高等学校计算机教材建设立项项目

高等学校计算机专业规划教材

数字签名与安全协议

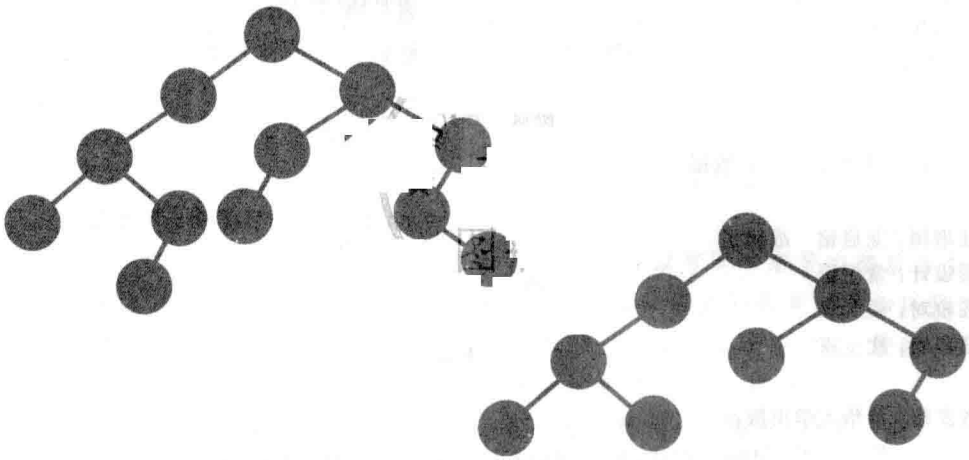
任　伟 编著

清华大学出版社

高等学校计算机专业规划教

数字签名与安全协议

任　伟　编著



清华大学出版社
北京

内 容 简 介

本书内容包括四个部分：基本数字签名(基于单向性的签名、基于离散对数的签名、基于离散对数签名的扩展讨论、基于身份识别协议的签名)，高级数字签名(盲签名、代理签名、多重数字签名、环签名、指定验证者签名等)，安全协议(实体认证协议、身份识别协议、密钥协商协议、比特承诺、零知识证明协议、不经意传输、秘密共享、安全多方计算)，基于身份的密码学和可证明安全性。本书的特点是注重介绍密码学方案的构造逻辑、设计规律，在给出方案的同时，还给出具有启发性的解释和讨论，解释方案的设计机理和思路，以培养学习者的逻辑推理能力。

本书主要面向高等学校信息安全、密码学、电子对抗、应用数学、计算机科学、通信工程、信息工程、软件工程等专业本科高年级学生和研究生，对具有密码学基础的研究人员也有启发作用和参考价值。

图书在版编目(CIP)数据

数字签名与安全协议/任伟编著. —北京：清华大学出版社，2015
高等学校计算机专业规划教材
ISBN 978-7-302-39746-5

Ⅰ. ①数…　Ⅱ. ①任…　Ⅲ. ①密码协议　Ⅳ. ①TN918.1

中国版本图书馆 CIP 数据核字(2015)第 077221 号

责任编辑：龙启铭　战晓雷
封面设计：常雪影
责任校对：梁　毅
责任印制：沈　露

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954

印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：10.5　　**字　　数**：259 千字
版　　次：2015 年 8 月第 1 版　　**印　　次**：2015 年 8 月第1次印刷
印　　数：1～2000
定　　价：25.00 元

产品编号：057786-01

前言

“密码学”是网络空间安全、信息安全、密码学、电子对抗与网络攻防等专业中一门重要的专业课，在学科知识体系中占据重要的地位。“数字签名与安全协议”把密码学基础知识融会贯通，是密码学中重要的应用部分，内容十分丰富。

作者在密码学课程教学过程中发现，很多学生只是停留在对密码学方案过程的记忆上，局限于记忆密码学方案的具体步骤，而未能思考和总结密码学方案的设计方法和一般规律。目前相关书籍在密码学设计机理等内在机制的讲解方面仍然有改进的空间，在思维的启发性以及学生创造性能力培养方面仍然有待完善。本书试图在这些方面做一点抛砖引玉的尝试，写作时遵循了以下思路：

(1) 注重启发性。注重对设计原理的分析以及对设计的动机和逻辑性的解释，让学习者知其然，也知其所以然。

(2) 注重知识点的逻辑联系和类比。注重章节间和章节内前后各个分离的知识点间的联系和类比关系，明确给出各知识点间的关联并加以强调，便于读者体会密码算法或协议设计的奥妙。大量采用类比法、比较法、归纳法、图示法，试图使读者对所学内容能够反复巩固，前后联系。

(3) 注重原理的总结和推广。在介绍具体构造方案后，给出一般性构造方案，或者加以讨论和提炼总结，有利于知识的理解和举一反三。

(4) 广度和深度兼具。基本原理、基本概念的讲解力求透彻，有深度。通过扩展阅读加大广度，便于回顾经典论文或者了解国内外发展动态。

全书共 15 章，分为 4 个部分，第 1 部分“基本数字签名”包括第 1 章“数字签名概述”、第 2 章“基于单向性的签名”、第 3 章“基于离散对数的签名”、第 4 章“离散对数签名的扩展*”、第 5 章“基于身份识别协议的签名*”。第 2 部分“高级数字签名”包括第 6 章“盲签名”、第 7 章“代理签名”、第 8 章“多重数字签名”、第 9 章“其他高级签名*”。第 3 部分“安全协议”包括第 10 章“实体认证协议”、第 11 章“身份识别协议”、第 12 章“密钥协商协议”、第 13 章“高级协议”。第 4 部分“基于身份的密码学和可证明安全性”包括第 14 章“基于身份的公钥密码学”和第 15 章“可证明安全签名和协议*”。

全书精心安排了示例。为帮助读者进一步对内容的拓展研究，有针对性地提供了扩展阅读建议，用于开展课外学习和论文研读讨论。每部分的小结归纳了本部分中的知识点，并指出重点和难点，便于复习。打 * 号的章

节可选学。

本书主要面向高等学校网络空间安全、信息安全、密码学、电子对抗、应用数学、计算机科学、通信工程、信息工程、软件工程等专业本科高年级学生和研究生，对具有密码学基础的研究人员也有启发作用和参考价值。

本书获得全国高等学校计算机教育研究会2013年度高等学校计算机教材建设立项资助，湖北省教育厅高等学校教学研究重点项目，以及国家自然科学基金面上项目(61170217)的资助，在此表示感谢。感谢研究生孙亚璐、林佳华、曹强的辅助工作。由于作者水平有限，在此衷心希望读者不吝赐教。

作　者

2015年4月

目录

第1部分　基本数字签名

第 3 部分 安全协议

第 1 部分

基本数字签名

第 1 章 数字签名概述

1.1 数字签名的一般模型

随着计算机网络的发展，特别是电子商务的兴起，需要对消息进行消息完整性保护，对消息源进行鉴别，对交易进行认证，以及提供不可抵赖性保障。数字签名是手写签名的数字化形式。手写签名的基本特点是：能与被签名的信息在物理上不可分割，签名者不能否认自己的签名，签名不能伪造，签名容易被验证。数字签名是一串二进制数，应与被签名的信息“绑定”在一起。通常，数字签名应具有以下特性：

(1) 签名是可信的。任何人都可以验证签名的有效性。

(2) 签名是不可伪造的。除合法的签名者之外，任何其他人伪造签名是困难的。

(3) 签名是不可复制的。对某个消息的签名不能通过复制变为对另一个消息的签名。如果对某个消息的签名是从别处复制得到的，则任何人都可以发现签名和消息不一致，从而可以拒绝签名的消息。

(4) 签名的消息是不可改变的。经签名的消息不能被篡改。一旦已签名的消息被篡改，则任何人都可以发现消息和签名之间的不一致性。

(5) 签名是不可抵赖的。签名者事后不能否认自己的签名。

定义 1.1 一个数字签名方案是一个 5 元组 $(M, S, K, \mathrm{SIGN}, \mathrm{VRFY})$，满足如下的条件：

(1) M 是一个可能消息的有限集。

(2) S 是一个可能签名的有限集。

(3) 密钥空间 K 是一个可能密钥的有限集。

(4) 对每一个 $k=(k_s, k_v)\in K$，都对应一个签名函数 $\mathrm{Sign}_{k_s}\in \mathrm{SIGN}$ 和验证算法 $\mathrm{Vrfy}_{k_v}\in \mathrm{VRFY}$。每一个 $\mathrm{Sign}_{k_s}: M\to S$ 和验证函数 $\mathrm{Vrfy}_{k_v}: M\times S\to\{\mathrm{True}, \mathrm{False}\}$ 是一个对任意消息 $m\in M$ 和任意签名 $s\in S$ 满足下列方程的函数：

$$\mathrm{Vrfy}(m,s)=\begin{cases}\mathrm{True} & s=\mathrm{Sign}_{k_s}(m)\\ \mathrm{False} & s\neq \mathrm{Sign}_{k_s}(m)\end{cases}$$

对每一个 $k\in K$，函数 Sign_{k_s} 和 Vrfy_{k_v} 都是多项式时间可计算的函数。Vrfy_{k_v} 是一个公开函数，k_v 为公钥(验证密钥)；Sign_{k_s} 是一个密码函数，k_s 为私钥(签名密钥)，要秘密保存。

1.2 数字签名的分类

基于数学难题的分类有基于离散对数问题的签名方案、基于大整数素数因子分解的签名方案、基于椭圆曲线离散对数问题的签名方案、基于二次剩余问题的签名方案。

基于数字签名是否具有恢复特性的分类有不具有消息恢复(message recovery)特性的签名和具有消息恢复特性的签名。

基于不同的加密方法的分类有基于对称加密算法的数字签名和基于公钥加密算法的数字签名。

基于签名用户的分类有单用户签名和多用户签名。多个用户的签名方案又称为多重签名方案。根据签名的过程不同,多重数字签名方案可分为有序多重数字签名方案和广播多重数字签名方案。

基于签名人对消息是否可见的分类:通常签名都是签名人对消息可见的,而盲签名方案表示签名者对消息不可见,但事后可以证明消息的存在。盲签名又根据签名者是否可以对消息者进行追踪分为弱盲签名方案和强盲签名方案。

基于签名人是否受别人委托签名的分类有普通签名方案和代理签名方案。如果授权的不是一个人,而是多个人,这时称为代理多重数字签名方案。

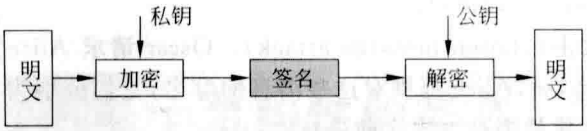
基于签名是否有仲裁的分类有直接数字签名和仲裁数字签名。直接数字签名是在签名者和签名接收者之间进行的,假设签名接收者知道签名者的公钥。仲裁数字签名在签名者、签名接收者和仲裁者之间进行。签名者和签名接收者共同信任仲裁者。签名者首先对消息进行数字签名,然后送给仲裁者。仲裁者首先对签名者送来的消息和签名进行验证,并对验证过的消息和签名附加一个验证日期和一个仲裁说明,然后把验证过的签名和消息发送给签名接收者。因为有仲裁者的验证,所以签名者无法否认自己签过的数字签名。

1.3 数字签名的设计原理*

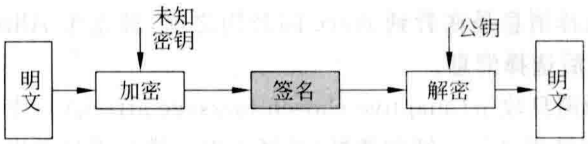
数字签名的设计主要依靠3种方法:单向陷门函数、从身份识别协议通过非交互零知识证明的机制转化而来的知识签名、利用可交换的公钥加密直接构造。

在利用单向陷门函数的数字签名中,陷门信息作为签名人的私钥,签名人对私钥的拥有表明签名的真实性。这种基于单向陷门函数的数字签名依据的是两条基本的假设:一是私钥是安全的,只有其拥有者才能获得;二是产生数字签名的唯一途径是使用私钥。尽管数字签名的安全性并没有得到证明,但超出这种假设,即使用未知的密钥而非私钥,或使用未知的算法而非数字签名算法得到的结果被公钥验证成功的例子尚未出现。因此,这两条假设的破坏是计算上不可行的,因而这两条假设被认为是成立的。数字签名的假设和例外如图1.1所示。

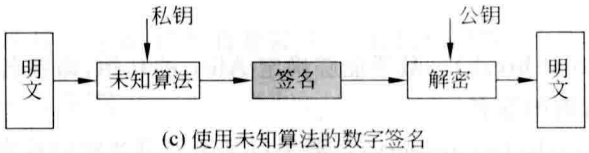
第二种是从身份识别协议通过非交互零知识证明的机制转化而来的知识签名。它从身份识别协议转化而来,转化的方法主要是利用非交互零知识的方法(也称为Fiat-



(a) 正常的数字签名



(b) 使用未知密钥的数字签名



(c) 使用未知算法的数字签名

图 1.1 数字签名的假设和例外

Shamir 启发式)。具体而言,通常包含 3 个部分,利用了单向函数的单向性构造一个承诺机制,对一个随机数进行承诺(承诺后不能再改变),然后利用哈希函数的单向性构造随机挑战值,该挑战值通常是消息和承诺值两者连接后的散列值,签名者利用对秘密知识的拥有构造相应的应答。该应答即是签名,签名接收者接收签名后验证签名的有效性。

还有一类签名可以利用可交换的公钥加密直接构造。可交换的公钥加密系统是指:设 E_e 是一个公钥加密算法,有消息空间 M 和密文空间 C,设 $M=C$。令 D_d 是对应 E_e 的解密算法,因 E_e 和 D_d 都是置换,且有

$$D_d(E_e(m)) = E_e(D_d(m)) = m, m \in M$$

称这种类型的公钥加密方案是可交换的。

于是可以简单地通过解密算法进行签名,如 RSA 签名方案和 Rabin 签名方案。

1.4 数字签名的安全性*

1988 年,Shafi Goldwasser、Silvio Micali 和 Ronald Rivest 第一次严格定义了数字签名的安全性,并提出了 GMR 签名方案,是第一个可证明满足选择消息攻击下的存在性不可伪造的签名。

本节只作简要介绍,以便读者理解后文中的一些概念。

首先需要明确安全需求,才能设计安全的数字签名方案。在明确安全需求之前,需要先明确敌手模型。

敌手的能力(假想攻击方为 Oscar,通信方为 Alice):

(1) 唯密钥攻击(key-only attack)。敌手拥有公钥以及签名验证函数 $\mathrm{Vrfy}_{pk}()$。

(2) 已知消息攻击(known message attack)。敌手 Oscar 拥有 Alice 已签署的一系列消息签名的列表,例如$(x_1, y_1), (x_2, y_2), \cdots$,其中 x_i 是消息,y_i 是 Alice 对这些消息的签

名(有 $y_i=\mathrm{Sign}_{sk}(x_i)$,$i=1,2,\cdots$)。

(3) 选择消息攻击(chosen message attack)。Oscar 请求 Alice 对一系列消息的签名,她选择消息 $x_1,x_2,\cdots$,Alice 提供对这些消息的签名,它们分别为 $y_i=\mathrm{Sign}_{sk}(x_i)$,$i=1,2,\cdots$。选择只能在挑战消息发出之前进行。

有的文献将选择消息攻击进一步划分为一般选择消息攻击和定向选择消息攻击。两者的区别是:前者选择消息是在看到 Alice 的公钥之前,独立于 Alice 的公钥;后者是在看到 Alice 的公钥之后选择消息。

(4) 自适应选择消息攻击(adaptive chosen message attack)。敌手可以选择 x_i,而且允许根据先前的访问结果进行后续的选择(选择可以在挑战消息发出之后继续)。

在后面,不再区分攻击(3)和(4),将其统称为选择消息攻击。

敌手的目标:

(1) 完全攻破(total break)。敌手能够确定 Alice 的私钥,即签名函数 $\mathrm{Sign}_{sk}()$,从而对任何消息都产生有效的签名。

(2) 选择性伪造(selective forgery)。敌手以某个不可忽略的概率对另外某个人选择的消息产生一个有效的签名。也就是说,如果给敌手一个消息 x,她能(以某种概率,该概率不可忽略)确定签名 y,使得 $\mathrm{Vrfy}_{pk}(x,y)=\mathrm{true}$,且该消息不是 Alice 曾经签名过的消息。

(3) 存在性伪造(existential forgery)。敌手至少能够为一则消息产生一个有效的签名。换句话说,敌手能产生一个消息和签名对(x,y),其中 x 是消息,y 是签名,而 $\mathrm{Vrfy}_{pk}(x,y)=\mathrm{true}$。该消息不是 Alice 曾经签名过的消息。

一个签名方案不可能是无条件安全的,因为对一个给定的消息 x,Oscar 使用公开算法 Vrfy_{pk} 测试所有可能的签名 y,直到发现一个有效的签名。因此,给定足够的时间,Oscar 总能对任何消息伪造 Alice 的签名。因此,和公钥密码体制一样,目标是找到计算上安全的签名方案。

第 2 章 基于单向性的签名

2.1 基于单向函数的签名

首先介绍一次性签名方案，因为其非常简洁，且具有构造签名的朴素思想。

2.1.1 Lamport 一次签名

1979 年，L. Lamport 提出基于任意单向函数的一次签名方案。该方案在单向函数是双射的条件下是可证明唯密钥攻击安全的。

所谓一次签名是指一对公、私钥只能用于对一个消息进行签名。每次签署消息都需要更新公钥。由于这种签名往往依赖单向函数或对称加密密钥算法，因而具有签名生成和签名验证高效的特点，故可应用在芯片卡等计算能力较低的环境。

Lamport 一次签名方案如下：

(1) 密钥生成。设 k 是一个正整数。假定 $f:Y\to Z$ 是一个单向函数，设随机选择的 $y_{i,j}\in Y, 1\leqslant i\leqslant k, j=0,1$。设 $z_{i,j}=f(y_{i,j}), 1\leqslant i\leqslant k, j=0,1$。密钥 K 由 $2k$ 个 y 和 $2k$ 个 z 构成，y 是私钥，z 是公钥。

(2) 签名生成。对于 $K=(y_{i,j},z_{i,j}: 1\leqslant i\leqslant k, j=0,1)$，定义

$$s=\mathrm{Sign}_K(x_1,x_2,\cdots,x_k)=(y_{1,x_1},y_{2,x_2},\cdots,y_{k,x_k})$$

(3) 签名验证。关于消息 $(x_1,x_2,\cdots,x_k)$ 的签名 $(s_1,s_2,\cdots,s_k)$ 验证如下：

$$\mathrm{Vrfy}_K((x_1,x_2,\cdots,x_k),(s_1,s_2,\cdots,s_k))=\mathrm{True}\Leftrightarrow f(s_i)=z_{i,x_i}$$

该签名方案的示意图如图 2.1 所示。根据消息的比特值，给出相应的私钥。非正式地说，有 $2k$ 套“锁-钥匙”对，即 $2k$ 把“锁”和 $2k$ 把“钥匙”。“锁”为公钥，“钥匙”为私钥(是秘密的)。明文中的每一位对应两套“锁-钥匙”对。根据明文中该位的比特为 0 或者为 1，亮出两把秘密“钥匙”中的一个。可见，一旦这把“钥匙”公开了，如果不更换“锁”，敌手就可以利用该“钥匙”伪造签名了。

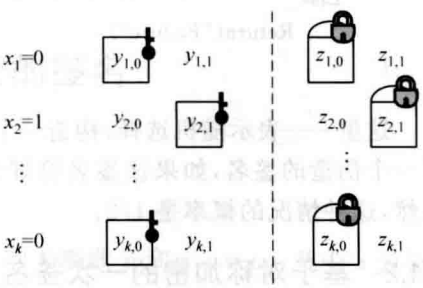


图 2.1 Lamport 一次签名方案

例 2.1 不妨设单向函数是 $f(x)=3^x \bmod 7879$，(3 是素数群 $\mathbb{Z}_{7879}^*$ 的生成元)，假定明文消息有 3 个比特，即 $k=3$。取私钥为

$$y_{1,0}=5831,\quad y_{1,1}=735$$
$$y_{2,0}=803,\quad y_{2,1}=2467$$
$$y_{3,0}=4285,\quad y_{3,1}=6449$$