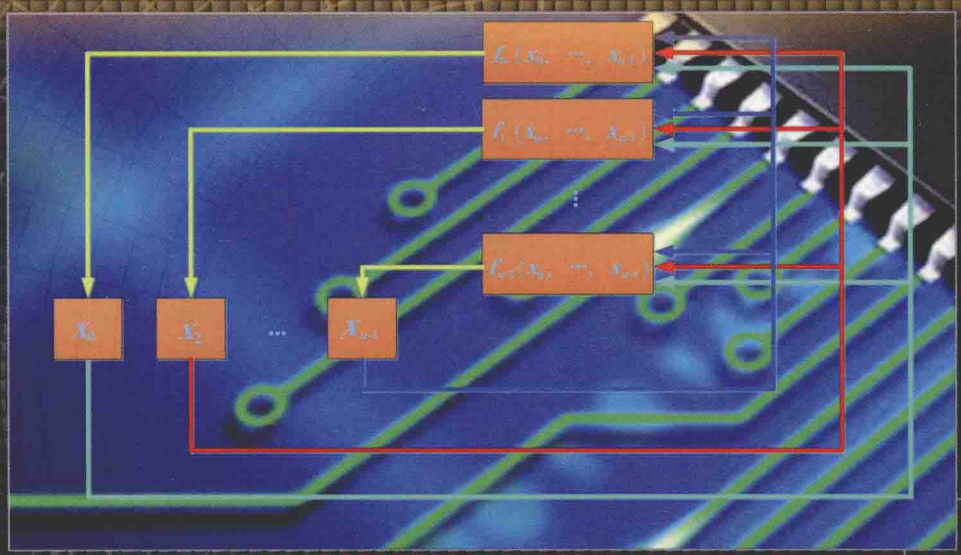
国防科技图书出版基金

网络与信息安全前沿技术丛书

布尔函数的设计与分析

周宇 胡予濮 董新锋 编著

Design and Analysis of Boolean Functions



国防工业出版社
National Defense Industry Press

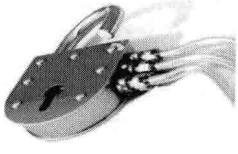
国防科技图书出版基金

网络与信息安全前沿技术丛书

周 宇 胡予濮 董新锋 编著

布尔函数的设计与分析

Design and Analysis of Boolean Functions



布尔函数是对称密码算法的重要部件。为集中展现布尔函数密码学性质、构造方法和应用方面的近期成果，本书对作者及其研究团队的成果进行提升，注重浅显易懂和实用性，对全局雪崩准则、非线性度、相关免疫性、代数免疫性等密码算法的安全性度量指标进行详细全面的论述，是该领域科研和技术人员系统了解和掌握布尔函数最新进展的荟萃集锦。

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

图书在版编目(CIP)数据

布尔函数的设计与分析 / 周宇，胡予濮，董新锋编著. —北京：国防工业出版社，2015.5
（网络与信息安全前沿技术丛书）
ISBN 978-7-118-10065-5

Ⅰ.①布… Ⅱ.①周… ②胡… ③董… Ⅲ.①布尔函数-研究 Ⅳ.①O153.2

中国版本图书馆 CIP 数据核字(2015)第 082582 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** 11¼　**字数** 203 千字
2015 年 5 月第 1 版第 1 次印刷　**印数** 1—3000 册　**定价** 68.00 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	陆　军	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
	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。

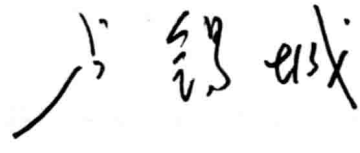
网络与信息安全是一门跨多个领域的综合性学科，涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等。“道高一尺、魔高一丈”，网络与信息安全技术在博弈中快速发展，出版一套覆盖面较全、反映网络与信息安全方面新知识、新技术、新发展的丛书有着十分迫切的现实需求。

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

随着信息化程度的加深，信息安全越来越受到重视，密码算法理论分析和研究与社会的信息保密越来越密切，如今密码算法被应用到国防、军事、政府、经济、文化等各个领域，布尔函数作为密码理论研究和算法设计中的最重要部件之一得到极大关注和认真研究，是密码理论研究和算法设计中的重要方向。

布尔函数是序列密码和分组密码的重要部件。在序列密码中，布尔函数主要用来设计线性移位寄存器中的反馈函数、前馈序列中的前馈函数和组合序列中的组合函数等，而在分组密码中主要用来设计 S 盒和 P 置换等，目的是达到混乱和扩散的效果。

布尔函数的各种密码学指标是随着各种攻击而提出的。Berlekamp - Massey 攻击要求序列密码的密钥流序列必须有较大的线性复杂度，而线性复杂度与布尔函数的非线性程度相关。密钥流序列与驱动序列之间相关性的强弱取决于密码算法中使用的布尔函数的相关免疫阶的高低，相关性越高，越易受到相关攻击，为了很好地量化相关性的程度，肖国镇和J. L. Massey 提出了相关免疫的谱刻画，该结果推动了从谱值角度研究布尔函数的各种密码学性质。布尔函数的代数免疫阶是为了抵抗代数攻击而提出的，日本政府征集的商用加密标准算法之一——Toyocrypt，就是由于标准代数攻击的出现而被淘汰。同时，为了保证密码算法产生伪随机性好的密钥流，对应的布尔函数也必须是平衡的。

目前，对布尔函数的研究主要集中在 3 个方面：①各种密码学指标之间的关系的研究，如平衡性、非线性度、相关免疫性、扩散性、全局雪崩准则、代数免疫性、正规性、代数厚度之间的关系等；②具有某些密码学性质的布尔函数的构造，如具有最优的代数免疫的布尔函数的构造，满足多个密码学指标的布尔函数的构造等；③针对布尔函数新的指标和新攻击的研究，如近来研究比较热的代数免疫等。在这三方面国内外学者取得了许多好的研究成果。本书提出了一些新的指标和构造方法，特别是在相关免疫性、全局雪崩准则、代数免疫性方面，构造了新的相关免疫函数和最优代数

免疫的布尔函数;同时提出了互相关的全局雪崩准则概念,得到了这个指标的上、下界以及与高阶非线性度的联系等。随着研究的进行也遗留了一些困难问题,如怎样构造新的具有最优代数免疫和较高的非线性度的布尔函数、怎样从自相关角度去刻画布尔函数、怎样完善布尔函数的密码学性质研究等。

为了集中展现在布尔函数性质、构造和应用方面的最新研究成果,也便于国内从事布尔函数研究的学生和学者以及工程技术人员对布尔函数有一个比较清晰的认识,作者试图对最近已有的和正在研究的布尔函数方面的成果进行归纳总结、提升,注重在算法中的实用性,通过实际例子对非线性度、相关免疫性、全局雪崩准则、代数免疫性等方面进行阐述。书中部分内容包含了作者及其研究团队在布尔函数研究方面的最新科研成果,如布尔函数全局雪崩准则的性质、具有最优代数免疫布尔函数的构造以及具有高非线性度的弹性函数构造等。

全书共分7章:第1章给出布尔函数和密码算法的研究现状;第2章给出布尔函数的安全性指标的概念和内涵;第3章给出布尔函数的非线性度,以及满足较高非线性度的函数的构造和性质等;第4章研究弹性函数的性质和构造;第5章研究布尔函数的全局雪崩准则性质,并对满足某些特定平方和指标的布尔函数进行了刻画;第6章研究具有最优代数免疫的布尔函数的性质和构造;第7章研究其他的密码学指标。

本书的第1章、第2章、第5章、第7章由周宇编写,第3章、第4章由胡予濮编写,第6章由董新锋编写。全书由周宇统稿,张文政、谯通旭、张凤荣等校稿。

国家信息化专家咨询委员会何德全院士和西安电子科技大学肖国镇教授对手稿进行了全面仔细的审核,提出了宝贵的意见和建议,在此表示衷心的感谢。西南交通大学唐小虎教授和保密通信重点实验室张文政研究员等对本书的出版给予了极大的鼓励和支持,在此表示感谢。全书的编写工作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,特别是曹云飞、申兵、王林、赵伟、汤殿华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、翔实、全面的核对和对该书付出的精心指导。

本书的出版得到国防科技图书出版基金的资助。此外,本书部分成果来自课题组承担的基金项目:国家自然科学基金项目(No:61309034)、四川省科技厅青年基金项目(No:2014JQ0055)、中国电子科技集团公司技术创新基金项目(No:JJ-QN-2013-32),在此特别表示感谢。

由于编者水平有限,书中难免存在不妥之处,恳请读者批评指正。

作 者

2015年3月20日

目　录

Contents