数字签名理论及应用

杜红珍 著

科学出版社

数字签名理论及应用

杜红珍 著

科学出版社
北京

内 容 简 介

本书全面讲解数字签名理论的基本知识，介绍国内外数字签名理论与技术的若干最新理论和应用成果. 全书共 11 章，第 1 章介绍数字签名的原理、功能、国内外研究现状及应用；第 2 章介绍数字签名的基础知识;第 3 章研究基于身份的数字签名体制；第 4～6 章研究基于身份的聚合签名、指定验证者签名和环签密等特殊签名体制;第 7 章提出无密钥托管的基于身份的数字签名体制；第 8 章介绍无证书数字签名体制；第 9～11 章分别研究无证书代理签名、指定验证者签名、聚合签名、多重签名和代理多重签名等.

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

数字签名理论及应用/杜红珍著. —北京：科学出版社, 2015. 9
ISBN 978-7-03-045735-6

Ⅰ. ①数… Ⅱ. ①杜… Ⅲ. ①电子计算机-密码术 Ⅳ. ①TP 309.7

中国版本图书馆 CIP 数据核字 (2015) 第 221823 号

责任编辑：胡海霞 / 责任校对：张凤琴
责任印制：徐晓晨 / 封面设计：迷底书装

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

北京京华虎彩印刷有限公司 印刷
科学出版社发行 各地新华书店经销
*
2015 年 9 月第 一 版 开本：720×1000 B5
2015 年 9 月第一次印刷 印张：15 1/8
字数：290 000

定价：59.00 元

(如有印装质量问题，我社负责调换)

前　言

随着计算机网络技术的飞速发展, 信息安全的重要性与日俱增. 数字签名技术可以在电子数据传输中提供认证性、完整性和不可否认性等安全服务, 是信息安全的核心技术之一, 也是安全电子商务和安全电子政务的关键技术之一. 因此, 数字签名技术的研究有着重要的理论意义和实际应用价值.

著名密码学家曹珍富提出 "密码学因应用需求而产生, 因应用需求而发展". 经过三十多年的发展, 数字签名技术已取得了丰硕的研究成果. 但随着对数字签名研究的不断深入及以物联网、云计算、命名数据网、大数据等为代表的新的网络形态及网络服务的出现, 普通的数字签名已经不能完全满足当前网络环境的需求, 所以除了研究普通数字签名以外, 还需研究具有特殊性质的多方参与的数字签名. 本书研究普通数字签名理论, 以及与新型网络形态发展紧密相关的带有特殊性质的数字签名, 如聚合签名、指定验证者签名、环签密、代理签名、多重签名和代理多重签名等.

基于身份的公钥密码体制是传统证书公钥密码体制的一个较好的替代. 本书围绕基于身份的数字签名方案的设计、安全性证明, 以及如何解决该体制存在的密钥托管问题而展开, 研究内容主要包括设计和安全性分析基于身份的短签名、基于身份的聚合签名、基于身份的指定验证者签名、基于身份的环签密、无密钥托管的基于身份的签名等.

在基于身份的公钥密码学中, 密钥托管会泄露用户的隐私, 导致基于身份的密码算法、协议等只能在一个封闭的内部安全环境中使用. 研究如何消除基于身份的公钥密码体制中的密钥托管问题成为热点. 无证书公钥密码学应运而生, 该体制汲取了基于身份的公钥密码体制和传统证书密码体制的优点, 同时无密钥托管和证书管理问题, 所以相比较而言是一种性能更好的公钥密码体制. 本书在无证书公钥密码体制下研究了普通数字签名和上述特殊签名等, 对其安全性、设计、证明等进行了详细研究, 将作者多年来的研究成果汇集于此书中, 同时吸取了在数字签名领域国内外学者的最新重要研究成果. 本书的出版将会对信息安全领域的学者、研究生、高年级本科生及该领域的爱好者的课题研究提供较好的参考.

本书得到国家自然科学基金项目 (项目编号: 61402015) 和宝鸡文理学院陕西省重点学科专项经费资助. 本书的出版得到了宝鸡文理学院副校长赵荣侠教授、学科建设与研究生教育管理处处长吴毅教授、数学与信息科学学院院长赵天绪教授

的大力支持, 在此深表感谢! 同时感谢科学出版社胡海霞编辑为此书的出版所付出的辛劳!

由于作者水平有限, 书中不当之处在所难免, 恳请专家和读者不吝赐教.

作　者

2015 年于宝鸡

目　　录

第 1 章　引言 ····· 1
1.1　信息安全与密码学 ····· 1
1.2　数字签名技术国内外研究现状 ····· 13
1.3　本章小结 ····· 17
参考文献 ····· 17
第 2 章　基础知识 ····· 24
2.1　基本数学难题 ····· 24
2.2　双线性对及相关困难问题 ····· 25
2.3　椭圆曲线密码学 ····· 27
2.4　复杂性理论基础 ····· 29
2.5　密码 Hash 函数与随机预言机模型 ····· 32
2.6　数字签名的安全性 ····· 34
2.7　基本的数字签名方案 ····· 38
2.8　短签名方案 ····· 41
2.9　本章小结 ····· 43
参考文献 ····· 43
第 3 章　基于身份的数字签名体制 ····· 45
3.1　公钥密码体制 ····· 45
3.2　基于身份的数字签名 ····· 47
3.3　几个常用的基于身份的数字签名方案 ····· 51
3.4　一个高效的基于身份的短签名方案 ····· 58
3.5　本章小结 ····· 62
参考文献 ····· 63
第 4 章　基于身份的聚合签名体制 ····· 65
4.1　聚合签名的研究意义 ····· 65
4.2　聚合签名国内外研究现状 ····· 66
4.3　基于身份的聚合签名的定义和安全模型 ····· 67
4.4　经典的基于身份的聚合签名方案 ····· 68
4.5　对一个基于身份的聚合签名方案的安全性分析 ····· 71
4.6　基于 ID 的聚合签名方案 ····· 72

4.7 基于 ID 的强代理聚合签名 ····· 76
4.8 一个高效的基于 ID 的强代理聚合签名方案 ····· 78
4.9 本章小结 ····· 85
参考文献 ····· 85
第 5 章 基于身份的指定验证者签名体制 ····· 88
5.1 指定验证者签名的发展现状 ····· 88
5.2 基于身份的指定验证者签名的定义和安全模型 ····· 89
5.3 基于身份的指定验证者签名的典型方案 ····· 92
5.4 基于身份的指定验证者签名方案的安全性分析 ····· 96
5.5 本章小结 ····· 104
参考文献 ····· 104
第 6 章 基于身份的环签密体制 ····· 107
6.1 环签密 ····· 107
6.2 一个高效的基于 ID 的签名方案 ····· 110
6.3 一个高效的基于身份的环签密方案 ····· 112
6.4 本章小结 ····· 116
参考文献 ····· 116
第 7 章 无密钥托管的基于身份的数字签名体制 ····· 118
7.1 解决密钥托管的方法介绍 ····· 118
7.2 T-IBS 的定义及安全模型 ····· 119
7.3 一个高效的 T-IBS 方案 ····· 120
7.4 本章小结 ····· 125
参考文献 ····· 125
第 8 章 无证书数字签名体制 ····· 127
8.1 无证书签名介绍及发展现状 ····· 127
8.2 无证书签名方案的形式化定义和安全模型 ····· 129
8.3 典型的无证书签名方案 ····· 132
8.4 无证书签名方案的密码学分析 ····· 135
8.5 一个高效的可证明安全的无证书短签名方案 ····· 143
8.6 本章小结 ····· 149
参考文献 ····· 149
第 9 章 无证书代理签名和指定验证者签名 ····· 151
9.1 代理签名介绍 ····· 151
9.2 无证书强代理签名的定义和安全模型 ····· 153
9.3 经典的无证书代理签名方案 ····· 156

9.4　高效的无证书强代理签名方案……159
9.5　无证书指定验证者签名方案……163
9.6　一个高效的无证书指定验证者签名方案……166
9.7　无证书指定验证者代理签名……171
9.8　本章小结……175
参考文献……175
第 10 章　无证书聚合签名体制……178
10.1　无证书聚合签名研究现状……178
10.2　无证书聚合签名的定义及安全模型……179
10.3　无证书聚合签名方案的安全性分析……180
10.4　改进的无证书聚合签名方案……191
10.5　无证书广义指定验证者聚合方案……194
10.6　高效的有固定长度的无证书聚合签名方案……198
10.7　本章小结……205
参考文献……205
第 11 章　无证书多重签名和代理多重签名体制……207
11.1　多重签名介绍……207
11.2　无证书多重签名的定义和安全模型……208
11.3　秦–吴的 CLMS 方案及安全性分析……209
11.4　许艳等的 CLMS 方案及正确性分析……213
11.5　改进的无证书有序多重签名方案……215
11.6　无证书代理多重签名……219
11.7　一个安全的无证书代理多重签名方案……223
11.8　本章小结……233
参考文献……233

第1章 引 言

数字签名技术在电子商务、电子政务、军事等领域有着重要的应用. 特别是随着网络的纵深发展和人们生活中各种实际需要的快速增长, 促使数字签名技术飞速发展, 并使各种带有特殊性质的数字签名方案应运而生. 数字签名不仅具有丰富的研究内容, 而且有广泛的应用领域. 本书以数字签名技术为研究对象, 本章主要介绍数字签名技术的研究背景、意义、功能、分类和形式化定义, 并详细描述数字签名的研究现状.

1.1 信息安全与密码学

1.1.1 信息安全的重要性与密码学

随着计算机网络以及通信技术的飞速发展, 社会已进入信息化时代, 数字化、网络化将成为全球信息化新的基础平台. 信息成为一种重要的战略资源, 信息的获取、处理和安全保障能力成为一个国家综合国力的重要组成部分. 信息安全事关国家安全、社会稳定. 然而, 信息世界并不是一个完美的世界. 信息技术一方面给人类带来巨大好处的同时, 另一方面又给人类带来前所未有的威胁. 由于信息的存储、传输和处理等过程往往是在开放的通信网络上进行, 所以信息容易受到窃听、截取、修改、伪造和重放等各种攻击手段的威胁. 因此, 信息安全问题成为信息社会急需解决的重要问题.

信息安全的概念在 20 世纪经历了一个漫长的历史阶段后, 到 20 世纪 90 年代得到了前所未有的深化. 信息安全的主要内容包括信息的机密性 (Confidentiality)、完整性 (Integrity)、可用性 (Availability)、可控性 (Controllability) 以及信息的不可否认性 (Non-repudiation), 其主要特征如下:

(1) 机密性: 信息在生成、传递、处理和保存等过程中, 不能被未授权者所提取.

(2) 完整性: 信息未经授权不能进行改变的特性, 即信息在生成、传递、处理和保存过程中, 不能被非法地篡改、删除、重放和伪造等.

(3) 可用性: 保证信息及服务可被授权用户使用的特性.

(4) 可控性: 对信息及信息系统实施安全监控管理. 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) 不可否认性：网络用户不能否认或抵赖自己的操作和做出的承诺, 包括信息发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.

综合起来说, 信息安全的主要目的就是能够保证数字信息的有效性. 解决信息安全问题是一个庞大的系统工程, 需要综合运用数学、计算机、信息论、编码学、密码学、通信技术、管理技术等各种学科和技术的研究成果, 并且需要在实践中不断提高和不断探索. 其中, 密码学给解决信息安全问题提供了许多有效的核心技术, 在保护信息的保密性、完整性及不可否认性等方面发挥着关键性的作用, 因此, 密码学可以说是信息安全的核心技术.

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, 密码学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.

简单地说, 密码学是研究信息系统安全的一门学科. 它主要包括两个分支, 即密码编码学 (Cryptography) 和密码分析学 (Cryptanalysis). 密码编码学是对信息进行编码以实现信息隐藏的一门学科, 其主要目的是寻求保护信息保密性和认证性的方法; 密码分析学是研究分析破译密码的学科, 其主要目的是研究加密消息的破译和消息的伪造, 密码编码学和密码分析学相互对立又相互促进地发展. 本书以图的形式给出了现代密码学的主要研究内容 (图 1.1).

密码技术的基本思想是对消息做秘密变换, 变换的算法即称为密码算法. 而决定秘密变换的秘密参数称为密钥. 在密钥的作用下, 把有意义的明文 (Plaintext) 变换成无意义的密文 (Ciphertext) 的变换称为加密算法 (Encryption). 相应的逆变换称为解密算法 (Decryption). 若在密钥的作用下把消息变换成一种 “证据”, 用来说明某个实体对消息内容的认可, 则称变换为签名算法 (Signature), 相应的逆算法称为验证算法 (Verification).

根据密钥的特点, 密码体制可分为对称密钥密码体制和公钥密码体制. 在对称密钥密码体制中, 一对加密或解密算法使用的密钥相同或实质相同; 在公钥密码体制中也有一对密钥, 只是其中一个密钥公开, 即公钥, 另一个密钥保密, 称为私钥, 加密或解密算法使用的密钥不同, 且很难从公钥推导出私钥. 公钥密码体制的显著优点是通信双方不需要事先交换密钥就能够进行保密通信, 而对称密码体制需要提前交换密钥才能进行保密通信.

1.1.2　数字签名技术的研究意义

数字签名技术 (电子签章技术) 对信息安全极为重要. 数字签名可以实现身份认证、数据完整性保护、防篡改、防冒充和不可否认性等网络数据传输中的重要需求, 因而是信息安全的核心技术之一. 诚如约翰 • 麦考密克在他的著作《改变未来的九大算法》中提到 “数字签名起着巨大的实际作用：没有数字签名, 我们所知

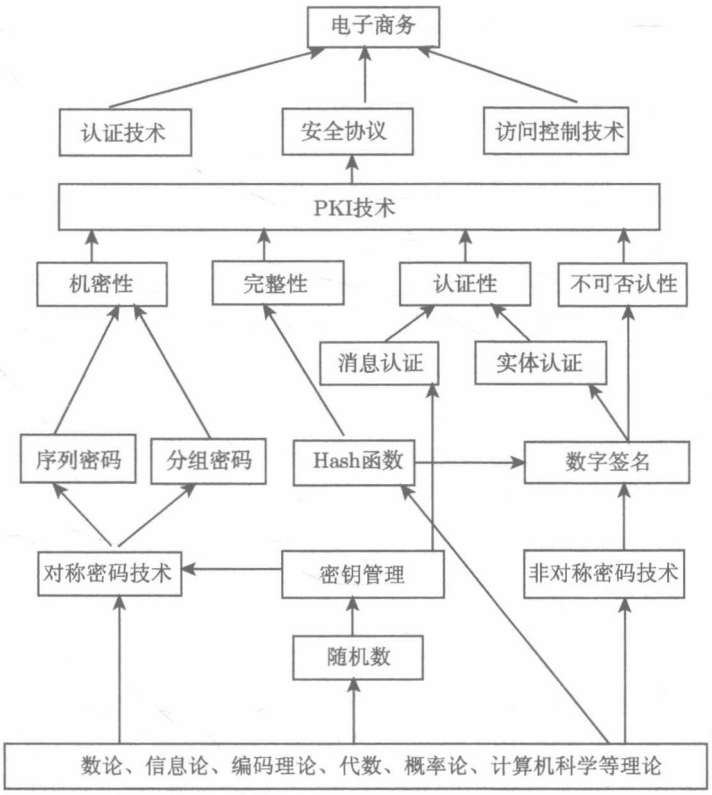

图 1.1 现代密码学主要研究内容

的互联网就不会存在. 数据仍可以通过加密安全交换, 但要验证接收数据的来源就要困难得多. 这一伟大思想和如此广泛的实际影响相结合, 无疑让数字签名成为计算机科学中最伟大的成就之一". 与传统的手写签名技术相比, 数字签名技术无疑拥有更多的优势. 例如, 在传统的商业领域和邮件通信等行业中, 几乎所有的交易业务都要求在交互过程中对交易的单据进行签名或者加盖印章, 以便证明其合法性, 而在电子商务领域和其他网络通信等行业中, 由于人们都是利用计算机或者手机等终端通过网络来传送消息, 因此在这个过程中, 人们可能是互不相见的, 所以手写的签名方式显然是行不通的. 于是, 在当前的计算机系统中, 人们很自然地想到采用数字签名技术来代替传统的手写签名技术, 从而通过数字签名来证明在电子数据交换过程中数据的合法性. 目前很多场合的信息安全保障都直接依赖于各种数字签名的安全性. 数字签名技术应用广泛, 比如公钥基础设施 PKI(Public Key Infrastructure), 目前已经标准化并得到了广泛的应用, 信息安全已经严重依赖于 PKI, 如果支撑 PKI 的数字签名不安全, 比如攻击者可以伪造签名和证书, 那么

整个信息安全体系都将受到严重的威胁或破坏. 可见数字签名的安全性对信息安全的影响非常重大. 数字签名是实现认证的重要工具, 在认证加密系统中也有着举足轻重的应用和研究价值. 所以, 开展数字签名技术的研究不仅具有重要的学术价值, 而且对国家安全和信息化建设具有极为重要的意义.

数字签名作为重要的数字证据, 美国、欧盟、新加坡、日本、韩国等电子商务开展得较早的国家和地区都相继通过法案赋予数字签名法律效力, 我国也于 2004 年 8 月通过了《中华人民共和国电子签名法》, 数字签名将与手写签名一样具有同等的法律效力. 数字签名最重要的应用之一是大型网络的公钥证书认证, 证书被用于可信任第三方绑定用户身份和其公钥信息. 此外, 数字签名已被广泛应用于电子商务和电子政务中. 目前, 数字签名技术已开始应用于商业、金融和办公自动化等系统中, 同时作为一种密码学的基础构件, 数字签名也被广泛用于设计电子支付、电子投标、电子拍卖、电子彩票、电子投票、电子出版和知识版权保护等应用层协议, 成为安全电子商务和安全电子政务的关键技术之一.

1.1.3　数字签名的原理、形式化定义、功能和分类

1. 数字签名的基本原理

自从 Diffie 和 Hellman[1] 提出公钥密码的思想后, 公钥密码学很快出现了. 在公钥密码体制中, 用户的密钥是由公钥和私钥组成的密钥对, 私钥秘密保存, 公钥公开. 由于从公钥不能推出私钥, 所以公开公钥不会损害私钥的安全. 数字签名就是签名方用自己的私钥对某消息进行加密, 验证方如果能够用签名方的公钥正确解密, 就肯定该消息是签名方签的, 这就是数字签名的基本原理.

2. 数字签名的形式化定义

数字签名是手写签名和印章的电子替代物, 它是一个由签名人的私钥和被签消息计算出来的比特串, 可用于消息的完整性认证和消息的源认证, 在电子商务和电子政务系统可用于保证消息的不可否认性和完整性. 数字签名其实是伴随着数字化编码的消息一起发送并与发送的信息有一定逻辑关联的数据项.

数字签名方案一般包括三个过程 (图 1.2): 系统的初始化过程、签名的产生过程和签名的验证过程. 系统的初始化过程产生数字签名方案用到的一切参数; 签名产生过程中, 用户用自己的私钥对消息进行签名; 签名验证过程中, 验证者利用公开的验证方法对给定消息的签名进行验证, 得出签名是否有效的结论.

定义 1(数字签名方案定义)　数字签名方案一般由以下 3 种算法组成:

(1) **密钥生成算法 K**　输入安全参数 k, 算法 K 产生一对匹配值 (k_p, k_s), 分别称为公钥和私钥, K 可以是概率算法.

(2) **签名算法 Σ**　给定消息 m 和 (k_p, k_s), Σ 产生签名 σ, Σ 可以是概率算法.

(3) **验证算法 V** 给定签名 σ、消息 m 以及公钥 k_p, V 检验 σ 是否是 m 的对应于公钥 k_p 的有效签名, 如果有效, 输出 1; 否则输出 0, 表示该签名无效. 通常情况下, V 是确定性算法.

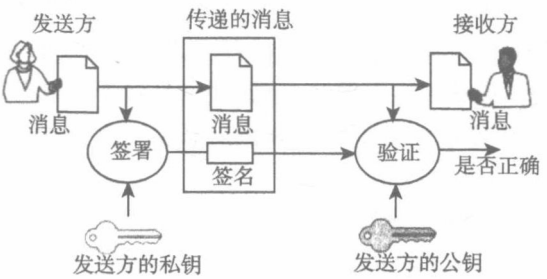

图 1.2 数字签名过程

3. *数字签名的功能*

数字签名技术可以解决伪造、篡改、冒充和抵赖等问题, 其功能主要有以下方面.

(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者的公钥进行加密, 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给接收者, 一旦信息被篡改, 接收者可以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得通过, 那么可以肯定签名人就是拥有私钥的人, 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) 防抵赖: 数字签名既可以作为身份认证的依据, 也可以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, 给发送者或可信任第三方.

(5) 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给 B 公司多份, 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.

4. *数字签名的分类*

1) (普通) 数字签名

仅具备上述签名功能, 代表算法有: Hash 签名、RSA 签名、Schnorr 签名、E1Gamal 签名、DSS 签名和椭圆曲线 ECC 签名等.

(Ⅰ) 基于 Hash 函数的签名

由于 Hash 函数的计算消耗小, 实现简单, 因此基于 Hash 函数的签名方案计算复杂度小, 应用范围广泛. 目前很多已经实现的交易系统都使用了基于 Hash 函数的签名方案. 在这类交易系统中, 算法计算速度快, 对整个服务资源的消耗低, 可以在一定程度上减轻网络和中央服务器的负担. 但是由于基于 Hash 函数的签名方案是在对称密码体制下设计的签名算法, 密钥无论是对于签名方还是验证方来说都是同一个, 因此存在一定的安全隐患, 即敌手如果攻破两方中的任何一方获得签名密钥, 就可以伪造签名.

(Ⅱ) RSA 签名和 ECC 签名

RSA 算法和 ECC 算法都是在非对称公钥密码体制下设计的加密算法, 即基于公钥密码体制的加密方案. 其中, RSA 算法是基于大素数素因子分解难题之上构造的方案, 该算法实现简单, 速度较快, 因此目前已经成为一种加密标准. 而 RSA 签名是基于 RSA 算法构造的签名方案, 同样该算法实现速度快, 实现简单. ECC 签名是基于 ECC 加密方式构造的签名方案, 由于该方案比 RSA 签名方案具有更低的计算消耗和更短的计算参数, 因此 ECC 签名方案的高效性和安全性已经得到了普遍的认同. 目前, 无论是 RSA 签名方案还是 ECC 签名方案, 和 Hash 签名方案相比, 由于签名方和验证方的密钥不同, 所以具有更好的安全保障.

2) 带有特殊性质 (附加功能) 的数字签名

这种签名是在普通数字签名基础上根据实际应用需要产生的特殊签名, 如代理签名、聚合签名、群签名、环签名、盲签名、指定验证者签名、多重签名、签密等.

(Ⅰ) 代理签名

代理签名就是当某签名人因公务或身体健康等原因不能行使自己的签名权力时, 将签名权委派给其他人替自己行使签名权.

根据已有的对代理数字签名的研究和分析, 普遍认为代理数字签名体制应该满足以下基本性质 [2,3].

性质 1(不可伪造性 (Unforgeability))　不可伪造性包括基本的不可伪造性和代理签名的不可伪造性两个性质. 基本的不可伪造性指除了原始签名人以外, 任何人 (包括代理签名人) 都不能生成原始签名人的普通数字签名. 这个性质也是任何数字签名体制都应当具备的性质, 它可以保证原始签名人的基本安全要求. 代理签名的不可伪造性是指除了代理签名人外, 任何人 (包括原始签名人) 都不能生成有效的代理签名. 特别地, 如果原始签名人委托了多个代理签名人, 那么要求任何代理签名人都不能伪造其他代理签名人的代理签名. 这个性质可以保证代理签名人的基本安全要求.

性质 2(可验证性 (Verifiability))　通过接收到的代理数字签名, 验证者能够验证原始签名人对代理签名人的代理签名权力的授权, 以及对接收到的代理签名的有

效性的验证.

性质 3(代理签名的可区分性 (Distinguishability)) 任何一个代理签名都应该与原始签名人的普通数字签名有着明显的区别; 不同代理签名人生成的代理签名之间也应具有明显的区别. 这个性质和性质 1、性质 2 结合起来可以防止签名人 (包括原始签名人和代理签名人) 之间对生成签名行为的相互抵赖和否认.

性质 4(不可抵赖性 (Undeniability)) 不论是原始签名人还是代理签名人, 在生成了一个数字签名以后, 就无法再对它加以否认.

性质 5(身份证实性 (Identifiability)) 原始签名人可以根据一个有效的代理签名确定出生成该代理签名的代理签名人的真实身份. 利用这个性质, 原始签名人可以对代理签名人进行监督, 使代理签名人不能滥用代理签名权力.

性质 6(密钥依赖性 (Key Dependation)) 代理签名密钥必须依赖于原始签名人的私有密钥.

性质 7(可注销性 (Revocation)) 当原始签名人不再希望代理签名人拥有代理他进行签名的权力时, 可以有效地对代理签名人的代理权力进行撤销.

性质 8(不可滥用性 (Prevention of Misuse)) 代理签名人仅能运用代理签名权力在原始签名人的授权范围内进行签名.

(Ⅱ) 盲签名

盲签名是根据电子商务具体的应用需要而产生的一种签名应用. 当需要某人对一个文件签名, 而又不让他知道文件的内容时就需要盲签名. 盲签名方案的基本思想如下: Alice 发送给 Bob 一段信息, Bob 对它签名并送回 Alice. 由于这个签名, Alice 能够计算 Bob 关于 Alice 预先所选消息 m 的签名. 协议完成时, Bob 既不知道消息 m, 也不知道消息的签名是何时所签、为谁所签.

盲签名的目的就是防止 Bob 看到消息和签名, 从而使 Bob 以后不能将所签消息和发送者 Alice 联系起来.

盲签名一般用于电子货币、电子拍卖和电子选举等领域.

特殊性质: ①盲性; ② 不可追踪性.

为了让大家更清楚理解这种特殊签名, 在此介绍一个典型的 Zhang 和 Kim 的盲签名方案 [4].

Zhang-Kim 的盲签名方案 该方案包括 5 个基本的算法: 初始化、密钥解析、盲签名协议、去盲算法和签名验证算法.

(1) **初始化** 设 G_1 为 q 阶加法循环群, G_2 为同阶乘法循环群, q 是一个大素数, P 为 G_1 的一个生成元. 双线性映射 e; $G_1 \times G_1 \to G_2$. 令 $H : \{0, 1\}^* \to G_1$, $H_1 : \{0, 1\}^* \times G_2 \to \mathbb{Z}_q$ 为两个 Hash 函数. 随机选择 $s \in \mathbb{Z}_q^*$, 并计算系统公钥 $P_{\text{pub}} = sP$. 则主密钥为 s.

(2) **密钥解析**　给定一个签名者的公开身份 $\mathrm{ID} \in \{0,\ 1\}^*$, 计算公钥为 $Q_{\mathrm{ID}} = H_1(\mathrm{ID})$, 私钥为 $S_{\mathrm{ID}} = sQ_{\mathrm{ID}}$.

(3) **盲签名协议**　给定一个签名者的私钥 S_{ID} 和一个消息 $m \in \{0,\ 1\}^*$.

a) 初始化: 签名者选择一个随机数 $r \in \mathbb{Z}_q$, 计算 $R{=}rP$, 并将 R 发送给用户;

b) 盲化算法: 用户选择随机数 $a,\ b \in \mathbb{Z}_q^*$ 作为盲化因子, 计算

$$c = H(m,\ e(bQ_{\mathrm{ID}} + R + aP,\ P_{\mathrm{pub}})) + b,$$

将 c 发送给签名者;

c) 消息签名: 签名者将 S 发送给用户, 其中 $S = cS_{\mathrm{ID}} + rP_{\mathrm{pub}}$;

(4) **去盲算法**　用户计算 $S' = S + aP_{\mathrm{pub}}$ 和 $c' = c - b$, 输出 $(m,\ S',\ c')$, 则 $(S',\ c')$ 为消息 m 的盲签名.

(5) **签名验证算法**　验证者检验式子 $c' = H(m,\ e(S', P)e(Q_{\mathrm{ID}}, P_{\mathrm{pub}})^{-c'})$, 如果等式成立则接受该签名, 否则不接受该签名.

(III) 聚合签名

聚合签名就是 $n(>1)$ 个用户 $P_i(1 \leqslant i \leqslant n)$ 对 n 个不同的消息 m_i 进行签名, 这 n 个 (单一) 签名可以被聚合成一个签名, 验证者只需对合成后的签名进行验证来确认是否是 P_i 对 m_i 做的签名 (图 1.3).

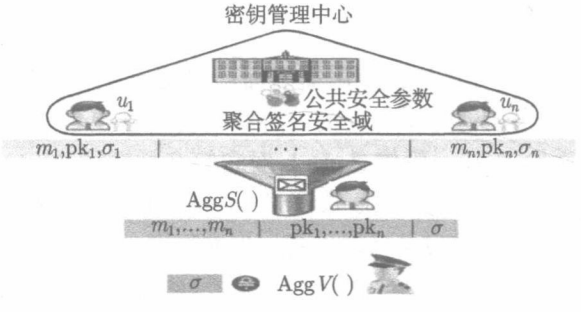

图 1.3　聚合签名原理示意图

聚合签名支持多个用户的身份认证、数据完整性和不可抵赖性等安全服务, 是数字签名领域的 "批处理" 和 "压缩" 技术, 可以被用于分级 PKI 中的证书链、RFID 物品追踪、WSN 的安全路由协议、WSN 网络数据融合、安全邮件、电子现金和安全交易、数据库外包、动态内容分发、车联网信息聚合、日志审计、云计算和分布式系统等诸多领域. 特别值得指出的是, 聚合签名的特性非常适合物联网领域, 以上很多应用都是和物联网密切相关的.

(IV) 群签名

在群签名方案中, 群体中的任意一个成员可以以匿名的方式代表整个群体对某个消息进行签名. 在群签名中, 一个群组成员能够使验证者相信他属于这个群而不需要公开他的身份. 一个群签名满足下面的三条性质:

(1) 只有群里的成员才能够对消息进行签名;

(2) 接收者能够验证它是来自这个群的有效签名, 但不知道是群里的哪个成员签署的;

(3) 如果事后发生争端, 签名能够由群管理员公开, 揭示签名者的身份.

群签名能够为群成员提供良好的匿名性, 但如果有纠纷时又可以通过群管理员揭示原始签名人的身份, 再加上其他安全特性, 使得群签名在电子投票系统、电子拍卖系统、竞标系统等领域应用很广. 例如, 群签名可以用于提交投标报价, 所有提供报价的公司组成群, 并且每个公司为其报价签署匿名的群签名, 一旦某个报价被选中, 获胜者的身份可以被跟踪, 而其他投标者仍是匿名的. 更一般地, 群签名可以隐藏组织结构. 例如, 当一个公司或政府机构发布一个签署的文件. 群签名还可以应用在电子现金系统中, 使几个银行可以安全地分配匿名的、不可跟踪的电子现金. 这种性质隐藏了发行电子现金银行的身份.

通常, 一个群签名方案由以下 5 个算法组成.

(1) 系统建立: 概率多项式时间算法, 输入安全参数, 输出群公钥和用户私钥.

(2) 成员加入: 一个新用户通过和群主管的交互协议请求加入, 协议执行完毕, 合法的新成员完成身份注册并获得一个秘密钥和一个成员资格证书.

(3) 生成签名: 给定消息 m, 群成员用私钥、成员资格证书对消息 m 生成群签名.

(4) 签名验证: 签名接收者利用验证算法验证消息 m 的签名的有效性.

(5) 匿名性揭示: 群主管输入 m, 消息的签名和自己的私钥, 提取成员资格证书并揭示签名者的真实身份.

(Ⅴ) 环签名

环签名是群签名的简化形式, 是一种特殊的群签名, 它支持自组织的子集生成并且在一般情况下并不需要专门建立子集, 允许一个成员代表一组人进行签名而不泄露签名人的身份. 在环签名中, 签名系统不需要群管理员, 用户没有组织结构程序, 不用协调一致. 签名产生后, 签名者对于验证者来说是无条件匿名的, 即验证者只知道签名者在这个签名环中, 但不知道具体是哪一个. 因此, 环签名具有的最大特点是保证签名者的隐匿性, 为签名者提供了一条发布消息但不暴露自己身份的途径, 同时对于签名验证者来说, 这条带有合法签名的消息绝对是可靠的, 只是无法知道这条消息到底是环中的哪个用户签发的. 由于环签名很好地提供了一种泄露机密但不暴露自己身份的机制, 因此环签名在商业领域中有着许多潜在的用途, 如在匿名电子选举、电子政务、电子现金系统、多方安全计算、密钥管理等方面有广泛的应用.

一个环签名方案必须满足无条件匿名性和不可伪造性两个基本的安全性要求.

(1) 无条件匿名性: 即使攻击者拥有无限的计算资源和计算能力, 也不能以高