

数学与现代科学技术丛书 7

可证明安全算法与协议

张 华 温巧燕 金正平 著



数学与现代科学技术丛书 7

可证明安全算法与协议

张 华 温巧燕 金正平 著



YZLI0890165502

科学出版社

北京

内 容 简 介

近年来,可证明安全算法与协议是信息安全、密码学等研究领域的重要问题之一.本书以作者及其课题组在该领域多年来的研究成果为主体,结合国内外学者的代表性成果,系统论述了可证明安全密码算法与协议的设计与分析,详细介绍了该研究方向的发展情况,并提出一些与之紧密相关的新研究课题.

全书分四部分,共17章.第一部分(第1~3章)系统介绍了密码算法和协议设计中的基础知识;第二部分(第4~6章)论述了可证明安全的加密体制;第三部分(第7~12章)对数字签名进行了深入研究;第四部分(第13~17章)阐述了可证明安全的密钥协商协议及其应用.

本书既可作为对可证明安全算法与协议感兴趣的读者的入门教材,也可作为可证明安全理论研究工作者的参考用书,同时适合密码学、信息安全、数学、计算机及相关学科的高年级本科生、研究生、教师和科研人员阅读参考.

图书在版编目(CIP)数据

可证明安全算法与协议/张华,温巧燕,金正平著. —北京:科学出版社, 2012

(数学与现代科学技术丛书; 7)

ISBN 978-7-03-033540-1

I. ①可… II. ①张… ②温… ③金… III. ①密码算法 ②密码协议
IV. ①TN918.1

中国版本图书馆CIP数据核字(2012)第022865号

责任编辑:王丽平 房 阳/责任校对:李 影

责任印制:钱玉芬/封面设计:陈 敬

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>

双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2012年3月第 一 版 开本:B5(720×1000)

2012年3月第一次印刷 印张:33 3/4

字数:656 000

定价:98.00 元

(如有印装质量问题,我社负责调换)

《数学与现代科学技术丛书》序

当代数学在向纵深发展的同时,被空前广泛地应用于几乎一切领域.一方面,它与其他学科交汇,形成了许许多多交叉学科(例如,信息科学、计算机科学、系统科学、数学物理、数学化学、生物数学、数学语言学、数量经济学、金融数学、复杂性科学、科学计算等);另一方面,它又被应用于高新技术的开发(例如,信息安全、信息传输、图像处理、语音识别、网络、海量数据处理、网页搜索、遥测遥感、交通管理、医疗诊断、手术方案、药物检验、商业广告等方面),成为一些高新技术的核心.应用数学的这种发展趋势急剧地扩展了数学的疆界,也深刻地改变了数学的面貌.

中国的经济正在迅猛发展,其中的科技含量也与日俱增.为了提高自主创新能力,我国已经有不少数学工作者投身于这类应用数学的研究中,还有更多的数学工作者则正在密切关注这方面的进展,看好它的前景.愈来愈多的人希望了解这类应用数学的现状,寻找入门之径.

《数学与现代科学技术丛书》是力图反映这个发展趋势的一套应用数学丛书,它将较全面地向我国读者介绍当今数学在现代科学技术各个领域中的应用的状况,通过必要的准备知识,逐步把读者引向相关的研究前沿.

从事交叉学科研究和高新技术开发的应用数学家,除了要精通所需的数学知识外,还必须深入了解其所研究问题的来龙去脉.“建模”是应用数学研究实际问题的关键.这也是一门数学艺术:从复杂的实际问题中抽象出关键的“量的关系”,使得既能反映出问题的基本特征,又能用现阶段的数学工具加以处理.有鉴于此,这套丛书的一个特点就是:不但要介绍有关的数学理论和方法,还必须介绍问题的来源与背景、数学建模以及如何运用数学工具来解决实际问题.

本书适用于数学及相关专业的大学生和研究生,以及与数学有关的各专业科技工作者.

张恭庆

2009年11月

前 言

随着全球信息化程度的日益提高,信息安全问题已经由个人、团体的隐私与机密保护问题上升为国家的战略性问题.密码算法和协议是解决网络安全问题最直接、最有效的手段之一,是构建安全信息系统的基本要素.在计算机网络和通信系统中,通信各方通过采用密码算法和协议实现消息加密、密钥分配、身份与消息认证、行为不可否认和安全电子交易等功能.

可证明安全性理论与技术是一种安全可靠的密码分析方法,它在适当的模型下,把高层的密码算法和协议的复杂安全性归约为底层的极微本原的简单安全性.它又是一种科学而高效的密码设计方法:其模块化的设计思路使得密码算法和协议的设计人员不再拘泥于极为困难的极微本原的设计,而是直接以极微本原为工具,以形式化的安全性定义为参照,再结合具体的模型来设计密码算法和协议,从而大大提高了设计效率.

加密体制、数字签名和密钥协商是密码算法和协议的核心内容.加密体制为保证信息的机密性提供了重要的技术手段.根据密钥的特点,可将加密体制分为对称密钥体制和非对称密钥体制两种.一般来说,对称密钥体制具有计算量少、效率高等优点,而非对称密钥体制具有无需预共享密钥的优势.因此,两类加密体制的研究都取得了长足的发展.与非对称密钥体制的思想类似,数字签名技术利用公私钥对实现了对消息的完整性认证、消息发送者身份的认证和不可抵赖性等功能.数字签名的研究是密码技术发展的重要分支之一,受到学术界与产业界的广泛关注.在此基础上,为满足实现需求的特殊功能,各种具有特殊功能的数字签名方案(如盲签名、代理签名、签密等)也相继出现,目前已取得了一系列的研究成果.密钥协商协议允许通信的双方或多方在一个不安全的开放网络上联合建立秘密密钥,是实现保密通信的重要技术手段之一.安全高效的密钥协商协议可用于构建安全、复杂、高层的安全协议,与数字签名等密码技术结合可以形成具有广泛应用价值的密码算法,在密钥管理、数据安全、保密通信以及各种电子商务中具有不可低估的应用价值.关于密钥协商协议的设计与分析研究也得到了蓬勃发展,适用于不同应用场景需求的密钥协商协议不断涌现.

近年来,可证明安全密码算法和协议的研究一直很活跃,出现了一系列的学术论文和博士、硕士学位论文,取得了丰硕的研究成果和较显著的发展.但从目前的研究情况看,可证明安全密码算法和协议的许多问题还值得进一步研究.

本书旨在系统论述现代密码学中可证明安全密码算法和协议,以作者及其课题

组多年的研究成果为重点,汇集了国内外学者在这方面的研究成果.对相关领域的理论工作者、研究生以及高年级本科生的专业课题研究有一定的参考价值.

全书共分四部分.第一部分重点论述了可证明安全理论以及密码算法和协议的基础理论.第二部分对加密体制进行了研究,除了介绍经典的加密算法外,重点介绍了典型的可证明安全加密体制.第三部分重点介绍了一系列可证明安全的数字签名及具有特殊功能的数字签名方案.第四部分重点介绍了可证明安全的密钥协商协议及其应用.作为专著,本书集中论述了课题组及国内外的相关成果,对密码学基础知识只做简单的介绍,感兴趣的读者可参考其他相关书籍.

作者对课题组成员李文敏博士、郭瑞博士、孙海燕博士、徐洁硕士、张敏硕士等给予的密切配合,以及北京邮电大学网络与交换技术国家重点实验室网络安全研究中心全体老师和支持表示感谢.本书第二部分由郭瑞博士协助完成,第四部分由李文敏博士、孙海燕博士协助完成,再次向他们深表谢意.

最后,本书的出版得到了以下项目的资助:国家自然科学基金项目(编号:60873191, 60821001, 60903152)、中央高校基本科研业务费专项资金资助项目(编号:BUPT2011YB01, BUPT2011RC0505, BUPT2011RCZJ15)等,在此特别表示感谢.

由于作者水平有限,时间仓促,书中不妥之处在所难免,恳请读者指正.

作 者

2011 年 6 月于北京

目 录

《数学与现代科学技术丛书》序

前言

第一部分 基础知识

第 1 章 数学基础	3
1.1 数论	3
1.1.1 同余及剩余类	3
1.1.2 中国剩余定理	6
1.1.3 欧拉函数 $\varphi(n)$	7
1.1.4 二次剩余	9
1.1.5 素性检测	11
1.2 复杂性理论	13
1.2.1 计算复杂性与时间复杂性	13
1.2.2 复杂性分类	15
1.2.3 随机算法	17
1.3 信息论	18
参考文献	24
第 2 章 密码学基础	27
2.1 密码体制	27
2.1.1 对称加密体制	28
2.1.2 公钥加密体制	29
2.1.3 两者的比较	29
2.2 数字签名	30
2.2.1 基本概念及原理	31
2.2.2 经典算法	32
2.3 Hash 函数	34
2.4 伪随机函数	35
2.4.1 伪随机序列生成器	35
2.4.2 伪随机函数	37

2.5 消息认证码	37
2.5.1 对 MAC 的要求	38
2.5.2 基于 DES 的 MAC	39
2.6 零知识证明	40
参考文献	42
第 3 章 可证明安全理论基础	44
3.1 基本思想	44
3.2 困难问题假设	45
3.3 安全模型	49
3.3.1 数字签名方案的安全模型	49
3.3.2 公钥加密方案的安全模型	51
3.4 RO 模型和标准模型方法论	52
参考文献	54

第二部分 加 密 体 制

第 4 章 对称加密	57
4.1 分组密码与数据加密标准	57
4.1.1 分组密码的设计原则	57
4.1.2 分组密码的结构	58
4.1.3 数据加密标准	59
4.1.4 分组密码分析	63
4.2 序列密码	63
4.2.1 序列密码原理	64
4.2.2 序列密码对密钥流的要求	64
4.2.3 密钥流生成器	65
4.2.4 移位寄存器序列	66
参考文献	69
第 5 章 公钥密码	71
5.1 RSA 密码体制	71
5.1.1 算法描述	71
5.1.2 RSA 的参数选择	72
5.1.3 RSA 的安全性	73
5.2 ElGamal 密码体制	75
5.3 椭圆曲线密码体制	76

5.3.1 椭圆曲线	76
5.3.2 椭圆曲线密码体制	77
参考文献	78
第 6 章 可证明安全加密体制	80
6.1 可证明安全的私钥加密体制	81
6.1.1 计算安全	81
6.1.2 计算安全的私钥加密体制	84
6.1.3 构造计算安全的私钥加密体制	88
6.1.4 私钥加密体制中的 CPA 与 CCA 安全	92
6.2 可证明安全的公钥加密体制	94
6.2.1 公钥加密方案的安全性	94
6.2.2 RSA-OAEP	102
6.2.3 Cramer-Shoup 公钥加密方案	106
6.2.4 可证明安全的混合密码体制	109
参考文献	111

第三部分 数 字 签 名

第 7 章 可证明安全数字签名方案	117
7.1 数字签名研究概述	117
7.2 基于身份的数字签名的定义及安全模型	120
7.3 几个典型的基于身份的数字签名方案	121
7.3.1 Shamir 的基于身份的数字签名方案	121
7.3.2 Hess 的基于身份的数字签名方案	122
7.3.3 Cha-Cheon 的基于身份的数字签名方案	123
7.3.4 Barreto-Libert-McCullagh-Quisquater (BLMQ) 签名方案	123
7.3.5 Paterson-Schuldt (PS) 签名方案	123
7.3.6 方案性能比较	124
7.4 一个高效的基于身份的短签名方案	125
7.4.1 基本方案	125
7.4.2 安全性分析	126
7.4.3 效率分析	128
7.5 无证书数字签名的定义及安全模型	129
7.6 一个高效的无证书短签名方案	131
7.6.1 方案构造	132

7.6.2 安全性分析	133
7.6.3 效率分析	137
7.7 可追踪的基于身份的数字签名的定义及安全模型	137
7.8 一个可追踪的基于身份的签名方案	139
7.8.1 基本方案	139
7.8.2 方案的安全性分析	140
7.8.3 效率分析	143
7.9 具有特殊功能的数字签名	144
参考文献	144
第 8 章 盲签名	152
8.1 盲签名简介	152
8.2 基于身份的盲签名	154
8.2.1 基于身份的盲签名定义及安全模型	154
8.2.2 经典方案	156
8.2.3 安全性分析	157
8.3 无证书盲签名方案的设计	158
8.3.1 方案描述	159
8.3.2 安全性分析	161
8.3.3 效率比较	162
8.4 具有消息恢复的无证书盲签名	162
8.4.1 方案描述	163
8.4.2 安全性分析	165
参考文献	166
第 9 章 代理签名	168
9.1 代理签名简介	168
9.1.1 代理签名的安全性	168
9.1.2 代理签名的分类	169
9.2 基于身份的代理签名	171
9.2.1 基于身份的代理签名定义及安全模型	171
9.2.2 经典方案	173
9.2.3 安全性分析	174
9.3 无证书代理签名	178
9.3.1 无证书强代理签名定义及安全模型	179
9.3.2 无证书强代理签名方案	180
9.3.3 无证书强代理签名方案的安全性与效率分析	181

9.4 无证书多重代理签名	184
9.4.1 多重代理签名简介	184
9.4.2 无证书多重代理签名的定义及安全模型	185
9.4.3 无证书多重代理签名方案	187
9.4.4 方案的安全性结果	189
参考文献	190
第 10 章 多重签名与聚合签名	193
10.1 多重签名简介	193
10.1.1 多重签名的分类	193
10.1.2 多重签名的研究概述	194
10.2 基于身份的多重签名	195
10.2.1 基于身份的多重签名的定义及安全模型	195
10.2.2 经典方案	196
10.2.3 安全性分析	198
10.3 无证书代理多重签名的形式化构造	201
10.3.1 无证书代理多重签名的定义及安全模型	202
10.3.2 无证书代理多重签名方案	204
10.3.3 方案的安全性证明	206
10.4 聚合签名简介	215
10.5 基于身份的聚合签名	216
10.5.1 基于身份的聚合签名的定义和安全模型	216
10.5.2 对 Song-Kim-Lee-Yoon 方案的安全性分析	217
10.5.3 基于身份的聚合签名方案	219
10.5.4 方案的安全性及效率分析	220
10.6 无证书聚合签名	223
10.6.1 无证书聚合签名的形式化定义	223
10.6.2 无证书聚合签名的安全模型	223
10.6.3 无证书聚合签名方案的设计	225
10.6.4 无证书聚合签名方案的安全性证明及效率比较	226
参考文献	232
第 11 章 指定验证者签名	237
11.1 指定验证者签名简介	237
11.2 基于身份的强指定验证者签名	239
11.2.1 形式化定义	240
11.2.2 安全性要求	240

11.3 基于身份的强指定验证者签名方案的分析与改进	241
11.3.1 Li 等基于身份的强指定验证者签名方案及安全性分析	241
11.3.2 改进方案	242
11.3.3 安全性证明及效率比较	244
11.4 无证书指定验证者签名方案	248
11.4.1 无证书指定验证者签名的定义	248
11.4.2 方案构造	249
11.4.3 安全性分析	250
11.4.4 效率分析	252
11.5 无证书指定验证者代理签名方案	253
11.5.1 方案描述	254
11.5.2 安全性分析	256
参考文献	256
第 12 章 签密	259
12.1 签密简介	259
12.2 基于身份的签密方案的定义和安全模型	262
12.3 基于身份的签密方案分析与改进	264
12.3.1 Yu 等基于身份的签密方案及其语义安全性分析	264
12.3.2 改进的基于身份的签密方案及其安全性证明	266
12.4 多 PKG 环境下基于身份的签密	269
12.4.1 多 PKG 环境下基于身份的签密定义及安全模型	270
12.4.2 多 PKG 环境下基于身份的签密方案	271
12.4.3 安全性和效率分析	273
12.5 无证书签密	279
12.5.1 无证书签密的定义及其安全模型	279
12.5.2 Liu 等的无证书签密方案及其存在的安全缺陷	283
12.5.3 对 Liu 等方案所存在漏洞的补救	285
参考文献	288

第四部分 密 钥 协 商

第 13 章 密钥协商概述	293
13.1 引言	293
13.2 密钥协商协议的分类	296
13.3 几个典型的密钥协商协议	298

13.3.1 最早的密钥协商协议 —— Diffie-Hellman 协议	298
13.3.2 Joux 的三方协议	299
13.3.3 Burmester 和 Desmedt 的组密钥协商协议	300
参考文献	300
第 14 章 基于 PKI 的密钥协商协议	303
14.1 CK 类模型下基于 PKI 的两方密钥协商协议	303
14.1.1 CK01 模型	304
14.1.2 eCK 模型	306
14.1.3 AM 下会话密钥安全的 DH 协议	307
14.1.4 UM 下会话密钥安全的 DH 协议	309
14.2 mBPR 模型下基于 PKI 的两方密钥协商协议	310
14.2.1 mBPR 模型介绍	310
14.2.2 T-KA 协议与安全性证明	311
14.3 mKY 模型下基于 PKI 的组密钥协商协议	312
14.3.1 mKY 模型介绍	313
14.3.2 TR-GKA 协议与安全性证明	314
参考文献	317
第 15 章 基于身份的密钥协商协议	321
15.1 ID-mBJM 模型下基于身份的两方密钥协商协议	321
15.1.1 ID-BJM 模型介绍	322
15.1.2 ID-mBJM 模型介绍	324
15.1.3 ID-mBJM 模型下的模块化证明方法	326
15.1.4 RYY ⁺ 协议与安全性证明	327
15.2 ID-eCK 模型下基于身份的两方密钥协商协议	332
15.2.1 ID-eCK 模型介绍	332
15.2.2 HC 协议与安全性证明	333
15.3 基于身份的树状群组密钥协商协议	342
15.3.1 STR-IDGKA 协议	342
15.3.2 基于 STR-IDGKA 协议的成员事件	344
15.3.3 STR-IDGKA 协议的安全性	345
15.3.4 协议的效率分析	348
15.4 ID-mBCPQ 模型下基于身份的常数轮群组密钥协商协议	348
15.4.1 ID-mBCPQ 模型介绍	349
15.4.2 协议描述和安全性证明	351
参考文献	353

第 16 章 基于口令的密钥协商协议	357
16.1 BPR 模型下基于口令的两方密钥协商协议	357
16.1.1 BPR 模型描述	358
16.1.2 定义	361
16.1.3 OEKE 协议及其安全性证明	362
16.1.4 KOY/GL 框架	369
16.1.5 JG/GK 框架	385
16.2 UC 模型下基于口令的两方密钥协商协议	390
16.2.1 UC 框架	391
16.2.2 组合 JUC	394
16.2.3 设计 UC 安全的密码学协议的步骤	395
16.2.4 常见的基于口令的两方密钥协商协议的理想功能	395
16.2.5 CAPKE 协议及其安全性证明	398
16.3 BPR 模型下基于口令的三方密钥协商协议	404
16.3.1 3PAKE 的 BPR 模型介绍	404
16.3.2 三个协议及其安全性证明	409
16.4 CK 类模型下基于口令的三方密钥协商协议	419
16.4.1 Y-eCK 模型描述	419
16.4.2 Y-3PAKE 协议及其安全性证明	423
16.5 ROR 模型下跨域的客户端到客户端的口令认证密钥协商协议	430
16.5.1 跨域的 C2C-PAKE 的 ROR 模型描述	430
16.5.2 C2C-GPAKE 协议及其安全性证明	433
16.6 UC 模型下跨域的客户端到客户端的口令认证密钥协商协议	438
16.6.1 跨域的 C2C-PAKE 的理想功能	438
16.6.2 C2C-HPAKE 协议及其安全性证明	439
16.7 验证元模型下基于口令的密钥协商协议	445
16.7.1 基于验证元的三方口令认证密钥协商协议	446
16.7.2 椭圆曲线下基于验证元的三方口令认证密钥协商协议	449
16.8 BPR 模型下基于口令的群组密钥协商协议	452
16.8.1 PGKE 的 BPR 模型介绍	452
16.8.2 两个协议及其安全性证明	456
16.9 ROR 模型下基于口令的群组密钥协商协议	465
16.9.1 PGAKE 的 ROR 模型介绍	465
16.9.2 WZ-PAGKE 协议及其安全性证明	466
参考文献	472

第 17 章 密钥协商协议的应用	479
17.1 密钥协商协议在 SIP 协议中的应用	480
17.1.1 SIP 协议介绍	480
17.1.2 CK 模型下适用于 SIP 的密钥协商协议	481
17.2 密钥协商协议在 RDP 协议中的应用	482
17.2.1 RDP 介绍	483
17.2.2 一个新的 RDP 密码学套件	485
17.3 密钥管理协议在 HSN 中的应用	490
17.3.1 异构传感器网络 HSN 介绍	490
17.3.2 HSN 跨层密钥管理设计思路	491
17.3.3 基于 E-G 方案的 HSN 跨层密钥管理协议	492
17.4 密钥协商协议在数字版权保护中的应用	496
17.4.1 数字版权保护介绍	496
17.4.2 一种基于身份标识的口令进化的会话密钥方案	497
17.5 密钥协商协议在移动应用中的应用	501
17.5.1 移动应用介绍	501
17.5.2 一个适用于移动应用的口令认证多密钥协商协议	503
17.6 密钥协商协议在车载自组织网络中的应用	509
17.6.1 车载自组织网络介绍	509
17.6.2 一个适用于车载自组织网络的电子支付协议	510
参考文献	519
《数学与现代科学技术丛书》已出版书目	522

第一部分 基础知识

