组合密码学

Combinatorial Cryptography

沈世镒 著

应用数学丛书

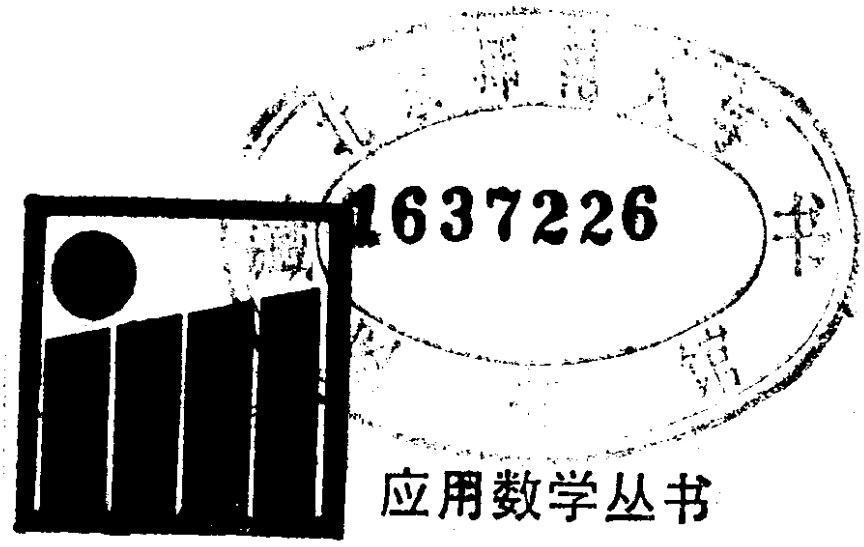
The Series of Applied Mathematics

组合密码学

沈世镒著

浙江科学技术出版社

J911546



组合密码学

沈世镒著

*

浙江科学技术出版社出版
江苏金坛县彩色印刷一厂排版
浙江新华印刷厂印刷
浙江省新华书店发行

开本：850×1168 1/32 印张：6
字数：135,000
1992年6月第一版
1992年6月第一次印刷
印数：1—1,500

ISBN 7-5341-0423-8/O·13
定价：7.00元

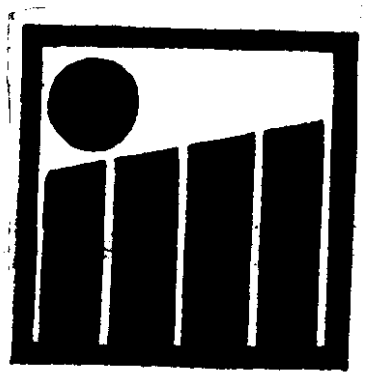
责任编辑：周伟元
封面封计：孙菁

Published by Zheiiang Pubjishing House
of Science and Technology
69 Tiyuchang Road, Hangzhou, Cnina
© 1992 by Shen Shzyi
First published 1992
Printed in Xinhua Printing Factory
Library of Congress Catalogue Card:
ISBN 7-5341-0423-8/O·13
Eitor: Zhou Weiyuan
Cover Design:Sun jing

Combinatorial Cryptography

Shen Shiyi

Zhejiang Publishing House of Science and Technology



The Series of Applied Mathematics

出版说明

在近代科技发展中，应用数学在国民经济和科学研究的各个领域的作用和地位显得日益重要，世界上许多发达国家对它非常重视，投入了大量的资金和研究力量。我国在这方面的研究工作也已有一定的规模和成果。我们为了推进和交流应用数学的成果，在苏步青教授、吴文俊教授的关怀下，由谷超豪教授为主编，组织出版这套“应用数学丛书”。

本“丛书”的出版，得到了数学界的重视。陈省身教授、杨振宁教授对此给予热情的鼓励和支持。国家自然科学基金会对“丛书”的出版非常重视。

为了反映应用数学在各主要分支的现代水平，特别是我国数学家的研究成果，以及国外的最新进展，向读者介绍应用数学的理论和各种方法、数学模型，“丛书”计划在数学物理、经济数学、组合设计、运筹学、控制理论、应用统计、通信理论、生物数学、几何造型等应用分支出版一些质量较高的专著。

我们希望“丛书”的出版，能为中国数学赶超世界水平作出一点贡献。

此为试读，需要完整PDF请访问：www.ertongbook.com

“应用数学丛书”编委会

名誉主编

苏步青　　吴文俊

主　　编

谷超豪

编委（按姓氏笔划）

王兴华	叶其孝	叶彦谦
刘鼎元	孙和生	史树中
李大潜	李训经	李翊神
吴　方	吴立德	萧树铁
张尧庭	林　群	俞文鉷
郭仲衡	郭竹瑞	游兆永
管梅谷		

Editorial Committee of Applied Mathematics Series

Honor Editor-in-Chief

Su Buqing Wu Wenjun

Editor-in-Chief

Gu Chaohao

Editorial Committee

Guan Meigu	Guo Zhongheng
Guo Zhurui	Li Daqian
Li Xunjing	Li Yishen
Lin Qun	Liu Dingyuan
Shi Shuzhong	Sun Hesheng
Wang Xinghua	Wu Fang
Wu Lide	Xiao Shutie
Ye Qixiao	Ye Yanqian
You Zhaoyong	Yu Wenci
Zhang Yaoting	

内 容 简 介

本书以组合方法为基础，讨论了非线性复杂度（NLC），*M*-序列的正规表示与复合前馈序列等问题。

对NLC我们给出了它的递推算法，引进了一个叫剩余度的问题。这是一个对任何已给的周期序列求全体非线性移位寄存器综合解的问题。我们还给出了对随机序列平均NLC的估计。所谓*M*-序列的正规表示，是把全体*M*-序列与一个密钥空间的密钥参数1-1对应，且有相应的算法计算。对复合前馈序列，我们给出了相关免疾函数的判别与构造。

许多结果为作者近期所得。本书可供从事数学、信息论与密码学的有关人员学习参考。

ABSTRACT

Based on combinatorial method, we consider the nonlinear complexity (NLC), normal representation of M-sequence and the composite feedforward sequences.

A recursive algorithm is given for the NLC. A redundancy problem is introduced, which is for finding all synthetic solutions of the nonlinear feedback shift regester is given any period sequence. The average NLC of a random sequence is estimated. The normal representation of M-sequence is to construct a key space and an algorithm. The space is to represent all M-sequence and the algorithm is an one-to-one correspondence between the key parameters and all M-sequences. For the composite feedforward sequences, we consider the construction and decision problem of the correlation-immunity function.

Many results are obtained recently by the author. This book has been written for related specialists in mathematics, information theory and cryptography.

序　言

在近代密码理论中，序列密码理论仍是一个十分重要的部分，其中移位寄存器理论是一个经典的代数问题，有许多论文与著作进行研究．近几年内，人们在M-序列的构造方面继续进行研究之外，对随机序列、复合前馈序列的研究十分重视．该书用组合方法对上述问题作进一步研究，在非线性复杂度、M-序列的规范表示，复合前馈序列的相关免疫性等方面获得了一系列重要结果．这是目前在国内外这方面研究的最新成果．

关于序列的复杂度（线性的或非线性的）问题是序列密钥体制的基础，但人们的注意力较多的集中在线性复杂度的情形．本书首先讨论了线性复杂度与非线性复杂度在序列密码理论中的不同作用，然后给出了非线性复杂度的一个递推算法，并讨论了非线性复杂度的剩余度问题，随机序

列的平均非线性复杂度等问题，得到相应的一系列结果．这样就对序列密码理论中的复杂度问题有一个比较全面的刻划．

关于M-序列的构造问题在移位寄存器理论中已有许多讨论．该书的特点是对它们的构造进行规范化表示，即对全部M-序列用相应的密钥参数与固定的算法确定．这对M-序列的使用无疑是有用的．对复合前馈序列的讨论重点是相关免疫性问题，本书给出了一系列判别条件与构造性质，从而在一定条件下可以构造相应的相关免疫函数．

综上所述，该书反映了作者近期在序列密码学方面的研究成果，较深入地运用了数学工具，探讨和解决了序列密码中的若干核心问题，可供有关研究工作者参考．

国家自然科学基金会副主任 胡国定

1991年10月于南开大学数学研究所

此为试读，需要完整PDF请访问：www.ertongbook.com

前　言

密码理论与技术在通信、计算机技术、军事、航天、金融、新闻等方面都有重要的应用，序列加密体制是近代密码学的一个重要组成部分，它以移位寄存器理论为核心，内容十分丰富，除了经典的线性、非线性理论外，近年来在随机周期序列、复合前馈序列等方面均有许多发展。本书以有限域上一般非线性函数的组合表示为基础，进一步讨论序列加密体制中的有关问题。主要内容由以下三个方面构成。

书中第一部分较系统地讨论了任意周期序列的非线性复杂度问题。所谓非线性复杂性，就是产生该周期序列的最小非线性移位寄存器的级数。对此，我们重点讨论了下面几个问题。

首先，我们讨论了线性复杂度与非线性复杂度指标在密码学中的作用

问题，针对线性复杂度的基本特征：即线性复杂度低的序列加密体制的抗攻击力必差，而线性复杂度高的加密体制抗攻击力不一定好的情况，进一步指出非线性复杂度的作用，提出了非线性复杂度与剩余度的概念。一般说，非线性复杂度总是大大低于线性复杂度，因此只有在剩余度较大时，密码体制才能真正安全。

其次，我们对非线性复杂度进行了一系列分析，其中包括非线性复杂度的递推算法，周期序列的剩余度计算公式及随机序列的平均非线性复杂度的估算。这些结果使我们对非线性复杂度有一个比较全面的认识。

第二部分对M-序列的构造问题作了进一步讨论。M-序列构造是一个经典的移位寄存器理论问题，本书的目的是使M-序列的构造进一步规范化，使全部n级M-序列以一定的参数表示出来。这些参数与全部M-序列相互对应，成为产生M-序列的一个密钥空间，而且由一定的算法来确定相应的M-序列。本书的讨论基本

上达到上述目的。

第三部分关于复合前馈序列，我们集中讨论了它们的相关免疫性问题，给出了一系列判别条件与构造性质，找到了直接构造全部一阶相关免疫函数的简单方法。

以上大部分结果是作者近期科研所获得的，为了保持全书的系统性，我们也介绍了有关的已知结果，尤其是 M-序列 的构造理论的若干方法，在许多文献与著作中均已有所论述。对于非线性复杂度与复合序列的有关讨论，在书中也予以指明。

感谢中国科学院系统科学研究所章照止研究员对本书的工作予以大力支持，在介绍资料及有关问题的讨论中给予许多帮助。

作者

1990年11月

目　录

CONTENTS

此为试读,需要完整PDF请访问: www.ertongbook.com