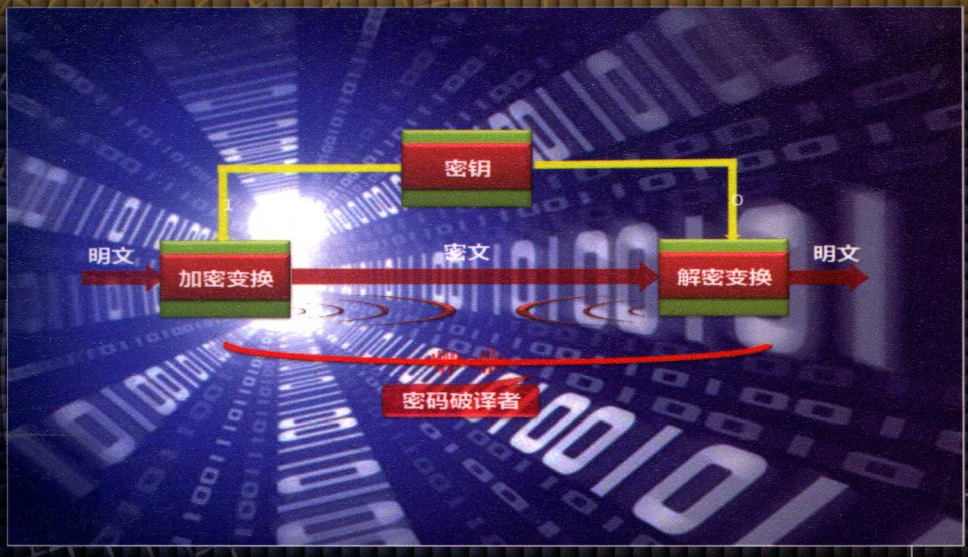
国防科技图书出版基金

网络与信息安全前沿技术丛书

密码学的基本理论与技术

张文政 陈克非 赵 伟 编著

Basic Theory and Technique of Cryptography



国防工业出版社
National Defense Industry Press

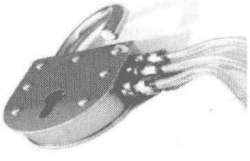
国防科技图书出版基金

网络与信息安全前沿技术丛书

张文政　陈克非　赵　伟　编著

密码学的基本理论与技术

Basic Theory and Technique of Cryptography



人们在享受信息网络带来的巨大利益的同时，也面临着信息安全问题的严峻考验。伪基站窃取个人信息，向用户强行发送垃圾信息或诈骗信息；移动互联网更易成为攻击的目标，攻击手段将会变得更加隐蔽和难防；物联网的安全问题也亟待解决，……解决这些问题的关键和核心技术就是密码学。本书全面给出了密码学的基本原理及其在实际中的应用；不仅回顾了古典密码，而且给出了密码学的最新研究成果。

国防工业出版社
National Defense Industry Press
·北京·

图书在版编目(CIP)数据

密码学的基本理论与技术 / 张文政,陈克非,赵伟编著. —北京:国防工业出版社,2015.11
(网络与信息安全前沿技术丛书)
ISBN 978-7-118-10223-9

Ⅰ.①密… Ⅱ.①张… ②陈… ③赵… Ⅲ.①密码-研究 Ⅳ.①TN918.1

中国版本图书馆 CIP 数据核字(2015)第 198232 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 710×1000 1/16 印张 19¼ 字数 353 千字
2015 年 11 月第 1 版第 1 次印刷 印数 1—3000 册 定价 98.00 元

国防书店:(010)88540777 发行邮购:(010)88540776
发行传真:(010)88540755 发行业务:(010)88540717

致 读 者

本书由国防科技图书出版基金资助出版。

国防科技图书出版工作是国防科技事业的一个重要方面。优秀的国防科技图书既是国防科技成果的一部分，又是国防科技水平的重要标志。为了促进国防科技和武器装备建设事业的发展，加强社会主义物质文明和精神文明建设，培养优秀科技人才，确保国防科技优秀图书的出版，原国防科工委于1988年初决定每年拨出专款，设立国防科技图书出版基金，成立评审委员会，扶持、审定出版国防科技优秀图书。

国防科技图书出版基金资助的对象是：

1. 在国防科学技术领域中，学术水平高，内容有创见，在学科上居领先地位的基础科学理论图书；在工程技术理论方面有突破的应用科学专著。

2. 学术思想新颖，内容具体、实用，对国防科技和武器装备发展具有较大推动作用的专著；密切结合国防现代化和武器装备现代化需要的高新技术内容的专著。

3. 有重要发展前景和有重大开拓使用价值，密切结合国防现代化和武器装备现代化需要的新工艺、新材料内容的专著。

4. 填补目前我国科技领域空白并具有军事应用前景的薄弱学科和边缘学科的科技图书。

国防科技图书出版基金评审委员会在总装备部的领导下开展工作，负责掌握出版基金的使用方向，评审受理的图书选题，决定资助的图书选题和资助金额，以及决定中断或取消资助等。经评审给予资助的图书，由总装备部国防工业出版社列选出版。

国防科技事业已经取得了举世瞩目的成就。国防科技图书承担着记载和弘扬这些成就，积累和传播科技知识的使命。在改革开放的新形势下，原国防科工委率先设立出版基金，扶持出版科技图书，这是一项具有深远意义的创举。此举势必促使国防科技图书的出版随着国防科技事业的发展更加兴旺。

设立出版基金是一件新生事物，是对出版工作的一项改革。因而，评审工作需

要不断地摸索、认真地总结和及时地改进，这样，才能使有限的基金发挥出巨大的效能。评审工作更需要国防科技和武器装备建设战线广大科技工作者、专家、教授，以及社会各界朋友的热情支持。

让我们携起手来，为祖国昌盛、科技腾飞、出版繁荣而共同奋斗！

国防科技图书出版基金
评审委员会

国防科技图书出版基金
第七届评审委员会组成人员

主任委员	潘银喜			
副主任委员	吴有生	傅兴男	杨崇新	
秘书长	杨崇新			
副秘书长	邢海鹰	谢晓阳		
委员 （按姓氏笔画排序）	才鸿年	马伟明	王小谟	王群书
	甘茂治	甘晓华	卢秉恒	巩水利
	刘泽金	孙秀冬	芮筱亭	李言荣
	李德仁	李德毅	杨　伟	肖志力
	吴宏鑫	张文栋	张信威	陆　军
	陈良惠	房建成	赵万生	赵凤起
	郭云飞	唐志共	陶西平	韩祖南
	傅惠民	魏炳波		

《网络与信息安全前沿技术丛书》编委会

丛书序

网络的触角正伸向全球各个角落，高速发展的信息技术已渗透到各行各业，不仅推动了产业革命、军事革命，还深刻改变着人们的工作、学习和生活方式。然而，在人们享受信息技术带来巨大利益的同时，一次又一次网络信息安全领域发生的重大事件告诫人们，网络与信息安全已直接关系到国家安全和社会稳定，成为我们面临的新的综合性挑战，没有过硬的技术，没有一支高水平的人才队伍，就不可能在未来国际博弈中赢得主动权。

网络与信息安全是一门跨多个领域的综合性学科，涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等。“道高一尺、魔高一丈”，网络与信息安全技术在博弈中快速发展，出版一套覆盖面较全、反映网络与信息安全方面新知识、新技术、新发展的丛书有着十分迫切的现实需求。

适逢此时，欣闻由我国网络与信息安全领域著名专家何德全院士任编委会主任，以国家保密通信重点实验室为核心，集聚国内信息安全界知名专家学者，潜心数年编写的《网络与信息安全前沿技术丛书》即将分期出版。丛书有如下特点：一是全面系统。丛书涵盖了密码理论与技术、网络与信息安全基础技术、信息安全防御体系，以及近年来快速发展的大数据、云计算、移动互联网、物联网等方面的安全问题。二是适应面宽。丛书既很好地阐述了相关概念、技术原理等基础性知识，又较全面介绍了相关领域前沿技术的最新发展，特别是凝聚了作者

们多年来在该领域从事科技攻关的实践经验，可适应不同层次读者的需求。三是权威性好。编委会由我国网络和信息安全领域权威专家学者组成，各分册作者又均为我国相关领域的知名学者、学术带头人，理论水平高，并有长期科研攻关的丰富积累。

我认为该丛书是一套难得的系统研究网络信息安全技术及应用的综合性书籍，相信丛书的出版既能为公众了解信息安全知识、提升安全防护意识提供很好的选择，又能为从事网络信息安全人才培养的教师和从事相关领域技术攻关的科技工作者提供重要的参考。

作为特别关注网络信息安全技术发展的一名科技人员，我特别感谢何德全院士等专家学者为撰写本书付出的艰辛劳动和做出的重要贡献，愿意向读者推荐该套丛书，并作序。

前言

信息技术的快速发展已经渗透到各行各业，特别是国际互联网的出现，改变了人们的生活、学习和工作模式，现在很多业务直接可从网络来操作，如网上购物、保密可视会议、保密信息的传递。信息技术也使得军事技术、武器装备、作战思想、作战方式、战争形态、军事原则、军事指令等都发生了深刻变化，从最近的伊拉克战争、阿富汗战争、利比亚战争到恐怖头目拉登的被击毙来看，现在战争都是信息化的一体化战争。信息的传递、存储和保护都离不开密码技术。信息安全的5个基本属性都需要用密码技术来保护，因此密码技术是信息安全的核心技术。其主要用途是对信息进行加密保护，对信息的来源进行鉴定，对信息的完整性进行检验。

本书内容实用，理论联系实际，反映了目前密码学的最新研究现状。本书强调理论与实际结合，传统密码理论与最新密码方法结合，公开研究成果与著者本人研究成果结合，有较高的学术水平和广泛的应用价值。

密码学技术本身发展也是很快的，所以本书的编写内容与当代密码技术的发展是适应的。

本书共分10章，包括引言、古典密码学、香农理论与计算复杂度、数论与近世代数基础、分组密码、序列密码、公钥密码、Hash算法、安全性证明、密钥管理。

本书的写作得到保密通信重点实验室基金项目(9140C110203140C11049)资助。

参与本书编写工作的有：张文政、陈克非，负责整本书的规划，并编写了第1章；赵伟主要编写了第6章；董新锋主要编写了第5章；张李军主要编写了第3章和第10章；汤殿华主要编写了第2章和第10章；毛贤平主要编写了第4章；王亮亮主要编写了第7章；叶君耀主要编写了第8章；王会歌主要编写了第9章。全书的编写得到了中国电子科技集团公司第三十研究所和保密通信重点实验室的支持，特别是祝世雄、田波、曾兵、刘义铭等给予了全力协作和帮助，在此一并对他们表示衷心的感谢！最后特别感谢国防工业出版社王晓光编辑认真、详实、全面的核对和对该书付出的

精心指导!

限于我们的水平和经验不足,书中的错误和缺憾在所难免,诚恳地希望读者对书中的错误和问题能够及时指出。我们欢迎对本书的批评和建议。

编著者

2015 年 6 月

于保密通信重点实验室

目　录