现代密码学中的布尔函数

温巧燕　钮心忻　杨义先　编著

科学出版社

国家科学技术学术著作出版基金资助出版

现代密码学中的布尔函数

温巧燕　钮心忻　杨义先　编著

科学出版社

2000

内 容 简 介

布尔函数作为密码体制设计与分析中一个不可缺少的工具，一直是密码学研究的重要问题之一。本书系统论述现代密码学中的布尔函数理论与方法，总结作者及课题组在这一领域多年的研究成果，其中包括已发表的论文和博士、硕士论文以及近期的最新研究成果，同时也包含了国内外学者在这一领域新的重要研究成果，并指出有待进一步研究的重要问题。

全书共分三篇，A 篇系统论述布尔函数的基础理论，B 篇和 C 篇分别对序列密码和分组密码中的布尔函数进行深入研究。该书在取材上力求前沿性和广泛性，在结构上力求严谨，在写法上深入浅出。

本书可作为通信与电子系统、信号与信息处理、计算机安全、密码学和应用数学等方面的理论工作者、高年级本科生、研究生参考书，对从事保密系统设计和算法研究的工程技术人员亦有一定的参考价值。

图书在版编目(CIP)数据

现代密码学中的布尔函数/温巧燕等编著. -北京：科学出版社，2000.8
ISBN 7-03-008530-2

Ⅰ.现… Ⅱ.温… Ⅲ.密码-布尔函数-研究 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字(2000)第 09416 号

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
源海印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2000 年 8 月第 一 版 开本：850×1168 1/32
2000 年 8 月第一次印刷 印张：10 1/4
印数：1—2 000 字数：350 000

定价：25.00 元

(如有印装质量问题，我社负责调换〈杨中〉)

前　言

在当今的信息社会里，信息安全越来越受到重视，从而极大地推动了信息安全的核心——现代密码学的研究。如今，密码理论与技术的应用已经覆盖了国防、军事、政府、金融、商业、文教等领域。随着信息化的到来，现代密码理论和技术与个人的信息保密密切相关，这些都给密码学的研究以极大的推动，也为密码理论与技术的应用提供了广阔的前景。

流密码和分组密码是密码体制实现的两种基本方式，而布尔函数又是实现密码体制的一个重要工具。特别是在流密码中，布尔函数更具有特殊的地位。因而，伴随着密码学的发展，布尔函数的研究一直很活跃，出现了一系列的学术论文和博士、硕士学位论文。从目前的研究情况看，布尔函数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的布尔函数理论与方法，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一领域新的重要研究成果，同时指出了有待进一步研究的问题。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与选题有一定的参考价值。本书叙述简单易懂，也适于工程技术人员阅读，在密码体制设计与安全性分析方面的结果对工程技术人员亦有一定的参考价值。

全书共分三篇。A 篇重点论述布尔函数的基础理论，对密码学中的布尔函数作了比较深入、系统的研究。B、C 两篇分别对序列密码和分组密码中的布尔函数进行了深入研究。除 A 篇第一章和第二章布尔函数基本概念和性质之外，其余三部分内容既前后连贯，又相对独立，读者可根据需要全部或部分阅读。作为专著，本书论述的重点是布尔函数的理论与方法，对密码体制是从布尔函数

的应用背景角度介绍的，有关密码学的系统理论可参考其他书籍。

北京邮电大学胡正名教授、周炯槃院士，中国科学院卿斯汉教授和章照止教授对本书给予了极大的支持，特此深表感谢。作者对课题组成员邢育森博士、田海建硕士等给予的密切配合以及北京邮电大学信息安全中心的全体老师和学生的配合表示感谢。张振涛博士等为书稿校对作了不少工作，在此一并表示感谢。本书第一作者还要感谢导师肖国镇教授、王育民教授、王新梅教授在攻读博士学位期间的指导与帮助。冯登国教授、谷大武博士和吴文玲博士等为本书提供了许多宝贵资料。其中第十二章的部分资料由冯登国教授提供，第十三章的部分资料由谷大武博士和吴文玲博士提供。在此向他们深表谢意。

最后，我们特别要感谢国家科学技术学术著作出版基金委员会对本书出版给予的支持。本书系国家重点基础研究规划发展项目（课题编号：G1999035805）的部分成果。

由于我们水平有限，时间仓促，书中不妥之处在所难免，恳请读者指正。

作　者

2000 年 5 月于北京

目　录

A 篇　布尔函数基础理论

B篇　序列密码设计与分析中的布尔函数

C篇　分组密码设计与分析中的布尔函数

A 篇　布尔函数基础理论

第一章　绪　　论

1.1　引　　言

在许许多多复杂的现代化设备中都少不了一个基本的元器件，即逻辑电路。这是一种在其输入和输出之间有一定逻辑关系的电路。这种电路的输入和输出通常都是用脉冲的有无或电位的高低来表示的。脉冲的有无、电位的高低、开关的通断、命题的真伪等，都是一对矛盾。如果把矛盾中的一方记为 1，另一方记为 0，就把这种矛盾性的概念数学化了，然后运用数学中一些基本的公理及定理对其进行数学运算，便可得到合乎逻辑的结果。在此基础上，发展出了一门重要学科，称为布尔代数学。它是用该学科的创始人乔治·布尔(George Boole)的名字来命名的。布尔代数研究 0，1 这两个量之间的逻辑运算。

布尔代数中的运算有“与”、“或”、“非”，习惯上分别用“$\wedge$”、“$\vee$”、“$-$”来表示。用 0，1 表示布尔代数中两个“数”(元素)，其运算如下：

$$\bar{1}=0,\quad \bar{0}=1$$

$$1\vee 1=1,\quad 1\vee 0=0\vee 1=1,\quad 0\vee 0=0$$

$$1\wedge 1=1,\quad 1\wedge 0=0\wedge 1=0,\quad 0\wedge 0=0$$

设 x_1,x_2 是布尔代数中任意数，则有

$$x_1\wedge x_2=\begin{cases}1, & \text{当 } x_1,x_2 \text{ 同时为 1 时}\\ 0, & \text{其他}\end{cases}$$

$$x_1\vee x_2=\begin{cases}0, & \text{当 } x_1,x_2 \text{ 同时为 0 时}\\ 1, & \text{其他}\end{cases}$$

若用“⊕”、“⊙”分别表示 GF(2)上的加、乘运算;1,0 看做 GF(2)上元素,则有

$$x_1 \wedge x_2 = x_1 \odot x_2$$
$$x_1 \vee x_2 = x_1 \oplus x_2 \oplus x_1 \odot x_2$$
$$\bar{x}_1 = x_1 \oplus 1$$

于是布尔代数中的运算可用 GF(2)上的函数来表示。自然地,人们也将GF(2)上的函数称为布尔函数。一般地,我们定义 n 元布尔函数为如下映射:

$$f:\ \mathrm{GF}(2)^n \to \mathrm{GF}(2)$$

记为 $f(x)$,其中

$$x \in \mathrm{GF}(2)^n,\quad f(x) \in \mathrm{GF}(2)$$

为简洁计,以后我们用普通加、乘记号分别表示 GF(2)上的“⊕”、“⊙”。如 $x_1 \oplus x_2$ 记为 $x_1 + x_2$,$x_1 \odot x_2$ 记为 $x_1 x_2$;有时仍用 $\bar{x}$ 记 $x+1$。需要特别强调模 2 运算时仍用“⊕”和“⊙”。

作为表示逻辑运算的函数,布尔函数是研究数字逻辑电路的重要数学工具,也是研究以此为基础的一切科学技术的重要工具,从而也是研究密码学和密码技术的重要工具。无论在流密码还是分组密码中,无论在私钥还是公钥密码中,布尔函数都有重要的应用。尤其在流密码中,所使用的主要数学工具之一就是布尔函数。本章我们介绍布尔函数的基本概念和研究方法。

1.2 布尔函数的表示

为了方便布尔函数的理论研究和应用,人们在不同的情况下对布尔函数采用了不同的表达方式。本节对布尔函数几种不同的表达方式加以介绍。

1.2.1 真值表

布尔函数,由于其定义域和值域都是有限集,自然可以用列表法表示。表 1.2.1 给出了一个 2 元函数 $f(x)=f(x_1,x_2)$。表中左

表 1.2.1 布尔函数的例子

x		$f(x)$
0	0	0
0	1	1
1	0	1
1	1	0

列是 x 的值，右列是相应的函数值 $f(x)$。我们把这样的一个表称为 $f(x)$的真值表，将右列函数值构成的矢量(向量)称为 $f(x)$的函数值向量。若将 0 到 2^n-1 之间的整数 N 表示成二进制数$(x_1,\cdots,x_n)$，则可将从 0 到 2^n-1 之间的整数和 $GF(2)^n$ 上的向量一一对应起来，即

$$N \longleftrightarrow (x_1,\cdots,x_n)$$

整数从小到大刚好对应 $GF(2)^n$ 中元素按字典序从小到大。今后在不引起混淆的情况下，我们将二者互用。对于一般的 n 元函数 $f(x)$，可将其函数值按 x 的字典序从小到大排列成一个向量：

$$(f(0),f(1),\cdots,f(2^n-1)) \tag{1.2.1}$$

亦将(1.2.1)式称为 $f(x)$的函数值向量或真值(表)，记为 $\vec{f}$。称一个 0,1 向量 α 的汉明重量为其“1”分量的个数，记为 $w(\alpha)$或 w_α。$\vec{f}$ 的汉明重量称为 $f(x)$的重量，记为 $w(f)$或 w_f。若 $w(f)=2^{n-1}$，则称 $f(x)$是平衡函数。

真值表示是一种列表法。通过真值表可以给出 $f(x)$的解析表达式。我们知道，列表法表示的实函数不一定有解析表达式。有趣的是，任何布尔函数都有解析表达式。

1.2.2 小项表示

对于 $x_i,c_i\in GF(2)$，规定

$$x_i^1=x_i,\quad x_i^0=\overline{x}_i$$

于是

$$x_i^{c_i} = \begin{cases} 1, & \text{当 } x_i = c_i \text{ 时} \\ 0, & \text{当 } x_i \neq c_i \text{ 时} \end{cases}$$

设

$$c = (c_1, \cdots, c_n), \quad x = (x_1, \cdots, x_n)$$

则有

$$x_1^{c_1} x_2^{c_2} \cdots x_n^{c_n} = \begin{cases} 1, \text{ 当}(x_1, \cdots, x_n) = (c_1, \cdots, c_n) \\ 0, \text{ 当}(x_1, \cdots, x_n) \neq (c_1, \cdots, c_n) \end{cases} \tag{1.2.2}$$

为了方便,今后亦记

$$x_1^{c_1} x_2^{c_2} \cdots x_n^{c_n} = x^c$$

于是

$$f(x) = \sum_{i=0}^{2^n-1} f(x) x^c \tag{1.2.3}$$

(1.2.3)式称为 $f(x)$的小项表示。小项表示实际上是布尔代数表达方式,即逻辑表达方式。此种表示法常用于布尔函数的设计实现。

例如,表 1.2.1 所示的布尔函数的小项表示为

$$\begin{aligned} f(x) &= 0 \cdot x_1^0 x_2^0 + 1 \cdot x_1^0 x_2^1 + x_1^1 x_2^0 + 0 \cdot x_1^1 x_2^1 \\ &= x_1^0 x_2^1 + x_1^1 x_2^0 \end{aligned} \tag{1.2.4}$$

1.2.3 多项式表示

在(1.2.4)式中,将 $x_1^0 = x_1 + 1$, $x_2^0 = x_2 + 1$ 代入并化简,得

$$f(x) = (x_1 + 1)x_2 + x_1(x_2 + 1) = x_1 + x_2$$

这是 $f(x)$的多项式表达式。显然,任意 n 元函数 $f(x)$都可根据(1.2.3)式化为多项式表达式:

$$\begin{aligned} f(x) &= a_0 + a_1 x_1 + \cdots + a_n x_n + a_{12} x_1 x_2 + \cdots \\ &\quad + a_{n-1\,n} x_{n-1} x_n + \cdots + a_{12\cdots n} x_1 x_2 \cdots x_n \\ &= a_0 + \sum_{\substack{1 \leqslant j_1 \leqslant \cdots \leqslant j_k \leqslant n \\ 1 \leqslant k \leqslant n}} a_{j_1} \cdots a_{j_k} x_{j_1} \cdots x_{j_k} \end{aligned} \tag{1.2.5}$$

(1.2.5)式称为 $f(x)$的代数标准型。

定义布尔函数 $f(x)$的次数为 $\max\{k|a_{j_1\cdots j_k}\neq 0\}$，记为 $\deg f$ 或 $\partial^0 f$。若 $f(x)=0$，则定义 $\partial^0 f=0$。若 $\partial^0 f=1$，则称 $f(x)$为仿射函数。当 $a_0=0$ 时，仿射函数被称为线性函数，有时也笼统地将仿射函数称为线性函数。当 $\partial^0 f\geqslant 2$ 时，称 $f(x)$为非线性函数。在电路设计中，实现一个线性函数的电路只需使用模 2 加法器，这是最简单的；而非线性函数还需乘法器，相对复杂些。

1.2.4 Walsh 谱表示

定义 1.2.1 设 $x=(x_1,\cdots,x_n)$，$w=(w_1,\cdots,w_n)\in \mathrm{GF}(2)^n$，$x$ 与 w 的点积定义为

$$x\cdot w = x_1w_1+\cdots+x_nw_n\in \mathrm{GF}(2)$$

n 元布尔函数 $f(x)$的 Walsh 变换定义为

$$S_f(w) = 2^{-n}\sum_{x=0}^{2^n-1}(-1)^{w\cdot x}f(x) \tag{1.2.6}$$

其逆变换为

$$f(x) = \sum_{w=0}^{2^n-1}S_f(w)(-1)^{w\cdot x} \tag{1.2.7}$$

$S_f(w)(w\in \mathrm{GF}(2)^n)$称为 $f(x)$的 Walsh 谱。

(1.2.7)式即为 $f(x)$的 Walsh 谱表示。若将 $f(x)$的 Walsh 谱 $S_f(w)$按 w 的字典序从小到大排列，便得一实向量：

$$(S_f(0),\cdots,S_f(2^n-1)) \tag{1.2.8}$$

Walsh 变换是可逆的，所以布尔函数的 Walsh 谱是唯一的。于是，(1.2.8)式便将布尔函数和 2^n 维实向量对应起来，从而可将布尔函数的某些问题转化为实向量的研究。

1.2.5 矩阵表示

定义 1.2.2 设 $f(x)$是一个 n 元布尔函数，$x\in \mathrm{GF}(2)^n$。若 $f(x)=1$，则称 x 为 $f(x)$的一个特征向量，记 $f(x)$的全体特征向量的集合为 D，

$$D = \{\alpha|f(\alpha)=1,\alpha\in \mathrm{GF}(2)^n\}$$

$$|D| = w$$

其中 w 表示 $f(x)$的重量。将 D 中 w 个向量按字典序从大到小排列，记第 i 个向量 $w_i=(c_{i1},\cdots,c_{in})$，$1\leqslant i\leqslant w$，则称 0，1 矩阵

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ c_{w1} & c_{w2} & \cdots & c_{wn} \end{pmatrix}$$

为 $f(x)$的特征矩阵，记为 C_f，或简记为 C。

布尔函数与其特征矩阵是一一对应的，于是可将布尔函数的某些问题的研究转化为矩阵问题的研究。注意，定义中的字典序是从大到小，有时为了方便也用从小到大或其他顺序。一个布尔函数的特征向量集合是唯一的，在不引起混淆的情况下，我们将按不同顺序所给出的定序特征矩阵不加区别。

此外，布尔函数还有状态图等其他表示方法，这里不再一一列举。

1.3 布尔函数的研究方法

上节介绍了布尔函数的几种表示方法。不同的表示方法在不同的研究背景中会显示出各自的优势。根据不同的表示方法，人们对布尔函数采用了不同的研究方法。目前主要有如下几种方法。

1. 代数分析方法

由于任何布尔函数都可表示为多项式形式，所以可用代数方法对其进行分析研究。从代数的角度分析布尔函数主要采用小项表示和多项式表示。如文献[1]、[2]中对布尔函数的研究多用代数方法。

2. 频谱方法

频谱分析是研究布尔函数的一个非常重要的工具，通过分析

布尔函数的 Walsh 谱特性，可给出布尔函数一系列重要的研究结果[1,3,4]。

3. 矩阵方法

矩阵表示是布尔函数的直观表示方法。由于在定序意义下，重量为 w 的 n 元布尔函数之集与 GF(2)上 $w\times n(1\leqslant w\leqslant 2^n)$ 矩阵之间是一一对应的。通过对矩阵的分析来研究布尔函数是一个直观有效的方法，在第三章我们将看到它的魅力。

4. 重量分析方法

前面我们定义过布尔函数的重量，即 $f(x)$ 真值表中 1 的个数，或 $f(x)$ 特征向量的个数。对于两个布尔函数 $f(x)=f(x_1,\cdots,x_n)$ 和 $g(x)=g(x_1,\cdots,x_n)$，定义 $f(x)$ 和 $g(x)$ 的距离为

$$w(f+g)$$

记为 $d(f,g)$，即

$$d(f,g)=w(f+g)$$

关于和函数的重量，有如下关系式：

$$w(f+g)=w(f)+w(g)-2w(fg) \qquad (1.3.1)$$

重量分析方法通过分析布尔函数的重量特征来研究布尔函数。如文献[6]采用重量分析方法得出了许多重要结果。这种方法简单易懂，很适合于工程应用。

这几种研究方法各有所长，适合于不同的研究背景。本书将在不同的章节采用不同的方法。此外，通过布尔函数的状态图表示，从图论角度进行研究，也是一个很有意义的工作。

1.4 布尔函数的研究问题

如本章引言所述，布尔函数在许多领域都有应用背景。人们在不同领域中对布尔函数进行了大量研究，特别是在密码学领域中，布尔函数一直是研究热点。研究的问题包括：布尔函数的表示；布

尔函数的研究方法；布尔函数的设计实现；布尔函数的性质；满足一定性质的布尔函数的特征刻画、存在性、分布、构造与计数；布尔函数不同性质之间等价、相斥、相容、制约等关系；在密码学中，布尔函数的一条性质反映一种安全性能指标，当不同性能指标相互制约时，如何折衷以提高综合性能；随着技术的发展和新的攻击方法的出现，新的性质的提出与研究，等等。总之，布尔函数的研究内容十分广泛，结果也十分丰富，当然也还有大量有待研究的问题，这些我们将在有关章节逐步介绍。由于篇幅所限，本书在介绍布尔函数基本概念和性质的基础上，以我们及课题组在布尔函数方面所做的工作为主线，重点介绍布尔函数的最新研究成果。需要了解更多内容的读者，可根据参考文献查找有关资料。

参 考 文 献

[1] 丁存生，肖国镇. 流密码学及其应用，北京：国防工业出版社，1994.

[2] 单炜娟. 相关免疫函数的结构与构造，应用数学学报，1991，14(3).

[3] 冯登国. 频谱理论及其在通信保密技术中的应用，博士学位论文，西安电子科技大学，1995.

[4] Xiao Guo-Zhen, J. L. Massey. A Spectral Characterization of Correlation-Immune Combining functions, IEEE Trans. on Inform. Theory, 1988, 34(3).

[5] 温巧燕. 密码学中的相关免疫函数研究，博士学位论文，西安电子科技大学，1997.

[6] 杨义先，林须端. 编码密码学，北京：人民邮电出版社，1992.

[7] 邢育森. 信息安全系统理论与关键技术研究，博士学位论文，北京邮电大学，1998.

[8] 田海建. 通信中的信息安全新方法——布尔函数方法，硕士学位论文，北京邮电大学，1996.

[9] 武传坤. 密码学中的布尔函数，博士学位论文，西安电子科技大学，1993.

[10] 吴文玲. 密码安全的度量指标，博士学位论文，西安电子科技大学，1997.

[11] 杨义先. 高维 Hadamard 矩阵理论与高维 Walsh-Hadamard 变换，硕士学位论文，北京邮电大学，1985.

[12] 杨义先. 通信理论中的并元方法——现代密码与 Hadamard 矩阵，博士学位论文，北京邮电大学，1998.

[13] 谷大武. 分组密码理论与某些关键技术研究，博士学位论文，西安电子科技大学，1998.