肖如良 著

超椭圆曲线密码体制的理论与实现

经济管理出版社
ECONOMY & MANAGEMENT PUBLISHING HOUSE

肖如良 著

超椭圆曲线密码体制的理论与实现

经济管理出版社
ECONOMY & MANAGEMENT PUBLISHING HOUSE

图书在版编目(CIP)数据

超椭圆曲线密码体制的理论与实现/肖如良著.
—北京:经济管理出版社,2006
ISBN 7-80207-623-4

Ⅰ.超… Ⅱ.肖… Ⅲ.密码—理论 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字(2006)第 075227 号

出版发行:经济管理出版社
北京市海淀区北蜂窝 8 号中雅大厦 11 层
电话:(010)51915602 邮编:100038
印刷:北京国马印刷厂 经销:新华书店
选题策划:王光艳 责任编辑:王光艳
技术编辑:蒋 方 责任校对:张晓艳
850mm×1168mm/32 6 印张 136 千字
2006 年 7 月第 1 版 2006 年 7 月第 1 次印刷
印数:1-3000 册 定价:20.00 元
书号:ISBN7-80207-623-4/F·539

总　序

近几年，为适应我国高等教育迅速发展的新形势，湖南财专的学校领导和广大职工针对高等专科学校科研工作如何定位、怎样处理科研与教学等工作的关系问题，进行了广泛讨论和深度思考，形成了如下共识：

其一，教学与科研的关系。高等专科学校和一般普通本科学校都应以教学为主，以应用型人才培养为主要目标，但这并不等于说教学应用型学校不需要科研。教学应用型学校同样要开展科学研究，只是在科研路径选择上可以适当突出教学的分量，即科研工作面向教育教学第一线，为教育教学实践和教育教学改革提供理论支撑。科研是基础，人才培养的学术水平源自科研，社会服务的应用成果来自科研。没有科研的支撑，人才培养和社会服务就成为无源之水，无本之木，学校的教育质量和学术地位就无从谈起。因此，科研在学校整体工作中具有不可替代的地位。

其二，学科与专业的关系。学科建设是高校建设的核心和提高教学、科研水平的重要基础，是一所院校综合实力的标志，它直接体现学校的学术水平、科研方向、办学特色及服务能力和社会地位。专业建设是教学建设的重要组成部分，是学校教学基本建设中最基础的工作之一，是教学内容和教学体系改革的主要内容。因此，作为一所全力向本科院校冲刺的学校，必须正确处理专业建设与学科建设的关系，尽快实现由单一专业建设向学科建设的提升，并通过学科带动专业的建设与发展。

其三，地方性与行业性的关系。我校是一所由省厅业务部门主管的以财经类见长的行业性学校，又是一所省管的地方院校。在高等教育大发展和全国高校管理体制改革不断深化的大背景下，许多高校包括一些行业性高校都纷纷亮出服务地方的底牌，制定出面向地方办学，立足地方经济与社会发展，为地方经济与社会发展培养应用型人才的发展战略，行业与地方的界线日渐模糊。我校也对这一当代高等教育发展的大趋势做出了积极回应，在科研方向上，注重科研内容的地域性，面向地方经济建设主战场，为区域经济建设和社会发展提供人才、智力支持。

基于上述办学理念，我们为加快学校发展步伐，提高科研地位，加强学科和专业建设，近年来先后启动了“教授培养工程”、“研究所建设工程”和“系列专著出版工程”等多项重要措施，为学校实现近期的“升本”目标和长远的可持续发展奠定了坚实的基础。这次首批资助出版的12本学术专著，内容涉及财政、金融、税收、会计、国际贸易、市场营销、法学、人口与社会保障、教育、计算机技术等方面，多角度、多层次地展示了财专学人的学术视野和研究旨趣。作者都是财专的业务骨干，长期工作在教学和科研第一线，既有丰富的教学经验，又有一定的学术积累和较好的研究基础。这些著作，有的是作者在博士论文的基础上加工而成，有的是作者的国家级课题和省部级课题的结题成果，有的是对近年来系列论文的进一步提升。这批学术专著的问世，标志着我校的办学理念开始转变，学科建设已经起步，科研特色进一步彰显。

本次组织出版的专著，不仅承继了财专既有的科研传统，而且将其发扬光大，在研究特色上更加鲜明。其中，有关农村金融制度和农产品出口贸易的研究，与“三农”问题最为突出的湖南省情关联度极高，“地方性”应该是作者从事研究的立论基础，试图破解此类难题实则蕴涵着作者对湖南地方经济、社会良性发展的某种期

待。对全球化进程中的人民币汇率体制与金融安全的研究，以及会计准则与会计制度、教育财政投入、企业并购规制、社会保障与人口发展、市场营销创新等方面的研究，既体现了财经类院校的行业性研究旨趣，也昭示出财专学人践行“三个代表”重要思想、“情为民所系，利为民所谋”的品格和经世致用的治学之道。

当然，这批专著在选题、内容等方面也存在着一些不足。对此，我们恳请学者贤达关注、批评、指正。

是为序。

伍中信

2006 年 5 月于湖南财经高等专科学校

目 录

第一章 绪 论

1.1 计算机网络和信息系统的安全

在一般的计算机系统中，人们首先注意到的问题是可不可以执行，其执行的效率如何，而信息安全是计算机应用中最后一个才考虑的问题。比如微软公司的 Windows 操作系统也是先求功能可以运行，再考虑效率，是在 NT 出现以后才有了其安全方面的策略。自从 www 的兴起，因特网越来越广泛地流行，人们通过网络获得想要的信息，网络应用的安全问题才越来越受到重视。

在计算机网络环境上所运行的信息系统的安全可以分为两个大的方面：其一是系统环境本身的不稳定性。网络设备、设施的本身以及软件系统长期工作所引起的“疲劳”，给系统造成了安全隐患；再又，一个组织或是一个公司，在工作上的各种作业规范都应包含在其中，如机密文件让没有这个权限的人看到，或是机密文件被带出了公司，在本书中，不考虑这方面的问题。其二是计算机网络及信息系统的安全策略存在缺陷。

计算机网络已经发展成为一门跨多学科的综合性学科，它包括通信技术、网络技术、计算机软件与硬件设计技术、密码学、网络安全与计算机安全等。

网络和信息系统是现代社会最重要的信息基础设施，已经渗透到社会的各个领域。保障网络和信息系统的安全关系到国家的

存亡、经济的发展、社会的稳定、优秀民族文化的继承和发扬。整个社会对 Internet、Intranet、Extranet 的使用，比以往具有更大的依赖性。随着企业间信息交互的不断增加，任何一种网络应用和增值服务的使用程度将取决于所使用网络的信息安全有无保障，网络安全已成为现代计算机网络应用的最大障碍，也是急需解决的难题之一。由于网络上经常要传输重要而敏感的数据，许多大的公司及一些著名的有关组织都相继推出了一些关于网络安全方面的协议和标准。网络安全可以在网络协议的各个层次上实现，如 IETF 已在数据链路层、网络层、传输层和应用层等层次，定义了安全协议或草案。

网络安全是目前研究的重点之一，因为它是网络电子商务、政府电子公务、军事等在 Internet 上应用的前提。过去，军队、政府、金融、证券都有独立的网络，而现在，全世界的计算机都能通过 Internet 连到一起，信息安全的内涵也就发生了根本的变化。信息系统的安全关系到国家的稳定和发展，计算机网络安全是我们国家经济建设的重要保证。它不仅从一般性的防卫变成了一种非常普通的防范，而且还从一种专门的领域变成了无处不在。所以，在这样一个信息化与网络化的时代，应该加强网络信息系统安全的研究。

随着 Internet 的日益普及，社会经济的快速发展依赖于一个错综复杂的信息网络，它改变着人们的生活方式、生产方式与管理方式，并对推进国家的现代化和社会文明的发展发挥着日益重大的作用。然而，任何事物都有两面性，网络在为我们提供快捷与便利的同时，由于其本身的开放性与匿名性，不可避免地存在着信息安全的隐患，安全性已经成为今后网络发展的瓶颈。为解决这个问题，人们不断探索如何去构建全面、完整的安全解决方案，经过多年的研究与探索，初步形成了一整套解决方案，即目前被广泛使用的 PKI 技术。

1.2 PKI 基础设施

Public Key Infrastructure，译为公共密钥基础，亦称为公钥基础设施，可缩写为 PKI。是利用公钥理论和技术建立的提供信息安全服务的基础设施，借助密码学来解决网络安全问题的一种方法。PKI 安全平台提供智能化的信任与有效授权服务。

一个安全的系统至少应该包含以下三点：①端系统安全，是指网络环境下各种端系统的安全，一般属于操作系统的范畴。②网络通信安全，包括保护通信子网内部的网络设备，传输链路以及通信软件，逻辑信道和基本网络服务等。③应用系统安全。

1.2.1 PKI 提供的基本安全服务

公钥基础设施 PKI 是解决信任和加密问题的基本解决方案。它遵循标准的利用公钥加密技术，为电子商务、电子政务的开展提供一整套安全的基础设施，使基础设施达到全面的安全性所采取的重要机制之一，就是保证大范围的组织实体和设施采用统一的方式使用、理解和处理密钥。基于 Internet 的保密性应用要求有一个真正可靠、稳定、高性能、安全、互操作性强、完全支持交叉认证的 PKI 系统。PKI 的本质就是实现大规模网络中的公钥分发问题，建立大规模网络中的信任基础。概括地说，PKI 是创建、处理、存储、分发和撤销基于公钥加密的公钥证书所需要的一套硬件、软件、策略和过程的集合。PKI 为开放的 Internet(或 Intranet)环境提供了四个基本的安全服务：

(1)认证。确认发送者和接收者的真实身份。向一个实体确认另一个实体是他自己。目前网络中常用的是基于口令的认证方式，口令在网络传输的过程中很容易被窃取和破译，不适用于安全性较高的场合，而且其认证是单向的，浏览器不能对服务器进行认

证。PKI体系采用数字证书管理公钥，通过第三方的可信机构CA(Certificate Authority)，把用户的公钥和其他标识信息(名称、E-mail、身份证号等)捆绑在一起，在Internet上验证用户的身份。通过使用CA颁发的数字证书，结合对应的私钥，完成对实体的单向或双向身份认证，克服了传统的口令认证的弊端，大大提高了身份认证的安全水平。在系统中，用户管理和登录需要使用数字证书，以确认用户，保证某一项网络行为是持有证书的用户所施，保证用户的真实性和合法性，同时防止用户抵赖行为。

(2)数据完整性。确保数据在传输过程中不能被有意或无意地修改。向一个实体确保没有被有意或无意地修改，除了接收者之外，无人能解读数据的关键部分。敏感、机密信息和数据在网络传输时，有可能在传输过程中被非法用户截取或恶意篡改，安全电子政务系统使用PKI技术来提供数据完整性服务，保证交互信息的数据完整性。典型的方案是以SSL协议为基础，系统由客户端和服务器端两部分组成。客户端的实现形式可以是Active X或Applet控件，或者是专用硬件或软件；服务器端的实现形式可以是服务程序，或者是专用硬件或软件。客户端和服务器端分别与浏览器和Web服务器协同工作，它们之间通过互相验证数字证书建立安全数据通道，通过PKI体系下的高强度加密技术，对敏感信息进行加密和解密，并进行完整性检验。

(3)不可否认性。通过验证，确保发送方不能否认其发送消息。有确认对方的身份，防抵赖的作用。为客户端和服务器端安全软件增加数字签名功能，可提供不可否认服务。比如在电子政务中，要真正实行无纸化办公，很重要的一点是实现电子公文的流转，而在这之中，数字签名问题变得很重要了。被签名的文件利用用户自己的私钥对原始数据的哈希摘要进行加密所得的数据。信息接收者使用信息发送者的公钥对附在原始信息后的数字签名进行解密后获得哈希摘要，

并通过与自己收到的原始数据产生的哈希摘要对照，便可确信原始信息是否被篡改。这样就保证了数据的不可否认性。

(4)机密性，确保数据不能被非授权的第三方访问。

另外，PKI 还提供了其他的安全服务，主要包括：①授权，确保发送者和接收者被授予访问数据、系统或应用程序的权力。②可用性，确保合法用户能正确访问信息和资源。

从广义上讲，所有提供公钥加密和电子签名服务的系统，都可称为 PKI 系统。PKI 的主要目的是通过自动管理密钥和证书，可以为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便地使用加密和电子签名技术，从而在技术上解决网络上的信任问题。

PKI 由认证机构、数字证书与证书库、密钥备份及恢复系统、证书撤销及处理系统以及客户端证书处理系统(或称为 PKI 应用接口系统)五项基本成分组成。PKI 框架一般描述为两个层次：第一层是安全技术，第二层是信息与网络服务。在 PKI 架构中，建立信赖关系的方式是由两个证书机构互相或是单方面发送证书所建立起来的。借助这种认证过程，可以产生一条信赖路径。当使用者收到一张证书，需要验证这张证书时，就可以依循一连串的信赖路径找到该证书的信赖起点(Trust Anchor)。借助建立信赖模式(Trust Model)方式，将证书使用者划分在不同的架构下，用来减少信赖关系的复杂度，同时也提高了被信赖的程度。PKI 的架构可细分成三大部分：简单型 PKI、企业型 PKI、复合型 PKI。

1.2.2 构建一个 PKI 系统主要包括的内容

基于前面所述的 PKI 基础设施，构建一个 PKI 系统主要包括以下一些内容：

(1)认证/审核机构。认证机构(Certificate Authority，简称 CA)是证书的签发机构，它是 PKI 的核心，是 PKI 中权威的、公正的、可信任的第三方。RA(Registry Authority，审核机构)是证书及其相

关业务的受理及审核机构，负责受理和审核多种形式的 PKI 服务申请，将合法的申请上传给 CA，此外，它还为进行离线申请的用户生成签名私钥并确保其安全性。主要提供认证和注册服务。

(2)证书库。证书库是证书的集中存放地，用以向公众提供查询和访问，是网上的一种公共信息库，用户可以从此处获得其他用户的证书和公钥。构造证书库的最佳方法是采用支持 LDAP (Lightweight Directory Acess Protocol，轻量级目录访问协议)的目录系统，用户或相关的应用通过 LDAP 来访问证书库。系统必须确保证书库的完整性，防止伪造、篡改证书。

(3)证书撤销处理系统。在实际使用时，由于有许多原因或者说不得以的情况而要对证书进行诸如作废、吊销、暂停、终止等有关的操作，通过证书相应的有关操作来进行实现。

(4)密钥备份及恢复系统。该系统能对用户的解密密钥进行备份，当用户的这一私钥发生丢失等情况时，进行系统恢复。当然，用户用以进行签名的签名密钥是不允许进行备份和恢复的。

(5)PKI 应用接口系统。PKI 应用的前提是在高度共享的计算机网络环境下，安全电子商务、安全通信、安全支付和保护人们秘密的关键手段，就是通过 PKI 应用接口系统来实现的。应用接口系统客户端软件安装在用户的机器上，一方面，在申请双证书时帮助用户生成签名密钥对；另一方面，它负责本地证书的管理，帮助用户对证书进行导入和导出，以便完成证书在应用系统中的认证作用；它以客户端的身份与 RA 通信，进行证书的申请与下载。该软件也可以插件的形式与浏览器集成在一起，帮助完成在线应用。

1.3 基于 PKI 的安全解决方案

基于上面的叙述，一个完整的 PKI 系统可由图 1－1 表示，图

中的虚线一方面表示了用户浏览器与 Web 服务器或目录服务器之间的安全通信，其通信协议可以采用 SSL(Secure Socket Layer，安全套接字层)的形式；另一方面，虚线也表示 PKI 系统内部各个子系统之间利用内部安全通信机制进行的信息交互。在整个 PKI 系统运行之前，加密机应先获得自签名证书，然后由它给 CA 和 RA 中的其他设备和人员分别签发设备证书或员工证书，并把这些证书发布到目录服务器上。这样，当分别安装在两个设备上的相关子系统需要通信的时候，为了保证安全传输，发送方需要对传输数据进行编码、加密(用接收方的公钥)和签名(用自己的私钥)，而接收方则需要解密，验证签名并解码。

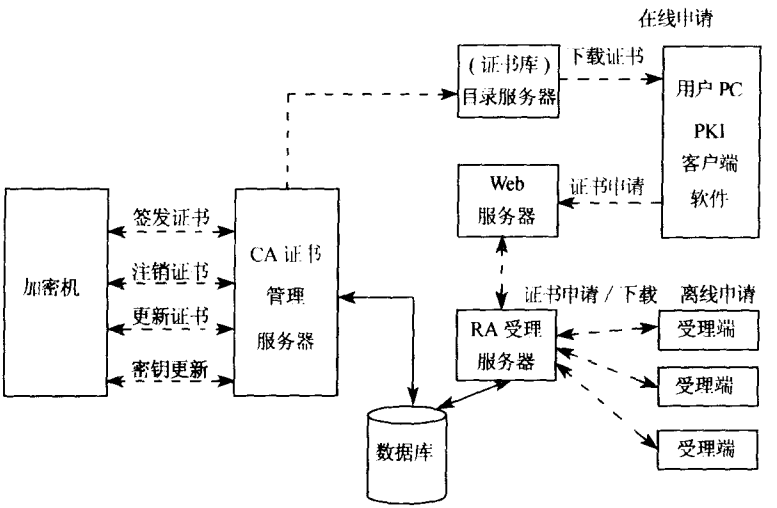

图 1—1 PKI 系统总体结构

按照组件化的思想，可以把 PKI 系统分成三个层次，其中每个层次都由一个或一个以上的子系统组成：

(1)PKI 业务管理层。包括 CA 端管理子系统，RA 端管理子系统，客户端软件。

(2)安全接口层。调用密码算法实现层的接口函数实现密钥生成、密钥更新、DER/BER 编码、数字签名、证书生成、更新、注销等功能，并通过安全内核的控制和调度，将密码运算与本层提供给上层的调用接口隔离开来。

(3)密码算法实现层。实现了包括 ECC、RSA、DES、SHA 等目前流行的密码算法。使用这种分层设计的优势在于当底层密码算法需要变动或升级时，只需在安全接口中做相关的改动，而 PKI 系统的上层应用不需任何改动或只需较少改动。

基于 PKI 技术来解决网络上的安全问题，可以采用安全接口技术的方式来实现(见图 1－2)。安全接口技术可以为现有的 C/S 应用或 B/S 应用提供有效的、简便的安全功能。

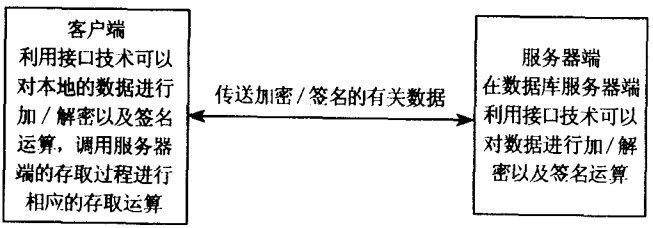

图 1－2 在 C/S 结构中以安全接口的方式应用 PKI

在 B/S 应用中，系统结构如图 1－3 所示。