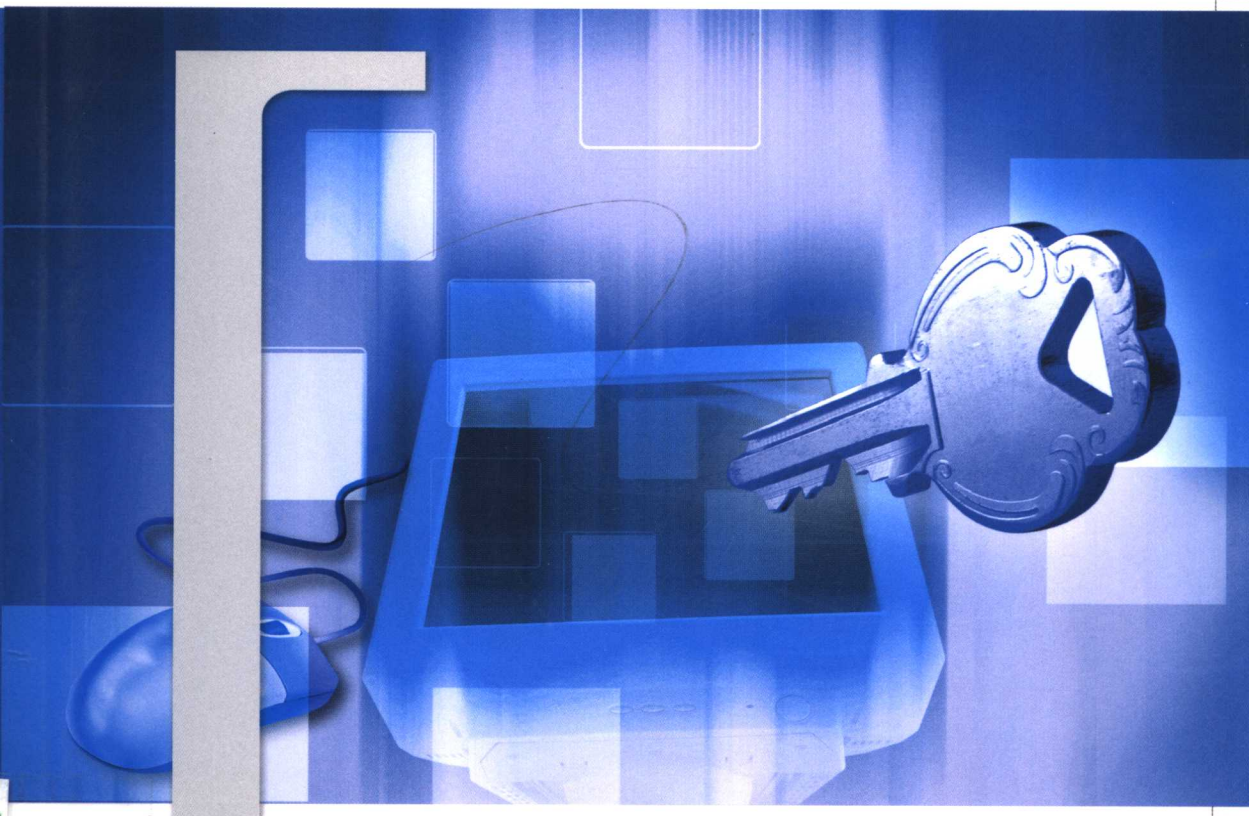
赵泽茂 著

数字签名理论



科学出版社
www.sciencep.com

数字签名理论

赵泽茂 著

科学出版社

内 容 简 介

数字签名技术是实现网络通信身份认证的核心技术，也是实现信息机密性、完整性和不可否认性的关键技术，广泛应用于网络通信、电子商务和电子政务等领域。本书全面讲解了数字签名理论的基本知识，介绍了国内外数字签名理论与技术的若干最新理论和应用成果，其中许多成果是作者多年来教学和研究的结晶。全书分 9 章，第 1、2 章介绍了数字签名的原理、功能、数学基础知识、分类、安全性和设计方法；第 3～5 章分别详细介绍了基于离散对数、椭圆曲线和身份的数字签名方案及相关的成果；第 6～9 章分别介绍了代理签名方案、盲签名方案、群签名方案、多重签名方案及近期最新理论研究成果。

本书可作为密码学、信息安全、应用数学、计算机科学、通信、信息科学及信号处理等专业的高年级本科生和研究生的教学参考书，也可作为信息安全、网络安全、密码学等领域的工程技术和研究人员的参考资料。

图书在版编目(CIP)数据

数字签名理论/赵泽茂著. —北京：科学出版社，2007

ISBN 978-7-03-018322-4

Ⅰ. 数 Ⅱ. 赵… Ⅲ. 密码-理论 Ⅳ. TN918.1

中国版本图书馆 CIP 数据核字（2007）第 002375 号

责任编辑：张 敏 潘继敏/责任校对：赵桂芬

责任印制：安春生/封面设计：嘉华永盛

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

新蕾印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2007 年 1 月第 一 版 开本：B5（720×1000）

2007 年 1 月第一次印刷 印张：15 1/4

印数：1—3 000 字数：283 000

定价：38.00 元

（如有印装质量问题，我社负责调换〈环伟〉）

前　言

近几年来，数字签名理论和技术得到了长足的发展，内容十分丰富，应用范围越来越广。在理论研究方面，越来越多地采用数学形式化的方法进行描述和论证；在应用方面，数字签名已发展成为人们在电子商务交易过程中必须办理的“手续”，成为保护消费者权益的护身符。

学习数字签名理论和技术，如果一开始就按照数学形式化的方法，局限于数学精确的计算、严格的定义、严密的逻辑证明，并视为学术“高端”的话，往往会令初学者望而却步。事实上，数字签名就像手写签名一样，来源于实际生活，并因计算机网络的发展和普及而催生成长，在电子邮件收发、在线电子交易、在线电子服务等方面有着广泛的应用，利用数字签名，可以确保交易双方的真实性和安全性，降低商业风险。在法庭上，书面签名、数字签名和电子签名具有同等法律效力。因此，数字签名理论，一方面要不断地发展和完善；另一方面，又不能脱离现实需求。在信息安全诸多应用领域，数字签名俨然不是一种纯理论意义上的知识，而是一种无处不在的技术，拥有着成千上万的用户，并且正被越来越多的用户接纳和使用，成为信息安全标志的名片。在众多的信息安全企业中，绝大多数企业都拥有数字签名技术的产品或作为产品的一部分，具有重要的商业价值。

本书在阐述数字签名内容时，主要采用描述性的方式向读者介绍数字签名理论研究的最新成果，其中虽涉及部分较深的数学理论基础，但力求避开特别精深的关于安全的“数学证明”，力图使本书成为一本在信息安全领域对读者提供帮助、缩短熟悉最新理论时间的入门参考书。

本书是关于数字签名理论的最新专业著作，是作者近几年来从事包括数字签名理论在内的信息安全技术课程的教学和科研成果的总结，可以作为信息安全、通信工程、信息工程、计算机专业高年级本科生和研究生的教材和参考读物，也可供从事数字签名理论研究和技术开发的人员参考使用。

在本书付梓之际，特别感谢我的导师——南京理工大学博士生导师刘凤玉教授，书中包含的部分成果是在作者攻读博士学位期间，在她的指导、关心和科研课题支持下取得的；还要感谢杭州电子科技大学科技处和通信工程学院的领导给

予本书出版的全力支持。

由于数字签名理论发展很快，研究文献层出不穷，疏漏和不当之处在所难免，敬请读者指正。

目　录

第 1 章　数字签名概述

1.1　研究背景和意义

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。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。普遍的观点认为，现代密码技术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，这些应用已完全渗透到我们的日常生活之中，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与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都能以最快的速度、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。

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，而且严重威胁到国家的政治、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。因此，不强化网络化的信息安全保障，不解决信息安全问题，信息化将不可能得到持续、健康的发展，与之相关的经济安全、政治安全、国家

安全将不可能得到可靠的保障。

什么是信息安全呢？从安全需求角度来讲，信息安全应包括五个基本要素：机密性(confidentiality)、完整性(integrity)、可用性(availability)、可控性(controllability)与不可抵赖性(non-repudiation)等，其主要特征如下。

(1) 机密性　机密性是指网络信息只为授权用户使用，不能泄露给非授权的用户、实体或进程，不能被非法利用，采用的技术手段是加密传输、数据的保密存储等。

(2) 完整性　完整性就是指网络信息未经授权不能进行改变的特性，即信息在传输或存储过程中，不能被偶然或蓄意地删除、修改、伪造、重排、插入等破坏和丢失的特性。简言之，完整性要求网络信息保持信息的原样不变。

(3) 可用性　可用性就是保证信息及服务可被授权用户使用的特性。

(4) 可控性　可控性是指网络信息的信息流流向、信息传播和信息内容等具有控制能力的特性。比如，系统资源的访问是可以控制的，网络用户的身份可以进行身份验证，用户活动记录是可以审计的。

(5) 不可抵赖性　也称作不可否认性，是指网络用户不能否认或抵赖自己的操作和作出的承诺，包括信息发送方不能否认已发送过的信息，信息接收方不能否认已接收到的信息。

概括地说，信息安全就是指通过计算机技术、网络技术、密码技术和网络安全技术等保护网络信息在传输、交换和存储过程中的机密性、完整性、可用性、可控性和不可抵赖性等。

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、法律和管理技术等的综合性学科。其中，密码理论占有重要的位置，是信息安全的核心和基石，甚至可以说，离开了密码学，信息安全就无从谈起，可见密码学在信息安全领域的重要地位和作用。

密码学(cryptology)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1世纪，古罗马皇帝恺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和Hellmann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，在密码学的发展历史上具有里程碑式的重要意义，具有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展到数字签名、消息认证、身份识别、防否认等新的课题。同时密码学不再局限于军事、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，使得一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。从某种角度来讲，正是因为存在的种种信息安全问题，才催生了信息安全技术的发展。

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，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。在当今高度信息化的社会里，信息安全关系到国家的全局和长远利益，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。信息的接收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。归纳起来,通信双方可能发生下列情况:

(1) 否认　发送方不承认自己发送过某一报文;

(2) 伪造　接收方自己伪造一份报文,并声称它来自发送方;

(3) 冒充　网络上的某个用户冒充另一个用户接收或发送报文;

(4) 篡改　接收方对收到的信息进行篡改。

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。

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。

正是由于数字签名具有的独特功能和实际用途,在一些特殊行业,比如金融、商业、军事等有着广泛的应用,尤其在数据完整性检验、身份鉴别、身份证明、防否认等方面,功能独特,满足这些要求的最好的办法就是使用数字签名技术。由此可见,数字签名技术在网络通信中的重要作用和特殊位置。

1.2 数字签名原理

在公钥密码学中,密钥是由公开密钥和私有密钥组成的密钥对。数字签名就是用私有密钥进行加密,接收方用公开密钥进行解密,由于从公开密钥不能推算出

私有密钥，所以公开密钥不会损害私有密钥的安全；公开密钥无须保密，可以公开传播，而私有密钥必须保密。因此，当某人用其私有密钥加密消息，能够用他的公开密钥正确解密，就可肯定该消息是某人签字的，这就是数字签名的基本原理。因为其他人的公开密钥不可能正确解密该加密过的消息，其他人也不可能拥有该人的私有密钥而制造出该加密过的消息。

实现数字签名的具体算法很多，任何公钥密码算法都可以用于实现数字签名。为了说明其工作原理，先介绍一个概念。

哈希函数又称为杂凑函数、散列函数、消息摘要或数据摘要等，它把任意长度的消息变换为一个固定长度的散列值。当消息哪怕只有一个比特位产生变化时，数据摘要“显著”地发生变化，不论消息的长度如何，其目的是把大的消息压缩了，变短了，因此，称数据摘要为“数据指纹”。当消息在插入、篡改、重排之后，其数据指纹也要发生变化，显然可以提供完整性服务。一般说来，数据的完整性检验方法如图 1.1 所示。

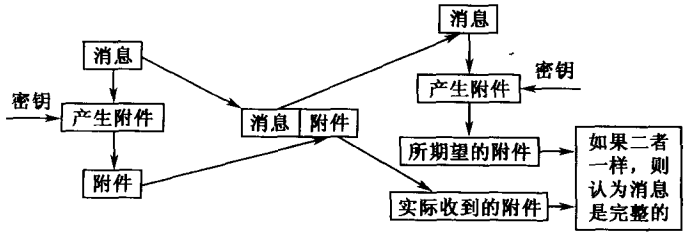


图 1.1　消息完整性检验

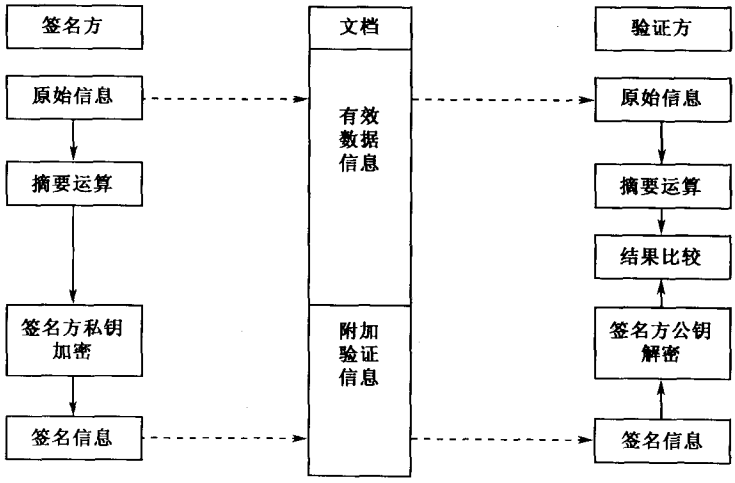


图 1.2　数字签名过程

通俗地说，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。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信息的真实性的一个证明，发送者不能抵赖。具有消息摘要的数字签名工作过程如图 1.2 所示，不带消息摘要的数字签名类似。

1.3 数字签名的功能

归纳起来，数字签名技术可以解决伪造、篡改、冒充、抵赖等问题，其功能表现在以下几方面。

(1) 机密性　数字签名中报文不要求加密，但在网络传输中，可以将报文信息用接收方的公钥进行加密，以保证信息的机密性。

(2) 完整性　数字签名与原始文件或其摘要一起发送给接收者，一旦信息被篡改，接收者可通过计算摘要和验证签名来判断该文件无效，从而保证了数据的完整性。

(3) 身份认证　在数字签名中，用户的公钥是其身份的标志，当使用私钥签名时，如果接收方或验证方用其公钥进行验证并获通过，那么可以肯定签名人就是拥有私钥的那个人，因为私钥是签名人唯一知道的秘密。身份认证包括通信实体认证和数据源认证。

(4) 防伪造　除签名人外，任何其他人不可能伪造消息的签名，因为签名密钥即私钥只有签名者自己知道，其他人不可能构造出正确的签名数据。

(5) 防抵赖　数字签名既可作为身份认证的依据，也可作为签名者签名操作的证据，防止抵赖。要防止接收者的抵赖，可以在数字签名系统中要求接收者返回一个自己签名的表示收到的报文，给发送者或受信任第三方。如果接收者不返回任何信息，此次通信可终止或重新开始，签名方也没有任何损失，由此双方均不可抵赖。

(6) 防重放攻击　如在电子商务中，公司 A 向公司 B 发送了一份商品订单，如果有攻击者中途截获订单并发送多份给公司 B，这样会导致公司 B 以为公司 A 订购了多批商品。在数字签名中，通常采用了对签名报文加盖时间戳或添加处理流水号等技术，可以防止这种重放攻击。

1.4 数字签名技术的应用

数字签名技术最早应用于用户登录过程，对于大多数用户来讲，“用户名＋口