汕頭大學
SHANTOU UNIVERSITY

硕 士 学 位 论 文

题　　目	两类优良代数免疫性质布尔函数的构造与分析
英文题目	Two Classes of Boolean Functions with Optimal Algebraic Immunity: Construction and Analysis

姓　　名	郭飞	学　　号	11609035
所在学院	工学院	导师姓名	陈银冬
专　　业	计算机软件与理论		
入学日期	2016. 09. 01	答辩日期	2019. 05. 31

学位论文原创性声明

本文是我个人在导师指导下进行的工作研究及取得的研究成果。论文中除了特别加以标注和致谢的地方外，不包含其他人或其它机构已经发表或撰写过的研究成果。对本文的研究做出贡献的个人和集体，均已在论文中以明确方式标明。本人完全意识到本声明的法律责任由本人承担。

作者签名：_____ 日期：_____年____月____日

学位论文使用授权声明

本人授权汕头大学保存本学位论文的电子和纸质文档，允许论文被查阅和借阅；学校可将本学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或其它复制手段保存和汇编论文；学校可以向国家有关部门或机构送交论文并授权其保存、借阅或上网公布本学位论文的全部或部分内容。对于保密的论文，按照保密的有关规定和程序处理。

作者签名：_____ 导师签名：_____

日期：_____年____月____日 日期：_____年____月____日

摘 要

布尔函数是许多密码系统的核心部件，其密码学性质优劣决定着整个密码系统的安全性强弱。为了抵抗各种已知攻击，布尔函数需同时满足几条性质：平衡性，良好的(快速)代数免疫度，高非线性度和高代数次数等。旋转对称布尔函数是一类输出在输入的循环移位下保持不变的布尔函数，具有结构简单、运算速度快、易于实现等优点，在密码系统中应用广泛。择多逻辑函数是结构最简单的具有最优代数免疫度的布尔函数，其快速代数免疫度仍然是个不解的问题。本文对具有最优代数免疫度的旋转对称布尔函数和择多逻辑函数的快速代数免疫度进行研究，主要工作有：

(1) 利用数论中一种整数拆分的相关结果，通过修改择多逻辑函数的支撑集，我们**构造了两类具有最优代数免疫度的奇数元平衡旋转对称布尔函数**，这两类函数的非线性度较已有构造有极大的提升，并且经测试具有几乎最优快速代数免疫度，第二类函数的代数次数在大多数变元下都能达到最优。

(2) 基于**择多逻辑函数**的对称性质，我们分析了其在变元数量在$2^m+2 \le \mathrm{n} < 2^{m+1}$(其中$m \ge 2$)范围内快速代数免疫度的下界，结合已有结论，进而得到了该类函数在**变元数量为2^m+2和2^m+3(其中$m \ge 2$)时的快速代数免疫度为$2^{m-1}+4$**。

关键词：布尔函数；旋转对称布尔函数；择多逻辑函数；(快速)代数免疫度；流密码

ABSTRACT

The Boolean function is the kernel component in some cryptosystems and its cryptographic properties directly determine the security of the cryptosystems. In order to resist unknown attacks, Boolean functions should satisfy some necessary criteria simultaneously, mainly balanced-ness, good (fast) algebraic immunity, high nonlinearity, high algebraic degree, etc. Rotation symmetric Boolean functions are invariant under the action of the cyclic group, which are popular in cryptosystems due to their simple structure, high operational speed and low implemental cost. The majority function is the simplest Boolean function with optimal algebraic immunity, of which the fast algebraic immunity still remains an open problem. This paper proposes a scheme of constructing rotation symmetric Boolean functions with optimal immunity and investigates the exact fast algebraic immunity of two subclasses of the majority logic function.

(1) With the results of the integer partition, by modifying the support of the majority function, we present two new classes of balanced odd-variable rotation symmetric Boolean functions with algebraic immunity. The nonlinearity is really higher than previous constructions. Moreover, such functions are tested and verified to possess very good resistance to fast algebraic attacks at least for small number of variables. The second construction reaches optimal algebraic degree in almost all cases of variables.

(2) Based on the symmetry of the majority logic function, we analyze and give a lower bound of its fast algebraic immunity on the number of variables from $2^m + 2$ to 2^{m+1}, where $m \geq 2$. Combining with previous results, the conclusion can be gained that the fast algebraic immunity of the majority logic function is exactly $2^{m-1} + 4$ when the number of variables equals $2^m + 2$ and $2^m + 3$.

Keywords：Boolean functions, rotation symmetric Boolean functions, majority logic function, (fast) algebraic immunity, stream cipher

目 录

第一章 绪 论

在信息时代飞速推进的今天，信息安全越来越受到人们的重视。它不仅与国家的政治、军事、外交等活动有关，还与各个团体、单位和个人都密切相关。习近平总书记曾在讲话中指出，没有网络安全就没有国家安全，没有信息化就没有现代化。因此，加快信息安全体系建设，确保国家安全和个人安全，是我国新时代的重大战略。密码学作为信息安全的基石和核心，在构建保密和安全的信息系统中起到重要作用。

布尔函数是许多密码系统的核心部件，其密码学性质的优劣直接决定密码系统的安全性强弱。本章首先介绍布尔函数的研究背景及意义；其次讲述布尔函数在流密码中的应用，流密码的(快速)代数攻击和安全布尔函数的设计准则；接着讲述国内外代数免疫最优旋转对称布尔函数构造和布尔函数快速代数免疫度的研究现状；最后对本文行文结构和主要工作做了简介。

1.1 研究背景及意义

尽管人们对密码学(Cryptography)的认知可以追溯到几千年前，但这一时期基本都是靠人工对信息进行加密、传输和放破译，其应用也主要局限于军事目的，只为少数人掌握和控制。所以，这一阶段密码学更像是一门技巧性很强的艺术，而不是一门学科，其发展受到了很大的限制。1949 年，Shannon[1]在《贝尔系统技术》杂志上发表了题为《保密系统的通信理论》(Communication theory of secrecy system)的文章，为密码学奠定了坚实的理论基础，使密码学发展成为一门真正的学科。后来，随着通信、军事等重要领域的需求，密码学受到人们的重视，1976 年到 1996 年是密码学发展的黄金时段，大量的密码学理论和方法创新成果在这段时间涌现。1976 年，Diffie 和 Hellman[2]发表了《密码学的新方向》(New direction in cryptography)文章，提出了公钥密码的思想，开辟了公钥密码学的研究分支。1977 年，美国国家标准局[3]正式公布了美国的数据加密标准(Date Encryption Standard，DES)，公开其算法并批准用于政府和商业上的保密通信。1978 年，Rivest，Shamir 和 Adleman[4]首次提出了实用的公钥密码体制——RSA 体制，该密码的安全性是基于大整数

因式分解的难解性，极大促进了公钥密码的发展。20 世纪末，随着计算机技术和电子通信技术的进步，出现了大批的密码算法和攻击，密码编码学和分析学相互促进，推动密码学理论蓬勃发展。1997 年，美国国家标准与技术研究机构[5]推出 AES（Advanced Encryption Standard）计划，呼吁寻求满足不同密钥长度且能在各种硬件上工作的密码算法以替代 DES，随后在世界范围内征集密码算法。最后，由比利时人 Daemen 和 Rijmen 设计的 Rijndael 算法[6]，在安全性、性能和实现特性等方面均占据绝对优势，被选定为 AES 算法。继美国 AES 计划之后，欧洲相继启动了 NESSIE 计划[7]和 ECRYPT 计划[8]，在世界范围内征集欧洲新世纪的各类密码算法标准。近几年，我国也在制定和更新各类密码标准。这些计划的兴起，使得密码学走上了“理论+应用”的道路，极大推动密码学理论和方法的迅速发展。

根据密钥的特点，Simmons[9]将密码体制分为两大类——对称密码（又称私钥密码）：加密密钥和解密密钥相同；非对称密码（又称公钥密码）：加解密密钥不同，一个公开发布（即公开密钥），另一个用户自己秘密保存（即私有密钥）。对称密码最大优势是加解密速度快，适于大数据量进行安全传输，但密钥管理困难。非对称密码机制较为灵活，但加解密速度相对较慢。按照对明文加密方式的不同，对称密码可分为分组密码（Block Cipher）和流密码（Stream Cipher）。分组密码是将明文分块，在每个时钟周期用相同的密钥加密一整个数据块。流密码在加密过程中密钥流序列的产生与密钥生成器在当前时钟的状态相关，在每一个时钟周期用一比特密钥加密一比特明文，所以要求密钥和明文等长。因此，相对于分组密码，流密码具有加密速度快、易于硬件实现、出错概率小等优点，被广泛应用于移动通信、军事通信、外交通信等领域。事实上，对于流密码的研究主要归结为对流密码系统所使用的布尔函数的研究。

我国在流密码研究方面也做出了凸出贡献，由中国科学院数据保护和通信安全研究所中心（DACAS）自主设计的祖冲之算法集（ZUC）受到国际密码学界高度关注[10]，此算法用于数据加密和完整性认证，包括祖冲之算法、加密算法 128-EEA3 和完整性算法 128-EIA3，已经被国际组织 3GPP 推荐为 4G 无线通信的第三套国际加密和完整性标准的候选算法。

布尔函数作为许多密码系统的核心部件，其密码学性质直接决定着密码系统的安全性。在 Shannon 的理论中[1]，设计安全的密码函数需考虑到两个基本原则——混淆（Confusion）和扩散（Diffusion）。混淆是尽量把密文和明文（或密钥）之间的统计关系复杂化，这样攻击者无法从密文中获得任何有效信息；扩散是修改明文（或密钥）的若干比特使其对密文的影响尽可能显著，这样可以隐蔽明文的统计特征。同时，为了抵抗各种已知密码攻击，密码系统中使用的布尔函数必须满足多项密码学性质，尤其是近年来提出的代数攻击[24]和快速

代数攻击[41]，对布尔函数提出了更高的要求。因此，布尔函数两方面的研究引起了国内外密码学者的高度关注：一是构造和设计满足多项密码学性质的布尔函数，二是深入研究布尔函数的密码学性质。

1.2 流密码与布尔函数

流密码系统中，布尔函数通常作为密钥流生成器的非线性部分，与反馈移位寄存器搭配产生安全强度较好的密钥流。并且，应用中的布尔函数需满足多种性质以抵抗已知攻击。

1.2.1 布尔函数在流密码中的应用

流密码也称序列密码，其加密和解密思想非常简单：用一个密钥序列与明文序列进行“异或”来产生密文，用同一个密钥序列与密文“异或”来恢复明文。流密码的模型如图 1-1 所示。当用来加密的序列是由满足均匀分布的离散无记忆信源产生的随机序列时，相应的序列密码就是所谓的“一次一密”密码体制。Shannon 已经证明“一次一密”密码体制在理论上是不可破译的，即密钥序列是随机序列。但随机序列的产生、存储和传送在现实中存在很大困难，因此并不适用于流密码的加解密过程。在实际应用中，用伪随机序列作为加解密序列则更为普遍。伪随即序列是将一个短的消息密钥按照一定的算法生成一个很长的序列。伪随即序列具有预先确定性和重复实现性，同时又具有随即序列的特性，这些特性称为序列的伪随机性。序列密码系统的安全性强弱取决于密钥流伪随机性的好坏。因此，如何设计出能生成周期较长、伪随机性较好序列的密钥流生成器就成了流密码研究的关键问题。

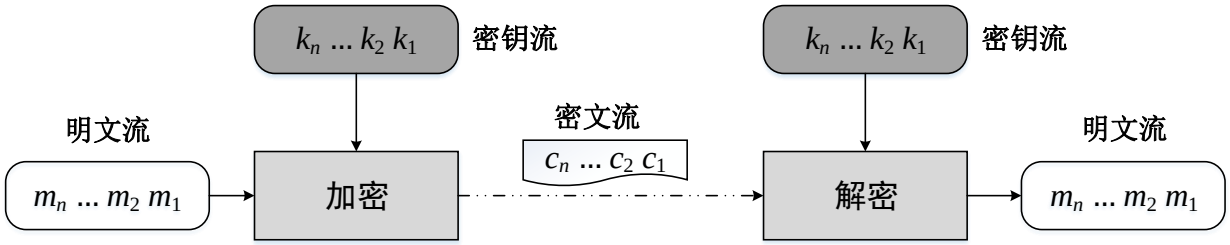

图 1-1 流密码模型

在流密码的研究中，人们通常把它分为两个部分：驱动部分和非线性组合部分。驱动

部分控制存储器的状态转移，负责提供若干供组合部分使用的周期大、统计特性好的序列；非线性组合部分则将驱动部分提供的序列组合生成满足要求且密码性能良好的密钥流序列。反馈移位寄存器是当代流密码设计的主流，目前技术也比较成熟，其基本部件是布尔函数，n级反馈移位寄存器模型结构如图 1-2 所示。若反馈布尔函数f是线性函数，则相应的反馈移位寄存器称为线性反馈移位寄存器（Linear Feedback Shift Register，LFSR），否则，称为非线性反馈移位寄存器（Non-Linear Feedback Shift Register，NLFSR）。LFSR 具有实现简单、速度快、便于分析和计算等优势，已广泛应用于各种数字电路中，是密钥算法中最重要的密钥流构成部件。

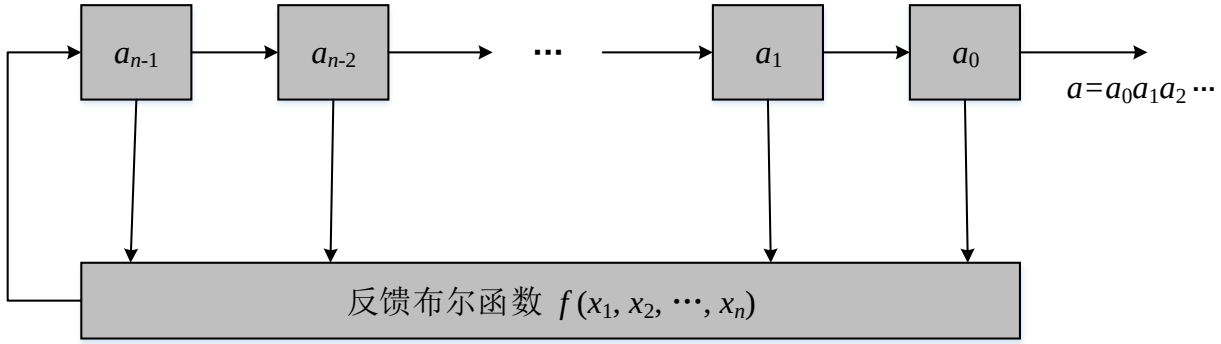

图 1-2 n级反馈移位寄存器模型

从加密角度来说，LSFR 产生的伪随机序列密码学性质极弱，不能作为加密密钥。现代密码学中，最常见的方式是用一个满足一定密码学性质的非线性布尔函数对一个具有大周期的 LFSR 进行滤波或者对多个具有大周期的 LFSR 进行组合，即滤波模式（图 1-3）和组合模式（图 1-4），这样既可以利用 LFSR 的周期性以便产生较长周期的伪随机序列，又能够将非线性性质引入到生成的序列中，以实现 Shannon 所提出的混淆和扩散原则，保证产生密钥流序列的安全强度。因此，可以说，基于 LFSR 的密钥流生成器实现了对“一次一密”的折中。

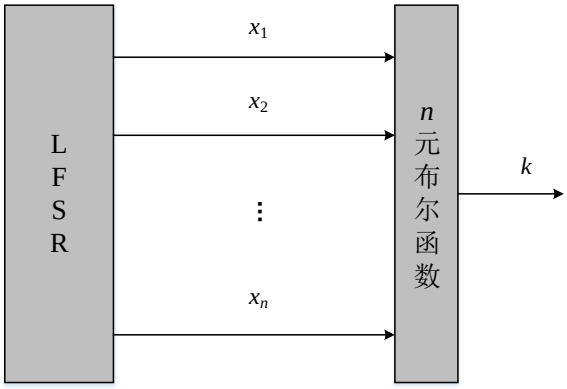

图 1-3 滤波模式

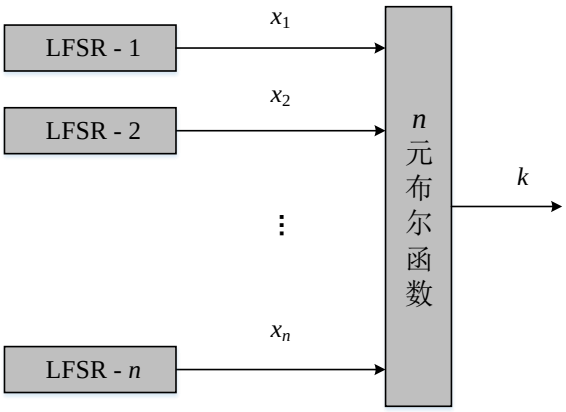

图 1-4 组合模式

1.2.2 流密码的(快速)代数攻击

代数攻击是一种在已掌握一些明文及其所对应的密文的条件下实施的攻击。其基本思想起源于 Shannon，他认为一个密码算法可以表示成一个大型的多变元方程组，求解这个方程组就可以获取密钥。根据 Kerckhoff 原则，密码算法的所有细节完全公开，因此，密码分析学者可以根据明文−密文对应关系以及密码算法的结构，建立起以密钥为未知变量的方程组。事实上，密码编码学者也正是基于此方程组求解的复杂度来保证密码系统的安全性。代数攻击正是抓住这一关键点，从建立方程的初步阶段找到了突破点——建立尽可能低次数的方程组，以降低方程组的求解复杂度。在 2003 年欧密会上，Courtois 和 Meier[24] 成功地将代数攻击用于流密码的分析破译，引起国内外密码学者的广泛关注，使用标准代数攻击，一些著名的密码系统被成功攻破，如日本政府 Cryptrec 计划中提到的 Toyocrypt 流密码算法和欧洲 NESSIE 工程的候选流密码算法 LILI-128 等。

下面介绍图1-3中非线性滤波函数生成器的代数攻击和快速代数攻击原理。设$S^0=(s_1, s_2, \cdots, s_n)$是LFSR的初始状态(通常与密钥直接相关)，$t$时刻状态为$S^t=L^t(S^0)$，输出密钥流比特用$z_t$表示，密码系统中过滤函数是$n$元布尔函数$f(x_1, x_2, \cdots, x_n)$。知道了密钥流比特$z_{k_1}, z_{k_2}, \cdots, z_{k_l}$，就能得到如下方程组

$$\begin{cases} f\left(L^{k_1}(S^0)\right)=z_{k_1} \\ f\left(L^{k_2}(S^0)\right)=z_{k_2} \\ \vdots \\ f\left(L^{k_l}(S^0)\right)=z_{k_l} \end{cases} \tag{1-1}$$

对于非线性滤波函数生成器也能列出类似的方程。理论上，如果知道足够多的z_{k_i}就能建立足够多的方程进而求出密钥。但是若非线性滤波函数的代数次数较高，则求解这个方程组的难度就很大。实际上，代数攻击和快速代数攻击都是在寻求降低上述方程组求解复杂度的方法。

Courtois 和 Meier[24]提出并证明了布尔函数的低次倍式存在定理：对于任意n元布尔函数f，存在次数不超过$\left\lceil\frac{n}{2}\right\rceil$的非零布尔函数$g$，使得$fg$的次数不超过$\left\lceil\frac{n+1}{2}\right\rceil$。基于该定理，对于高次函数$f$，考虑其较低次数的倍式$fg=h$，其中$g\neq 0$且$g$的代数次数不超过$\left\lceil\frac{n}{2}\right\rceil$。用$g$乘以$f\left(L^t(S^0)\right)=z_t$的两边得

$$f\left(L^t(S^0)\right)g\left(L^t(S^0)\right)=z_t g\left(L^t(S^0)\right),$$

若$z_t=0$，则$f\left(L^t(S^0)\right)g\left(L^t(S^0)\right)=h\left(L^t(S^0)\right)=0$；若$z_t=1$，则$g\left(L^t(S^0)\right)+h\left(L^t(S^0)\right)=0$。因此，方程组(1-1)能转化为以初始状态$S^0$为未知数关于$g$或$h$的低次方程组，大大降低了求解复杂度。2004年，Meier等[25]将该问题归结为求解布尔函数及其反函数的低次非零零化子的问题，进而提出了代数免疫度(Algebraic Immunity，AI)的概念。自那时起，国内外密码学者提出了多种具有优良代数免疫度的布尔函数构造方法[13-17, 48, 49, 54, 56]。

后来在2003年美密会上，Courtois[41]改进标准代数攻击并提出了快速代数攻击：考虑f的倍式$fg=h$，其中$h\neq 0$且h的代数次数远小于n，g的代数次数小于h的代数次数。在获取了一些连续的密钥流比特$z_t, z_{t+1}, z_{t+2}, \cdots$之后，通过找到关于$h$的一个线性组合$\sum_i \alpha_i h(L^{t+i}(S^0))=0$，来得到关于$g$的一个线性组合$\sum_i \alpha_i z_{t+i} g(L^{t+i}(S^0))=0$。显然，快速代数攻击的实施不需要求出大量的线性无关零化子来建立方程，只需要找到关于f的一个

特殊的倍式关系，但是需要更多的明文-密文来获得连续的密钥比特流。因此，快速代数攻击对布尔函数提出了更高的要求。快速代数攻击对 Toyocrypt、LILI-128 和蓝牙通信中的 E0 密码算法都非常有效。为了衡量布尔函数抵抗快速代数攻击的能力，文献[45]引进了快速代数免疫度（Fast Algebraic Immunity，FAI）的概念。目前对于快速代数免疫度的研究还处于起步阶段，只有极少数布尔函数的快速代数免疫度得到严格证明，更为普遍的做法是用计算机程序对较小变元的函数进行测试，以此来说明该类函数抵抗快速代数攻击的能力。标准代数攻击和快速代数攻击的复杂度比较见表 1-1。

表 1-1 两类代数攻击方法的复杂度比较

攻击方法	计算复杂度	空间复杂度
标准代数攻击	$O(D^3)$	$O(D)$
快速代数攻击	$O(D\log^2 D)$	$O(E^3+ED\log D)$

注：表中$D=\sum_{i=0}^{\mathrm{AI}(f)}\binom{n}{i}$，$E=\sum_{i=0}^{\deg(g)}\binom{n}{i}$，$n$是线性反馈移位寄存器的级数，$\mathrm{AI}(f)$是$f$的代数免疫度，$\deg(g)$是$g$的代数次数。

1.2.3 安全的布尔函数设计准则

为了抵抗各种已知密码攻击，密码系统中使用的布尔函数需同时满足多项密码学性质，目前主要包括平衡性，高非线性度，高代数次数，较好的（快速）代数免疫度等[21]。

- **平衡性**

平衡性（Balancedness）是指布尔函数的输出序列中 0 和 1 的个数各占一半。若密码系统中使用的布尔函数不具有平衡性，则密码系统无法抵抗基于统计分析的概率攻击。平衡性是布尔函数在应用中需具备的最基本的性质。

- **代数次数**

代数次数（Algebraic Degree）是指布尔函数的多项式表达式的次数。若密码系统中布尔函数的代数次数过低，则可能遭受 Berlekamp-Massey 算法攻击[18,19]和 Rønjom-Helleseth 攻击[20]。因此，要求密码系统中的布尔函数具备较高的代数次数。

- **非线性度**

非线性度（Nonlinearity）是指布尔函数与全体仿射函数（代数次数不超过 1）的最小汉明

距离。为了抵抗最佳仿射逼近[21]和快速相关攻击[22]，密码系统中的布尔函数需尽量远离仿射函数，也即具有较高的非线性度。

- **代数免疫度**

代数免疫度（Algebraic Immunity，AI）[23, 25]是指布尔函数及其反函数的非零零化子的代数次数最小值，它描述布尔函数抵抗代数攻击的能力。密码系统中使用的布尔函数应具备较高的代数免疫度以抵抗代数攻击。n元布尔函数的代数免疫度不超过$\left\lceil \frac{n}{2} \right\rceil$[25]，若达到该上界，则称布尔函数具有最优代数免疫度。

- **快速代数免疫度**

快速代数免疫度（Fast Algebraic Immunity，FAI）[45]是衡量布尔函数抵抗快速代数攻击能力的指标，定义为$2\mathrm{AI}(f)$与$\min\{\deg(g)+\deg(fg)|1\le\deg(g)<\mathrm{AI}(f)\}$的较小值，其中$\mathrm{AI}(f)$表示$f$的代数免疫度，$\deg(g)$表示$g$的代数次数。密码系统中布尔函数应具备较高的快速代数免疫度。n元布尔函数的快速代数免疫度若达到n（或$n-1$），则称该函数具有最优（或几乎最优）快速代数免疫度。

1.3 国内外研究现状

大量研究表明，旋转对称布尔函数（Rotation Symmetric Boolean Functions，RSBFs）具有良好的密码学性质，是密码函数的一类良好选择[26, 27]。快速代数攻击和快速代数免疫度是近年来新提出的概念，相关的研究还比较薄弱。对于给定的构造函数，探究其快速代数免疫度还停留在程序测试的层面，很少有函数的快速代数免疫度能得到理论证明。下面，我们介绍近年来具有最优代数免疫度的旋转对称布尔函数构造和布尔函数快速代数免疫度的研究现状。

1.3.1 具有最优代数免疫度的旋转对称布尔函数

旋转对称布尔函数，又称幂等函数，是一类输出值在输入的循环移位下保持不变的布尔函数。这种旋转对称性质使得该类函数具有结构简单、运算速度快、实现代价小等优点，主要应用于分组密码 S 盒和压缩函数的设计中。

到目前为止，关于代数免疫最优旋转对称布尔函数的构造已取得了较多的成果。2007年，Sarkar 等[28]率先给出一类具有最优代数免疫度的奇数元 RSBFs 的构造，所构函数非线性度为$2^{n-1}-\binom{n-1}{\frac{n-1}{2}}+2$。 2009 年，Sarkar 等[29]构造的偶数元代数免疫最优 RSBFs 非线性度高于$2^{n-1}-\binom{n-1}{\frac{n}{2}}+4$。2011 年，付绍静等[30]提出了一类$2^m$元代数免疫最优 RSBFs 构造方法，非线性度为$2^{n-1}-\binom{n-1}{\frac{n}{2}}+3+\frac{(n-4)(n-6)}{8}$。显然，所构 RSBFs 的非线性度高出$2^{n-1}-\binom{n-1}{\lfloor\frac{n}{2}\rfloor}$的部分从$O(1)$提升到了$O(n^2)$。2013 年，付绍静等[31]构造了一类具有最优代数免疫度偶数元 RSBFs，当$\frac{n}{2}$是奇数时，其非线性度是$2^{n-1}-\binom{n-1}{\frac{n}{2}}+\frac{(n-6)^2}{4}$；当$\frac{n}{2}$是偶数时，其非线性度是$2^{n-1}-\binom{n-1}{\frac{n}{2}}+\frac{(n-4)^2}{4}$。然而，由这些方法得到的 RSBFs 非线性度性质表现并不是很理想，其数值仅略微高于 Lobanov 界$2^{n-1}-\binom{n-1}{\lfloor\frac{n}{2}\rfloor}$[32]，而这个界是布尔函数达到代数免疫度最优非线性度的最小值。

2014 年，苏四红和唐小虎[33]基于整数拆分理论构造了两类代数免疫最优 RSBFs，其非线性度分别为$2^{n-1}-\binom{n-1}{\frac{n-1}{2}}+2^{\frac{n-1}{2}}-2$（其中$n$是奇数且$n\geq 11$）和$2^{n-1}-\binom{n-1}{\frac{n}{2}}+\frac{3}{4}\cdot 2^{\frac{n}{2}}-2$（其中$n$是偶数且$n\geq 10$）。很明显，所构 RSBFs 的非线性度高出$2^{n-1}-\binom{n-1}{\lfloor\frac{n}{2}\rfloor}$的部分从$O(n^2)$提升到了$O(2^{\lfloor\frac{n}{2}\rfloor})$。在同一年，陈银冬等[34]改进苏四红的方法构造了一类具有最优代数免疫度的偶数元 RSBFs，该类函数有更高的非线性度$2^{n-1}-\binom{n-1}{\frac{n}{2}}+2^{\frac{n}{2}}-n$（其中$n\geq 12$）。2016 年，付绍静等[35]构造了一类奇数元代数免疫最优 RSBFs，其非线性度为$2^{n-1}-\binom{n-1}{\frac{n-1}{2}}+\frac{5}{4}\cdot 2^{\frac{n-1}{2}}-\frac{n-1}{2}$（其中$n\geq 13$）。在同一年，孙磊等[37]给出了一类$2p$元（其中$p$是素数）具有最优代数免疫度和高非线性度的 RSBFs 构造方法。2018 年，孙磊等[36]基于一种新型整数拆分理论构造了一类奇数元代数免疫最优 RSBFs，该类函数经测试具有很好的快速代数免疫度，其非线性度对比已有构造有很大提升。2019 年，赵庆兰等[38]提出了一类具有最优代数免疫度的奇数元 RSBFs 构造方法，其非线性度为$2^{n-1}-\binom{n-1}{\frac{n-1}{2}}+\frac{3}{2}\cdot 2^{\frac{n-1}{2}}-n+1$（其中$n\geq 11$），陈银冬等[39]构造了一类代数免疫最优奇数元 RSBFs，非线性度为$2^{n-1}-\binom{n-1}{\frac{n-1}{2}}+2\cdot 2^{\frac{n-1}{2}}-\frac{n^2+7}{4}$（其中$n\geq 11$），并且这两类函数经测试具有良好的抵抗快速代数攻击的能力。在同一年，Zhang 等[40]提出了两类具有最优代数免疫度旋转对称布尔函数的构

造方法，其非线性度分别为$2^{n-1}-\binom{n-1}{\frac{n-1}{2}}+(n-11)2^{\frac{n-5}{2}}+n+1$（其中$n$是奇数且$n\geq 11$）和$2^{n-1}-\binom{n-1}{\frac{n}{2}}+(n-3)2^{\frac{n-8}{2}}-2n+10$（其中$n$是偶数且$n\geq 10$），并且对于变元数量较小时经测试这两类函数都有较好的快速代数免疫度。显然，所构 RSBFs 的非线性度高出$2^{n-1}-\binom{n-1}{\lfloor\frac{n}{2}\rfloor}$的部分从$O(2^{\lfloor\frac{n}{2}\rfloor})$提升到了$O(n2^{\lfloor\frac{n}{2}\rfloor})$。

1.3.2 布尔函数的快速代数免疫度

对于n元布尔函数f，若存在一个代数次数较低的函数g使得$g\cdot f$的代数次数不大于$\frac{n}{2}$，那么快速代数攻击对于f就是有效的[41-43]。为了抵抗快速代数攻击，密码系统中使用的布尔函数需满足较高的快速代数免疫度[44, 45]。2012 年，刘美成等[46]提出了完美代数免疫（Perfect Algebraic Immune, PAI）的概念，f是n元布尔函数，e是任意正整数且$e<\frac{n}{2}$，若对于任意次数不小于e的函数g都有$g\cdot f$的代数次数不小于$n-e$，则称f是完美代数免疫函数。并且他们[46]证明了n元布尔函数具有完美代数免疫度当且仅当$n=2^s$或$n=2^s+1$；并且仅当变元数量是2^s+1，存在平衡完美代数免疫函数，仅当变元数量是2^s，存在不平衡完美代数免疫函数。实际上，完美代数免疫函数具有最优代数免疫度和最优快速代数免疫，且代数次数不低于是$n-1$[46]。2012 年，王启春等[47]给出了快速代数免疫度关于高阶非线性度的一个上界。Carlet-Feng 函数[14]和 T-C-T 函数[49]是目前比较有代表性的两类布尔函数，它们都有最优代数免疫度、高非线性度、最优代数次数和较好的快速代数免疫度等性质。2012 年，刘美成等[46]证明了变元数量为2^s+1的 Carlet-Feng 函数是完美代数免疫函数；2014 年，他们[50]还证明了 T-C-T 函数对于任意变元都有几乎最优快速代数免疫度。2014 年，张寅等[51]分析了旋转对称布尔函数的快速代数免疫度，指出偶数非 2 方幂变元数量的旋转对称布尔函数的快速代数免疫度上界是$n-1$。2017 年，唐灯等[52]构造了一大类代数免疫最优 1 阶弹性函数，这类函数兼有最优代数次数和很高的非线性度下界等良好性质，且能从理论上证明其快速代数免疫度不小于$n-6$。这是 1 阶弹性函数的快速代数免疫度下界第一次得到理论上的证明。然而到目前为止，对于变元数量大于 16 的布尔函数，即使是依靠计算机程序辅助计算，确定其快速代数免疫度仍然是非常困难的事情。

择多逻辑函数[21]是一类特殊的对称布尔函数，也是发现的第一类具有最优代数免疫度

的对称函数[54]，当输入向量汉明重量大于等于$\left\lceil \frac{n}{2} \right\rceil$时，函数值取 1，其余取 0。2006 年欧密会上，Armknecht 等[59]提出了一种高效的计算布尔函数快速代数免疫度的算法，并且他们证明了择多逻辑函数具有很低的快速代数免疫度：假设$2^m \le n < 2^{m+1}$，对于n元择多逻辑函数F_M，有$\mathrm{FAI}(F_M) \le n - 2^{m-1} + \mathrm{c}$，其中，当$n$为偶数时$c = 2$，当$n$为奇数时$c = 1$。2011 年，刘美成等[62]证明了几乎所有的对称布尔函数(包括一些代数免疫最优对称布尔函数)对快速代数攻击的抵抗能力都很弱：对于变元数量为n(其中$2^m \le n \le 2^m + 2^{m-1} - 1$)的对称布尔函数$f$，则有$\mathrm{AI}(f) \le 2^{m-1} - 1$或者$\mathrm{FAI}(f) \le 2n - 3 \cdot 2^{m-1} + 2$ [62]。因此，对于变元数量在 2 的方幂附近的择多逻辑函数，其快速代数免疫度都很低。2016 年，唐灯等[63]基于择多逻辑函数的对称性，给出了其快速代数免疫度的一个下界$\mathrm{FAI}(F_M) \ge \left\lfloor \frac{n}{2} \right\rfloor + 2$(其中$n \ge 3$)。而对于变元$2^m$和$2^m + 1$，这一下界恰好与文献[59]中的上界相等。由此得出结论：择多逻辑函数在变元数量为2^m和$2^m + 1$时(其中$m \ge 2$)快速代数免疫度为$2^{m-1} + 2$。这是对称布尔函数的快速代数免疫度准确值第一次得到理论上的证明。

1.4 本文内容及结构

本文提出了两种具有最优代数免疫度的奇数元旋转对称布尔函数构造方法，并分析了择多逻辑函数的在两类特殊变元下的快速代数免疫度。论文的研究内容和组织结构如下：

第二章主要介绍布尔函数的基本概念，包括布尔函数的常见表示方法、主要密码学性质以及三类特殊的布尔函数。

第三章提出一种具有最优代数免疫度的奇数元旋转对称布尔函数构造方法，所构函数兼具平衡性、高非线性度、较好的快速代数免疫度等性质，其代数次数在特殊变元达到最优。通过简单的修改，构造了另一类相似的具有很好代数次数的旋转对称布尔函数。

第四章通过分析择多逻辑函数对称性给出了其快速代数免疫度在变元数量为$2^m + 2 \le n < 2^{m+1}$(其中$m \ge 2$)时的一个下界，结合已有结论，可以得出$2^m + 2$和$2^m + 3$变元的择多逻辑函数快速代数免疫度为$2^{m-1} + 4$。

第五章对本文完成的主要工作做了总结，并对进一步的工作进行了展望。

第二章 预备知识

本章首先介绍向量空间和布尔函数的基本概念；其次介绍三类重要的布尔函数：旋转对称布尔函数、对称布尔函数和择多逻辑函数；最后介绍安全的布尔函数需满足的密码学性质。

2.1 向量空间

令$\mathbb{F}_2^n$表示有限域$\mathbb{F}_2=\{0,1\}$上的n维向量空间。对于给定向量$\alpha=(a_1,a_2,\cdots,a_n)\in\mathbb{F}_2^n$，$\alpha$的支撑集定义为集合$\mathrm{supp}(\alpha)=\{i|a_i=1,1\le i\le n\}$；$\alpha$的汉明重量$\mathrm{w_H}(\alpha)$定义为其各个分量中取值为 1 的个数，也即支撑集的势，即$\mathrm{w_H}(\alpha)=|\mathrm{supp}(\alpha)|$。

本文中，为了方便表示，定义$\mathbb{F}_2^n$上的两个子集如下：

$$\mathrm{W}^{\le i}=\{\alpha\in\mathbb{F}_2^n|\mathrm{w_H}(\alpha)\le i\},$$

$$\mathrm{W}^{i}=\{\alpha\in\mathbb{F}_2^n|\mathrm{w_H}(\alpha)=i\}.$$

对于任给向量$\alpha=(a_1,a_2,\cdots,a_n)\in\mathbb{F}_2^n$和$u=(u_1,u_2,\cdots,u_n)\in\mathbb{F}_2^n$，若对所有的$1\le i\le n$都有$a_i\le u_i$，则称向量$\alpha$被向量$u$覆盖（或者向量$u$覆盖向量$\alpha$），记为$\alpha\preccurlyeq u$；若存在$a_j>u_j$，其中$1\le j\le n$，则称向量$\alpha$不被向量$u$覆盖（或者向量$u$不覆盖向量$\alpha$），记为$\alpha\not\preccurlyeq u$。向量$\alpha$与向量$u$模 2 内积定义为$\alpha\cdot u=a_1u_1\oplus a_2u_2\oplus\cdots\oplus a_nu_n$。

给定向量$x=(x_1,x_2,\cdots,x_n)\in\mathbb{F}_2^n$，对于其中任意一个分量$x_i$（其中$1\le i\le n$）和整数$0\le k<n$，定义

$$\rho_n^k(x_i)=\begin{cases}x_{i+k}, & i+k\le n,\\ x_{i+k-n}, & \text{其他}.\end{cases}$$

把该定义推广到向量上为：

$$\rho_n^k(x_1,x_2,\cdots,x_n)=(\rho_n^k(x_1),\rho_n^k(x_2),\cdots,\rho_n^k(x_n)).$$

实际上ρ_n^k作用在向量上也就是对该向量的各个分量都做k次循环左移。向量空间$\mathbb{F}_2^n$中向量$x=(x_1,x_2,\cdots,x_n)$的轨道定义为

$$G_n(x) = \{\rho_n^k(x_1, x_2, \cdots, x_n) | 0 \le k < n\}.$$

显然，向量空间$\mathbb{F}_2^n$中所有轨道长度(轨道中包含的向量个数)不超过n。另外，向量空间$\mathbb{F}_2^n$可以表示为若干互不相交的轨道的并集。例如，当$n=4$，向量空间$\mathbb{F}_2^4$可以写成下面 6 个轨道的并集：

$$\begin{cases} G_4(0,0,0,0) = \{(0,0,0,0)\}; \\ G_4(1,0,0,0) = \{(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\}; \\ G_4(1,1,0,0) = \{(1,1,0,0),(0,1,1,0),(0,0,1,1),(1,0,0,1)\}; \\ G_4(1,0,1,0) = \{(1,0,1,0),(0,1,0,1)\}; \\ G_4(1,1,1,0) = \{(1,1,1,0),(0,1,1,1),(1,0,1,1),(1,1,0,1)\}; \\ G_4(1,1,1,1) = \{(1,1,1,1)\}. \end{cases}$$

2.2 布尔函数的基本概念

一个n元布尔函数是指$\mathbb{F}_2^n \to \mathbb{F}_2$的一个映射。将全体$n$元布尔函数构成的集合用$\mathcal{B}_n$表示，显然，$|\mathcal{B}_n| = 2^{2^n}$。 下面介绍布尔函数常见的几种表示方法。

- **真值表**

任意一个n元布尔函数都可以唯一表示成长度为2^n的二进制序列(按照字典序)，称为布尔函数真值表，即

$$f = [f(0,0,\cdots,0), f(1,0,\cdots,0), \cdots, f(0,1,\cdots,1), f(1,1,\cdots,1)].$$

f的支撑集$\mathrm{supp}(f)$定义为集合$\{x \in \mathbb{F}_2^n | f(x) = 1\}$，$f$的汉明重量定义为真值表中 1 出现的次数，即支撑集的势。若布尔函数$f \in \mathcal{B}_n$的真值表中 0 和 1 的数量相同，即$|\mathrm{supp}(f)| = 2^{n-1}$，则称$f$是平衡的。

布尔函数f的反函数是指真值表中所有元素取反(与 1 异或)得到的函数，即$1 + f(x)$，简记为$1 + f$。两个布尔函数$f, g \in \mathcal{B}_n$的汉明距离定义为

$$\mathrm{d_H}(f,g) = |\{x \in \mathbb{F}_2^n | f(x) \ne \mathrm{g}(x)\}| = \mathrm{w_H}(f+g).$$

- **代数正规型**

任意一个n元布尔函数都可以表示成$\mathbb{F}_2[x_1, x_2, \cdots, x_n]/\{x_i^2 + x_i\}_{1 \le i \le n}$上的多项式形式，即

$$f(x_1, x_2, \cdots, x_n) = \sum_{u \in \mathbb{F}_2^n} \lambda_u \prod_{j=1}^{n} x_j^{u_j}, \tag{2-1}$$

其中$\lambda_u \in \mathbb{F}_2$，$u=(u_1,u_2,\cdots,u_n)\in\mathbb{F}_2^n$，$\Sigma$ 表示$\mathbb{F}_2$域上的加法，这种表示方法称为代数正规型（Algebraic Normal Form，ANF）。单项式x^u的系数λ_u可由 Möbius 逆变换[1, 12]确定：

$$\lambda_u=\sum_{x\in\mathbb{F}_2^n,x\preceq u} f(x). \tag{2-2}$$

布尔函数$f\in\mathcal{B}_n$的代数次数$\deg(f)$定义为所有满足$\lambda_u\neq 0$的向量u的汉明重量最大值，即$\deg(f)=\max\{\mathrm{w_H}(u)|\lambda_u\neq 0\}$。代数次数不超过 1 的布尔函数称为仿射函数，所有n元仿射函数构成的集合用$\mathcal{A}_n$表示。

- **Walsh 谱**

一个n元布尔函数f在向量$\omega\in\mathbb{F}_2^n$的 Walsh 谱（变换）定义为

$$W_f(\omega)=\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus\omega\cdot x}, \tag{2-3}$$

其中，Σ 表示整数域上的加法。布尔函数在$\mathbb{F}_2^n$中所有元素的 Walsh 变换的值构成的多重集称为 Walsh 谱。Walsh 谱是研究布尔函数的一项重要工具，布尔函数的很多性质都可以用 Walsh 谱来刻画。

2.3 三类特殊的布尔函数

布尔函数的研究是由简入繁的过程，一些结构简单的布尔函数起到了重要作用。下面介绍三类特殊的布尔函数。

2.3.1 旋转对称布尔函数

定义 2.1 ([26]) 如果一个布尔函数$f\in\mathcal{B}_n$满足，对任意的$x=(x_1,x_2,\cdots,x_n)\in\mathbb{F}_2^n$和$1\le k<n$都有

$$f\left(\rho_n^k(x_1,x_2,\cdots,x_n)\right)=f(x_1,x_2,\cdots,x_n),$$

则称f是旋转对称布尔函数（Rotation Symmetric Boolean Function，RSBF）。也即是，旋转对称布尔函数在同一轨道输入下函数值相等。

n元旋转对称布尔函数$f(x_1,x_2,\cdots,x_n)$的短代数正规型可以表示为

$$a \oplus a_1 x_1 \oplus a_{12} x_1 x_2 \oplus \cdots \oplus a_{12\cdots n} x_1 x_2 \cdots x_n,$$

其中，$a, a_1, a_{12}, \cdots, a_{12\cdots n} \in \mathbb{F}_2$，代表项$x_1 x_{i_1} \cdots x_{i_t}$出现在上式中就表示$G_n\left(x_1 x_{i_1} \cdots x_{i_t}\right)$中所有项都出现在$f$的代数正规型中，其中$G_n\left(x_1 x_{i_1} \cdots x_{i_t}\right)$表示$x_1 x_{i_1} \cdots x_{i_t}$做循环左移得到了所有项。

2.3.2 对称布尔函数

定义 2.2 ([1]) 如果一个布尔函数$f \in \mathcal{B}_n$满足，对任意的$x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n$都有

$$f\left(\tau(x_1, x_2, \cdots, x_n)\right) = f(x_1, x_2, \cdots, x_n),$$

其中，$\tau(x_1, x_2, \cdots, x_n)$表示$\{x_1, x_2, \cdots, x_n\}$的任意排列组成的向量，则称$f$是对称布尔函数。也即是对称布尔函数在汉明重量相同的向量输入下取值相等。

因此，对称布尔函数是一类特殊的旋转对称布尔函数。所有的n元对称布尔函数组成的集合用$\mathcal{SB}_n$表示。显然，任意的n元对称布尔函数f都可由一个$n+1$维向量表示

$$v_f = \left(v_f(0), v_f(1), \cdots, v_f(n)\right) \in \mathbb{F}_2^{n+1},$$

其中，$v_f(i) = f(\alpha)$，$\alpha \in \mathrm{W}^i$，$0 \le i \le n$。向量v_f称为对称布尔函数f的简化真值表。

n元对称布尔函数f是对称的当且仅当f的代数正规型可以写成

$$f(x_1, x_2, \cdots, x_n) = \sum_{i=0}^{n} \lambda_f(i)\sigma_i, \tag{2-4}$$

其中，$\lambda_f(i) \in \mathbb{F}_2$，$\sigma_i$是所有$i$次齐次项之和构成的初等对称布尔函数，即$\sigma_0 = 1$，$\sigma_1 = \bigoplus_{i=1}^{n} x_i$，$\sigma_2 = \bigoplus_{1 \le i < j \le n} x_i x_j$，$\cdots$，$\sigma_n = x_1 x_2 \cdots x_n$。

2.3.3 择多逻辑函数

定义 2.3 ([21]) 变元数量为n的择多逻辑函数F_M在输入向量汉明重量大于等于$\left\lceil \frac{n}{2} \right\rceil$时取值为1，余下取值为0，即

$$F_M(x)=\begin{cases}1, & \mathrm{w_H}(x)\geq\left\lceil\frac{n}{2}\right\rceil,\\ 0, & \text{其他.}\end{cases} \tag{2-5}$$

显然，择多逻辑函数是一类特殊的对称布尔函数。丁存生等[21]在 1991 年首先提出择多逻辑函数的概念，Dalai 等[54]在 2006 年证明了此类函数具有最优代数免疫度，代数次数$2^{\lfloor\log_2 n\rfloor}$和非线性度$2^{n-1}-\binom{n-1}{\lfloor\frac{n}{2}\rfloor}$。由 Lobanov 界[32]可知，其非线性度几乎是布尔函数达到最优代数免疫度非线性度的最小值。后来，人们按照一定的规则修改择多逻辑函数的支撑集，得到了诸多具有最优代数免疫度的旋转对称布尔函数[28-40]。

对于奇数元择多逻辑函数，其 Walsh 谱有如下特征。

引理 2.1 ([28, 54]) 令F_M表示n元择多逻辑函数，其中$n=2k+1$。对于任意的$\omega\in\mathbb{F}_2^n$，有下面结论：

(1) 如果$\mathrm{w_H}(\omega)=1$，那么$W_{F_M}(\omega)=2\binom{n-1}{k}$；

(2) 如果$\mathrm{w_H}(\omega)=n$，那么$W_{F_M}(\omega)=2(-1)^k\binom{n-1}{k}$；

(3) 如果$2\leq\mathrm{w_H}(\omega)\leq n-1$，那么$|W_{F_M}(\omega)|\leq 2[\binom{n-3}{k-1}-\binom{n-3}{k}]$，其中$n\geq 7$。

2.4 布尔函数的密码学性质

密码系统中所使用的布尔函数必须同时满足多项密码学性质以抵抗各种已知攻击，主要包括平衡性，高非线性度，高代数次数，较好的(快速)代数免疫度等。

- **平衡性**

密钥流生成器产生的密钥流是否具有伪随机特性决定流密码系统的安全性强弱。平衡性是衡量伪随机性的一个重要方面。若密码系统中使用的布尔函数输出序列中 0 和 1 数量不等，那么密码系统就无法抵抗基于统计分析的概率攻击。因此，平衡性是安全的布尔函数基本设计准则之一。布尔函数平衡性可由 Walsh 变换来描述。

引理 2.2 若布尔函数$f\in\mathcal{B}_n$是平衡的，则$W_f(0_n)=0$。

- **代数次数**

为了抵抗 Berlekamp-Massey 算法攻击[18, 19]和 Rønjom-Helleseth 攻击[20]，应用中的布尔

函数应具有较高的代数次数。因此，高代数次数也是安全的布尔函数的基本设计准则之一。

对于n元平衡布尔函数f，其中$n \geq 2$，即f的汉明重量是偶数，由(2-2)式计算$x_1x_2\cdots x_n$的系数为

$$\lambda_{1_n} = \sum_{x\in\mathbb{F}_2^n} f(x) = 0.$$

因此有如下引理：

引理 2.3 若布尔函数$f \in \mathcal{B}_n$的汉明重量是偶数，则$\deg(f) \leq n-1$。

- **非线性度**

为了抵抗最佳仿射逼近[21]和快速相关攻击[22]，密码系统中的布尔函数与所有仿射函数的汉明距离应尽可能大。由此产生了非线性度的定义。

定义 2.4 布尔函数的非线性度是其与所有仿射函数的最小汉明距离。对于布尔函数$f \in \mathcal{B}_n$，其非线性度为

$$\mathrm{NL}(f) = \min_{g\in\mathcal{A}_n} \mathrm{d_H}(f,g).$$

另外，对于$\omega \in \mathbb{F}_2^n$，由 Walsh 谱的定义可得

$$\begin{aligned} W_f(\omega) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\omega\cdot x} \\ &= |\{x\in\mathbb{F}_2^n | f(x) = \omega\cdot x\}| - |\{x\in\mathbb{F}_2^n | f(x) \neq \omega\cdot x\}| \\ &= 2^n - 2\mathrm{w_H}(f+\omega\cdot x). \end{aligned}$$

因此，布尔函数的非线性度可由 Walsh 变换等价表示为

$$\mathrm{NL}(f) = 2^{n-1} - \frac{1}{2}\max_{\omega\in\mathbb{F}_2^n} W_f(\omega). \tag{2-6}$$

- **（快速）代数免疫度**

代数免疫度[23, 25]是衡量布尔函数抵抗代数攻击的能力，代数攻击的基本思路是将密码系统破译问题归结到代数方程组的求解问题。若密码系统使用的布尔函数或其反函数存在低次零化子，那么代数攻击对该密码系统就是有效的。

定义 2.5 ([25]) 对于两个布尔函数$f, g \in \mathcal{B}_n$，若$(f\cdot g)(x) = f(x)\cdot g(x) = 0$，则称$g$是$f$的一个零化子。$n$元布尔函数$f$的所有零化子组成的集合记为$\mathrm{Ann}(f) = \{g\in\mathcal{B}_n | f\cdot g = 0\}$。布尔函数$f$的代数免疫度$\mathrm{AI}(f)$定义为$f$及$1+f$所有非零零化子代数次数的最小值，即

$$\mathrm{AI}(f) = \min\{\deg(g) | 0 \neq g \in \mathrm{Ann}(f) \cup \mathrm{Ann}(1+f)\}.$$

若n元布尔函数的代数免疫度达到了上界$\left\lceil \frac{n}{2} \right\rceil$[25]，则称$f$具有最优代数免疫度。

布尔函数具有较高的代数免疫度是抵抗代数攻击的必要条件，而绝非充要条件。对于n元布尔函数f，若存在一个代数次数较低的非零函数g使得$g \cdot f$的代数次数远小于n，那么快速代数攻击对于f就是有效的[41-43]。为了抵抗快速代数攻击，密码系统中使用的布尔函数需满足较高的快速代数免疫度[44, 45]。

定义 2.6 ([45]) 布尔函数$f \in \mathcal{B}_n$的快速代数免疫度为

$$\mathrm{FAI}(f) = \min\{2\mathrm{AI}(f), \min\{\deg(g) + \deg(fg) | 1 \leq \deg(g) < \mathrm{AI}(f)\}\}.$$

若f的快速代数免疫度达到n（或$n-1$），则称f具有最优（或几乎最优）快速代数免疫度。

第三章 具有最优代数免疫度的奇数元旋转对称布尔函数

本章首先给出了一类奇数元旋转对称布尔函数的构造方法，证明了其最优代数免疫度、高非线性度等性质，并验证了在较小变元时有较好的快速代数免疫度。接着给出了第二类具有最优代数免疫度和高代数次数的旋转对称布尔函数的构造方法，可用其弥补第一类函数的代数次数不足的缺陷。

3.1 整数拆分

正整数k的拆分是指一些满足$k_1+k_2+\cdots+k_m=k$的正整数序列$(k_1,k_2,\cdots,k_m)$，要考虑到其中的顺序，因此，序列中不同的排列对应不同的拆分方式。易知，把正整数k拆分成m部分共有$\binom{k-1}{m-1}$种拆分方式。

对于给定的k和m，把同时满足下面两个条件的所有拆分方式的数量记为$p_m(k)$，

- $k_1+k_2+\cdots+k_m=k$;
- $k_1\le k_2\le\cdots\le k_m$.

$p_m(k)$的直接求解是个比较困难的问题，文献[64]给出了其递归求解的方法，即$p_m(k)=p_{m-1}(k-1)+p_m(k-m)$，规定$p_1(k)=p_k(k)=1$。

3.2 构造方法一

令$k\ge5$，$n=2k+1$，$H=\{h|3\le h\le k\}$。根据整数拆分的结果，对$h\in H$，$1\le m\le h-2$，定义$\mathbb{F}_2^n$上的集合$T_{h,m}$为

$$T_{h,m}=\{(\underbrace{1,\cdots,1}_{k_1},\underbrace{0,\cdots,0}_{d_1},\cdots,\underbrace{1,\cdots,1}_{k_m},\underbrace{0,\cdots,0}_{d_m},\underbrace{0,\cdots,0}_{2(k+1-h)})\in \mathrm{W}^h|$$

若$m=1,k_1=h,d_1=h-1$;

若$m\ge2,k_1,k_m\ge2,k_2,\cdots,k_{m-1}\ge1,d_m>d_{m-1}\ge d_{m-2}\ge\cdots\ge d_1\ge1\}$.

显然，$k_1+k_2+\cdots+k_m=h$，$d_1+d_2+\cdots+d_m=h-1$。因此，对于每个$\alpha\in T_{h,m}$都包含了两组拆分：h拆分成m部分$(k_1,k_2,\cdots,k_m)$，$h-1$拆分成m部分$(d_1,d_2,\cdots,d_m)$。这两部分的拆分结果的集合分别用$C_{h,m}^1$和$C_{h-1,m}^0$表示。则

$$C_{h,m}^1=\{(k_1,k_2,\cdots,k_m)|k_1+k_2+\cdots+k_m=h,$$

$$若m=1,k_1=h;若m\geq 2,k_1,k_m\geq 2,k_2,\cdots,k_{m-1}\geq 1\};$$

$$C_{h-1,m}^0=\{(d_1,d_2,\cdots,d_m)|d_1+d_2+\cdots+d_m=h-1,$$

$$若m=1,d_1=h-1;若m\geq 2,d_m>d_{m-1}\geq d_{m-2}\geq\cdots\geq d_1\geq 1\}.$$

根据整数拆分的相关结论易知，$\left|C_{h-1,m}^0\right|=p_m(h-2)$，$\left|C_{h,m}^1\right|=\binom{h-3}{m-1}$。因此，$\left|T_{h,m}\right|=\left|C_{h-1,m}^0\right|\cdot\left|C_{h,m}^1\right|$。

令$T_h=\bigcup_{m=1}^{h-2}T_{h,m}$，则

$$|T_h|=\sum_{m=1}^{h-2}p_m(h-2)\binom{h-3}{m-1}. \tag{3-1}$$

把T_h集合中的向量按照字典序排列为

$$T_h=\left\{\alpha_{h_1},\alpha_{h_2},\cdots,\alpha_{h_{|T_h|}}\right\}.$$

对于$3\leq h\leq k$，定义$\mathbb{F}_2^n$上的另一个集合$U_h\subseteq \mathrm{W}^{k+1}$为

$$U_h=\{u_{h_s}=\alpha_{h_s}\oplus(0,\cdots,0,\underbrace{1,0,\cdots,1,0}_{2(k+1-h)})|\alpha_{h_s}\in T_h\}.$$

显然，对于任意的$\alpha_{h_i}\in T_h$，$u_{h_i}\in U_h$，都有$\mathrm{w_H}(\alpha_{h_i})=h$，$\mathrm{w_H}(u_{h_i})=k+1$。令$T=\bigcup_{h=3}^{k}T_h$，$U=\bigcup_{h=3}^{k}U_h$，因这两个集合中元素存在严格一一对应关系，所以$|T|=|U|$。为方便起见，令$L_k=|T|$，由(3-1)式得

$$L_k=\sum_{h=3}^{k}|T|=\sum_{h=3}^{k}\sum_{m=1}^{h-2}p_m(h-2)\binom{h-3}{m-1}. \tag{3-2}$$

列出T和U集合中各个元素为

$$T=\left\{\alpha_{3_1},\alpha_{4_1},\alpha_{4_2},\alpha_{5_1},\cdots,\alpha_{5_4},\cdots,\cdots,\alpha_{k_1},\cdots,\alpha_{k_{|T_h|}}\right\},$$

$$U=\left\{u_{3_1},u_{4_1},u_{4_2},u_{5_1},\cdots,u_{5_4},\cdots,\cdots,u_{k_1},\cdots,u_{k_{|T_h|}}\right\}.$$

为方便起见，简记为

$$T = \{\alpha_1, \alpha_2, \cdots, \alpha_{L_k}\},$$

$$U = \{u_1, u_2, \cdots, u_{L_k}\}.$$

对于给定向量$x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n$，定义

$$(x)_i^j = (x_i, \cdots, x_j),$$

也即是，截取x向量的第i个到第j个分量所构成的向量。

引理 3.1 对于任意的$h, h' \in H$，$1 \le s, t \le |T_h|$，$1 \le r \le |T_{h'}|$，$\alpha_{h_s} \in T_h$，$\alpha_{h'_r} \in T_{h'}$，u_{h_s}，$u_{h_t} \in U_h$，则下列结论成立。

(1) $\rho_n^l(\alpha_{h_s}) \preccurlyeq \rho_n^l(u_{h_s})$，其中$0 \le l < n$；

(2) $\rho_n^l(\alpha_{h_s}) \ne \alpha_{h_s}$，$\rho_n^l(u_{h_s}) \ne u_{h_s}$，其中$1 \le l < n$；

(3) $\alpha_{h_s} \not\preccurlyeq \rho_n^l(u_{h_s})$，其中$1 \le l < n$；

(4) $\alpha_{h'_r} \not\preccurlyeq \rho_n^l(u_{h_s})$，其中$h' > h$，$1 \le l < n$；

(5) $\alpha_{h_s} \not\preccurlyeq \rho_n^l(u_{h_t})$，其中$s > t$，$0 \le l < n$。

证明： 令$\alpha_{h_s} \in T_{h,m}$，则可表示为

$$\alpha_{h_s} = (\underbrace{1, \cdots, 1}_{k_1}, \underbrace{0, \cdots, 0}_{d_1}, \cdots, \underbrace{1, \cdots, 1}_{k_m}, \underbrace{0, \cdots, 0}_{d_m}, \underbrace{0, \cdots, 0}_{2(k+1-h)}),$$

其中$k_1 + k_2 + \cdots + k_m = h$，$d_1 + d_2 + \cdots + d_m = h - 1$。令$d = k_1 + k_2 + \cdots + k_m + d_1 + d_2 + \cdots + d_{m-1}$。

根据集合T_h和U_h的定义，(1)显然成立。

首先，对任意$1 \le l < n$，$\left[\rho_n^l(\alpha_{h_s})\right]_{d+1}^n \ne (\underbrace{0, \cdots, 0}_{d_m+2(k+1-h)}) = (\alpha_{h_s})_{d+1}^n$，故$\rho_n^l(\alpha_{h_s}) \ne \alpha_{h_s}$。同样的方法可证对任意$1 \le l < n$，$\rho_n^l(u_{h_s}) \ne u_{h_s}$成立。因此，(2)成立。

其次，若$1 \le l < d$，$\left[\rho_n^l(u_{h_s})\right]_{d+1-l}^{d+d_m-l} = (\underbrace{0, \cdots, 0}_{d_m}) \ne (\alpha_{h_s})_{d+1-l}^{d+d_m-l}$；若$d \le l < n$，$(\alpha_{h_s})_1^2 = (1, 1) \ne \left[\rho_n^l(u_{h_s})\right]_1^2$。因此，对任意$1 \le l < n$，$\alpha_{h_s} \not\preccurlyeq \rho_n^l(u_{h_s})$，即(3)成立。

再次，假设存在$\alpha_{h'_r} \in T_{h',m}$使得$\alpha_{h'_r} \preccurlyeq \rho_n^l(u_{h_s})$，其中$h \le h'$，$0 \le l < n$。不妨表示为

$$\alpha_{h'_r} = (\underbrace{1, \cdots, 1}_{k'_1}, \underbrace{0, \cdots, 0}_{d'_1}, \cdots, \underbrace{1, \cdots, 1}_{k'_{m'}}, \underbrace{0, \cdots, 0}_{d'_{m'}}, \underbrace{0, \cdots, 0}_{2(k+1-h')}),$$

$$\rho_n^l(u_{h_s}) = (\underbrace{1,\cdots,1}_{k_{i+1}-\Delta},\underbrace{0,\cdots,0}_{d_{i+1}},\cdots,\underbrace{1,\cdots,1}_{k_m},\underbrace{0,\cdots,0}_{d_m},\underbrace{1,0,\cdots,1,0}_{2(k+1-h)},$$

$$\underbrace{1,\cdots,1}_{k_1},\cdots,\underbrace{1,\cdots,1}_{k_i},\underbrace{0,\cdots,0}_{d_i},\underbrace{1,\cdots,1}_{\Delta}),$$

其中$i \geq 0$。因$k'_{m'} \geq 2$，则$k'_1 + d'_1 + \cdots + k'_{m'} \leq k_{i+1} - \Delta + d_{i+1} + \cdots + k_m$，这意味着$h' = k'_1 + k'_2 + \cdots + k'_{m'} \leq k_{i+1} - \Delta + \cdots + k_m \leq h$。因此$h' = h$且$l = 0$。进而$\alpha_{h'_r} = \alpha_{h_s}$，矛盾。因此，对任意的$h' > h$，$1 \leq l < n$，$\alpha_{h'_r} \preccurlyeq \rho_n^l(u_{h_s})$成立。故(4)得到证明。

最后，(5)可以用(4)中同样的方法得以证明。

证明完成。 □

引理 3.2 令$n = 2k + 1$，当$k \geq 5$时下面式子成立

$$3n\sum_{m=1}^{k-1} p_m(k-1)\binom{k-2}{m-1} < \binom{n}{k}.$$

证明：对$1 \leq m \leq k-1$，定义集合

$$A_m = \{(\underbrace{1,\cdots,1}_{k_1},\underbrace{0,\cdots,0}_{d_1},\cdots,\underbrace{1,\cdots,1}_{k_m},\underbrace{0,\cdots,0}_{d_m}) \in \mathrm{W}^{k+1}|$$

若$m = 1, k_1 = k+1, d_1 = k$;

若$m \geq 2, k_1, k_m \geq 2, k_2, \cdots, k_{m-1} \geq 1, d_m > d_{m-1} \geq d_{m-2} \geq \cdots \geq d_1 \geq 1\}$.

显然，$|A_m| = p_m(k-1)\binom{k-2}{m-1}$。令$A = \cup_{m=1}^{k-1} A_m$，对于$1 \leq m \leq k-1$，定义集合$A_m^* \subseteq \mathrm{W}^{k+1}$且满足$A_m^* \cap A_m = \emptyset$。

对于$m = 1$，令

$$A_1^* = \{(\underbrace{1,\cdots,1}_{k},0,1,\underbrace{0,\cdots,0}_{k-1}),(\underbrace{1,\cdots,1}_{k},0,0,1,\underbrace{0,\cdots,0}_{k-2})\}.$$

对于$m = 2$，令

$$A_2^* = \{(\underbrace{1,\cdots,1}_{k_1},\underbrace{0,\cdots,0}_{d_1},\underbrace{1,\cdots,1}_{k_2-1},0,1,\underbrace{0,\cdots,0}_{d_2-1}),$$
$$(\underbrace{1,\cdots,1}_{k_1},\underbrace{0,\cdots,0}_{d_1},\underbrace{1,\cdots,1}_{k_2-1},\underbrace{0,\cdots,0}_{d_2-1},1,0)|$$
$$(\underbrace{1,\cdots,1}_{k_1},\underbrace{0,\cdots,0}_{d_1},\underbrace{1,\cdots,1}_{k_2},\underbrace{0,\cdots,0}_{d_2}) \in A_2\}.$$

对于$3 \leq m \leq k-2$，令

$$A_m^* = \{(1,\underbrace{0,\cdots,0}_{d_1},\underbrace{1,\cdots,1}_{k_2},\cdots,\underbrace{1,\cdots,1}_{k_{m-1}},\underbrace{0,\cdots,0}_{d_{m-1}},\underbrace{1,\cdots,1}_{k_1-1},0,\underbrace{1,\cdots,1}_{k_m},\underbrace{0,\cdots,0}_{d_m-1}),$$

$$(\underbrace{1,\cdots,1}_{k_1},\underbrace{0,\cdots,0}_{d_1},\cdots,\underbrace{1,\cdots,1}_{k_{m-1}},\underbrace{0,\cdots,0}_{d_{m-1}},\underbrace{1,\cdots,1}_{k_m-1},0,1,\underbrace{0,\cdots,0}_{d_m-1})|$$
$$(\underbrace{1,\cdots,1}_{k_1},\underbrace{0,\cdots,0}_{d_1},\cdots,\underbrace{1,\cdots,1}_{k_{m-1}},\underbrace{0,\cdots,0}_{d_{m-1}},\underbrace{1,\cdots,1}_{k_m},\underbrace{0,\cdots,0}_{d_m})\in A_m\}.$$

对于$m=k-1$，令

$$A_{k-1}^{*}=\{(1,\underbrace{1,0,\cdots,1,0}_{k对\ 1,0}),(1,0,\underbrace{1,\cdots,1}_{k},\underbrace{0,\cdots,0}_{k-1})\}.$$

因此，对所有的$1\le m\le k-1$，都有$|A_m^*|=2|A_m|$成立。令$A^*=\bigcup_{m=1}^{k-1}A_m^*$，则$|A^*|=2|A|$。又因$A\cap A^*=\emptyset$，且$|G_n(\alpha)|=n$对任意$\alpha\in A\cup A^*$都成立，所以$3n|A|<\binom{n}{k}$成立。

证明完成。 □

由引理 3.1 中(2)知，对于$1\le i\le L_k$，$\alpha_i\in T$和$u_i\in U$，则

$$|G_n(\alpha_i)|=|G_n(u_i)|=n.$$

令

$$\tilde{T}=\{G_n(\alpha_1),G_n(\alpha_2),\cdots,G_n(\alpha_{L_k})\},$$

$$\tilde{U}=\{G_n(u_1),G_n(u_2),\cdots,G_n(u_{L_k})\}.$$

利用上述定义的向量空间$\mathbb{F}_2^n$上的子集合$\tilde{T}$和$\tilde{U}$，我们给出一类新型n元旋转对称布尔函数构造如下

$$f(x)=\begin{cases}F_M(x)\oplus 1, & x\in\tilde{T}\cup\tilde{U},\\ F_M(x), & 其他.\end{cases}\tag{3-3}$$

其中，$F_M\in\mathcal{SB}_n$是定义 2.3 中给出的择多逻辑函数。

附录 1 给出了所构 11 元旋转对称布尔函数例子。

3.2.1 代数免疫度

引理 3.3 ([15]) 令$n=2k+1$，集合$T=\{\alpha_1,\alpha_2,\cdots,\alpha_l\}\subseteq \mathrm{W}^{\le k}$，集合$U=\{u_1,u_2,\cdots,u_l\}\subseteq \mathrm{W}^{k+1}$，其中$\alpha_i,u_i\in\mathbb{F}_2^n$，$1\le i\le l$，$0<l\le\binom{n}{k}$。如果$T$和$U$中的向量满足下面两个条件

- $\alpha_i\preccurlyeq u_i$对于任意$1\le i\le l$都成立
- $\alpha_i\not\preccurlyeq u_j$对于任意$1\le i<j\le l$(或$1\le j<i\le l$)都成立

则布尔函数

$$f_1(x)=\begin{cases}F_M(x)\oplus 1, & x\in T\cup U,\\ F_M(x), & \text{其他}\end{cases}$$

具有最优代数免疫度，其中F_M是择多逻辑函数。

定理 3.1 (3-3)式中的n元旋转对称布尔函数f具有最优代数免疫度。

证明：要证(3-3)式中的函数具有最优的代数免疫度，按照引理 3.3，只需验证$\tilde{T}$和$\tilde{U}$中的向量同时满足下列三个条件：

- $\rho_n^l(\alpha_s)\preccurlyeq \rho_n^l(u_s)$，其中$1\le s\le L_k$，$0\le l<n$；
- $\rho_n^m(\alpha_s)\not\preccurlyeq \rho_n^l(u_s)$，其中$1\le s\le L_k$，$1\le m<l<n$；
- $\rho_n^m(\alpha_s)\not\preccurlyeq \rho_n^l(u_t)$，其中$1\le s\le L_k$，$1\le m<l<n$。

事实上，由引理 3.1 可知上面三个条件显然成立。

证明完成。 □

3.2.2 非线性度

引理 3.4 令$n=2k+1$，对于$k\ge 5$，下面不等式成立

$$\binom{n}{k}>4(3k-1)L_k.$$

证明：为了证明该不等式成立，我们构造一个辅助函数

$$g(k)=\frac{1}{4(3k-1)}\binom{n}{k}-L_k.$$

只需证明对任意$k\ge 5$，$g(k)>0$成立。

$$\begin{aligned}g(k+1)-g(k)&=\frac{1}{4(3k+2)}\binom{n+2}{k+1}-L_{k+1}-\frac{1}{4(3k-1)}\binom{n}{k}+L_k\\&=\left[\frac{2k+3}{2(3k+2)(k+2)}-\frac{1}{4(3k-1)}\right]\binom{n}{k}-\sum_{m=1}^{k-1}p_m(k-1)\binom{k-2}{m-1}.\end{aligned}$$

对于$k\ge 5$下面不等式显然成立

$$\frac{2k+3}{2(3k+2)(k+2)}-\frac{1}{4(3k-1)}>\frac{1}{3(2k+1)}.$$

所以，结合引理 3.2 可得

$$g(k+1)-g(k)>\frac{1}{3n}\binom{n}{k}-\sum_{m=1}^{k-1}p_m(k-1)\binom{k-2}{m-1}>0.$$

因此，$g(k)$在$k \geq 5$的定义域内是单调增加的，故$g(k) \geq g(5) = \frac{33}{4} - 7 > 0$。

证明完成。 □

定理 3.2 (3-3)式中的n元（其中$n = 2k + 1 \geq 11$）旋转对称布尔函数f的非线性度为

$$\mathrm{NL}(f) = 2^{n-1} - \binom{n-1}{k} + \sum_{h=3}^{k} (n-2h)|T_h| + L_k.$$

证明：对于$\omega \in \mathbb{F}_2^n$，根据(2-3)式和(2-5)式可得

$$\begin{aligned} W_f(\omega) &= \sum_{x \in \tilde{T} \cup \tilde{U}} (-1)^{F_M(x) \oplus 1 \oplus x \cdot \omega} + \sum_{x \notin \tilde{T} \cup \tilde{U}} (-1)^{F_M(x) \oplus x \cdot \omega} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{F_M(x) \oplus x \cdot \omega} + 2 \sum_{x \in \tilde{T} \cup \tilde{U}} (-1)^{F_M(x) \oplus 1 \oplus x \cdot \omega} \\ &= W_{F_M}(\omega) - 2 \sum_{x \in \tilde{T}} (-1)^{x \cdot \omega} + 2 \sum_{x \in \tilde{U}} (-1)^{x \cdot \omega} \\ &= W_{F_M}(\omega) - 2 \sum_{h=3}^{k} \sum_{i=1}^{|T_h|} \sum_{x \in G_n(\alpha_{h_i})} (-1)^{x \cdot \omega} + 2 \sum_{h=3}^{k} \sum_{i=1}^{|T_h|} \sum_{x \in G_n(u_{h_i})} (-1)^{x \cdot \omega}. \end{aligned}$$

下面按照$\mathrm{w_H}(\omega)$分为四种情况分别计算$W_f(\omega)$。

(1) $\mathrm{w_H}(\omega) = 0$，即$\omega = (0, 0, \cdots, 0)$，用$W_f(\omega)_0$表示$\omega$处的 Walsh 变换的值。因为$f$是平衡函数，由引理 2.2 易得$W_f(\omega)_0 = 0$。

(2) $\mathrm{w_H}(\omega) = 1$，则 $\sum_{x \in G_n(\alpha_{h_i})} (-1)^{x \cdot \omega} = n - 2\mathrm{w_H}(\alpha_{h_i})$，$\sum_{x \in G_n(u_{h_i})} (-1)^{x \cdot \omega} = n - 2\mathrm{w_H}(u_{h_i})$，用$W_f(\omega)_1$表示$\omega$处的 Walsh 变换的值。由引理 2.1 中(1)可得

$$\begin{aligned} W_f(\omega)_1 &= 2\left[\binom{n-1}{k} - \sum_{h=3}^{k} \sum_{i=1}^{|T_h|} \left(n - 2\mathrm{w_H}(\alpha_{h_i})\right) + \sum_{h=3}^{k} \sum_{i=1}^{|T_h|} \left(n - 2\mathrm{w_H}(u_{h_i})\right)\right] \\ &= 2\left[\binom{n-1}{k} - \sum_{h=3}^{k} (n-2h)|T_h| - \sum_{h=3}^{k} \sum_{i=1}^{|T_h|} 1\right] \\ &= 2\left[\binom{n-1}{k} - \sum_{h=3}^{k} (n-2h)|T_h| - L_k\right]. \end{aligned}$$

(3) $\mathrm{w_H}(\omega) = n$，即 $\omega = (1, 1, \cdots, 1)$，则 $\sum_{x \in G_n(\alpha_{h_i})} (-1)^{x \cdot \omega} = n(-1)^h$，

$\sum_{x\in G_n(u_{h_i})}(-1)^{x\cdot\omega}=n(-1)^{k+1}$，用$W_f(\omega)_n$表示$\omega$处的 Walsh 变换的值。由引理 2.1 中(2)可得

$$\begin{aligned}W_f(\omega)_n&=2\left[(-1)^k\binom{n-1}{k}-\sum_{h=3}^{k}|T_h|\cdot n(-1)^h+nL_k\cdot(-1)^{k+1}\right]\\&=2(-1)^k\left[\binom{n-1}{k}-\sum_{h=3}^{k}|T_h|\cdot n(-1)^{h+k}-nL_k\right].\end{aligned}$$

(4) $2\le \mathrm{w_H}(\omega)\le n-1$，用$W_f(\omega)_2$表示$\omega$处的 Walsh 变换的值。由引理 2.1 中(3)可得

$$\begin{aligned}W_f(\omega)_2&\le 2\binom{n-3}{k-1}-2\binom{n-3}{k}+4n|T_k|+4n|T_{k-1}|+\cdots+4n|T_3|\\&=2\left[\binom{n-3}{k-1}-\binom{n-3}{k}-2nL_k\right].\end{aligned}$$

显然，$|W_f(\omega)_0|<|W_f(\omega)_1|$，$|W_f(\omega)_n|<|W_f(\omega)_1|$。下面计算

$$\begin{aligned}|W_f(\omega)_1|-|W_f(\omega)_2|&\ge 2\left[\binom{n-1}{k}-\binom{n-3}{k-1}+\binom{n-3}{k}-3nL_k+2\sum_{h=3}^{k}h|T_h|-L_k\right]\\&=2\left[\frac{4k^2+k-3}{2(4k^2-1)}\binom{n}{k}-3nL_k+2\sum_{h=3}^{k}h|T_h|-L_k\right]\\&>2\left[\frac{1}{2}\binom{n}{k}-(3n+1)L_k+2\sum_{h=3}^{k}h|T_h|\right]\\&>2\left[2(3k-1)L_k-(3n+1)L_k+2\sum_{h=3}^{k}h|T_h|\right]\\&=2\left[2\sum_{h=3}^{k}h|T_h|-6L_k\right]\\&>0,\end{aligned}$$

其中，第一个不等式是直接将$|W_f(\omega)_1|$和$|W_f(\omega)_2|$做减法运算所得；第二个不等式成立是因为$4k^2+k-3>4k^2-1$对任意$k\ge 5$都成立；由引理 3.4 可知第三个不等式成立；第四个不等式成立是因为对于$k\ge 5$时，$\sum_{h=3}^{k}h|T_h|-3L_k=\sum_{h=3}^{k}(h-3)|T_h|>0$。

最后，综合上述所讨论的四种情况可得

$$\max_{\omega\in\mathbb{F}_2^n}|W_f(\omega)|=2\left[\binom{n-1}{k}-\sum_{h=3}^{k}(n-2h)|T_h|-L_k\right].$$

因此，由(2-6)式可知，(3-3)式中的n元旋转对称布尔函数f的非线性度为

$$\mathrm{NL}(f) = 2^{n-1} - \binom{n-1}{k} + \sum_{h=3}^{k}(n-2h)|T_h| + L_k.$$

证明完成。 □

在表 3-1 中，对于奇数变元数量在$11 \le n \le 31$范围，我们列出了文献[33, 38-40]及(3-3)式中所构造的旋转对称布尔函数的非线性度高出$2^{n-1} - \binom{n-1}{k}$部分的值。可以明显看出，我们提出的(3-3)式的构造方法在$n \ge 23$时具有最高的非线性度，且随着变元的增加其非线性度较其他函数的优势愈加突出。

表 3-1 几类奇数变元旋转对称布尔函数的非线性度高出$2^{n-1} - \binom{n-1}{k}$部分的比较

n	文献[33]	文献[38]	文献[39]	文献[40]	(3-3)中f
11	30	**38**	32	12	22
13	62	**84**	**84**	46	58
15	126	178	**198**	144	146
17	254	368	**438**	402	378
19	510	750	932	**1044**	962
21	1022	1516	1936	**2582**	2474
23	2046	3050	3962	6168	**6282**
25	4094	6120	8034	14362	**15962**
27	8190	12262	16200	32796	**40034**
29	16382	24548	32556	73758	**100256**
31	32766	49122	65294	163872	**248364**

3.2.3 代数次数

定理 3.3 (3-3)式中的n元旋转对称布尔函数f的代数次数为

$$\begin{cases}\deg(f) = n-1, & 2^m+2 \le n \le 2^{m+1}\text{且}N=1, \text{或}\, n=2^m+1\ \text{且}N=0\\ \deg(f) \le n-2, & 2^m+2 \le n \le 2^{m+1}\text{且}N=0, \text{或}\, n=2^m+1\ \text{且}N=1\end{cases}$$

其中$n = 2k+1 \ge 11$，m为正整数，$N = \sum_{h=3}^{k}(k+1-h)|T_h| \pmod 2$。

证明：把f表示为

$$f(x)=F_M(x)+R(x),$$

其中R是n元旋转对称布尔函数

$$R(x)=\begin{cases}1, & x\in\tilde{T}\cup\tilde{U},\\ 0, & \text{其他}.\end{cases}$$

令$\alpha_i=(a_{i_1},a_{i_2},\cdots,a_{i_n})\in T$，$u_i=(b_{i_1},b_{i_2},\cdots,b_{i_n})\in U$，其中$1\le i\le L_k$。则$R$的代数正规型可表示为

$$R(x)=\sum_{i=1}^{L_k}\sum_{l=0}^{n-1}\left[\prod_{j=0}^{n-1}\left(x_j+\rho_n^l(a_{i_j})+1\right)\oplus\prod_{j=0}^{n-1}\left(x_j+\rho_n^l(b_{i_j})+1\right)\right],$$

其中，$x=(x_1,x_2,\cdots,x_n)$，Σ 表示$\mathbb{F}_2$域上的加法。

因为$\mathrm{w_H}(R)=2|\tilde{T}|$是偶数，由引理 2.3 知$\deg(R)\le n-1$。并且$R$函数代数正规型中$x_1x_2\cdots x_n/x_i(1\le i\le n)$项的系数等于集合$\{G_n(x)|x\in\tilde{T}\cup\tilde{U}\}$中所有第$i$比特为 0 的向量的个数$\bmod 2$。事实上，将给定向量$x=(x_1,x_2,\cdots,x_n)$连续循环左移$n$次，每一个比特都会在第$i$位置出现一次，因此

$$\begin{aligned}N&=\sum_{h=3}^{k}(2k+1-h)|T_h|+\sum_{h=3}^{k}k|T_h|\\&=\sum_{h=3}^{k}(k+1-h)|T_h|\ (\bmod 2).\end{aligned}$$

若$N=1(\bmod 2)$，$\deg(R)=n-1$；若$N=0(\bmod 2)$，$\deg(R)<n-1$。

变元数量为n的择多逻辑函数的代数次数为$\deg(F_M)=2^{\lfloor\log_2(n)\rfloor}$，对于$n=2k+1\ge 11$，若$n=2^m+1$，$\deg(F_M)=n-1$；否则，$\deg(F_M)<n-1$。

所以，若$n=2^m+1$且$N=1(\bmod 2)$，$\deg(f)\le n-2$，因为由(2-4)式及旋转对称布尔函数性质知，F_M和R的代数正规型中都包含所有$x_1x_2\cdots x_n/x_i(1\le i\le n)$项。类似地，若$2^m+2\le n\le 2^{m+1}$且$N=0(\bmod 2)$，$\deg(f)\le n-2$。用同样的方法可以得出，若$n=2^m+1$且$N=0(\bmod 2)$，或$2^m+2\le n\le 2^{m+1}$且$N=1(\bmod 2)$，$\deg(f)=n-1$。

证明完成。 □

通过计算机程序辅助计算，对于$5\le k\le 35$，其代数次数分布为：

- $k=5,6,7,9,10,11,12,13,22,27,28,29,30,31,32,33,34$，$\deg(f)=n-1$；
- $k=8,14,15,16,17,18,19,20,21,23,24,25,26,35$，$\deg(f)\le n-2$。

3.2.4 快速代数免疫度

目前，快速代数免疫度的研究还是一个难点。对于一类普通函数，只能用计算机程序计算其在变元数量较小时抵抗快速代数攻击的能力。对于(3-3)式中的n元旋转对称布尔函数f，我们用计算机程序算出$n=11,13,15$的真值表。令$g,h\in\mathcal{B}_n$，满足$\deg(g)=e$，$\deg(g)=e$，且$fg=h$。利用 Fischer 实现文献[59]中算法 2 的程序[60]，将满足$1\le e<\left\lceil\frac{n}{2}\right\rceil$和$e+d<n$条件的所有$(e,d)$作为程序输入。实验结果显示：对于这三个变元，不存在满足$e+d<n-1$的(e,d)，所有的(e,d)都满足$e+d\ge n-1$。即，变元数量为$n=11,13,15$旋转对称布尔函数f，其快速代数免疫度$\mathrm{FAI}(f)=n-1$（几乎最优）。由于计算机内存限制，变元数量大于等于 17 的函数快速代数免疫度无法计算。另外，文献[61]证明了n元平衡布尔函数具有最优的快速代数免疫度，必有$n=2^m+1$。因此，从这个层面上来说，(3-3)式中的旋转对称布尔函数在变元数量为$11,13,15$对于快速代数攻击具有最优的抵抗性。

3.3 构造方法二

(3-3)式中的旋转对称布尔函数具有平衡性、最优代数免疫度、高非线性度和较好的抵抗快速代数攻击的能力等良好性质。尽管其代数次数在某些变元数量下能达到平衡布尔函数的上界$n-1$，但是对于其他较多的变元其值仍小于等于$n-2$，且很难直接计算其代数次数的准确值。本节通过修改T和U集合来修正这一缺点。

根据T_h和U_h的定义，重新定义两个集合T_h'和U_h'。对于$3\le h\le 6$，令$T_h'=T_h$。对于$h\ge 7$，若$|T_h|$是偶数，令$T_h'=T_h$；若$|T_h|$是奇数，令

$$T_h'=T_h\backslash\{(1,1,0,\underbrace{1,0,\cdots,1,0}_{2(h-4)},1,1,0,0,\underbrace{0,\cdots,0}_{2(k+1-h)})\}.$$

因此，$h\ge 7$时，$|T_h'|=2\left\lfloor\frac{T_h}{2}\right\rfloor$。再定义

$$U_h'=\{\alpha'_{h_s}\oplus(0,\cdots,0,\underbrace{1,0,1,0,\cdots,1,0}_{2(k+1-h)})|\alpha'_{h_s}\in T_h'\}.$$

令

$$T'=\bigcup_{h=3}^{k}T_h',\ U'=\bigcup_{h=3}^{k}U_h'$$

和

$$\tilde{T}' = \bigcup_{x\in T'} G_n(x),\ \tilde{U}' = \bigcup_{x\in U'} G_n(x).$$

显然，$\tilde{T}' \subseteq \tilde{T}$，$\tilde{U}' \subseteq \tilde{U}$，且$|\tilde{T}'| = |\tilde{U}'|$。令$F_M$表示(2-5)式中给出的择多逻辑函数，下面我们给出第二类旋转对称布尔函数

$$f'(x) = \begin{cases} F_M(x) \oplus 1, & x \in \tilde{T}' \cup \tilde{U}', \\ F_M(x), & \text{其他}. \end{cases} \tag{3-4}$$

下面分析(3-4)式中旋转对称布尔函数f'的代数次数。通过计算得，$|T_3'| = |T_3| = 1$，$|T_4'| = |T_4| = 2$，$|T_5'| = |T_5| = 4$，$|T_6'| = |T_6| = 11$。类似于定理 3.3 的证明过程，把f'表示为$f'(x) = F_M(x) + R'(x)$，然后计算R'函数代数正规型中$x_1x_2\cdots x_n/x_i\,(1 \le i \le n)$项的系数

$$\begin{aligned} N' &= \sum_{h=3}^{k}(2k+1-h)|T_h'| + \sum_{h=3}^{k} k|T_h'| \\ &= \sum_{h=3}^{k}(k+1-h)|T_h'| \,(\mathrm{mod}\ 2). \end{aligned}$$

当$k = 5, 6$时，容易计算出$N' = 1(\mathrm{mod}\ 2)$。

当$k \ge 7$时，

$$\begin{aligned} N' &= \sum_{h=3}^{6}(k+1-h)|T_h'| + \sum_{h=7}^{k}(k+1-h)|T_h'| \\ &= [(k-2) + 11(k-5)](\mathrm{mod}\ 2) \\ &= 1(\mathrm{mod}\ 2). \end{aligned}$$

因此，可得下面定理。

定理 3.4 (3-4)式中的n元旋转对称布尔函数f'的代数次数为

$$\begin{cases} \deg(f') = n-1, & 2^m + 2 \le n \le 2^{m+1}, \\ \deg(f') \le n-2, & n = 2^m + 1, \end{cases}$$

其中，$n = 2k+1 \ge 11$，m是正整数。

显然，f'的代数次数在大多情况下都能达到平衡函数的上界$n-1$。

定理 3.5 (3-4)式中的n元旋转对称布尔函数f'具有最优代数免疫度，其非线性度为

$$\mathrm{NL}(f') = 2^{n-1} - \binom{n-1}{k} + \sum_{h=3}^{k}(n-2h)|T_h'| + L_k',$$

其中$n = 2k+1 \geq 11$，$L_k' = \sum_{h=3}^{k}|T_h'|$。

证明：参照定理 3.1 和定理 3.2 的证明过程，该定理很容易得到证明。

□

下面对于(3-3)式中f函数的代数次数小于等于$n-2$的那些变元，求(3-4)式中f'函数的非线性度。表 3-2 列出了这些变元下f'与f非线性度超出$2^{n-1} - \binom{n-1}{k}$部分的比较。其中β满足$\mathrm{NL}(f) - \mathrm{NL}(f') = \beta\left[\mathrm{NL}(f) - 2^{n-1} - \binom{n-1}{k}\right]$。从表格可以看出，$\beta$非常接近 0，并且随着变元数量增加呈现减小的趋势。因此，f'与f非线性度的差值非常小，可以忽略不计。所以，(3-3)式中f函数的那些变元数量下代数次数小于等于$n-2$的劣势，可以用(3-4) 式中f'函数加以弥补。

表 3-2 f'与f非线性度超出$2^{n-1} - \binom{n-1}{k}$部分的比较

k	14	15	17	18	19	20
f	100256	248364	1501148	3661428	8867880	21402764
f'	100254	248358	1501130	3661402	8867846	21402722
β	1.9949E-5	2.4158E-5	1.1991E-5	7.1011E-6	3.8241E-6	1.9624E-6

k	21	23	24	25	26	35
f	51353288	292201972	693093396	1617469360	3757768560	969457741364
f'	51353238	292201902	693093314	1617469266	3757768454	969457741102
β	9.7365E-7	2.3956E-7	1.1831E-7	5.8116E-8	2.8208E-8	2.7025E-10

3.4 本章小结

本章中，基于整数拆分的结果通过修改择多逻辑函数的支撑集构造了一类变元数量为奇数的旋转对称布尔函数，兼有平衡性、最优代数免疫度、高非线性度和较好的快速代数免疫度等良好性质，其代数次数存在些许劣势，我们进而构造了第二类具有较好代数次数

的奇数元旋转对称布尔函数以弥补第一类的不足。

此部分研究工作已整理成文章 Constructing odd-variable RSBFs with optimal algebraic immunity, good nonlinearity and good behavior against fast algebraic attacks，并于 2019 年 6 月发表在 Discrete Applied Mathematics 期刊。

第四章 特殊变元择多逻辑函数的快速代数免疫度

本章通过分析择多逻辑函数的对称性，给出了其快速代数免疫度在变元数量为$2^m + 2 \le n < 2^{m+1}$(其中$m \ge 2$)时的一个下界，结合已有结论，可以得出$2^m + 2$和$2^m + 3$变元的择多逻辑函数快速代数免疫度为$2^{m-1} + 4$。

4.1 择多逻辑函数的快速代数免疫度已有结论

本节介绍择多逻辑函数的快速代数免疫度的几个重要结论。

引理 4.1 ([54]) 令$F_M \in \mathcal{SB}_n$表示择多逻辑函数，则

- $\deg(F_M) = 2^{\lfloor \log_2(n) \rfloor}$;
- $\mathrm{AI}(F_M) = \left\lceil \frac{n}{2} \right\rceil$。

引理 4.2 ([63]) 令$f \in \mathcal{B}_n$是任意布尔函数，则

- $\mathrm{FAI}(f) \le n$;
- $\mathrm{FAI}(f) = \mathrm{FAI}(f + 1)$。

2011 年，刘美成等[62]证明了包括择多逻辑函数在内的几乎所有的对称布尔函数对快速代数攻击的抵抗能力都很弱。

引理 4.3 ([62]) 令$f \in \mathcal{SB}_n$表示任意对称布尔函数，其中$2^m \le n < 2^m + 2^{m-1} - 1$。则必有$\mathrm{AI}(f) \le 2^{m-1} - 1$或者$\deg(\sigma_e f) = 2^{m-1} + e$且$e = n - 2^m + 1$，其中$\sigma_e$表示所有的$e$次齐次项之和构成的初等对称布尔函数。

因为择多逻辑函数具有最优代数免疫度，故变元数量在$2^m \le n < 2^m + 2^{m-1} - 1$范围内，有$\mathrm{FAI}(F_M) \le 2^{m-1} + 2e = 2n - 3 \cdot 2^{m-1} + 2$。因此，择多逻辑函数在变元数量大于 8 时对于快速代数攻击的表现都不好，尤其是变元数量在 2 的方幂附近，其快速代数免疫度都很低。事实上，在 2006 年欧密会上，Armknecht 等[59]给出关于择多逻辑函数快速代数免疫度的一个更为有用的结论。

引理 4.4 ([59]) 令$F_M \in \mathcal{SB}_n$表示择多逻辑函数，其中$2^m \le n < 2^{m+1}$。则必存在n元布尔函数g和h使得$F_M \cdot g = h$，其中$d = \deg(h) = \left\lfloor \frac{n}{2} \right\rfloor + 1$，$e = \deg(\mathrm{g}) = d - 2^j$，$j$是使得$e > 0$的最大整数。

该引理进一步说明了变元数量在$[2^m, 2^m + 2^{m-1}]$范围内的择多逻辑函数抵抗快速代数攻击的能力都很差。显然，由该引理可以进一步推论出：$\mathrm{FAI}(F_M) \le n - 2^{m-1} + \mathrm{c}$，其中若$n$为偶数$c = 2$，若$n$为奇数$c = 1$。

2016 年，唐灯等[63]基于择多逻辑函数的对称性，给出了其快速代数免疫度的一个下界$\mathrm{FAI}(F_M) \ge \left\lfloor \frac{n}{2} \right\rfloor + 2$(其中$n \ge 3$)。而对于变元数量$2^m$和$2^m + 1$，这一下界恰好与文献[59]中的上界相等。由此得出结论：择多逻辑函数在变元数量为2^m和$2^m + 1$时(其中$m \ge 2$)快速代数免疫度为$2^{m-1} + 2$。

4.2 $2^m + 2$和$2^m + 3$变元择多逻辑函数的快速代数免疫度

本节中，基于择多逻辑函数的对称性，我们分析其在变元数量为$2^m + 2$和$2^m + 3$时的快速代数免疫度。

引理 4.5 令$F_M \in \mathcal{SB}_n$表示择多逻辑函数，其中$2^m + 2 \le n < 2^{m+1}$，$m \ge 2$。对任意的 1 次布尔函数g，都有$\deg(F_M g) = \deg(F_M) + 1$。

证明：由引理 4.1 知，$\deg(F_M) = 2^{\lfloor \log_2(n) \rfloor} = 2^m$，因此由(2-4)式，$F_M$的代数正规型中包含了所有的$2^m$次项。为证$\deg(F_M g) = 2^m + 1$，只需证$F_M g$乘积中存在特定某一$2^m + 1$次项，且其出现奇数次。

(1) 假设$g(x) = x_1 + x_2 + \cdots + x_n$，则$x_1 x_2 \cdots x_{2^m+1}$项在$F_M g$中出现了$2^m + 1$次；

(2) 假设$g(x) = x_1 + x_2 + \cdots + x_n - x_i$，其中$1 \le i \le n$。为了方便，令$x_i = x_n$，因为$x_n$不会影响$F_M g$中$x_1 x_2 \cdots x_{2^m+1}$项，所以此种情况对(1)不构成影响。也即，$x_1 x_2 \cdots x_{2^m+1}$项在$F_M g$中出现了$2^m + 1$次；

(3) 假设$g(x) = x_1 + x_2 + \cdots + x_n - X$，其中$X$表示不同的偶数项$x_i$相加，$1 \le i \le n$。为了方便，令$X = x_1 + \cdots + x_l$，即从头开始取连续的$l$项，$l$是偶数。则$x_1 x_2 \cdots x_{2^m+1}$项在$F_M g$中出现了$2^m + 1 - l$次，显然$2^m + 1 - l$是奇数；

(4) 假设$g(x)=x_1+x_2+\cdots+x_n-X-x_j$，其中$X$与(3)定义的相同，$x_j$不包含在$X$中，$1\le j\le n$。为了方便，令$X=x_1+\cdots+x_l$，即从头开始取连续的$l$项，$l$是偶数，$x_j=x_n$。则$x_n$对(3)中的情形不构成影响，即$x_1x_2\cdots x_{2^m+1}$项在$F_Mg$中出现了$2^m+1-l$次，即奇数次。

另外，很显然，g函数代数正规型中是否含常量 1 对结果都不构成影响。综合上述所讨论的情形，根据择多逻辑函数的高度对称性可以推断，对任意$\deg(g)=1$，都有$\deg(F_Mg)=\deg(F_M)+1$。

证明完成。 □

引理 4.6 令$F_M\in\mathcal{SB}_n$表示择多逻辑函数，其中$2^m+2\le n<2^{m+1}$，$m\ge 2$。定义$\mathrm{A}=\min\{\deg(h)\,|0\ne h\in\mathrm{Ann}(F_M)\}$。则下面不等式成立

$$\mathrm{FAI}(F_M)\ge \mathrm{A}+2\ge \mathrm{AI}(F_M)+2.$$

证明：首先，给出一个推论

$$\min_{1\le\deg(g)<AI(F_M)}\{\deg(g)+\deg((F_M+1)g)\}\ge \mathrm{A}+2\ge \mathrm{AI}(F_M)+2. \tag{4-1}$$

该推论成立基于下面三个事实：

- $\mathrm{AI}(F_M)\le A\le\deg(F_M)$，因为$F_M(F_M+1)=0$，$F_M+1\ne 0$且$\deg(F_M+1)=\deg(F_M)$；
- $\mathrm{AI}(F_M)=\mathrm{AI}(F_M+1)$，由定义 2.5；
- 若$\deg(g)=1$，由引理 4.5 可得$\deg((F_M+1)g)=\deg(F_Mg)=\deg(F_M)+1\ge \mathrm{A}+1$；若$\deg(g)\ge 2$，因为$F_M(F_M+1)g=0$且$(F_M+1)g\ne 0$，所以$\deg((F_M+1)g)\ge \mathrm{A}$。

其次，给出另一个推论

$$2\mathrm{AI}(F_M+1)\ge \mathrm{A}+2. \tag{4-2}$$

该推论成立基于下面三个事实：

- $A\le\deg(F_M+1)=2^m$，由引理 4.1；
- $\mathrm{AI}(F_M)=\mathrm{AI}(F_M+1)$，由定义 2.5；
- 当$2^m+2\le n<2^{m+1}$，由引理 4.1 知，若n为偶数，$2\mathrm{AI}(F_M)=n$；若n为奇数，$2\mathrm{AI}(F_M)=n+1$。这两种情形都表明，$2\mathrm{AI}(F_M+1)\ge 2^m+2\ge \mathrm{A}+2$。

因此，结合(4-1)式和(4-2)式，由定义 2.5 和引理 4.2 可得

$$\mathrm{FAI}(F_M) = \mathrm{FAI}(F_M + 1) \geq \mathrm{A} + 2 \geq \mathrm{AI}(F_M) + 2.$$

证明完成。 □

下面，我们给出择多逻辑函数在变元数量在$2^m + 2 \leq n < 2^{m+1}$(其中$m \geq 2$)范围内快速代数免疫度的一个下界。

引理 4.7 令$F_M \in \mathcal{SB}_n$表示择多逻辑函数，其中$2^m + 2 \leq n < 2^{m+1}$，$m \geq 2$。则

$$\mathrm{FAI}(F_M) \geq \left\lfloor \frac{n}{2} \right\rfloor + 3.$$

证明：按照变元数量n的奇偶性分为下面两种情形：

(1) n是偶数。根据引理 4.6，需证F_M没有代数次数小于$\frac{n}{2} + 1$的零化子。令$F'_M = F_M(x_1 + 1, x_2 + 1, \cdots, x_n + 1)$，则只需证没有代数次数小于$\frac{n}{2} + 1$的零化子。因为假如存在代数次数小于$\frac{n}{2} + 1$的布尔函数$g$使得$F'_M g = 0$，则有$F_M g' = 0$，其中$g'(x_1, x_2, \cdots, x_n) = g(x_1 + 1, x_2 + 1, \cdots, x_n + 1)$。假设$g$是$F'_M$的零化子，且满足$\deg(g) \leq \frac{n}{2}$。将函数$g$的代数正规型表示为

$$g(x) = \sum_{u \in \mathbb{F}_2^n, wt(u) \leq \frac{n}{2}} \lambda_u x^u .$$

因为g是F'_M一个零化子，所以对任意$wt(x) \leq \frac{n}{2}$，都有$g(x) = 0$。因此，对任意的$u \in \mathbb{F}_2^n$且$wt(u) \leq \frac{n}{2}$，都有$\lambda_u = 0$成立。这意味着$g = 0$，即F'_M没有代数次数小于$\frac{n}{2} + 1$的零化子。

(2) n是奇数。由引理 4.6 可得，$\mathrm{FAI}(F_M) \geq \mathrm{AI}(F_M) + 2 \geq \left\lfloor \frac{n}{2} \right\rfloor + 3$。

证明完成。 □

结合引理 4.4 和引理 4.7，可以得出本章最重要的定理。

定理 4. 1 令$F_M \in \mathcal{SB}_n$表示择多逻辑函数，若$n \in \{2^m + 2, 2^m + 3\}$，其中$m \geq 2$，则

$$\mathrm{FAI}(F_M) = 2^{m-1} + 4.$$

4.3 本章小结

本章基于择多逻辑函数的对称性，分析并给出了其在变元数量$2^m+2 \le n < 2^{m+1}$（其中$m \ge 2$）范围内快速代数免疫度的一个下界$\mathrm{FAI}(F_M) \ge \left\lfloor \frac{n}{2} \right\rfloor + 3$，当变元数量是$2^m+2$和$2^m+3$时，该下界恰好与文献[59]给出的择多逻辑函数快速代数免疫度上界一致，由此得出结论：变元数量为2^m+2和2^m+3的择多逻辑函数的快速代数免疫度为$2^{m-1}+4$。

此部分研究工作已整理成文章 Fast algebraic immunity of 2^m+2 & 2^m+3 variables majority function，并于 2019 年 3 月在 Cryptology ePrint Archive 平台发表。

第五章 总结与展望

本章对论文完成的工作进行总结，并对后续可开展的研究工作进行展望。

5.1 论文工作总结

在实际应用中，满足多项密码学性质的布尔函数对于维护密码系统的安全性发挥关键性作用。为了抵抗各种已知密码攻击，密码系统中使用的布尔函数应同时满足以下几个性质：平衡性，良好的(快速)代数免疫度，高非线性度，高代数次数等。本文主要对布尔函数的密码学性质进行研究，并提供了一种密码学性质良好的布尔函数构造方法。

本文完成的研究工作及取得的创新性研究成果主要包括：

(1) 提出了两种具有最优代数免疫度的奇数元旋转对称布尔函数的构造方法。根据数论中整数拆分的结果，通过修改择多逻辑函数的支撑集，构造了具有最优代数免疫度的奇数元旋转对称布尔函数，所构函数兼有平衡性、高非线性度、高代数次数等优良性质。在变元数量较小时，通过计算机程序证实了此类函数具有较好的快速代数免疫度。

(2) 研究了择多逻辑函数在特殊变元时的快速代数免疫度。基于择多逻辑函数的对称性，分析并给出了其快速代数免疫度的一个下界，结合已有的结论，得出择多逻辑函数在两类特殊变元的快速代数免疫度准确值。

5.2 后续研究工作展望

结合本文的研究工作，下一步的研究工作主要包括：

(1) 构造兼有多种良好密码学性质的旋转对称布尔函数。目前，代数免疫最优旋转对称布尔函数的构造研究已取得较多的成果，但所有的构造其非线性度都远远低于 Carlet-Feng 函数和 T-C-T 函数，因此在保证代数免疫最优的基础上大幅提升其非线性度是一个很重要的研究方向。

(2) 研究择多逻辑函数的快速代数免疫度。快速代数攻击和快速代数免疫度一直是布

尔函数研究的难点。择多逻辑函数是结构最简单的具有最优代数免疫度的布尔函数，因此可以将此类函数作为快速代数免疫度研究的“突破口”。

(3) 研究(旋转)对称布尔函数的快速代数免疫度。(旋转)对称布尔函数结构复杂性介于择多逻辑函数与普通布尔函数之间，因此研究其快速代数免疫度能为进一步研究普通布尔函数的快速代数免疫度提供理论和方法支撑。

参考文献

[1] Shannon C E. Communication theory of secrecy systems [J]. Bell Labs Tech. J., 1949, 28 (4): 656-715.

[2] Diffie W, Hellman M. New direction in cryptography [J]. IEEE Trans. Inf. Theory, 1976, 22 (6): 644-654.

[3] NBS. Data Encryption Standard [S]. Washington D C: FLIPS PUB 46, National Bureau of Standards, 1977.

[4] Rivest R L, Shamir A, Adleman L M. A method for obtaining digital signatures and public-key cryptosystems [J]. Communication of the ACM, 1978, 21 (2): 120-126.

[5] NIST. Advanced Encryption Standard (AES) [S]. Washington D C: Federal Information Processing Standards, 2001.

[6] Daemen J, Rijmen V. The design of Rijndael: AES-The Advanced Encryption Standard [C]. Berlin: Springer-Verlag, 2002: 221-227.

[7] European IST. NESSIE Project [EB/OL]. http://www.cryptonessie.org.

[8] European IST. ECRYPT Project [EB/OL]. http://www.nist.gov/aes.

[9] Simmons G J. Symmetric and Asymmetric Encryption [J]. Acm Computing Surveys, 1979, 11 (4): 305-330.

[10] http://dacas.cn.

[11] Canteaut A, Videau M. Symmetric Boolean functions [J]. IEEE Trans. Inf. Theory, 2005, 51 (8): 2791-2811.

[12] Carlet C. Boolean functions for cryptography and error-correcting codes [M]. Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge, U.K.: Cambridge Univ. Press, 2010, vol.2: 257-397.

[13] Carlet C, Dalai D K, Gupta K C, Maitra S. Algebraic immunity for cryptographically significant Boolean functions: analysis and construction [J]. IEEE Trans. Inform. Theory, 2006, 52 (7): 3105-3121.

[14] Carlet C, Feng K Q. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity [C]. Advances in Cryptology, ASIACRYPT 2008, Berlin, Germany, Lecture Notes in Computer Science, 2008, 5350: 425-440.

[15] Carlet C, Zeng X Y, Li C, Hu L. Further properties of several classes of Boolean functions with optimum algebraic immunity [J]. Des. Codes Cryptogr., 2009, 52 (3): 303-338.

[16] Chen Y D, Lu P Z. Two classes of symmetric Boolean functions with optimum algebraic immunity: Construction and analysis [J]. IEEE Trans. Inform. Theory, 2011, 57 (4): 2522-2538.

[17] Li J, Carlet C, Zeng X Y, Li C L, Hu L, Shan J Y. Two constructions of balanced Boolean functions with optimal algebraic immunity, high nonlinearity and good behavior against fast algebraic attacks [J]. Des. Codes Cryptogr., 2015, 76 (2): 279-305.

[18] Massey J. Shift-register synthesis and BCH decoding [J]. IEEE Trans. Inf. Theory, 1969, 15(1): 122-127.

[19] Rueppel R, Staffelbach O. Products of linear recurring sequences with maximum complexity [J]. IEEE Trans. Inf. Theory, 1987, 33(1): 124-131.

[20] Ronjom S, Helleseth T. A new attack on the filter generator [J]. IEEE Trans. Inf. Theory, 2007, 53(5): 1752-1758.

[21] Ding C S, Xiao G Z, Shan W J. The stability theory of stream ciphers [M]. In: Lecture Notes in Computer Science, Springer Berlin Heidelberg, Berlin, Heidelberg, 1991, 561: 81-129.

[22] Meier W, Staffelbach O. Fast correlation attacks on stream ciphers [C]. Advances in Cryptology, EUROCRYPT 1988, Lecture Notes in Computer Science, 1988, 330: 301-314.

[23] Dalai D K, Gupta K C, Maitra S. Results on algebraic immunity for cryptographically significant Boolean functions [C]. International Conference on Cryptology in India, INDOCRYPT 2004, Lecture Notes in Computer Science, 2004, 3348: 92-106.

[24] Courtois N T, Meier W. Algebraic attacks on stream ciphers with linear feedback [C]. Advances in Cryptology, EUROCRYPT 2003, Lecture Notes in Computer Science, 2003, 2656: 345-359.

[25] Meier W, Pasalic E, Carlet C. Algebraic attacks and decomposition of Boolean functions [C]. Advances in Cryptology, EUROCRYPT 2004, Lecture Notes in Computer Science, 2004, 3027: 474-491.

[26] Stănică P, Maitra S. Rotation symmetric Boolean functions–count and cryptographic properties [J]. Electronic Notes in Discrete Mathematics, 2003, 15: 139-145.

[27] Filiol E, Fontaine C. Highly nonlinear balanced Boolean functions with a good correlation-immunity[C]. Advances in Cryptology, EUROCRYPT 1998, Springer Berlin Heidelberg, Lecture Notes in Computer Science, 1998, 1403: 475-488.

[28] Sarkar S, Maitra S. Construction of rotation symmetric Boolean functions with maximum algebraic immunity on odd number of variables [C]. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC 2007), Lecture Notes in Computer Science, 2007, 4851: 271-280.

[29] Sarkar S, Maitra S. Construction of rotation symmetric Boolean functions with optimal algebraic immunity

[J]. Comput. Syst., 2009, 12(3): 267-284.

[30] Fu S J, Qu L J, Li C, Sun B. Balanced rotation symmetric Boolean functions with maximum algebraic immunity [J]. IET Information Security, 2011, 5(2): 93-99.

[31] Fu S J, Li C, Matsuura K, Qu L J. Construction of even-variable rotation symmetric Boolean functions with maximum algebraic immunity [J]. Science China Information Sciences, 2013, 56(3): 1-9.

[32] Lobanov M. Tight bound between nonlinearity and algebraic immunity [Online]. Available online, http://eprint.iacr.org/2005/441, 2005.

[33] Su S H, Tang X H. Construction of rotation symmetric boolean functions with optimal algebraic immunity and high nonlinearity [J]. Des. Codes Cryptogr., 2014, 71(2): 183-199.

[34] 陈银冬, 张亚楠, 田威. 具有最优代数免疫度的偶数元旋转对称布尔函数的构造[J]. 密码学报, 2014, 1 (5): 437-448.

[35] Fu S J, Du J, Qu L J, Li C. Construction of odd-variable rotation symmetric boolean functions with maximum algebraic immunity [J]. IEICE Trans. Fundamentals, 2016, 99(4): 853-855.

[36] Sun L, Fu F W. Constructions of balanced odd-variable rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity [J]. Theoretical Computer Science, 2018, 738: 13-24.

[37] Sun L, Fu F W. Balanced 2p-variable rotation symmetric Boolean functions with optimal algebraic immunity [J]. Discrete Applied Mathematics, 2016, 215: 20-30.

[38] Zhao Q L, Han G, Zheng D, Li X X. Constructing odd-variable rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity [J]. Chinese Journal of Electronics, 2019, 28(1): 45-51.

[39] Chen Y D, Guo F, Xiang H Y, Cai W H, He X M. Balanced odd-variable RSBFs with optimum AI, high nonlinearity and good behavior against FAAs [J]. IEICE Trans. Fundamentals, 2019, E102-A (06): 818-824.

[40] Zhang H, Su S H. A new construction of rotation symmetric Boolean functions with optimal algebraic immunity and higher nonlinearity [J]. Discret. Appl. Math., 2019, 262: 13-28.

[41] Courtois N T. Fast algebraic attacks on stream ciphers with linear feedback [C]. Advances in Cryptology, CRYPTO 2003, Springer Berlin Heidelberg, Berlin, Heidelberg, Lecture Notes in Computer Science, 2003, 2729: 176-194.

[42] Armknecht F. Improving fast algebraic attacks [C]. Fast Software Encryption, Springer Berlin Heidelberg, Berlin, Heidelberg, Lecture Notes in Computer Science, 2004, 3017: 65-82.

[43] Hawkes P, Rose G G. Rewriting variables: The complexity of fast algebraic attacks on stream ciphers [C].

Advances in Cryptology, CRYPTO 2004, Springer Berlin Heidelberg, Berlin, Heidelberg, Lecture Notes in Computer Science, 2004, 3152: 390-406.

[44] Carlet C, Tang D. Enhanced Boolean functions suitable for the filter model of pseudo-random generator [J]. Des. Codes Cryptogr., 2015, 76(3): 571-587.

[45] Liu M C, Lin D D. Fast algebraic attacks and decomposition of symmetric Boolean functions [Online]. ArXiv preprint, available online: https://arxiv.org/pdf/0910.4632, 2009.

[46] Liu M C, Zhang Y, Lin D D. Perfect algebraic immune functions [C]. Advances in Cryptology, ASIACRYPT 2012, Springer Berlin Heidelberg, Berlin, Heidelberg, Lecture Notes in Computer Science, 2012, 7658: 172-189.

[47] Wang Q C, Johansson T, Kan H B. Some results on fast algebraic attacks and higher-order non-linearities [J]. IET Information Security, 2012, 6(1): 41-46.

[48] Tu Z R, Deng Y P. A conjecture on binary string and its applications on constructing boolean functions of optimal algebraic immunity [J]. Des. Codes Cryptogr., 2011, 60 (1): 1-14.

[49] Tang D, Carlet C, Tang X H. Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks [J]. IEEE Trans. Inf. Theory, 2013, 59 (1): 653-664.

[50] Liu M C, Lin D D. Almost perfect algebraic immune functions with good nonlinearity [C]. 2014 IEEE International Symposium on Information Theory, 2014, 1837-1841.

[51] Zhang Y, Liu M C, Lin D D. On the immunity of rotation symmetric Boolean functions against fast algebraic attacks [J]. Discrete Applied Mathematics, 2014, 162: 17-27.

[52] Tang D, Carlet C, Tang X H, Zhou Z C. Construction of Highly Nonlinear 1-Resilient Boolean Functions With Optimal Algebraic Immunity and Provably High Fast Algebraic Immunity [J]. IEEE Trans. Inf. Theory, 2017, 63 (9): 6113-6125.

[53] Wegener I. The complexity of Boolean functions [M]. New York: Wiley, 1987.

[54] Dalai D K, Maitra S, Sarkar S. Basic theory in construction of Boolean functions with maximum possible annihilator immunity [J]. Des. Codes Cryptogr., 2006, 40 (1): 41-58.

[55] Qu L J, Li C, Feng K Q. A note on symmetric Boolean functions with maximum algebraic immunity in odd number of variables [J]. IEEE Trans. Inf. Theory, 2007, 53 (8): 2908-2910.

[56] Qu L J, Feng K Q, Liu F, Wang L. Constructing symmetric Boolean functions with maximum algebraic immunity [J]. IEEE Trans.Inf. Theory, 2009, 55 (5): 2406-2412.

[57] Peng J, Wu Q S, Kan H B. On symmetric Boolean functions with high algebraic immunity on even number

of variables [J]. IEEE Trans. Inf. Theory, 2011, 57 (10): 7205-7220.

[58] Wang H, Peng J, Li Y, Kan H B. On $2k$-variable symmetric Boolean functions with maximum algebraic immunity k [J]. IEEE Trans. Inf. Theory, 2012, 58 (8): 5612-5624.

[59] Armknecht F, Carlet C, Gaborit P, Künzli S, Meier W, Ruatta O. Efficient computation of algebraic immunity for algebraic and fast algebraic attacks [C]. Advances in Cryptology, EUROCRYPT 2006, Springer Berlin Heidelberg, Berlin, Heidelberg, Lecture Notes in Computer Science, 2006, 4004: 147–164.

[60] Fischer S. FAA equation finder version 1 [Online]. Available online, http://www.simonfischer.ch/software/FAA.php, 2008.

[61] Du Y S, Zhang F G. On the existence of Boolean functions with optimal resistance against fast algebraic attacks [Online]. Available online, https://eprint.iacr.org/2012/210, 2012.

[62] Liu M C, Lin D D, Pei D Y. Fast algebraic attacks and decomposition of symmetric Boolean functions [J]. IEEE Trans. Inf. Theory, 2011, 57 (7): 4817-4821.

[63] Tang D, Luo R, Du X N. The exact fast algebraic immunity of two subclasses of the majority function [J]. IEICE Trans. Fundamentals, 2016, 99 (11): 2084-2088.

[64] Heubach S, Mansour T. Combinatorics of Compositions and Words [M], CRC Press, Boca Raton, 2009.

附 录

附录 1 (3-3)式中 11 元旋转对称布尔函数

令$n=11$，则根据T_h的定义可得

$T_3=\{(1,1,1,0,0,0,0,0,0,0,0)\}$,

$T_4=\{(1,1,1,1,0,0,0,0,0,0,0),(1,1,0,1,1,0,0,0,0,0,0)\}$,

$T_5=\{(1,1,1,1,1,0,0,0,0,0,0),(1,1,1,0,1,1,0,0,0,0,0),$

$(1,1,0,1,1,1,0,0,0,0,0),(1,1,0,1,0,1,1,0,0,0,0)\}$.

根据U_h的定义可得

$U_3=\{(1,1,1,0,0,1,0,1,0,1,0)\}$,

$U_4=\{(1,1,1,1,0,0,0,1,0,1,0),(1,1,0,1,1,0,0,1,0,1,0)\}$,

$U_5=\{(1,1,1,1,1,0,0,0,0,1,0),(1,1,1,0,1,1,0,0,0,1,0),$

$(1,1,0,1,1,1,0,0,0,1,0),(1,1,0,1,0,1,1,0,0,1,0)\}$.

令$T_{eg}=T_3\cup T_4\cup T_5$，$U_{eg}=U_3\cup U_4\cup U_5$。显然，对任意$\alpha\in T_{eg}$和$u\in U_{eg}$，等式$|G_{11}(\alpha)|=|G_{11}(u)|=11$成立。令

$$\tilde{T}_{eg}=\cup_{\alpha\in T_{eg}}G_{11}(\alpha),\ \tilde{U}_{eg}=\cup_{u\in U_{eg}}G_{11}(u).$$

定义 11 元旋转对称布尔函数为

$$f_{eg}(x)=\begin{cases}F_{M\_11}(x)\oplus 1, & x\in\tilde{T}_{eg}\cup\tilde{U}_{eg}\\ F_{M\_11}(x), & \text{其他}\end{cases}$$

其中，F_{M_11}是11元择多逻辑函数。

用计算机程序实现该函数，其真值表十六进制表示为：

080C 008D 0000 0C9D 0000 0000 008D 1C9F 0000 0008 0000

000A 0008 0C9F 188F 9EFF 0000 0008 0008 088E 0008 000A

080A 8AEE 0008 088E 088F 9EFF 188E 8EFF 9EEF FFFF 0000

0008 0008 088E 0008 088E 088E 8EEF 0008 088E 088A 8ACE

880E 8ACE 8CEE CFEF 880A 008E 080C 8EEF 088E 8EDF 9CEF

DFFF	980E	8CEF	8EEF	DFFF	9CEF	EFFF	DFFF	FFFF	880A	008A
0000	0A8E	0008	000C	088E	8EEF	0008	088E	080C	8CEF	088E
8EEF	8EEF	EFFF	0008	088E	088E	8EEF	088E	8EEE	ACEE	AFEF
AC0E	88EF	8EEE	AFEF	ACAF	EFEF	AFFF	EFFF	AC0E	00CE	0808
8EEF	088E	88AF	8EEF	EFFF	088E	8EEF	8EEF	BFFF	BCAF	EFFF
BFFF	FFFF	BC0E	88EF	8EAF	EFFF	8EEF	EFFF	BFFF	FFFF	BCAF
EFFF	EFFF	FFFF	BFFF	FFFF	FFFF	FFFF				

我们用计算机程序验证了其代数免疫度是6，代数次数是10，非线性度是794。另外，对于所构造的13和15变元的旋转对称布尔函数，我们也用计算机程序做了代数免疫度、代数次数、非线性度等性质的验证，其结果都与理论值一致。

致谢辞

感谢我的硕士导师陈银冬老师，是他带领我走进神奇的密码学世界，引领我从事有趣的布尔函数研究。陈老师为学严谨，为人谦和，从他身上我学到了很多做人和求知的道理。在此向陈老师表示衷心的感谢！

感谢科研团队学科负责人蔡伟鸿老师，是他悉心培养我们良好的科研习惯，精心提升我们的科研素养，并为我们提供了整洁舒适的科研环境。

感谢科研团队熊智老师、蔡玲如老师和其他同学给予我的帮助。

感谢我的父母，他们的信任、坚守和默默付出无时无刻不在激励着我。他们是我最坚实的后盾，让我在求学路上能走得更远，更坚定。这篇论文也是我送给他们的第一份礼物。

感谢汕大求学的三年时光。

攻读硕士学位期间的科研成果

1. Chen Yindong, **Guo Fei**, Gong Zhangquan, and Cai Weihong. One note about the Tu-Deng conjecture in case $w(t) = 5$. IEEE ACCESS, 2019, 7: 13079-13082.
2. Chen Yindong, **Guo Fei**, and Ruan Jie. Constructing odd-variable RSBFs with optimal algebraic immunity, good nonlinearity and good behavior against fast algebraic attacks. Discrete Applied Mathematics, 2019, 262: 1-12.
3. Chen Yindong, **Guo Fei**, Xiang Hongyan, Cai Weihong, and He Xianmang. Balanced odd-variable RSBFs with optimum AI, high nonlinearity and good behavior against FAAs. IEICE Transactions on Fundamentals of Electronics Communications and Computer Science, 2019, E102-A (06): 818-824.
4. Chen Yindong, **Guo Fei**, and Zhang Liu. Fast algebraic immunity of $2^m + 2$ & $2^m + 3$ variables majority function. Cryptology ePrint Archive, 2019, available online: https://eprint.iacr.org/2019/286.