲线的运算为给定椭圆曲线 E 上的一个基点 G 和一个整数(1 1)n κ κ ≤≤，求数乘(mod)GQ p κ =，Q 也是 E 上的一点，计算...GGG G κ =+++(κ 个 G 相加)相对容易；但若给定椭圆曲线上两点 G 和 Q，求一整数 κ，使(mod)GQ p κ =，特别是当 G 是较高阶的基点时，则非常困难。这就是椭圆曲线离散对数问题。基于椭圆曲线离散对数问题的难解性，形成了 ECC 体制。

1. 椭圆曲线密码

椭圆曲线密码系统有多种形式，典型的如 EIGamal 系统。Diffie-Hellman 密钥交换协议：设 E 是一个素数域()GF p 上的椭圆曲线，G 是曲线上公开的点,其阶为 n。A 秘密的选定一个随机整数 AA(11)ddn≤≤，计算点 AdG,发送给 B；同样，B 秘密的选定一个随机整数 BA(11)ddn≤≤，计算点 BdG，发送给 A。公钥为 ABQddG=，A 用自己的私钥 Ad 乘以从 B 收到的 AdG 计算得到 Q；B 用自己的私钥 Bd 乘以从 A 收到的 AdG 计算得到 Q。窃听者必须得确定 ABQddG=，只知 G,AdG，和 BdG，但无法推出 Ad 或 Bd. EIGamal 系统：假定信息序列已经通过编码嵌入到椭圆曲线 E 上，并且 A，B 双方已经通过 Diffie-Hellman 协议互相交换了 AdG 和 BdG，A 要向 B 发送信息 m,A 发送给 B 数对：[]AAB；()dGm d dG+. B 用其私钥 Bd 乘以第一项，再用第二项减去它，就解出信息 m。

2. 几种典型的基于 ECC 的数字签名方案

基于公钥密码的数字签名体制的基本原理是：当用户用私钥签名时,签名与用户本身联系在一起,且具有法律效率，接收方用签名者的公钥来验证签名。一般地，对于相同规模的参数,椭圆曲线密码每一位密钥的强度要大得多，173 位的椭圆曲线密码系统相当于 1024 位的 EIGmal 或 DSA 系统。实现速度比 DSA，RSA 等其它公钥系统更为快捷，效率高。

2.1 基于 ECC 的 EIGamal 签名方案

此方案是由传统 EIGamal 签名体制移植到椭圆曲线上而产生。

1)初始化:构造素数域()GFp 上非超奇异的椭圆曲线 E，选择公开的基点 G E ∈，其阶为 n；将信息序列 m 通过编码嵌入到 E 上,即 m E ∈。

2)密钥生成：用户 A 随机选取[]A1, 2... 1dn∈，将公开点 AQdG=作为公钥。

3)签名：A 随机选择(1, 2...)n κ ∈，计算(,)RGxy κ ==，再计算 1A()modsmdxn κ ≡ ,然后输出签名[],,mRs。

4)验证：B 收到签名信息后，验证 1VxQsR=+和 2VmG=，若 12VV=则验证为真签名；否则为假。

因为 1AAAA2()() ()VxQsRxdG mdxGxdGmdxGmGVκκ =+= + = + ==。

2.2 ECDSA 签名方案 [1]

设素数域()GFp 上非超奇异的椭圆曲线 E，选择公开的基点 G E ∈,其阶为 n；将信息序列 m 通过编码嵌入到 E 上，即 m E ∈。假定 A 用自己的私钥 Ad 对信息 m 签名，B 用 A 的公钥 AAQdG=对上述签名进行验证。

2.2.1 签名 A 产生一随机整数[]1, 2... 1n κ ∈，使 00(,)xyG κ =× 令 0(mod)rx n=，[]1A() (mod)shmrd n κ =+，其中()hi 是一个单向 Hash 函数。

然后，A 将签名信息 (,)rs 和信息 m 发送给 B。

2.2.2 验证 B 收到[],(,)mrs 后计算

1() (mod),uhms n = 1

2(mod)urs n =

然后计算 "00 1 2(,)AxyuGuQ=+，并令 0(mod)vx n=，如果 vr=，则验证通过。

因为

[]

[][]

11

12A A

11 1

AA

1"

AA00

()

() ()

() () (,)

uG uQ h m s G rs Q

hms G rs dG s hm rd G

hm rd hm rd G G x yκκ

+= +=

+=+=

++==

2.3 以上基于 ECC 签名方案的算法分析

EIGamal 方案中只将传统的模 p 操作替代为模 n(n 为椭圆曲线 E 的阶)操作。ECDSA 方案的特点是通过 Hash 函数来计算信息 m 的杂凑值，对信息做非线性变换，进一步提高了签名的安全性。但是，直接对此 Hash 值进行签字，由于 Hash 值(MD5 为 128 位，SHA 则为 160 位的二进制序列)其数值很大，做签名运算较费时。此外，其算法中信息明文 m 未经加密而直接传送，信息 m 的安全性不能得到保障。鉴于此，本文提出了一种兼顾安全性和运算效率一种具有信息恢复的数字签名方案。

3 一种基于 ECC 的签名改进方案

本文提出以消息 Hash 值的 Hamming 重量做签名，对信息 m 也经过加密后与签名一起发送，使接收的信息具有可恢复性。

3.1 参数选择

1)选定一个 Hash 函数 MD5，用 32bit 软件易于高速实现。MD5 输入消息长度任意，输出压缩值为 128bit。若直接对此 Hash 值进行签字，由于 Hash128 位的二进制序列，其数值很大，用其计算签名，运行时间很长。由于 Hash 函数的 Hamming 重量对消息的变化很敏感,若消息变化，Hamming 重量发生变化的概率为 90%以上，本文对此结论用 MATLAB 进行大量的实验验证,结果一致.故本文提出以 Hash 值的 Hamming 重量做签名，对于 128 位二进制序列其值不超过 128，可使运算大为简化。

2)建立一个椭圆曲线域参数(),,,,,TpabGnh=，其中，p 表示一个有限域()GFp，元素，()abGF p∈，非超奇异椭圆曲线 E 上的点满足方程 23yxaxb=++，并且 E 上基点的个数为#( )pEF，称为椭圆曲线 E 的阶。G 表示椭圆曲线 E 上的一个基点，n 为点 G 的阶且为大于 1602 的大素数，它的长度决定了 ECC 的密钥长度。h 是小整数称为余因子且#( )/phEFn=。有关椭圆曲线的点加，减法及数乘等运算规则，阶的计算，基点选取等，其中 E ,()GF p, G,n 公开。

3)将信息序列 m 通过编码嵌入到素数域()GFp 上，即 m∈()GF p。

4)[]AB,1,2,,1dd n∈，A 的私钥是 Ad，用作签名密钥，A 的公钥是 AAQdG=，AQ 作签名验证密钥；B 的的私钥是 Bd，公钥是 BBQdG=，BQ 作信息 m 的加密密钥，Bd 作信息解密密钥。其中 AB，QQ 公开。

3.2 签名及验证

3.2.1 A 生成签名：随机选取一个整数 к，[]1, 2, , 1n к ∈，根据公开的 G 计算椭圆曲线上的点 11(,)，xyG к = 令 1(mod)rx n=，若 r 为 0 重新选择 к；计算信息 m 的 Hash 值，()ehm=，并求此 Hash 值的 Hamming 重量 w，计算签名(( ))(mod)Aswrdn к =++。A 发送信息 m 的签名(,)sr 给 B。

3.2.2 A 用 B 的公钥 BQ 对 m 的加密：计算点 22 B(,)xyQ к =，如果 20x=，则重新选择 к；计算 2cmx=×；传送 m 的加密数据()11,,xyc 给 B。

3.2.3 B 用私钥 Bd 解密消息 m B 接收到加密数据()11,,xyc,计算()"22 B11 B B,(,)xydxydGQкк===，解出 "12mcx =。

3.2.4 B 验证签名：根据解密出的信息 m，计算()ehm=，并计算 Hamming 重量 w；再对收到的签名(,)sr；计算( )(mod)uwr n=+，及"11 A(,)xysGuQ= ，令"1(mod)rx n=，如果'rr=，则收到的(,)sr 为 A 对 m 的正确签名。因为

11 A

AA

AA

(,)

[( )]( )

() ()

xy sGuQ

wrdG wrQ

GwrdGwrQ G

к

к к

= =

++ + =

++ + =

3.3 本文方案的算法分析

先对信息 m 使用了安全性较高的 Hash 函数 MD5 进行散列，即对 m 做了非线性变换后做签名。由于 Hash 函数具有单向，无碰撞特性，因此找不到两个数 12，mm，使 12() ()hash m hash m=，攻击者不可能进行代换攻击，与 ECDSA 具有相同的安全级别；对散列值的 Hamming 重量进行签名而非对散列值直接签名，相比提高了运算效率。并且对信息 m 也经过加密后与

签名一起发送，使接收的信息具有可恢复性。

4 基于 ECC 签名的性能分析

基于椭圆曲线密码的数字签名(ECDSA),其破译难度相当于椭圆曲线离散对数问题的难解性，迄今为止没有找到有效的攻击方法。

本文算法在 ECDSA 的基础上，进一步提高安全性。签名时，考虑到信息明文的保护，以便于明文恢复；没有对信息明文直接签名而用其散列值的汉明重量做签名运算。

本文方案着重考虑了运算效率的提高。算法在已有一些方案的基础上做了进一步的优化，对 Hash 函数的 Hamming 重量做签名,除椭圆曲线上的数乘运算和取模运算外，其余均为代数运算,运算复杂度较低，大大提高了运算速度。

下面具体分析各项性能：签名可确认。当 B 用 A 的公钥 AQ 验证消息时，B 可确认是 A 的签名；签名不可伪造。只有 A 知道其私钥 Ad，别人无法分析得到。即便椭圆曲线上的基点 G 和 AA()QdG=是公开的，但推出 Ad 是椭圆曲线离散对数问题，目前情况是不可解的；签名不可否认。B 或其他人只需用 A 的公钥 AQ 能验证 A 的签名，一旦被验证，A 事后不可否认；签名不可重复使用.因为采用了单向散列 Hash 函数对信息原文进行散列，形成信息摘要，再在此摘要基础上对其汉明重量签名。利用 Hash 函数产生的原始信息的信息摘要对原始信息的轻微变化十分敏感，汉明重量对原始信息变化也很敏感.签名是信息原文的函数，不同的信息原文其散列值不同，签名也不同；⑤被签名的信息是可恢复的。A 用 BQ 作信息 m 的加密密钥，对信息明文进行了 ECC 加密，B 用 Bd 作信息解密密钥很容易对其恢复。

本文方案可进一步实际应用，如对图像或文本等信息的数字签名是下一步要做的工作。涉及到如何准确地将信息原文嵌入椭圆曲线上，以及有关椭圆曲线快速算法等问题将另文讨论。

5. 一种椭圆曲线数字签名方案

椭圆曲线密码属于一种公钥密码体制，除了能对数据加密外，它的另一个应用是进行数字签名。随着分布式计算机技术的提高和广泛应用，计算能力大大增强。要获得更高的安全，RSA 需要更长的密钥比特，占用很大资源，这样更加影响加密和签名速度，不合适用于智能卡等资源有限的硬件设计，而椭圆曲线具有同等安全开销小的优点，椭圆曲线的数字签名

的研究和产品设计逐渐成为人们的研究热点。

椭圆曲线数字签名与 ElGamal 数字签名很相似，只是椭圆曲线数字签名是基于椭圆曲线离散对数问题(ECDLP)，而 ElGamal 数字签名是基于一般有限域的离散对数问题(DLP)。所以我们可以利用这种相似性，对上述六种不同类型的签名方程进行适当的变换，从而得到更简便的椭圆曲线签名方程。我们由上一节给出第(5)个签名方程推导出一种椭圆曲线数字签名方案。在方程 $mk = s + r'x$ 中，我们用 m^{-1} 代替 m，则方程变为 $m^{-1}k = s + r'x$，两边同乘以 m，得 $k = ms + mr'x$。

因为 m 是已知消息，它可以是 hash 值 $e = h(m)$，是签名发起方和验收方都知道的，我们可以令 $s' = ms$，可以用 (s', r) 代替 (s, r) 作为消息 m 的签名，这样，上面的签名方程就可以变为如下：

$$k = s + m\,r\,;$$

从而用这个签名方程来构造一个签名方案，步骤如下：

选取一条安全的椭圆曲线，椭圆曲线参数和上面第 1 部分相同。

(1) 签名者 Alice 在 E 上选择私有密钥 x，g 为 E 的基点，计算 $y = xg$，y 作为公开密钥发出，Alice 对明文 m 计算 $e = h(m)$；

(2) Alice 选择随机整数 k (k 保密)，并计算 $r = kg = (r_0, r_1)$，且 $s = k - er_0 x$；

(3) (s, r)作为对消息 m 的签名，并将(s, r, e)发送给验证者 Bob；

(4) Bob 计算 $r' = sg + er_0 y$，并判断 $r' = r$。

以上是我们推导出的签名方案，该方案避免了求逆的过程，能解决了 ECDSA 算法的不足之处。本方案比 ECDSA 算法简单，实验结果表明，此算法比 ElGamal 方案、Schnorr 方案快约 28%。

ECC elliptic curve numeral encryption

ECC is based on the gal o is field in, elliptic curve set of points Econ statutes on the group defines separate logarithm system In gal o is field elliptic curve choice, Should avoid using the ultra strange curve, guarantees thee no ugh security The elliptic curve operation for assigns on elliptic curve E basic point G and The integer (1 1) n kappa kappa <= <=, asks the number to ride(mod) GQ p kappa =, Q also is on E, computation.. GGG G kappa =+++(kappa G Adds together) is relatively easy; But if assigns in thee l l iptic curve two G and Q, asks an integer kappa, causes (mod) GQ p kappa =, specially when G is compares When Gao Jie basic point, then is extremely difficult This is the elliptic curve separate logarithm question. Based on the elliptic curve separate logarithm question difficult solution, to have formed the ECC system.

1. elliptic curves password

The elliptic curve cryptographic system has the many kinds of forms, typical like Epigamic system Diffie-Hellman key swap agreement :Supposes E is an element number field () on the GF p elliptic curve, Gis in the curve the public spot, its step is n. A secret designation stochastic integer AA (1 1) d d n <= <=, the computation selects AdG,the transmission for B; Similarly, B secret designation stochastic integer BA (1 1) ddn <= <=, the computation selects BdG, the transmission for A. The male key is A B Q d d G=, A while by the Ad computation which receives from B obtains Q with own private key Ad; B with own private key B d while by the A d G computation which receives from A obtains Q. The interception must result in determines A B Q d d G=,only knows G, A d G, with BdG, but is unable to promote Ad or Bd. The EIGamal system: Supposed the information sequence already to insert through the code to the elliptic curve Epsilon on, and A, B both sides already passed The Diffie-Hellman agreement has mutually exchanged A d G and B d G. A must to B transmission information m Epsilon ∈, A transmission for B several pairs: [ ] AAB; () d Gm d d G+. B with its private key B d while by the first item, uses the second item to subtract it again, solves information m.

2. several kinds typical based on ECC digital signature plan

Based on the male key password digital signature system basic principle is: When the user signs with the private key, signs with user itself relates in together, also Has the legal efficiency, the receiving end confirms with the male key signs.

Generally, regarding the same scale parameter, the elliptic curve password each key intensity must be bigger much,,173 elliptic curve password department The series is equal to 1,024 EIGmal or the DSA system There allegation speed compared to DSA, RSA and so on other male key systems, the efficiency is more quickly high.

2.1 based on ECC EIGamal signature plan

This plan is transplants from the traditional EIGamal signature system to the elliptic curve in produces 1) initialization: The structure element number field () on GF p then on- ultra strange elliptic curve Epsilon, chooses public basic point G Epsilon ∈, its step is n; Information sequence m inserts through the code to Epsilon on ,namely m Epsilon ∈ 2) key production: The user A stochastic selection [ ] A1, 2... 1dn∈, will publicize selects A Q d G= to take the male key 3) signature: The A stochastic choice (1, 2...) n kappa ∈, the computation () R G x y kappa ==, calculates 1 again A () modsmdxn kappa ≡, then loses Leaves signs [ ], mRs. 4) confirms: After B receives the signature information ,confirms 1VxQsR=+ and 2VmG=, if 12VV= confirms for really signs ;Otherwise is the vacation.

Because 1AAAA2 () () () V x Q s R x d G m d x G x d G m d x G m G V kappa kappa =+= + = +==. 2.2 ECDSA signature plan [1] Supposes the element number field () on GF p the non- ultra strange elliptic curve Epsilon, chooses public basic point G Epsilon∈, its step is n; Passes information sequence m The code inserts to Epsilon on, namely m Epsilon ∈ Supposes A with own private key Ad to the information m signature, B uses A male key A A Q d G= to the above bamboo slip The name carries on the confirmation 2.2.1 signs A to have a stochastic integer [ ] 1, 2... 1n kappa ∈,causes 00 () x y G kappa =× Make 0 (mod) rx n=, [ ] 1 A () (mod) shmrd n kappa =+, () hi is an unidirectional Hash function Then, A will sign the information () rs and

information m transmission for B. 2.2.2 confirms B to receive [ ], (, after) mrs calculates.

2.2.2 confirms B to receive [ ], (, after) mrs calculates1 () (mod), uhms n = 1 2 (mod) urs n = Then calculates ' ' 001 2 () AxyuGuQ=+, and make ' 0 (mod) vx n=, if vr=, then confirms passes Because

[]

[][]

11

12A A

11 1

AA

1"

AA00

()

() ()

() () (,)

uG uQ h m s G rs Q

hms G rs dG s hm rd G

hm rd hm rd G G x yкк

+= +=

+=+=

++==

2.3 Above based on ECC signature plan algorithmic analysis

In the EIG a mal plan only (n is elliptic curve Epsilon step) operates the traditional mold p operation substitution for mold n The ECDSA plan characteristic is calculates information m through the Hash function mixed to collect the value, makes the nonlinear trans formation to the information, further enhanced the bamboo slip Famous security But, directly regarding this the Hash value carries on the signature, because the Hash value (MD5 is 128, SHA is160 binary sequences) it Value very big, makes the signature operation to be more time-consuming In addition, in its algorithm information definite orders m but directly has not transmitted after the encryption, the information m security

cannot Obtains the safeguard In view of this, this article propose done kind of proper attention to both security and the operation efficiency one kind has the information retrieval the digital signature plan.

3. One kind based on ECC signature improvement program

This article proposed weight makes the signature by news Hash the value Hamming, also passes through after information m the encryption with to sign transmits together, causes the receive The information has may restore.

3.1 Parameter choice

1) Designated Hash function MD5, easy high speed to realize MD5 the input news length with 32bit software free, the output compression value is128bit. If directly regarding this the Hash value carries on the signature, because Hash is 128 binary sequences, its value very big ,calculates the signature with it, the running time is very long Because Hash function Hamming weight to news change very sensitive, if the news change, the Hamming weight changes the probability is above90%, this article conclusion carries on the massive experimental confirmation regarding this with MATLAB, the result is consistent Therefore this article proposed weight makes the signature by Hash the value Hamming, does not surpass 128, regarding 128 binary sequence sits value to be possible to cause the operation greatly for the simplification.

2) Establishes a elliptic curve territory parameter (),,, T pabGnh=,among, p expressed a gal o is field () GF p, the element, () a b GF p∈, the non- ultra strange elliptic curve Epsilon on spot satisfies equation 23yxaxb=++, and Epsilon on the basic point integer for # ()p EF, is called elliptic curve Epsilon step G expression elliptic curve Epsilon on a basic point, n is selects G the step also for is bigger than 1,602 big prime numbers, its length had decided the ECC key length h is the small integer is called -odd factor also # () /ph EF n=Related elliptic curve spot Canada, the subtraction and the number while and so on the operational rule, the step computation, description and so on basic point selection see also the literature [1-3] E, () GF p, G, n is public.

3) Inserts information sequence m through the code to the element number field ()on GF p, namely m∈()GF p.

3.3 This article plan algorithmic analysis

First used secure higher Hash for information m function MD5 to enter the row, namely made the nonlinear transformation after m to do signs As a result of Hash The function has unidirectional, non- collision characteristic, therefore cannot find two several 12, mm, causes 12 ()() hash m hash m=, the aggressor not to be impossible to carry on the generation Trades the attack, has the same security rank with ECDSA; To disperses a row value the Hamming weight to carry on signs but non- to disperses the row value direct signature, compares Enhanced the operation efficiency And also passes through after information m the encryption with to sign transmits together, enable the receive the information to have may restore.

4.Performance analysis signs which based on ECC

Based on the elliptic curve password digital signature (ECDSA), it breaks a code the difficulty to be equal to the elliptic curve separate logarithm question difficult solution, up to now Up to had not found the effective method of attack, the related ECDSA secure analysis, the literature [1] has a more detailed analysis This article algorithm in the ECDSA foundation, further enhances the security When signature, considers the information definite orders the protection, in order to is extensive to the definite orders Duplicate; Has not used it to the information definite orders direct signature to disperse a row value the Chinese bright weight to make the signature operation.

This article plan has emphatically considered the operation efficiency enhancement The algorithm in had some plans in the foundation to make the further optimization, to Hash letter The number Hamming weight makes the signature, and takes the mold operation besides the elliptic curve in number while the operation, other are the algebraic operation, operation complex compares Low, greatly enhanced the operating speed.

Under specifically analyzes each performance: (1) The signature may confirm When B with A male key AQ confirmation news, B may confirm is the A signature; (2) Bamboo slip The name cannot fabricate Only some A knew its private key Ad, the others are unable to analyze obtain Even if in elliptic curve basic point G and AA () QdG= is public But promotes Ad is the elliptic curve separate logarithm question, at present the situation is unsolvable; (3) The

signature did not acknowledge B or other people only must use A Male key AQ can confirm A the signature, once is confirmed, A afterwards did not acknowledge ; (4) Signs cannot duplicate uses Because used has unidirectional dispersed arranges in order Hash The function enters the row to the information original text, forms the hash, again signs in this abstract foundation to its Chinese bright weight Produces originally using the Hash function Beginning information hash to primary information slight change extremely sensitive, the Chinese bright weight very is also sensitive to the primary information change The signature is the information original text The function, different information original text it disperses a row value to be different, signs also differently; (5) The information which signs is may restore A makes information m with BQ The encryption key, carried on the ECC encryption to the information definite orders, B has made the information decipher key with Bd very easily to restore to it.

This article plan may go a step further the practical application, like to information the and so on picture or text digital signature is the work which next step must do How involves to Firmly inserts the information original text in the elliptic curve, as well as question and so on related elliptic curve fast algorithm separate article discussion.

5. An elliptic curve digital signature scheme

Elliptic Curve Cryptosystem is a public-key cryptosystem, in addition to data encryption, it is another application for digital signatures. With distributed computer technology to enhance and extensive application of computing power increased greatly. To achieve greater security, RSA needs of the key bit longer, tie up huge resources, This affected more encryption and signature speed, inappropriate for smart cards and other resources limited hardware design, Elliptic Curve and has the same security advantages of the small overhead, Elliptic Curve Digital Signature research and product design gradually become the hotspot.

Elliptic Curve Digital Signature and ElGamal digital signature is very similar, only elliptic curve digital signature is based on the elliptic curve discrete logarithm problem (Eclipse), ElGamal digital signature and is based on

generally limited domain of discrete logarithm problem (DLP). Therefore, we can use this similarity, right above the six different types of signatures equation appropriate transform, thus be more convenient Elliptic Curve signature equation. Our last article is a (5) Signed an equation derived Elliptic Curve Digital Signature program. In Equation

$mk = s + r'x$

We used m^{-1} to replace m, then the equation into $m^{-1}k = s + r'x$, With both sides multiplied by m, $k = ms + mr'x$;

Because m is known the news, It can be hash $e = h(m)$, Signed was launched and the acceptance side know, We can make $s' = ms$,can use (s', y) substitute (s, r) As news m signatures, Thus, the above equation can be signed into as follows : $k = s + mrx$

Signed in order to use this equation to construct a signature program, the steps are as follows : Selecting a security elliptic curve, ellipse curve parameters and Para a part of the same.

(1) Signed Alice on E choice private Key x, g for E Bp, calculation $y = xg$,

y as a public key issued, Alice explicit calculation of m $e = h(m)$;

(2) Alice choice integer random k (k secrets),(s,r,e)will be sent to the verifier Bob;

These are our signatures derived program, which avoids the inverse process, solve the ECDSA algorithm inadequate. The program than ECDSA simple algorithm, the experimental results show that the algorithm than ElGamal, Schnorr program about 28% faster.

附录 4 程序

```
#include "ibe.h"
using namespace std;
#define PROJECTIVE
#define ADD 1
#define SUB 2

void g(ECn& A,ECn& B,ZZn2& Qx,ZZn& Qy,ZZn2& num,ZZn2& denom,int as,BOOL first)
{
    ZZn    lam,mQy;
    ZZn2 d,u;
    big ptr;
    ECn P=A;

    if (as==ADD)
    {
        ptr=A.add(B);

        if (A.iszero())     { u=vertical(P,Qx); d=1; }
        else
        {
            if (ptr==NULL) u=1;
            else
            {
                lam=ptr;
                u=line(P,A,lam,Qx,Qy);
            }

            d=vertical(A,Qx);
```

```
            }
        }
        else
        {
            u=vertical(A,Qx);
            ptr=A.sub(B);

            if (A.iszero())     { d=u;    }
            else
            {
                mQy=-Qy;
                if (ptr==NULL) d=1;
                else
                {
                    lam=ptr;
                    d=line(P,A,lam,Qx,mQy);
                }
            }
        }

        if (first) {num= u; denom= d; }
        else            {num*=u; denom*=d; }
}
Big H1(char *string)
{
        Big h,p;
        char s[HASH_LEN];
        int i,j;
        sha256 sh;
        shs256_init(&sh);

        for (i=0;;i++)
```

```
        {
            if (string[i]==0) break;
            shs256_process(&sh,string[i]);
        }
        shs256_hash(&sh,s);
        p=get_modulus();
        h=1; j=0; i=1;
        forever
        {
            h*=256;
            if (j==HASH_LEN)    {h+=i++; j=0;}
            else                h+=s[j++];
            if (h>=p) break;
        }
        h%=p;
        return h;
}

    ECn map_to_point(char *ID)
{
        ECn Q;
        Big x0,y0=H1(ID);

        x0=getx(y0);

        Q.set(x0,y0);

        return Q;
}

BOOL ibe_enc(long seed,char *id,char* ifname)
{
```

```
        miracl *mip=mirsys(18,0);
        ifstream common("common.ibe");
        ifstream plaintext;
        ofstream key_file,ciphertext;
        ECn U,P,Ppub,Qid,infinity;
        ZZn2 gid,cube,w;
        char
key[HASH_LEN],pad[HASH_LEN],rho[HASH_LEN],V[HASH_LEN],W[HA
SH_LEN];
        char ofname[100],ch,iv[16];
        Big p,q,r,x,y,cof;
        int i,bits;
        aes a;
        irand(seed);
        common >> bits;
        mip->IOBASE=16;
        common >> p >> q;
        cof=(p+1)/q;
        common >> x >> y;
        EBrick B(x,y,(Big)0,(Big)1,p,8,QBITS);

    #ifdef AFFINE
        ecurve(0,1,p,MR_AFFINE);
    #endif
    #ifdef PROJECTIVE
        ecurve(0,1,p,MR_PROJECTIVE);
    #endif

        P.set(x,y);

        common >> x >> y;
        Ppub.set(x,y);
```

```
common >> x >> y;
cube.set(x,y);

mip->IOBASE=10;
Qid=map_to_point(id);

if (!ecap(Ppub,Qid,q,cube,gid))
{
	cout << "Bad Parameters" << endl;
	exit(0);
}
for (i=0;i<HASH_LEN;i++) key[i]=(char)brand();
for (i=0;i<16;i++) iv[i]=i; // set CFB IV

aes_init(&a,MR_CFB1,16,key,iv);
strcpy(ofname,ifname);
strip(ofname);
strcat(ofname,".ibe");
plaintext.open(ifname,ios::in);
if (!plaintext)
{
	cout << "Unable to open file " << ifname << "\n";
	return 0;
}
cout << "encoding message\n";
ciphertext.open(ofname,ios::binary|ios::out);
forever
{
	plaintext.get(ch);
	if (plaintext.eof()) break;
	aes_encrypt(&a,&ch);
```

```
            ciphertext << ch;
        }
        aes_end(&a);
    for (i=0;i<HASH_LEN;i++) rho[i]=(char)brand();
        r=H3(rho,key);
        B.mul(r,x,y);
        U.set(x,y);
        w=pow(gid,r);
        H2(w,pad);
        for (i=0;i<HASH_LEN;i++)
        {
            V[i]=rho[i]^pad[i];
            pad[i]=0;
        }
        H4(rho,rho);
        for (i=0;i<HASH_LEN;i++)
        {
            W[i]=key[i]^rho[i];
            rho[i]=0;
        }
        strip(ofname);
        strcat(ofname,".key");
        mip->IOBASE=16;
        key_file.open(ofname);
        U.get(x,y);
        key_file << y << endl;
        x=from_binary(HASH_LEN,V);
        key_file << x << endl;
        x=from_binary(HASH_LEN,W);
        key_file << x << endl;
        return 0;
    }
```