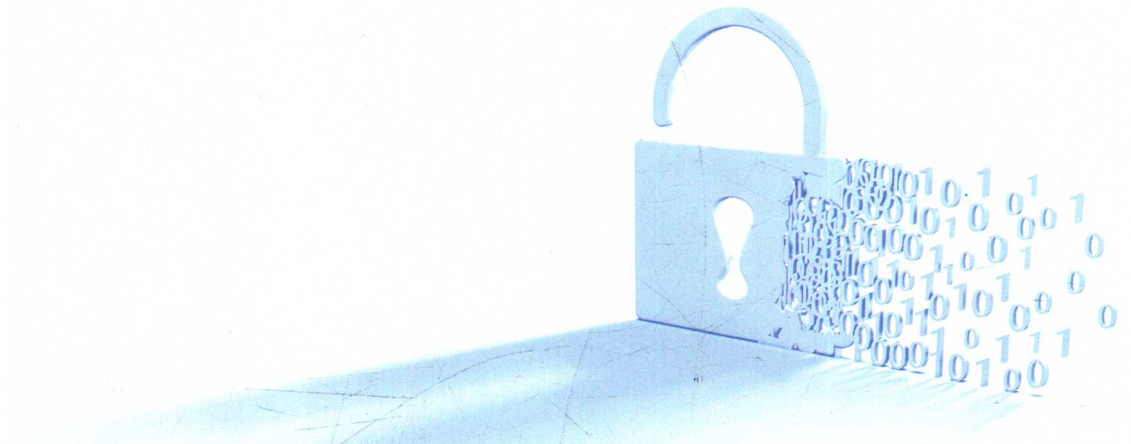

新型数字签名的设计与分析

伍　玮　黄欣沂　杨文杰◎著

Design and Analysis of New Digital Signatures

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

新型数字签名的设计与分析

伍　玮　黄欣沂　杨文杰◎著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书内容围绕新型数字签名的研究热点和难点展开。本书分为基础背景、具有不可否认性质的数字签名研究、仅指定验证者可验证的数字签名研究、基于新型公钥密码体制的数字签名研究四部分。第一部分对数字签名中涉及的理论知识和技术路线进行概述。第二部分从基于配对具体构造、代理属性延拓一般化通用构造、云计算中应用及基于身份体制下的扩展等方面描述和分析了具有不可否认性质数字签名机制。第三部分从标准模型下安全方案的论证、代理属性的规避、指定者权利的限制、签名长度的精简及与代理签名高效融合等方面阐释了具有指定验证者性质数字签名机制。第四部分从首个具体方案安全性分析、安全模型的精准刻画、指定验证者性质的有效扩展、生成中心能力的削弱及基于证书体制下的通用构造等方面研究了新型公钥密码体制下的数字签名机制。

图书在版编目（CIP）数据

新型数字签名的设计与分析/伍玮，黄欣沂，杨文杰著. —北京：电子工业出版社，2019.6
ISBN 978-7-121-36848-6

Ⅰ. ①新… Ⅱ. ①伍… ②黄… ③杨… Ⅲ. ①电子计算机－密码术 Ⅳ. ①TP309.7

中国版本图书馆 CIP 数据核字（2019）第 112640 号

责任编辑：朱雨萌　　特约编辑：王　纲
印　　刷：三河市双峰印刷装订有限公司
装　　订：三河市双峰印刷装订有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：720×1 000　1/16　印张：18.25　　字数：321 千字
版　　次：2019 年 6 月第 1 版
印　　次：2019 年 6 月第 1 次印刷
定　　价：68.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）88254750。

前　言

伴随着经济社会数字化程度的不断深入，如何保证数字资源的完整性、有效性及认证性受到了人们的极大关注。数字签名作为手写签名的一种数字化表现形式为上述问题的解决提供了一个很好的技术支撑。发展至今，数字签名及其针对不同应用场景的有效扩展已经在电子商务、数字医疗、分布式计算、物联网等相关领域得到了广泛的应用。

本书基于作者在数字签名领域多年的研究工作编写而成。本书的主要目的就是紧扣信息安全中数字签名技术这一主题，希望对从事该领域研究的研究生、教师及对该领域感兴趣的专家学者起到一定的参考和引导作用。

具体来说，本书由四大部分共 17 章构成。第 1 章，我们分别介绍了数字签名技术的研究背景与意义，以及具有不可否认性质数字签名、仅指定验证者可验证数字签名和基于新型公钥密码体制数字签名等典型方案的现状及工作总结。第 2 章，我们简明回顾了研究过程中涉及的相关数学理论知识和密码学等基本工具。第 3 章，我们形式化地定义了全新的可转换不可否认数字签名的安全模型，并论证了隐藏性与匿名性之间的内在关联。同时，我们还给出了一个随机预言机模型下可证明安全的可转换不可否认短签名方案。第 4 章，我们针对签名者可能会临时缺席这一实际情况，提出了可转换不可否认代理数字签名的概念。进一步形式化地定义了可转换不可否认代理数字签名的安全模型，并构造了第一个具体的签名方案。第 5 章，基于一个经典的强存在不可伪造签名、一个选择性转换不可否认签名及一个抗碰撞哈希函数，我们给出了可转换不可否认数字签名的一种通用构造方法，并在标准模型下论证了该构造方法的安全性。第 6 章，我们重点关注在云环境中如何实现具有隐私保护功能的源不可否认性。在此，我们对其做了形式化定义，并给出了一个实用的通信协议。第 7 章，我们将可转换不可否认签名的概念推广到了基于身份公钥密码体系，并形

式化定义了基于身份可转换不可否认签名的安全模型。同时，我们还给出了一个基于经典困难问题假设的具体构造方案。第 8 章，我们在对已有泛指定验证者签名进行分析的基础之上给出了一个具体的在标准模型下可证明安全的泛指定验证者签名。第 9 章，我们形式化地定义了针对泛指定验证者数字签名的“代理攻击”，并给出了一个抗代理攻击泛指定验证者数字签名的具体构造。第 10 章，我们针对指定验证者次数受限的具体应用场景给出了一个限定性泛指定验证者数字签名方案。第 11 章，我们针对传统指定验证者签名中的效率优化问题给出了一个指定验证者短数字签名方案，并将其在基于身份公钥密码体系中进行了有效扩展。第 12 章，我们将代理签名与指定验证者签名的概念进行了有机融合，并给出了指定验证者代理数字签名的雏形。同时，我们还给出了首个在随机预言机模型中可证明安全的指定验证者代理短数字签名。第 13 章，我们对首个无证书数字签名方案做了安全性分析，并给出了一个具体的公钥替换攻击实例。同时，我们还构造了一个有效的改进方案。第 14 章，我们系统化地定义了无证书数字签名的安全模型，并给出了多个安全的具体构造实例。第 15 章，我们提出了在无证书密码体系下的指定验证者数字签名的概念，并设计了一个在随机预言机模型下可证明安全的具体方案。第 16 章，我们对恶意密钥生成中心的概念进行了深入探讨，并提出了一个抗此类攻击的无证书代理数字签名方案。第 17 章，我们给出了一个由无证书数字签名方案到基于证书数字签名方案的通用转换，并基于其构造了一个具体的基于证书数字签名。

本书的出版得到了国家自然科学基金（61822202，61872089）的资助。同时，福建师范大学数学与信息学院、福建省网络安全与密码技术重点实验室对本书的撰写也给予了大力支持，在此深表感谢。

由于作者的水平有限，书中错漏之处在所难免，恳请国内同行和广大读者不吝赐教。

目　录

第一部分　基础背景

第二部分　具有不可否认性质的数字签名研究

第三部分 仅指定验证者可验证的数字签名研究

第一部分

基础背景

第1章 引 言

1.1 数字签名研究的背景

进入 21 世纪以来，随着计算机及网络技术的高速发展，许多传统服务，如拍卖、投票及购物等都转为线上服务。作为保证线上服务机密性与可靠性的关键技术手段，密码学受到了极大的关注。数字签名技术作为密码学的重要组成部分，它能够高效地提供如下可靠性需求。

1. 确保消息完整有效

在许多实际应用场景中，收发双方之间需要一种机制来保证经过传输后的消息依然完整有效。尽管加密技术可以为消息内容提供机密性需求，但并不能确定消息在传输过程中是否遭到篡改。当一个消息经过发送方数字签名之后，消息的任何变更都会导致原数字签名失效。此外，不存在一个多项式时间算法能够根据一个有效的消息数字签名对产生该消息变更后的有效数字签名。因此，数字签名技术保证了信息传输后的完整有效性。

2. 发送方身份认证

在信息传输过程中，一般都包含发送方身份的相关信息，但是这种声明式的认证方法往往不太具有说服力。数字签名技术要求只有掌握发送方私钥信息的数字签名服务器才能够为特定消息产生一个有效的数字签名。当接收方收到

一条消息后，只要能够验证与该消息相关的数字签名是有效的，就可以确认这条消息的来源。因此，数字签名技术保证了发送方身份的真实性。

3．发送方行为不可否认

数字签名是非对称密码技术的一种应用，代表着对所签消息的认可。其安全性要求除发送者外的任何第三方都不能根据发送者的公钥信息及已有的有效数字签名信息伪造出某一新消息的有效数字签名信息。数字签名只能由被认证过公钥对应私钥的拥有者签发。因此，数字签名技术有效地防止了抵赖行为的发生，避免了很多不必要的纠纷。

基于上述极具吸引力的特性，数字签名技术已成为线上活动不可或缺的一项安全技术措施，同时也是确保线上行为真实可靠、实现认证的重要工具。至今，数字签名技术已在商业、金融、军事等领域，特别是在电子贸易、电子支票、电子购物、电子政务及知识产权保护等方面有着广泛的应用。未来，随着日常生活数字化程度的进一步提高，开展数字签名技术的研究不仅具有非常重要的学术价值，而且对国家的经济发展与信息化建设等都有十分重要的意义。

1.2 数字签名发展现状

基于公钥密码学的思想，Diffie 和 Hellman[1]于 1976 年提出了数字签名的概念。它的基本原理就是，在不存在一个多项式时间算法可根据实体公钥信息提取相应私钥信息的条件下，数字签名服务器利用自身掌握的实体私钥信息生成某一消息的数字签名，而其他任何感兴趣者都可以借助实体被认证过的相应公钥信息来完成该数字签名的有效性验证。数字签名技术的流程如图 1-1 所示。

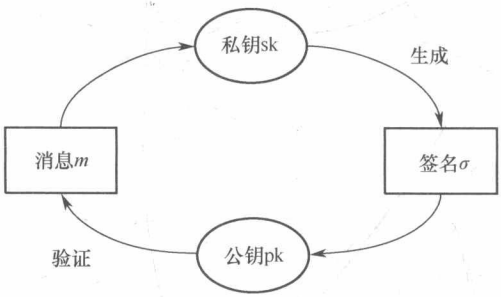

图 1-1　数字签名技术的流程

作为公钥密码学的一个重要分支，数字签名技术按照签名者公钥与其身份之间关联认证方式的不同，大体经历了传统公钥密码体系、基于身份公钥密码体系和无证书公钥密码体系三个发展阶段。

在传统公钥密码体系中，每个签名者独立地选取自身的公私钥对。此时，公钥通常是一个没有任何含义的独立随机串。为了使验证者相信某个公钥隶属于某个特定的签名者而没有遭到恶意第三方篡改或替换，人们引进了公钥证书的概念。详细来说，公钥基础设施（Public Key Infrastructure，PKI）中的证书颁发机构（Certificate Authority，CA）为绑定签名者的公钥与相应的身份信息颁发一个数字认证证书，其中记录着签名者身份、公钥及其有效期等相关参数。1978 年，基于 Diffie 和 Hellman 提出的数字签名思想，Rivest 等人构造了首个具体的数字签名协议，即著名的 RSA 数字签名协议。之后，又有很多经典的数字签名协议被提出，如 Okamoto 数字签名协议[2]、Schnorr 数字签名协议[3]和 ElGamal 数字签名协议[4]等。同时，为了满足一些特定场景的应用需求，研究者们还设计了很多扩展的数字签名协议，比如门限数字签名[5-8]、代理数字签名[9-12]、聚合数字签名[13-16]、盲数字签名[17-22]及签密[23-25]等。但在实际应用中，随着用户数量的增加，证书的生成、存储、分发和撤销等管理问题变得极为复杂。此外，验证者在使用公钥验证数字签名有效性之前都需要检测该公钥对应数字证书的有效性，这也会给验证者带来很大的计算代价。

为了克服传统公钥密码体系下证书管理复杂及验证者需要重复检测证书有效性等问题，Shamir 于 1984 年首次提出了基于身份公钥密码体系的概念[26]。在该密码体系中，签名者使用自己的公开身份信息（如身份证号、电话号码、E-mail 地址和 IP 地址等）作为公钥信息，而数字签名所用的私钥则统一由一个完全可信的第三方——私钥生成中心（Private Key Generator，PKG）生成。该方法巧妙地解决了公钥密码体系中实体公钥的认证问题，同时又不涉及复杂的证书管理问题。随后，密码学家给出了基于身份数字签名协议的一些前期设计[27-29]。可惜的是，这些早期设计都因其低效性而未得到部署。接下来，学者们基于双线性配对分别构造了一些经典的随机预言机模型下可证明安全的基于身份数字签名协议[30-35]和标准模型下可证明安全的基于身份数字签名协议[36-40]。同样，在具有特殊性质的基于身份数字签名协议的研究方面，也有很多实用的具体构造被提出[41-56]。但是，由于基于身份公钥密码体系中 PKG 知道每个签名