装备科技翻译图书基金资助专著
国家自然科学基金面上项目资助（No.61170217）

[美]Jonathan Katz 著
任 伟 译
杨义先 审

数字签名

Digital Sig

国防工业出版社
National Defense Industry Press

装备科技翻译图书基金资助专著
国家自然科学基金面上项目资助(No.61170217)

数字签名

Digital Signatures

[美] Jonathan Katz(乔纳森·卡茨) 著
任 伟 译
杨义先 审

国防工业出版社
·北京·

著作权合同登记　图字:军-2011-113号

图书在版编目(CIP)数据

数字签名/(美)卡茨(Katz,J.)著;任伟译.—北京:国防工业出版社,2012.1

书名原文:Digital Signatures

ISBN 978-7-118-07810-7

Ⅰ.①数...　Ⅱ.①卡...②任...　Ⅲ.①密码-理论-高等学校-教材　Ⅳ.①TN918.1

中国版本图书馆CIP数据核字(2012)第001534号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路23号　邮政编码100048)

北京嘉恒彩色印刷有限责任公司

新华书店经售

*

开本700×1000　1/16　印张11¾　字数200千字

2012年1月第1版第1次印刷　印数1—2500册　定价39.00元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777　　发行邮购:(010)88540776

发行传真:(010)88540755　　发行业务:(010)88540717

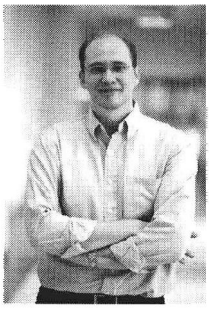
Preface to Chinese Edition

The goal of this book is to provide an accessible and comprehensive introduction to digital signature schemes, intended for graduate students and researchers in cryptography. In writing this book, I had hoped to reach a wide audience; I am thus particularly pleased that the book will now find an audience in China.

It was fortunate to be able to visit China a few years ago. While there, I had a chance to see the tremendous variety of academic cryptography research taking place in China, and to see the large number of students interested in this subject. I hope this book will inspire the next generation of researchers, and help foster international cooperation and collaboration for the advancement of scientific knowledge.

November 9, 2011

Jonathan Katz
Associate Professor
Department of Computer Science and UMIACS
Department of Electrical and Computer Engineering (affiliate)
Department of Applied Mathematics and Scientific Computation (affiliate)
University of Maryland



译者序

《数字签名》("Digital Signatures")是 Jonathan Katz 在 2010 年出版的一本专著,是在其出版了"Introduction of Modern Crytography-Principles and Protocols"(其中文版名为《现代密码学——原理与协议》,由国防工业出版社于 2011 年出版,也由本人翻译)一书后的又一本力作。

该书是第一本全面运用现代密码学方式(严谨的安全假设,精确的安全定义,严格的安全证明)对数字签名方案进行论述的专著。它全面介绍了可证明安全数字签名的最新进展、设计原理、构造方法和常用技术。全书内容包括三个部分:

(1) 预备知识:包括第 1 章数字签名的背景和定义,第 2 章密码学困难假设;

(2) 不需要随机预言模型的数字签名方案:包括第 3 章基于通用假设的构造方法,第 4 章基于(强)RSA 假设的签名方案,第 5 章基于双线性映射构造的方案;

(3) 基于随机预言模型的数字签名方案:包括第 6 章随机预言模型,第 7 章全域 Hash(及其相关)签名,第 8 章基于身份识别的签名方案。

全书论述严谨、深入浅出、选材新颖、逻辑清晰、形式统一规范,代表了当今可证明安全数字签名类专著的世界领先水平。可供从事现代密码学、信息安全和可证明安全理论及其应用的研究者、高等院校教师和研究生学习参考。

感谢中国密码学会副理事长、北京邮电大学长江学者杨义先教授审阅了译稿。感谢武汉大学张焕国教授和海军工程大学吴晓平教授的大力推荐。感谢新加坡管理大学 Robert H. Deng(邓慧杰)教授的大力帮助。感谢 Jonathan Katz 在百忙之中专门为中文版写序。感谢中国密码学会教育工作委员会的支持。感谢国防工业出版社和 Springer 出版社各位编辑的协助。本书的出版得到了 2011 年中国人民解放军总装备部装备科技翻译图书基金

资助,国家自然科学基金面上项目(No. 61170217)、中央高校基本科研业务费专项资金(No.090109)的资助,在此表示感谢。

由于本专著的翻译难度高,时间紧,加之译者水平有限,不足之处在所难免,敬请同行读者批评和指正。我的 Email 是:weirencs@cug.edu.cn。

任伟

2011 年 11 月于中国地质大学(武汉)

前　言

刚读研究生的时候，我曾经为缺乏学习（理论）密码学的资料而感到苦恼。这个困惑是：为什么没有更多讲述密码学基本知识的导论书籍呢？约10年之后的今天，作为一名大学教授，学生问我：什么是学习密码学（各个专题）的最佳资料？至少在数字签名方面，这本专著便是针对这两个问题的回答。①

基于以上动机，在写作本书的时候我一直牢记所要针对的读者群，即低年级研究生，他们对研究密码学感兴趣，并学习了一门密码学导论课程，但是并不清楚应该继续学些什么。虽然本书主要针对上述读者，我同样希望高年级研究生和研究人员能够发现本书的价值。在用统一的框架介绍各种构造数字签名方案的同时，本书可作为一个介绍各种研究成果的纲要，这些研究成果可能还没有得到应有的重视。本书还可作为研究生高级密码学研讨班的教材；在这一研讨课程中，我期望可在一个学期里轻松讲授完本书，并可留有时间涉足相关论题。但愿本书被证明对其他领域的研究生和研究人员同样是有帮助的，如从事计算机安全或数学研究的人员，即那些想彻底了解数字签名以及想获知该领域的一些研究结果的人。

本书唯一的预备知识是学习过一门涵盖现代密码学基础知识的课程（本科生或者研究生水平）。明确地说，本书假定读者已经学习了一门涵盖了我和 Yehuda Lindell 合著的《现代密码学——原理与协议》[72]一书②内容的课程。了解形式化定义和证明，熟悉诸如 RSA 问题、离散对数问题，以及单向函数的概念。在努力介绍所有的必要的背景知识的同时，读者会发现具备上述背景知识将会感到阅读起来更加容易。

本书分为三个部分：

- 第一部分——预备知识：这一部分包括相关背景知识，数字签名概

① 幸运的是，在过去的几年里出版了一些优秀的介绍密码学全貌以及密码学专题的书籍。

② 中文版已由国防工业出版社 2011 年 1 月出版，译者注。

论,签名方案的安全定义。即使是具备良好密码学背景知识的读者也应该浏览这一部分,因为这里包括如抗已知/随机消息攻击的"非标准"的定义,以及数字签名的"强"安全定义。

- 第二部分——不需要随机预言模型的数字签名方案。本书第二部分和第三部分涵盖了数字签名的构造。第二部分重点讲述不需要随机预言模型("random oracle" model)的可证明安全方案。(第6章简短地介绍了随机预言模型。)这一部分从一个重要的理论结果开始介绍:数字签名能从任何单向函数构造(仅给出一个基于单向置换的完整证明)。然后,介绍基于RSA和强RSA假设的构造方法。最后,介绍一些最近提出的基于双线性映射的构造方案。

据我所知,第二部分基本上描述了所有已经知道的不依赖随机预言模型的签名方案。

- 第三部分——需要随机预言模型的数字签名方案。在第二部分中描述的签名方案总体上来说不太实用。取而代之,可使用基于随机预言模型进行安全证明的更高效的方案。在简要介绍了随机预言模型(包括其优点和缺点)之后,我们讨论两种主要的构造方法:从基于身份识别方案构造签名;以及使用陷门置换或其变种通过"哈希然后签名"方法设计签名。

不幸的是,本书中省略了对基于包括背包问题、格、编码理论,以及多项式等式等"非数论"假设构造的签名方案的讨论。我同时决定重点讲述"标准"的签名方案,而不涵盖任何变种(如不可抵赖签名、环签名、群签名、同态签名等)。但是,从基本的理论角度而言本书仍具备一定的综合性,并且愿它能成为更多专题文献的入门读物。

建议和勘误

非常乐意收到反馈和建设性的批评意见使我能够改进本书。并始终感激(虽有点伤感)能够听到关于本书的错误或遗漏。请将任何意见电邮至 jkatz@ cs. umd. edu,并请在主题栏注明"Digital Signatures Book"。

鸣谢

非常感谢妻子 Jill 在写作本书期间所给予的坚定支持。感谢 Yehuda Lindell 和 Bob Stern 允许我在本书中选用文献[72]中的部分内容。最后,感谢 Susan Lagerstrom – Fife 在本书写作期间的耐心和鼓励(激励)。

本书部分内容是我在 IBM 进行学术休假期间完成的。非常感谢 Tal

Rabin 以及密码学研究组的所有成员在此期间的盛情相待。

本书部分工作受国家自然科学基金的资助，项目号 0447075，0627306 以及 0716651。本书中表达的任何观点、发现、结论或者建议都是我个人的，不必代表国家自然科学基金委员会的观点。

大学园（College Park），马里兰大学

Jonathan Katz

2010 年 3 月

目　录

第一部分　预备知识

第二部分 不需要随机预言模型的数字签名方案

第三部分 基于随机预言模型的数字签名方案

第一部分

预备知识

第1章
数字签名的背景和定义

1.1 数字签名方案简介

简单地说，数字签名方案提供了手写签名的密码学类比，其实它提供了更强的安全保障。数字签名作为一种强大的工具已被多个国家接受为具有法律效力；可用于合同或证书文件的证明，用于对个人或公司的认证，并可作为复杂安全协议的组成部分。数字签名同时能够用于安全的分发和传输公钥，因此从实用角度而言，它是所有公钥密码学的基础。

数字签名方案通常用于某个“签名者”和某个潜在的“验证者”集合。（这里的讨论将是非正式的；正式的定义将在后面给出。）签名者开始运行某个“密钥生成算法”，产生一对密钥(pk, sk)，这里pk称为签名者的公钥，因为它将在某个时刻公开，sk是签名者的私钥（有时候也称为“秘密密钥”）。签名者公开其公钥，本书将假定任何潜在的验证者都拥有（或能获取）一份经认证的该签名者公钥pk的拷贝。于是将不再关注签名者如何分发公钥的具体细节；实际上可以想象存在一个公开的目录将签名者和其公钥关联在一起，且该目录被妥善管理，即某人想以他人的名字登记公钥是不可行的。但是需要强调的是，通常存在多个签名者，每个均拥有自己的公钥，因而任何潜在的验证者必须知道合法的公钥的集合，而且也必须知道这些公钥是属于自己感兴趣的哪个签名者的。

一旦签名者如上所述建立了公钥pk，数字签名方案允许签名者以如下方式“验证”（或“签署”）某个消息：任何知道pk的其他人员可验证消息来自于签名者，并且未以任何方式被修改。具体而言，对于任意消息m（简单视其为一个比特串），签名者能够使用其私钥sk对m应用某个“签名算法”，生成签名σ，该签名可以被任何知道pk的人员利用“验证算法”进行验证。

在此考虑一个数字签名方案的典型应用：考虑某个软件公司以一种可认证的方式发布软件补丁或更新包，即当公司需要发布软件补丁的时候，其客户需要确认这一补丁是认证的，敌对的第三方将不能愚弄客户接受某个不是由公司发布的补丁。为了做到这一点，公司能够生成一个公钥pk及其私钥sk，然后以某种可靠的方式发布pk给其客户（可能在初次发布软件的时候捆绑发布公钥）。当发布补丁m时，公司使用其私钥sk计算关于m的签名σ，然后发布(m,σ)到网站上。每个客户都能在下载前使用相应的公钥pk，通过检查σ是否为合法签名来验证m的真实性。

敌对方可能通过篡改公司主页并发布(m',σ')来试图发布假补丁包，这里m'表示一个从未被公司发布的补丁。这个m'可能是某个以前发布的补丁m的修改版本，或者是崭新的与以前的补丁毫无关联。如果签名方案是“安全的”（后面将给出所谓“安全的”更详细的定义），那么当客户试图验证σ'时，将发现这是一个相对于pk的关于m'的“无效的”签名，因而将“拒绝”该签名。注意，在这一应用中一个十分关键的地方是：即使伪造的补丁m'仅仅是真正补丁的略微修改，客户也会拒绝这个签名。

上述不仅仅是一个数字签名的理论应用，而且在当今被大量的使用。（例如，微软公司在更新其视窗操作系统时就是使用该方法。）

他方能够获取签名者公钥的合法拷贝这一假设意味着签名者能够以一种可靠和认证的方式至少传输一个消息（即pk本身）。既然这样，有人可能会疑惑为什么还需要签名方案。这里的关键之处在于：可靠地发布pk是一个困难的任务，但是使用签名方案意味着这一过程只需要执行一次，此后不限数量的消息可以被可靠地发送。况且，签名方案本身用于在公钥基础设施（PKI）中确保可靠地发布其他的公钥。

数字签名的属性

如上，可看到数字签名提供了认证公开信道上传输的消息的一种方式。签名方案提供更强的属性，下面将通过比较消息鉴别码（message authentiction codes）来说明这些属性，消息鉴别码是数字签名在对称密钥情形下的类比。

消息鉴别码的定义如下：在某个发送者和某个接收者之间共享一个秘密密钥s。发送者使用s通过消息鉴别算法生成消息m的“标签”t。接收者收到m和t，能使用同样的s运用相应的验证过程验证m的真实性。如同数字签名，消息鉴别码提供的安全保证在于：没有一个敌对第三方在不知道s的情况下能够伪造一个对任意未曾认证过的消息m'而言是有效的标签t'（建议读者阅读文献[72]获得对消息鉴别码更深层次的讨论）。

因此，消息鉴别码和数字签名方案能用于确保传输消息的完整性（或认