汕頭大學
SHANTOU UNIVERSITY

硕 士 学 位 论 文

题　　目　布尔函数平移等价性及快速代数免疫度下界研究

英文题目　Translation equivalence of Boolean functions and lower bound of fast algebraic immunity

姓　　名　张柳　　学　　号　111709030

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　2017. 09. 01　　答辩日期　2020. 06. 13

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

序列密码是对称密码体制的重要实现方式之一，在密码算法的设计中，常常使用非线性函数作为基本的密码部件，使用布尔函数是实现非线性函数的一种有效途径。为了抵抗已知的密码攻击手段，非线性布尔函数必须具有理论可证明的能够有效抵抗已知密码攻击的性能。2003 年之前，在流密码中使用的布尔函数必须同时兼具以下几个性质：平衡性，高非线性度，高代数次数，高的弹性阶以及良好的自相关性质。 Courtois 和 Meier 于 2003 年将代数攻击（Algebraic Attack, AA）应用于以线性反馈移位寄存器为基础的流密码算法，随后，Courtois 在 AA 的基础上进行了改进从而提出了快速代数攻击（Fast Algebraic Attack, FAA）。布尔函数应分别具有高的代数免疫度和良好的快速代数免疫度才能有效的抵抗 AA 和 FAA。本文对一些基于有限域表示的布尔函数的仿射等价关系和快速代数免疫度性质进行研究，主要工作有：

(1) 在使用计算机进行辅助验证的基础上，研究了 Carlet-Feng 函数， Tu-Deng 函数，Tang-Carlet-Tang 函数的仿射等价关系。基于有限域表示的这三类函数，它们的支撑集中都含有共同的参数 s （$0 \le s \le 2^n - 2$）,从而能得到大量性质优良的布尔函数。经研究发现，**当参数 s 取不同值时，这些布尔函数是具有仿射等价的关系**。

(2) 在之前的研究中，主要是通过计算机计算布尔函数的快速代数免疫度。在唐灯的方法的启发下，我们通过数学证明的方法得到了**一类一阶弹性函数的快速代数免疫度大于等于 n-6**。于此同时，**也证明了一些起源于 Tu-Deng 猜想的组合事实**。

关键词：流密码；布尔函数；仿射等价；(快速)代数免疫度

ABSTRACT

Sequence cipher is one of the important ways to realize symmetric cipher system. In the design of cryptographic algorithm, nonlinear function is often used as the basic cipher component, and Boolean function is an effective way to realize these nonlinear functions. In order to resist the known cryptographic attack, the nonlinear Boolean function must have the provable performance to resist the known cryptographic attack. Before 2003, The Boolean functions used in stream cipher must meet the following properties： balancedness, large nonlinerarity, high algebraic degree, high order resiliency and good autocorrelation properites. In 2003, Courtois and Meier applied algebraic attack to stream cipher algorithm based on linear feedback shift register at European cipher annual conference. Later, Courtois improved algebraic attacks to come up with fast algebraic attacks. Boolean functions should have high algebraic immunity and good fast algebraic immunity respectively to resist algebraic attack and fast algebraic attack effectively. In this paper, affine equivalence relations and fast algebraic immunity of Boolean functions based on finite field representation are studied.

(1) On the basis of computer-aided verification, we study the affine equivalence of Carlet-Feng function, Tu-Deng function and Tang-Carlet-Tang function. These three kinds of functions based on the finite field representation have the same parameter s in their support, which makes them reach a large number of Boolean functions with excellent properties. **It is found that these Boolean functions have affine equivalence when the parameter s is different.**

(2) In the previous research, the fast algebraic immunity of Boolean function was calculated by computer. Inspired by Tang Deng's method, we get the fast algebraic immunity of **a class of first-order resilient functions by the method of mathematical proof**. At the same time, **we also prove some combinatorial facts originated from Tu-Deng conjecture.**

Keywords：stream cipher, Boolean functions, affine equivalence, (fast) algebraic immunity

目　录

第一章 绪 论

1.1. 研究背景及意义

在信息化时代的浪潮中，信息安全已经渐渐位于核心区域。密码算法的分析和研究与社会信息安全之间的关系越来越密切，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。密码学是以研究如何在一个不安全的信息通道中秘密的传递消息为目的，即保护要秘密传输的消息，防止第三方窃取信息的一门科学。在信息的传输过程中，我们一般将具有实际可理解意义的字符或者比特集称为明文，而将可直接理解的明文转换为不可直接解读的字符或比特集的算法称为加密算法，得到的字符或者比特集称为密文。加密和解密是一个过程完全相反的操作。无论是在加密过程中，还是在解密操作中，我们都需要用到一组满足一定条件的随机序列，我们称这个序列分别为加密/解密密钥，它们可以相同，也可以不同。

根据密钥的特点，流密码和分组密码共同组成了对称密钥体制。在流密码的加密过程中，密钥流序列的产生与密钥生成器在当前时钟周期的值有关。分组密码在加密过程中每一个时钟周期则使用相同的密钥加密一个数据单元。通常，流密码在每一个时钟周期用一个比特的加密密钥与一个比特明文进行异或操作；分组密码则在每一个时钟周期加密一个固定长度的数据块。

1.2. 流密码与布尔函数

在流密码系统中，布尔函数通常作为密钥流生成器的非线性组件，与反馈移位寄存器搭配产生安全强度高的密钥流。布尔函数的各种密码学指标都是根据各种攻击提出的。

1.2.1. 布尔函数在流密码中的应用

流密码也叫做序列密码，加解密过程非常简单。通过将可直接理解的明文与有密钥流生成器产生的密钥进行异或操作从未生成不可直接理解的密文。反之，则是将密文与密钥序列进行同样的异或操作从而恢复可直接理解的明文。流密码的模型如图 1-1 所示。Shannon 证明了“一次一密”密码体制在理论上是不可破解的。当用于加解密过程的密钥是由离散无记忆信源产生的满足均匀分布的随机序列时，这样的密码体制就满足“一次一密”的要求了。但随机序列的产生、存储和传送需要花费大量的资源和时间，在实际工作中需

要高昂的代价，因此用于流密码的加解密过程并不合适。在实际应用过程中，更为常见的做法是用伪随机序列去替代随机序列。伪随机序列是将一个长度较短的消息密钥按照一定的算法在最大程度满足随机特性的条件下生成一个很长的序列。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。

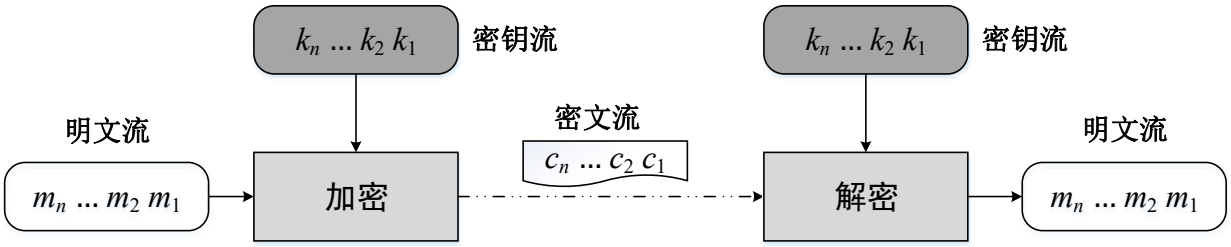

图 1-1 流密码模型

流密码是由驱动部分（Driving System, DS）和非线性组合部分（Nonlinear Composite System, NCS）组成。DS 主要是用来控制状态生成器根据时钟周期进行状态转移，从而生成大周期、统计性能好的序列提供给 NCS 使用。而 NCS 的职责是将由 DS 生成的序列进行组合，从而生成具有良好密码学性能的密钥流序列。目前比较成熟的技术是使用反馈移位寄存器（FSR）来设计流密码，布尔函数是FSR 的基本组件，n 级FSR 模型结构如图 1-2 所示。线性反馈移位寄存器（LFSR）拥有实现过程简单、生成序列的速度快的优点，并且便于分析和计算，在具有这些优势的情况下，它被广泛的应用在各种数字电路中，成为了密钥生成算法的重要构成组件。

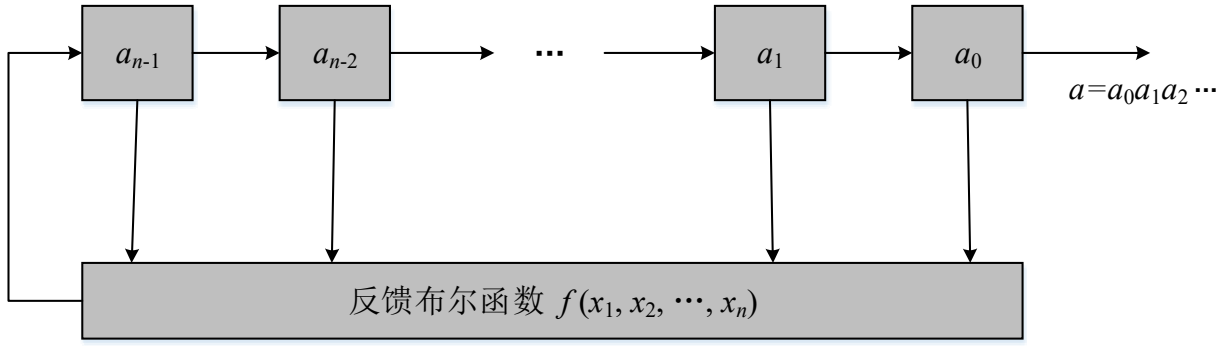

图 1-2 n 级反馈移位寄存器模型

为了保证加密系统的安全性，由LFSR 生成的随机序列是不能被直接使用的，因为它的密码学性质太弱。为了解决这个问题，在现代密码学中最常见的方法是使用一个密码学性质及其优良的非线性布尔函数对随机序列进行滤波或者组合，这就是滤波模式(图 1-3)和组合模式(图 1-4)，这样既能生成长周期的伪随机序列，又能保证生成的序列具有好的非

线性性质，从而满足Shannon所提出的混淆和扩散原则，通过此种方式生成的密钥流序列才有足够的安全强度。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。

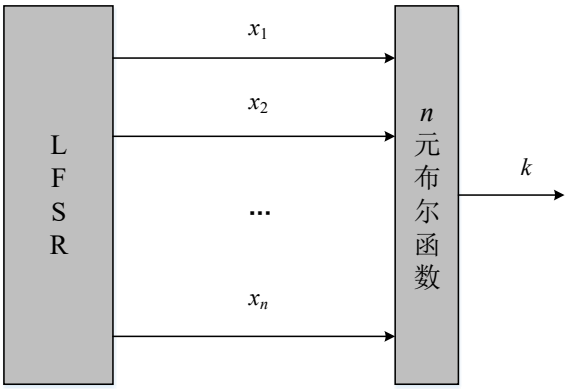

图 1-3 滤波模式

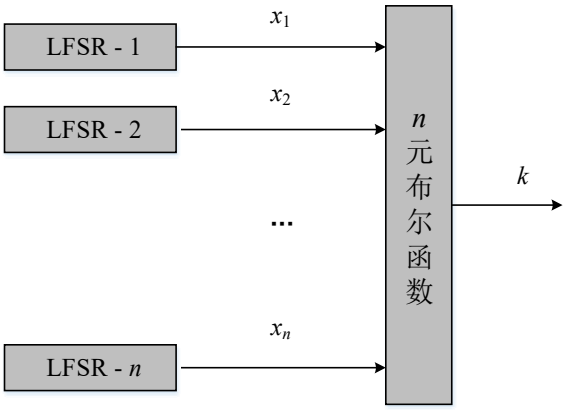

图 1-4 组合模式

1.2.2. 流密码的(快速)代数攻击

代数攻击是已知明文攻击，攻击思路是将一个密码算法理解为一个大型的多变元方程组，通过有效的求解方程组从而获取密钥。一个合格的密码算法，要对外公布所有的算法细节，只需要保证密钥不被他人所知即可。因此，密码研究者根据明密文之间的关系配合密码算法的结构，建立了一个以密钥为未知量的方程组。这个方法同时被密码编码者和密码分析者所指，所以密码编码学者也是利用方程组高的求解复杂度来保证系统的安全性，如同RSA是以大整数分解这个数学问题求解的困难性保证密码系统的安全。那么AA的关键点就是如何降低求解方程组的复杂度。既然无法有效的降低已知方程组求解的复杂度，那么我们就从问题的源头出发：建立次数尽可能低的方程组。Courtois和Meier[22] 在2003年的欧密会上成功了利用AA破译了一些流密码，这引起了国内外密码学者的对AA的兴趣。

下面介绍图 1-3 中非线性滤波函数生成器的AA 和FAA 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$f(x_1,x_2,\cdots,x_n)$。在已知密钥流比特z_{k_1}，z_{k_2},…，z_{k_l}的情况下，从而得到如下方程组

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

实际上，AA 和FAA 都是通过降低上述方程组求解复杂度从而进行攻击的。Courtois 和 Meier[22]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，如果存在次数不超过$\left\lceil \frac{n}{2} \right\rceil$的非零布尔函数$g$，使得$fg$的代数次数不超过$\left\lceil \frac{n+1}{2} \right\rceil$。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$f(L^t(S^0))=z_t$的两边得

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

若$z_t=0$，则$f(L^t(S^0))g(L^t(S^0))=hg(L^t(S^0))=0$；若$z_t=1$，则$g(L^t(S^0))+h(L^t(S^0))=0$。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[23]将如何降低方程组次数的问题转化为了寻找布尔函数及其反函数的低次非零零化子的问题，从而提出了代数免疫度（AI）的概念。为了满足代数免疫度的要求，密码研究者们提出了多种具有优良代数免疫度的布尔函数构造方法[11-15, 31, 32,44,45]。

后来在 2003 年美密会上，Courtois [24]在标准AA 的基础上进行改进并提出了快速代数攻击（FAA）：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。在得到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$\sum_i \alpha_i z_{t+i} g(L^{t+i}(S^0))=0$。

通过研究发现，我们可以简化FAA 的流程，它并不需要求出大量的零化子来建立线性无关方程组，只要找到一个关于f的特殊倍式关系，就可以发动AA 。FAA 对 Toyocrypt、

LILI-128 和蓝牙通信中的 E0 密码算法都非常有效。在文献[28]中，作者提出了快速代数免疫度(FAI)的概念，以用来评判布尔函数抵御FAA 的能力。目前对于FAI 的研究在处于起步阶段，好的研究成果还是比较少的，只有极少数布尔函数的FAI 得到严格证明。目前，大部分学者在学术论文中仍是通过计算机程序对较小变元的函数进行计算，从而得到FAI 的具体值。标准AA 和FAA 的时间与空间复杂度对比见表 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

为了评价布尔函数抵抗各种密码分析方法的能力，才随之诞生了这些安全指标。布尔函数的主要安全性指标如下图 1-5 所示。

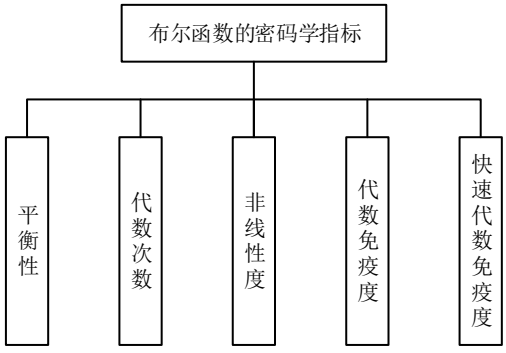

图 1-5 布尔函数的主要密码学指标

1.3. 国内外研究现状

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 $f\cdot g$ 的代数次数不大于 $\frac{n}{2}$，那么FAA 对于 f 就是有效的[24-26]。为了抵御FAA，密码系统中使用的布尔函数需具有较高的FAI[27, 28]。2012 年，刘美成等[29]提出了完美代数免疫(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$f\cdot g$的代数次数不小于$n-e$，则称f是PAI函数。他们[29]同时证明了n元布尔函数是PAI函数当且仅当$n=2^s$或$n=2^s+1$；并且仅当变元数量是2^s+1时，存在平衡PAI函数，仅当变元数量是2^s，存在不平衡PAI函数。实际上，PAI函数具有最优AI和最优FAI，且代数次数不低于$n-1$[29]。2012年，王启春等[30]给出了FAI关于高阶非线性度的一个上界。Carlet-Feng函数[12]和Tang-Carlet-Tang函数[32]是目前比较有代表性的两类布尔函数，它们都能有效的抵抗已知的密码攻击。2012年，刘美成等[29]证明了变元数量为2^s+1的Carlet-Feng函数是PAI函数；2014年，他们[33]还证明了Tang-Carlet-Tang函数对于任意变元都有几乎最优FAI。2017年，唐灯等[34]构造了一大类代数免疫最优1阶弹性函数，这类函数兼具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FAI不小于$n-6$。这是1阶弹性函数的FAI下界首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FAI的实际值仍然是非常困难的事情。

1.4. 本文内容及结构

本文对一些基于有限域表示的布尔函数的仿射等价关系和FAI进行研究，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一些相关概念，包括布尔函数的常见表示方法、主要密码学性质。

第三章研究了Carlet-Feng函数，Tu-Deng函数，Tang-Carlet-Tang函数的仿射等价关系。基于有限域表示的这三类函数，它们的支撑集中都含有共同的参数s（$0\le s\le 2^n-2$），从而能得到大量性质优良的布尔函数。经研究发现，当参数s取不同值时，这些布尔函数是具有仿射等价的关系。

第四章介绍通过数学证明的方法得到了一类一阶弹性函数的FAI大于等于6。于此同时，我们也证明了一些起源于Tu-Deng猜想的组合事实。

第五章总结本文完成的主要工作，并对下一步的工作进行了展望。

第二章 预备知识

本章首先介绍布尔函数及其表示的基本概念；其次介绍一些关于序列表示和布尔函数等价关系的基础知识。

2.1. 布尔函数的基本概念

设$\mathbb{F}_2$是二元有限域，n为正整数，$\mathbb{F}_2^n$是$\mathbb{F}_2$上的n维向量空间，从$\mathbb{F}_2^n$到$\mathbb{F}_2$的映射$f:\mathbb{F}_2^n \to \mathbb{F}_2$称为$n$元布尔函数。定义全体$n$元布尔函数的集合为$\mathbb{B}_n$，则$\mathbb{B}_n$中元素个数为$2^{2^n}$，也就是说，共有$2^{2^n}$个不同的布尔函数。

任意一个n变元布尔函数f都可以用一个长为2^n的真值表

$$(f(0,\cdots 0,0), f(0,\cdots 0,1), f(0,\cdots 1,0),\cdots, f(1,\cdots 1,1))$$

唯一表示。f的支撑集$supp(f)$定义为：满足$x \in \mathbb{F}_2^n$且$f(x)=1$的全体元素的集合。集合$supp(f)$中所含元素的个数称为f的Hamming重量，记为$wt(f)$。如果一个n元布尔函数f满足$wt(f)=2^{n-1}$，则称该函数是平衡的，即

$$|\{x \in \mathbb{F}_2^n \mid f(x)=1\}| = |\{x \in \mathbb{F}_2^n \mid f(x)=0\}| = 2^{n-1},$$

这里$|S|$表示集合S中所含元素的个数。

设$f,g \in \mathbb{B}_n$，f和g的Hamming距离定义为

$$d(f,g) = |\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}|。$$

由定义可知，f和g的Hamming距离实际上为差函数$f(x)-g(x)$的Hamming重量，即

$$d(f,g) = wt(f-g)。$$

一个n元布尔函数f可以用一个 $\mathbb{F}_2$上的含n个变元的多项式表示：

$$f(x_1,x_2,\cdots,x_n) = \sum_{a_i \in \mathbb{F}_2} f(a_1,a_2,\cdots,a_n)(x_1+a_1+1)(x_2+a_2+1)\cdots(x_n+a_n+1)$$

$$= \sum_{a_i \in \mathbb{F}_2} f(a_1,a_2,\cdots,a_n) x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \qquad (2\text{-}1)$$

这里，$x_i^{a_i} = x_i + a_i + 1, i = 1,2,\cdots,n$，“+”表示$\mathbb{F}_2$中的加法运算，即模2加运算。式（2-1）

称为布尔函数 f 的小项表示。在进行合并同类项后可得到多项式：

$$f(x_1,x_2,\cdots,x_n)=a_0+\sum_{i=0}^{n}a_ix_i+\sum_{1\le i<j\le n}a_{i,j}x_ix_j+\cdots$$
$$+\sum_{1\le i_1<\cdots<i_d\le n}a_{i_1,\cdots,i_d}x_{i_1}\cdots x_{i_d}+\cdots+a_{1,\cdots,n}x_{1,\cdots,n}, \quad (2\text{-}2)$$

这里系数 $a_0,a_i,a_{i,j},\cdots,a_{1,\cdots,n}\in\mathbb{F}_2$。

布尔函数 f 形如式（2-2）的表示形式存在且唯一，该表示形式为 f 的代数正规型（Algebraic Normal Form， ANF ）。若记集合 $N=\{1,2,\cdots,n\}$，用 $P(N)$ 表示 N 的幂集，即 N 的所有子集构成的集合，则 f 的ANF 还可以表示为

$$f(x_1,x_2,\cdots,x_n)=\sum_{I\in P(N)}a_I(\prod_{i\in I}x_i)=\sum_{I\in P(N)}a_Ix^I, \quad (2\text{-}3)$$

这里 $x^I=\prod_{i\in I}x_i$。

非零布尔函数 f 的 ANF 中系数为非零的项所含有变元个数的最大值定义为它的代数次数，记为 $\deg f$，即

$$\deg f=\max\{|\,I\mid a_I\neq 0,I\in P(N)\},$$

仿射函数的代数次数不超过 1，全体 n 元仿射函数的集合记为 A_n，即

$$A_n=\left\{f(x_1,x_2,\cdots,x_n)=\sum_{i=1}^{n}a_ix_i+a_0\mid a_0,a_1,a_2,\cdots a_n\in\mathbb{F}_2\right\}。$$

线性函数是常数项等于 0 的仿射函数，L_n 表示全体 n 元线性函数的集合，即

$$L_n=\left\{f(x_1,x_2,\cdots,x_n)=\sum_{i=1}^{n}a_ix_i\mid a_1,a_2,\cdots a_n\in\mathbb{F}_2\right\}。$$

由于 $x^I=1$ 当且仅当对任意 $i\in I$，都有 $x_i=1$，于是对任意给定的 $x=(x_1,x_2,\cdots,x_n)\in\mathbb{F}_2$，令 $supp(x)=\{1\le i\le n\mid x_i=1\}$,则布尔函数 f 在元素 x 处的值可以表示为

$$f(x_1,x_2,\cdots,x_n)=\sum_{I\in supp(x)}a_I。 \quad (2\text{-}4)$$

2.2. 布尔函数的密码学性质

密码系统中所使用的布尔函数为了抵抗各种已知攻击必须同时满足多项密码学性质，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**

为了保证由序列密码产生的密钥流具有高的安全强度，首先就要确保它们具有好的伪随机特性。高平衡性是保证序列具有伪随机性的一个重要条件。当序列中不同元素出现的次数至多相差一个时，称序列是平衡的。如果密码系统中使用的布尔函数不是平衡的，那么利用统计分析的方法，密码系统就无法抵抗概率攻击。布尔函数平衡性可由 Walsh 变换来描述。

引理 2.1 若布尔函数 $f \in \mathbb{B}_n$ 是平衡的，则 $W_f(0_n) = 0$。

➢ **代数次数**

为了有效抵抗 Berlekamp – Massey 算法攻击[16, 17]和 Ronjom-Helleseth 攻击[18]，布尔函数应具有较高的代数次数。对于 n 元平衡布尔函数 f，其中 $n \geq 2$，f 的汉明重量是偶数，由式(2-2)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 2.2 若布尔函数 $f \in \mathbb{B}_n$ 的汉明重量是偶数，则 $\deg(f) \leq n-1$。

➢ **非线性度**

为了保证密码系统中使用的布尔函数能够抵抗最佳仿射逼近（Best Affine Approximation Attack）[19]和快速相关攻击（Fast Correlation Attack）[20]，布尔函数与所有仿射函数保持较大的汉明距离。

定义 2.1 布尔函数与所有仿射函数的最小汉明距离定义为非线性度。对于布尔函数 $f \in \mathbb{B}_n$，其非线性度为

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

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

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

因此，布尔函数的非线性度可由 Walsh 变换等价表示为

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

- **(快速)代数免疫度**

代数免疫度（AI）[21, 23]是评价布尔函数抵抗AA能力的指标，攻击思路是将一个密码算法理解为一个大型的多变元方程组，通过有效的求解方程组从而获取密钥，而求解方程组的复杂度就取决于方程组的次数。如果密码系统中使用的布尔函数f或者$f+1$具有低次的零化子，那么密码系统对AA的抵抗能力较弱。

定义 2.2 ([23]) 对于两个布尔函数$f, g \in \mathbb{B}_n$，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$\mathrm{Ann}(f) = \{g \in \mathbb{B}_n \mid f\cdot g = 0\}$。布尔函数$f$的代数免疫度$AI(f)$定义为：

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

若n元布尔函数的AI到了上界$\left\lceil \frac{n}{2} \right\rceil$[23]，则称$f$具有最优AI。

布尔函数仅仅具有较高的AI对于抵抗AA是不够的，这仅仅是必要条件，而不是充要条件。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，那么就能有效的对f发动FAA [24-26]。为了抵抗FAA，密码系统中使用的布尔函数需具有较高的FAI [27, 28]。

定义 2.3 ([28]) 布尔函数$f \in \mathbb{B}_n$的快速代数免疫度为

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

若f的FAI达到n(或$n-1$)，则称f具有最优(或几乎最优) FAI。

2.3. 序列表示和布尔函数的等价性

两个n元布尔函数f和g是仿射等价的当且仅当存在一个$\mathbb{F}_2$上的$n\times n$的可逆矩阵A和一个$\mathbb{F}_2^n$上的向量a使得：

$$f(X) = g(X\cdot A \oplus a),$$

这里$X = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$。因为仿射等价布尔函数之间是有相同的代数次数，与此同时

也拥有相同的AI。因此，布尔函数的代数次数和AI是仿射不变量。

令寄存器生成一个周期为$q-1$的m序列，并且序列$\{s_t\}$满足递归关系：

$$\sum_{j=0}^{n} m_j s_{t+j} = 0, m_j \in F_2,$$

这里$m_0 = m_n = 1$。与此同时，$m(x) = 1 + m_1 x + \cdots + m_{n-1}x^{n-1} + x^n$是它的生成多项式并且是本源的。（转置）伴随矩阵$M$（我们称它为序列的生成矩阵）是

$$M = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 1 \\ m_0 & m_1 & \cdots & m_{n-2} & m_{n-1} \end{pmatrix}。$$

令$(s_t, s_{t+1}, ..., s_{t+n-1})^T$为时刻$t$时寄存器的状态。下一刻寄存器的状态可以表示为：

$$(s_{t+1}, s_{t+2}, ..., s_{t+n})^T = M(s_t, s_{t+1}, ..., s_{t+n-1})^T = M^{t+1}(s_0, s_1, ..., s_{n-1})^T.$$

如果寄存器的初始状态是b，那么序列能被表示为$S = (b, Mb, ..., M^{q-2}b)$。这里$b$可以是任意非零$n$维列向量，因此这里有$q-1$个$S$对应于$q-1$个不同的$m$序列。令$b_0 = (1, 0, ..., 0)^T$，序列能够表示为

$$S_k = (M^k b_0, M^{k+1} b_0, ..., M^{k+q-2} b_0),$$

这里$0 \le k \le q-2$。

因为次数为n的本源多项式的数量是$\phi(q-1)/n$，所以这有$\phi(q-1)/n$个$LFSRs$生成m序列，并且不同的$LFSRs$则对应不同的序列。因为，这存在$(q-1)\phi(q-1)/n$个m序列，每个序列能够表示为

$$S_{j,k} = (M_j^k b_0, M_j^{k+1} b_0, ..., M_j^{k+q-2} b_0),$$

这里$1 \le j \le \phi(q-1)/n$，M_j是序列的生成矩阵，并且$1 \le k \le q-2$。显而易见，$M_j^k b_0$是$LFSR$的初始状态。

令$T = \mathbb{F}_2^n - \{\mathbf{0}\}$。显而易见，这存在两个$f \in \mathbb{B}_n$使得$1_f \bigcap T = T_0$，这里$T_0$是$T$的一个子集。我们定义两个函数为$f_1$和$f_2$。那么$f_1$与$f_2$不相同仅当$x=0$和$f_1 = f_2 + (x_1+1)(x_2+1)...(x_n+1)$。给定任意的$LFSR$，通过使用$f_1$和$f_2$作为滤波函数生成的密钥流是相同的。因此，$f_1$和$f_2$能够被看成相同的函数。令

$$\mathbb{B}_n^* = \mathbb{B}_n / \{0,(x_1+1)(x_2+1)...(x_n+1)\}。$$

那么任意的 $f \in \mathbb{B}_n^*$ 能够通过它的支撑集表示为如下形式

$$1_f = \{M_j^{i_1}b_0, M_j^{i_2}b_0, ..., M_j^{i_w}b_0\},$$

这里 M_j 的寄存器的生成矩阵，并且 $0 \le i_1 < i_2 < ... < i_w \le q-2$。

Ronjom 和 Cid 提出了布尔函数的非线性等价性，定义如下[41]：

定义 2.4 如果这存在一个被 f_2 过滤和能产生相同密钥流的 $LFSR$，那么 $f_2 \in \mathbb{B}_n^*$ 是与 f_1 等价的。特别的是，如果这两个 $LFSRs$ 有相同的生成多项式，我们说 f_1 和 f_2 是线性等价的，并且定义为 $f_1 \sim_L f_2$。否则，f_1 和 f_2 是非线性等价的，并且定义为 $f_1 \sim_N f_2$。

第三章 基于本源元表示的布尔函数的平移等价性

本章首先证明了Carlet-Feng函数支撑集的平移等价关系。接着采用相似的证明方法证明了Tu-Deng函数和Tang-Carlet-Tang函数支撑集的平移等价关系。

3.1. Carlet-Feng函数支撑集的平移等价关系

Carlet和冯克勤基于有限域的本源元和布尔函数的单变元表示构造了一类具有最优AI的布尔函数（Carlet-Feng函数）。

构造3.1（[37]）令n为大于1的整数，α为$\mathbb{F}_2^n$上的本源元。当f是一个n元的布尔函数，$supp(f)$为

$$\{0,\alpha^s,\alpha^{s+1},...,\alpha^{s+2^{n-1}-2}\},$$

这里$0\le s<2^n-1$是一个整数，布尔函数f有最优AI$\left\lceil\frac{n}{2}\right\rceil$。

在原先的构造思路中，Carlet-Feng函数的支撑集中存在一个参数s，如果对s取不同值时，那么Carlet-Feng函数的支撑集是不相同的，随之对应的布尔函数自然而然也是不相同的。因此在之前的设想中，我们可以同时得到大量具有最优AI的布尔函数。然而，经研究发现当参数s取不同值时，得到的布尔函数是仿射等价的，并且它的代数次数、AI和非线性度是不变量。

随后，王启春利用$\mathbb{F}_2$上的本源多项式的伴随矩阵构造了一类具有最优AI的布尔函数[38]。构造1的主要结果完全等价于通过代替二元m序列的本源多项式的伴随矩阵生成的构造2.

构造3.2（[38]）令n为大于1的整数，$\underline{s}=(s_t)_{t\ge0}$是长度为$n$的$m$序列。当$f$是一个$n$元的布尔函数，$supp(f)$为

$$\{\mathbf{0}\}\cup\{s_t,s_{t+1},...,s_{t+n-1}\mid 0\le t\le 2^{n-1}-2\}$$

这里$\mathbf{0}$定义为$\mathbb{F}_2^n$上的全零向量，那么布尔函数f有最优AI$\left\lceil\frac{n}{2}\right\rceil$。

事实上，构造1和构造2已经被证明是仿射等价的[39]。

引理3.1（[39]）令n为大于1的整数，$m(x)$是$\mathbb{F}_2$上的次数为n的本源多项式。如果$\alpha\in\mathbb{F}_{2^n}$

是 $m(x)$ 的一个根，并且 $\underline{s}=(s_t)_{t\geq 0}\in G(m(x))$ 是一个非零序列，这存在一个 $\mathbb{F}_{2^n}$ 上的基 $\{\beta_0,\beta_1,...,\beta_{n-1}\}$ 使得

$$s_t\beta_0\oplus s_{t+1}\beta_1\oplus\cdots\oplus s_{t+n-1}\beta_{n-1}=\alpha^t, t\geq 0\text{。}$$

引理 3.2 （**[40]**）令 $f\in\mathbb{B}_n$,并且

$$1_f=\{M_1^{k_1+i_1}b_0, M_1^{k_1+i_2}b_0,..., M_1^{k_1+i_w}b_0\},$$

这里 M_1 是序列的生成矩阵，$0\leq i_1<i_2<...<i_w\leq q-2$。清晰可见，任意 $g\sim f$ 能够被表示为

$$1_g=\{M_j^{k_2+i_1}b_0, M_j^{k_2+i_2}b_0,..., M_j^{k_2+i_w}b_0\},$$

这里 $1\leq j\leq \phi(q-1)/n$， M_j 是一个生成矩阵，并且 $0\leq k_2\leq q-2$。

定理 3.1 令 n 为大于 1 的整数，α 为 $\mathbb{F}_2^n$ 上的本源元。当 f 是一个 n 元的布尔函数，它的支撑集为

$$\{0,\alpha^s,\alpha^{s+1},...,\alpha^{s+2^{n-1}-2}\},$$

这里 $0\leq s<2^n-1$ 是一个整数。当参数 s 取不同值时，所生成的布尔函数具有仿射等价的关系。

证明： 从引理 3.1 中得知每一个在 Carlet-Feng 函数支撑集中的 α^t 都有一个非零序列 $\{s_t,s_{t+1},...,s_{t+n-1}\}$ 与之相对应。令 $(s_t,s_{t+1},\cdots,s_{t+n-1})^T$ 为 t 时刻寄存器中的状态。那么下一时刻的状态为

$$(s_{t+1},s_{t+2},...,s_{t+n})^T=M(s_t,s_{t+1},...,s_{t+n-1})^T=M^{t+1}(s_0,s_1,...,s_{n-1})^T.$$

如果寄存器的初始状态是 b_0，那么这个序列能够表示为

$$(s_{t+1},s_{t+2},...,s_{t+n})=(M^tb_0,M^{t+1}b_0,...,M^{t+n-1}b_0)\text{。}$$

因为

$$s_t\beta_0\oplus s_{t+1}\beta_1\oplus\cdots\oplus s_{t+n-1}\beta_{n-1}=\alpha^t, t\geq 0,$$

所以

$$M^tb_0\beta_0\oplus M^{t+1}b_0\beta_1\oplus\cdots\oplus M^{t+n-1}b_{n-1}\beta_0=\alpha^t, t\geq 0\text{。}$$

因此，我们能将 Carlet-Feng 函数表示为

$$1_f=\{0\}\cup\{M_1^{i+s}b_0\mid i=0,1,...,2^{n-1}-2, 0\leq s<2^n-1\}\text{。}$$

从引理 3.2 可知给定一个 $LFSR$，它的生成矩阵为 M_1，令 $f_1 \in \mathbb{B}_n^*$，并且

$$1_{f_1} = \{M_1^i b_0 \mid i = 0,1,...,2^{n-1}-1\}。$$

显而易见，任意 $g \sim_L f_1$ 能够被表示为

$$1_g = \{M_1^{s+i} b_0 \mid i = 0,1,...,2^{n-1}-1\},$$

M_1 为一个生成矩阵，$0 \le s < 2^n - 1$。因此，当参数 s 取不同值时，所生成的 Carlet-Feng 函数是仿射等价的。

3.2. Tu-Deng 函数和 Tang-Carlet-Tang 函数支撑集的平移等价关系

涂自然和邓映蒲构造了一类具有最优 AI 的 $bent$ 函数，它是属于 Dillon 定义的 PS^- 类[31]。在稍微修改它的真值表后，可以得到一个平衡的布尔函数。虽然会稍微降低它的非线性度，但不会改变它最优 AI 的性质，我们称它为 Tu-Deng 函数。然而在本文中，我们的研究重点是仿射等价关系。

构造 3.3（[31]） 令 $n = 2k$，α 是 $\mathbb{F}_{2^k}$ 上的本源元。布尔函数 $g : \mathbb{F}_{2^k} \to \mathbb{F}_2$ 定义如下

$$supp(g) = \{1 = \alpha^s, \alpha^{s+1}, ..., \alpha^{2^{k-1}+s-1}\}。$$

布尔函数 $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ 定义如下

$$f(x,y) = g(x / y)。$$

定理 3.2 令 $n = 2k$，β 是 $\mathbb{F}_{2^n}$ 上的本源元。布尔函数 $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ 定义如下

$$f(x,y) = g(x / y),$$

布尔函数 f 的支撑集能被定义为

$$supp(f) = \{\beta^{(2^k+1)(i+s)} + \beta^{2^k-1} \cdot \beta^{(2^k+1)j}\},$$

这里 $i \in (0,2^k), j \in (0,2^k), (i-j) \left(\mathrm{mod}\, 2^k - 1\right) \in (0,2^{k-1}-1)$，$0 \le s < 2^k - 1$ 是一个整数。

证明 我们假定 α 是 $\mathbb{F}_{2^k}$ 上的本源元，β 是 $\mathbb{F}_{2^n}$ 上的本源元，所以 $\alpha = \beta^{(2^n-1)/(2^k-1)} = \beta^{2^k+1}$。通过构造 3.3，我们能假设 $x = \alpha^i, y = \alpha^j$，因此

$$f(x,y) = f(\alpha^i, \alpha^j) = g(\alpha^{i-j}),$$

并且 $x = \beta^{(2^k+1)i}, y = \beta^{(2^k+1)j}$。令 ω 为 $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^{n/2}}$ 上的任一元素。$(1,\omega)$ 是 $F_{2^{n/2}}$-向量空间 F_2^n 的

一个基。因此，我们有 $F_{2^n} = F_{2^{n/2}} + \omega F_{2^{n/2}}$ 。令 $\omega = \beta^{(2^n-1)/(2^k+1)} = \beta^{2^k-1}$ ，所以 $f(x,y) = f(\alpha^i, \alpha^j) = f(\alpha^i + \omega\alpha^j)$ 。通过 g 的支撑集，我们知道当 $(i-j)\left(\bmod 2^k-1\right) \in (0, 2^{k-1}-1)$ 时， $g(\alpha^{i-j}) = 1$ 。最后，我们知道布尔函数 f 的支撑集为 $supp(f) = \{\beta^{(2^k+1)i} + \beta^{2^k-1} \cdot \beta^{(2^k+1)j}\}$ 。

在Tu-Deng函数的启发下，唐灯将函数 $g(x/y)$ 替换为 $g(xy)$ 得到了两类变元为 $n = 2k$ 的具有优良性质的布尔函数，称之为Tang-Carlet-Tang函数。第一类函数是不平衡的，它的汉明重量为 $2^{n-1} - 2^{k-1}$ ，代数次数为 $n-2$ ，并且具有非常高的非线性度。

构造 3.4 （**[32]**）令 $n = 2k > 4$ ， α 为 $\mathbb{F}_{2^k}$ 上的一个本源元。集合 $\Delta = \{\alpha^s, ..., \alpha^{2^{k-1}+s-1}\}$ ， $0 \le s < 2^k - 1$ 为一个整数。布尔函数 $f \in \mathbb{B}_n$ 定义如下

$$f(x,y) = g(xy),$$

这里布尔函数 g 的支撑集为 Δ 。

定理 3.3 令 $n = 2k$ ， β 是 $\mathbb{F}_{2^n}$ 上的本源元。布尔函数 $f: \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ 定义如下

$$f(x,y) = g(xy),$$

布尔函数 f 的支撑集能被定义为

$$supp(f) = \{\beta^{(2^k+1)(i+s)} + \beta^{2^k-1} \cdot \beta^{(2^k+1)j}\},$$

这里 $i \in (0, 2^k), j \in (0, 2^k), (i+j)\left(\bmod 2^k-1\right) \in (0, 2^{k-1}-1)$ ， $0 \le s < 2^k - 1$ 是一个整数。

证明 证明过程与定理 3.2 相似。

定理 3.4 当参数 s 取不同值时，Tang-Carlet-Tang函数是仿射等价的。与此同时，Tu-Deng函数也是仿射等价的。

证明 我们首先证明Tang-Carlet-Tang函数是仿射等价的当参数 s 取不同值时。Tang-Carlet-Tang函数的支撑集可以写作

$$supp(f) = \{\beta^{(2^k+1)(i+s)} + \beta^{2^k-1} \cdot \beta^{(2^k+1)j}\}。$$

我们能将Tang-Carlet-Tang函数的支撑集的每个元素看作是两部分，以+作为分隔。我们令 $Part_1 = \beta^{(2^k+1)(i+s)}$ ， $Part_2 = \beta^{2^k-1} \cdot \beta^{(2^k+1)j}$ 。从定理 3.1 得知当参数 s 取不同值时，由 $Part_1$ 得到的布尔函数是仿射等价的。此外， $Part_2$ 的使用仅仅是设置 $Part_1$ 后的第 $Part_2$ 个位置的值为 1，这样增加了真值表中 1 的数量。只要 $Part_1$ 是确定的，那么 $Part_2$ 的位置就是在

$Part_1$后不断移动的。因此$Part_2$不会影响支撑集的平移等价性。故当参数s取不同值时，Tang-Carlet-Tang函数是仿射等价的。相同的证明过程可以得到Tu-Deng函数也是仿射等价的。

3.3. 本章小结

本章研究了基于$\mathbb{F}_{2^n}$上的本源元构造的布尔函数的仿射等价关系。尽管这三个构造被证明并没有提供大量的性质优良的布尔函数，但它们都具有出色的密码学性质。同时，研究布尔函数的仿射等价性有助于构造布尔函数。

此部分研究工作已整理成文章 Translation equivalence of Boolean functions expressed by primitive element，并于 2019 年 4 月发表在 IEICE TRANS.FUNDAMENTALS 期刊。

第四章 一类 1 阶弹性布尔函数的快速代数免疫度的下界

本章通过数学证明的方法得到了一类一阶弹性函数的FAI大于等于 n-6。在之前的研究中，主要是通过计算机辅助计算布尔函数的FAI。于此同时，我们也证明了一些起源于Tu-Deng猜想的组合事实。

4.1. 一类具有几乎最优代数免疫度的布尔函数

近些年，利用Carlet-Feng函数作为一个组件，使用二元多项式表达的方法已经得到了大量优秀的构造。在 2013 年，唐灯提出了两类具有非常优秀密码学性质的布尔函数，但是它们不是 1 阶弹性的，这是一个缺点当布尔函数作为一个滤波函数使用时[32]。

构造 4.1 （[32]）令 $n=2k\geq 4$，α 是 $\mathbb{F}_{2^k}$ 上的一个本原元，$\Delta_s=\{s,s+1,\cdots,s+2^{k-1}-1\}$，这里 $0\leq s<2^k-1$。布尔函数 $b_s(x,y)\in\mathbb{B}_n$ 定义如下：

$$b_s(x,y)=g_s(xy) \qquad (4\text{-}1)$$

这里 g_s 定义在 $\mathbb{F}_{2^k}$ 上，并且 $supp(g_s)=\{\alpha^i \mid i\in\Delta_s\}$。

命题 4.1 （[32]）构造 4.1 中 n 变元布尔函数 $b_s(x,y)$ 包括四个密码学性质：

1) $b_s(x,y)=\sum_{i=1}^{2^k-2}\alpha^{-is}(1+\alpha^{-i})^{2^{k-1}-1}(xy)^i$ ，$\deg(b_s)=n-2$；

2) $AI(b_s)=k$；

3) $nl(b_s)>2^{n-1}-(\frac{\ln 2}{\pi}+0.42)2^k-1$；

4) $FAI(b_s)\geq n-2$。

命题 1 构造 2 中 n 变元布尔函数 $b_s(x,y)$ 包括两个密码学性质：

1) $AI(b_s)=k$；

2) $FAI(b_s)\geq n-2$。

由于后续证明的需要，我们修改构造 4.1 从而得到了一类具有次优代数免疫度的布尔

函数。在构造 4.1 中，Δ_s 的基数是 2^{k-1}。我们会减少 Δ_s 的基数从而获得基数为 $2^{k-1}-2$ 的 Δ_m。

构造 4.2 令 $n=2k\geq 4$，α 是 $\mathbb{F}_{2^k}$ 上的一个本原元，$\Delta_m=\{m+2,m+3,\cdots,m+2^{k-1}-1\}$，这里 $0\leq m<2^k-1$。布尔函数 $b_m(x,y)\in\mathbb{B}_n$ 定义如下：

$$b_m(x,y)=g_m(xy) \qquad (4\text{-}2)$$

这里 g_m 定义在在 $\mathbb{F}_{2^k}$ 上，并且 $supp(g_m)=\{\alpha^j \mid j\in\Delta_m\}$。

为了证明构造 4.2 的代数免疫度，我们需要去证明一些通过修改 Tu-Deng 猜想[31]产生的组合事实。最后，我们得到了一些新的引理。

引理 4.1 **（[42]）**对于 $k\geq 3, 1\leq t\leq 2^k-2$，令

$$M_{\leq k-1,t}=\left\{(a,b)\in\mathbb{Z}^2 \left| \begin{array}{c} 0\leq a,b\leq 2^k-2, \\ a-b\equiv t(\mathrm{mod}\,2^k-1), \\ wt(\bar{a})+wt(\bar{b})\leq k-1 \end{array} \right.\right\}。$$

那么 $\left|M_{\leq k-1,t}\right|\leq 2^{k-1}-1$。

引理 4.2 对于 $k\geq 3, 1\leq t\leq 2^k-2$，令

$$M_{\leq k-1,t}=\left\{(a,b)\in\mathbb{Z}^2 \left| \begin{array}{c} 0\leq a,b\leq 2^k-2, \\ a-b\equiv t(\mathrm{mod}\,2^k-1), \\ wt(\bar{a})+wt(\bar{b})=k-1 \end{array} \right.\right\}。$$

那么 $\left|M_{k-1,t}\right|\geq 1$。

证明 因为移位等价性，t 能够被表示为如下的形式：

$$t=\underbrace{0\cdots0}_{n_1}\underbrace{1\cdots1}_{n_2}\underbrace{0\cdots0}_{n_3}\underbrace{1\cdots1}_{n_4}\cdots\underbrace{0\cdots0}_{n_{2r-1}}\underbrace{1\cdots1}_{n_{2r}},$$

这里 $\sum_{i=1}^{2r}n_i=k,\ n_i\geq 1\ (1\leq i\leq 2r,\ r\geq 1)$。

如果 $wt(t)=k-1$，即 $t=\underbrace{011\cdots1}_{k}$，令

$$a=\underbrace{1001\cdots1}_{k},\ b=\underbrace{0010\cdots0}_{k},$$

那么 $a-b=t$ 和 $wt(\bar{a})+wt(\bar{b})=(k-2)+1=k-1$。因此 $(a,b)\in M_{k-1,t}$。

假设现在 $wt(t)<k-1$，并且令 $\mu=(k-1)-wt(t)$，那么

$$n_1 + n_3 + \cdots + n_{2r-1} = \sum_{i=1}^{r} n_{2i-1} = k - wt(t) = \mu + 1 。$$

情形 1：μ 是偶数。令

$$\begin{cases} a = \underbrace{0\cdots0}_{n_1}\overbrace{1\cdots1}^{m_1}\underbrace{1\cdots1}_{n_2}\underbrace{0\cdots0}_{n_3}\overbrace{1\cdots1}^{m_2}\underbrace{1\cdots1}_{n_4}\cdots\underbrace{0\cdots0}_{n_{2r-1}}\overbrace{1\cdots1}^{m_r}\underbrace{1\cdots1}_{n_{2r}}, \\ b = \underbrace{0\cdots0}_{n_1}\overbrace{1\cdots1}^{m_1}\underbrace{0\cdots0}_{n_2}\underbrace{0\cdots0}_{n_3}\overbrace{1\cdots1}^{m_2}\underbrace{0\cdots0}_{n_4}\cdots\underbrace{0\cdots0}_{n_{2r-1}}\overbrace{1\cdots1}^{m_r}\underbrace{0\cdots0}_{n_{2r}}, \end{cases}$$

这里 $\sum_{i=1}^{r} m_i = \frac{\mu}{2}, 0 \le m_i \le n_{2i-1}\ (1 \le i \le r)$。因为

$$\sum_{i=1}^{r} m_i = \frac{\mu}{2} < \mu + 1 = \sum_{i=1}^{r} n_{2i-1} ,$$

所以 (a,b) 存在。显而易见，$a - b = t$，并且

$$wt(a) + wt(b) = (wt(t) + \frac{\mu}{2}) + \frac{\mu}{2} = wt(t) + \mu = k - 1 。$$

因此 $(a,b) \in M_{k-1,t}$。

情形 1：μ 是奇数。令

$$\begin{cases} a = \underbrace{0\cdots0}_{n_1}\overbrace{1\cdots1}^{m_1}\underbrace{1\mathbf{0}1\cdots1}_{n_2}\underbrace{0\cdots0}_{n_3}\overbrace{1\cdots1}^{m_2}\underbrace{1\cdots1}_{n_4}\cdots\underbrace{0\cdots0}_{n_{2r-1}}\overbrace{1\cdots1}^{m_r}\underbrace{1\cdots1}_{n_{2r}}, \\ b = \underbrace{0\cdots0}_{n_1}\overbrace{1\cdots1}^{m_1}\underbrace{0}_{n_2}\underbrace{0\cdots0}_{n_3}\overbrace{1\cdots1}^{m_2}\underbrace{0\cdots0}_{n_4}\cdots\underbrace{0\cdots0}_{n_{2r-1}}\overbrace{1\cdots1}^{m_r}\underbrace{0\cdots0}_{n_{2r}}, \end{cases}$$

这里 $\sum_{i=1}^{r} m_i = \frac{\mu - 1}{2}, 0 \le m_1 \le n_1 - 1, 0 \le m_i \le n_{2i-1}\ (2 \le i \le r)$。因为

$$\sum_{i=1}^{r} m_i = \frac{\mu - 1}{2} < \mu = \sum_{i=1}^{r} n_{2i-1} - 1 = (n_1 - 1) + \sum_{i=2}^{r} n_{2i-1} ,$$

所以 (a,b) 存在。显而易见，$a - b = t$，并且

$$wt(a) + wt(b) = (wt(t) - 1 + 1 + \frac{\mu - 1}{2}) + (\frac{\mu - 1}{2} + 1) = wt(t) + \mu = k - 1 。$$

因此 $(a,b) \in M_{k-1,t}$。

因此，对于任意的 $1 \le t \le 2^k - 2$，这总是存在至少一个 $(a,b) \in M_{k-1,t}$，所以 $| M_{k-1,t} | \ge 1$。

引理 4.3 对于$k \geq 3, 1 \leq t \leq 2^k - 2$，令

$$M_{\leq k-2,t} = \left\{ (a,b) \in \mathbb{Z}^2 \left| \begin{array}{c} 0 \leq a,b \leq 2^k - 2, \\ a - b \equiv t (\mathrm{mod}\, 2^k - 1), \\ wt(\bar{a}) + wt(\bar{b}) \leq k-2 \end{array} \right. \right\}。$$

那么$\left| M_{\leq k-2,t} \right| \leq 2^{k-1} - 2$。

证明 显而易见，

$$\begin{cases} M_{\leq k-1,\,t} = M_{k-1,\,t} \cup M_{\leq k-2,\,t} \\ M_{k-1,\,t} \cap M_{\leq k-2,\,t} = \varnothing \end{cases}。$$

从引理 4.1 和引理 4.2，可知$| M_{\leq k-1,\,t} | \leq 2^{k-1} - 1$和$| M_{k-1,\,t} | \geq 1$。因此

$$| M_{\leq k-2,\,t} | = | M_{\leq k-1,\,t} | - | M_{k-1,\,t} | \leq (2^{k-1} - 1) - 1 \leq 2^{k-1} - 2.$$

引理 4.4 对于$k \geq 3, t = 0$，令

$$M_{\leq k-2,0} = \left\{ (a,b) \in \mathbb{Z}^2 \left| \begin{array}{c} 0 \leq a,b \leq 2^k - 2, \\ a - b \equiv t (\mathrm{mod}\, 2^k - 1), \\ wt(\bar{a}) + wt(\bar{b}) \leq k-2 \end{array} \right. \right\}。$$

那么$\left| M_{\leq k-2,0} \right| \leq 2^{k-1} - 2$。

证明 当$t = 0$，$a = b$，并且$2wt(\bar{a}) \leq k-2$，即$wt(\bar{a}) \leq (k-2)/2$。

情形 1：k是奇数。我们有$0 \leq wt(\bar{a}) \leq \left\lfloor \frac{k-2}{2} \right\rfloor = \frac{k-3}{2}$。所以

$$\begin{aligned} | M_{\leq k-2,\,0} | &= \sum_{i=0}^{\frac{k-3}{2}} \binom{k}{i} = \frac{1}{2} \left(\sum_{i=0}^{\frac{k-3}{2}} \binom{k}{i} + \sum_{i=\frac{k+3}{2}}^{k} \binom{k}{i} \right) \\ &= \frac{1}{2} \left(\sum_{i=0}^{k} \binom{k}{i} - \binom{k}{\frac{k-1}{2}} - \binom{k}{\frac{k+1}{2}} \right) \\ &= 2^{k-1} - \binom{k}{\frac{k-1}{2}} \\ &\leq 2^{k-1} - 2, \end{aligned}$$

因为对于奇数 $k \geq 3$，$\binom{k}{\frac{k-1}{2}} \geq 2$。

情形 1：k 是偶数。我们有 $0 \leq wt(\bar{a}) \leq \frac{k-2}{2}$。所以

$$|M_{\leq k-2,0}| = \sum_{i=0}^{\frac{k-2}{2}} \binom{k}{i} = \frac{1}{2}\left(\sum_{i=0}^{\frac{k-2}{2}} \binom{k}{i} + \sum_{i=\frac{k+2}{2}}^{k} \binom{k}{i}\right)$$

$$= \frac{1}{2}\left(\sum_{i=0}^{k} \binom{k}{i} - \binom{k}{\frac{k}{2}}\right)$$

$$= 2^{k-1} - \frac{1}{2}\binom{k}{\frac{k}{2}}$$

$$\leq 2^{k-1} - 2。$$

因为对于偶数 $k \geq 4$，$\binom{k}{\frac{k}{2}} \geq 4$。

证明完成。

从引理 4.3 和引理 4.4，我们能推断出以下引理：

引理 4.5 对于 $k \geq 3, 0 \leq t \leq 2^k - 2$ ，令

$$M_{\leq k-2,t} = \left\{ (a,b) \in \mathbb{Z}^2 \left| \begin{array}{c} 0 \leq a,b \leq 2^k - 2, \\ a - b \equiv t (\mathrm{mod}\, 2^k - 1), \\ wt(\bar{a}) + wt(\bar{b}) \leq k-2 \end{array} \right. \right\}。$$

那么 $\left|M_{\leq k-2,t}\right| \leq 2^{k-1} - 2$。

定理 4.1 令 f 为构造 4.2 中 $2k$ 变元的布尔函数。那么 $AI(f)$ 是 $k-1$。

证明 从构造 4.2 中，我们能看出 $supp(f) = \{(\gamma y^{2^k-2}, y) \mid y \in \mathbb{F}_{2^k}^*, \gamma \in \Delta_m\}$。

首先，假定 $h(x,y) = \sum_{i=0}^{2^k-1}\sum_{j=0}^{2^k-1} h_{i,j} x^i y^j \in \mathbb{B}_n$ 是 f 的一个代数次数小于 $k-1$ 的零化子，即

1) 对于所有的 $y \in \mathbb{F}_{2^k}^*, \gamma \in \Delta_m$， $h(\gamma y^{2^k} - 2, y) = 0$。

2) 当 $wt(\overline{i})+wt(\overline{j})\geq k-1$ 时，$h_{i,j}=0$。这暗示当 $0\leq i,j<2^k-1$ 时，

$$h_{2^k-1,j}=h_{i,2^k-1}=h_{2^k-2,j}=h_{i,2^k-2}=0\text{。}$$

因此

$$h(\gamma y^{2^k-2},y)=\sum_{i=0}^{2^k-3}\sum_{j=0}^{2^k-3}h_{i,j}\gamma^i y^{j-i}=\sum_{t=0}^{2^k-3}h_t(\gamma)y^t,$$

这里

$$\begin{aligned}h_t(\gamma)&=\sum_{0\leq i,j\leq 2^k-3,j-i\equiv t(\bmod 2^k-1)}h_{i,j}\gamma^i\\&=\sum_{i=0}^{2^k-3-t}h_{i,t+i}\gamma^i+\sum_{i=2^k-2-t}^{2^k-3}h_{i,t+i-(2^k-1)}\gamma^i,\end{aligned}$$

当 $\gamma\in\Delta_m, h(\gamma y^{2^k-2},y)=0$ 对于 $y\in\mathbb{F}_{2^k}^*$ 时，$h_t(r)=0, 0\leq t\leq 2^k-3$。

因此，当 $0\leq t\leq 2^k-3$，向量

$$(h_{0,t},h_{1,t+1},\cdots,h_{2^k-2-t,0},h_{2^k-1-t,1},\cdots,h_{2^k-3,t-1})$$

是一个 BCH 码的码字，它的长度为 2^k-2，设计距离为 $2^{k-1}-1$。此外，当它有元素在 Δ_m 中时，它的码字为零。由于 BCH 界，当它的码字为非零时，它的汉明重量不少于 $2^{k-1}-1$。但从引理 4.5 得知，它的汉明重量不超过 $2^{k-1}-2$。因为，这个码字不得不为零，即

$$(h_{0,t},h_{1,t+1},\cdots,h_{2^k-2-t,0},h_{2^k-1-t,1},\cdots,h_{2^k-3,t-1})=\mathbf{0},$$

这里 $0\leq t\leq 2^k-3$。因此，我们能得到 $h_{i,j}=0$ 当 $0\leq i,j\leq 2^k-1$。所以，$h=0$。

现在讨论 $f+1$ 的情况。假定 $h(x,y)=\sum_{i=0}^{2^k-1}\sum_{j=0}^{2^k-1}h_{i,j}x^i y^j\in\mathbb{B}_n$ 是 $f+1$ 的一个代数次数小于 $k-1$ 的零化子。相似的，

$$h_t(r)=0,\forall\gamma\in\mathbb{F}_{2^k}^*\setminus\Delta_m,$$

这里 $0\leq t\leq 2^k-3$。因此，向量

$$(h_{0,t},h_{1,t+1},\cdots,h_{2^k-2-t,0},h_{2^k-1-t,1},\cdots,h_{2^k-3,t-1})$$

是一个 BCH 码的码字，它的长度为 2^k-2，设计距离为 $2^{k-1}+2$。此外，当它有元素在 $\mathbb{F}_{2^k}^*\setminus\Delta_m$ 中时，它的码字为零。然而由 BCH 界的定义可知，当它的码字为非零时，它的汉明重量至少为 $2^{k-1}+2$。从引理 4.5，可以推断它的汉明重量最多 $2^{k-1}-2$，产生了一个矛盾。所以，$h=0$。

从以上的讨论可知，f 和 $f+1$ 的零化子的代数次数最小值不小于 $k-1$。所以，$AI(f)=k-1$。

4.2. 一类 1 阶弹性布尔函数的快速代数免疫度的下界

唐灯通过稍微修改构造 4.1，得到了一类具有极其优秀密码学性质的 1 阶弹性函数[43]。

构造 4.3 （[43]） 令 $n=2k\geq 10$，α 是 $\mathbb{F}_{2^k}$ 上的一个本原元，$\Delta_s=\{s,s+1,\cdots,s+2^{k-1}-1\}$ 和 $\overline{\Delta_s}=\mathbb{Z}_{2^k-1}\setminus\Delta_s$，这里 $0\leq s<2^{k-1}-1$。布尔函数 $f_s\in\mathbb{B}_n$ 定义如下；

$$f_s(x,y)=b_s(x,y)+u_s(x,y) \qquad (4\text{-}3)$$

这里 $b_s(x,y)\in\mathbb{B}_n$ 属于（4-1），并且 $supp(u_s)$ 包括以下三部分：

- $\{(\alpha^i,\alpha^{s+2^{k-1}-i-1})\mid i\in\{0,\cdots,s+2^{k-1}-1\}\}\cup\{(\alpha^i,\alpha^{s-i-1})\mid s>i\in\overline{\Delta_s}\}$；
- $\{(0,\alpha^i)\mid i\in\Delta_s\}$；
- $\{(\alpha^i,0)\mid i\in\Delta_s\}$。

换句话说，$supp(f_s)$ 包括以下四部分：

- $\{(\alpha^i,\alpha^{j-i})\mid i\in\mathbb{Z}_{2^k-1},j\in\Delta_s\setminus\{s+2^{k-1}-1\}\}$；
- $\{(\alpha^i,\alpha^{s+2^{k-1}-i-1})\mid s+2^{k-1}-1<i\in\overline{\Delta_s}\}\cup\{(\alpha^i,\alpha^{s-i-1})\mid s>i\in\overline{\Delta_s}\}$；
- $\{(0,\alpha^i)\mid i\in\Delta_s\}$；
- $\{(\alpha^i,0)\mid i\in\Delta_s\}$。

定理 4.2 （[43]） 令 $n=2k$，f_s 是构造 4.3 中的 n 元布尔函数。那么布尔函数 f_s 的代数免疫度是 k，即 $AI(f_s)=k$。

我们将会给出构造 4.3 的一个 FAI 的下界。与此同时，我们需要如下的两个引理。

引理 4.6 令 $n=2k\geq 10$，α 是 $\mathbb{F}_{2^k}$ 上的一个本原元，

$$T_s=\{(x,0)\mid x\in F_{2^k}\}\cup\{(0,y)\mid y\in\mathbb{F}_{2^k}\}\cup\{(z,\alpha^{s+2^{k-1}-1}z^{2^k-2})\mid z\in\mathbb{F}_{2^k}^*\}\cup\{(z,\alpha^{s-1}z^{2^k-2})\mid z\in\mathbb{F}_{2^k}^*\}$$

这里 $0\leq s<2^{k-1}-1$。当布尔函数 $g\in\mathbb{B}_n$ 有 $supp(g)\subseteq T_s$ 时，g 的代数次数大于等于 $k-1$，这里 $0\leq s<2^{k-1}-1$。

证明 首先，从定理 4.1 中可知，$b_m \in \mathbb{B}_n$ 有代数免疫度 $k-1$ 当 $0 < m < 2^k - 2$ 和 $b_m(x,y) = g_m(xy) \in \mathbb{F}_{2^n}$ 是（4-2）中定义的布尔函数。因此，b_m 的非零零化子的代数次数不小于 $k-1$。其次，很容易看出当 $m = s + 2^{k-1} - 2$ 时，g 是构造 4.2 中的 b_m 的一个非零零化子。因此，g 的代数次数大于等于 $k-1$。证明完毕。

引理 4.7 令 $n = 2k \geq 10$，α 是 $\mathbb{F}_{2^k}$ 上的一个本原元，

$$T_s = \{(0,y) \mid y \in \mathbb{F}_{2^k}\} \cup \{(x,0) \mid x \in \mathbb{F}_{2^k}\} \cup \{(\gamma, \alpha^{s+2^{k-1}-1}\gamma^{2^k-2}) \mid \gamma \in \mathbb{F}_{2^k}^*\} \cup \{(\gamma, \alpha^{s-1}\gamma^{2^k-2}) \mid \gamma \in \mathbb{F}_{2^k}^*\}$$

这里 $0 \leq s < 2^{k-1} - 1$ 和 $U' = \{z \in \mathbb{F}_{2^k}^* \mid tr_1^k(z) = 0\}$。对于每个 $0 \leq s < 2^{k-1} - 1$，如果我们选择一个任意元素 $(a,b) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \setminus T_s$，那么这将会有 $2(2^{k-2}(2^{k-2}-1))$ 个不同的对 (z',r') 使得 $g'(x,y) = tr_1^k(z'\alpha^{2^{k-1}-s}xy + r'\alpha^{2^k-s}xy)$ 等于 1 如果 $(x,y) = (a,b)$，这里 $z', r' \in U'$。

证明 很容易看出 $\alpha^{2^{k-1}-s}ab \neq 1$ 因为 $\alpha^{2^{k-1}-s}ab = 1$ 当且仅当 $ab = \alpha^{s+2^{k-1}-1}$ 和 $(a,b) \in \{(\gamma, \alpha^{s+2^{k-1}-1}\gamma^{2^k-2}) \mid \gamma \in \mathbb{F}_{2^k}^*\}$，这里与条件 $(a,b) \notin T_s$ 矛盾。显而易见，$\alpha^{2^{k-1}-s}ab \neq 0$ 因为 $(a,b) \notin \{(x,0) \mid x \in \mathbb{F}_{2^k}\} \cup \{(0,y) \mid y \in \mathbb{F}_{2^k}\}$。那么我们得到 $\alpha^{2^{k-1}-s}ab \in \mathbb{F}_{2^k} \setminus \{0,1\}$。换句话说，我们也有 $\alpha^{2^k-s}ab \in \mathbb{F}_{2^k} \setminus \{0,1\}$。因此，为了去证明这存在 $2(2^{k-2}(2^{k-2}-1))$ 不同的元素对 $(z',r') \in U'$ 使得 $g'(x,y) = tr_1^k(z'\alpha^{2^{k-1}-s}xy + r'\alpha^{2^k-s}xy)$ 等于 1，我们必须证明对于任意的 $\lambda, \mu \in \mathbb{F}_{2^k} \setminus \{0,1\}$，这有 $2(2^{k-2}(2^{k-2}-1))$ 不同的元素对 $(z',r') \in U'$ 使得 $tr_1^k(\lambda z' + \mu r') = 1$。由于

$$\begin{cases} \sum_{z \in U'} (-1)^{tr_1^k(\lambda z)} + \sum_{z \in \mathbb{F}_{2^k}^* \setminus U'} (-1)^{tr_1^k(\lambda z)} = -1 \\ \sum_{z \in U'} (-1)^{tr_1^k(\lambda z + z)} + \sum_{z \in \mathbb{F}_{2^k}^* \setminus U'} (-1)^{tr_1^k(\lambda z + z)} = -1 \end{cases}$$

注意 $tr_1^k(z) = 0$ 如果 $z \in U'$、$tr_1^k(z) = 1$、$z \in \mathbb{F}_{2^k}^* \setminus U'$。由以上两个等式可得 $\sum_{z \in U'} (-1)^{tr_1^k(\lambda z)} = -1$，即 $|\{z \in U' \mid tr_1^k(\lambda z) = 0\}| - |\{z \in U' \mid tr_1^k(\lambda z) = 1\}| = -1$。$U'$ 的基数是 $2^{k-1} - 1$。也就是说，$|\{z \in U' \mid tr_1^k(\lambda z) = 0\}| + |\{z \in U' \mid tr_1^k(\lambda z) = 1\}| = 2^{k-1} - 1$。因此 $|\{z \in U' \mid tr_1^k(\lambda z) = 1\}| = 2^{k-2}$，并且 $|\{z \in U' \mid tr_1^k(\lambda z) = 0\}| = 2^{k-2} - 1$。当 $tr_1^k(\lambda z' + \mu r') = 1$，有两种情况需要去考虑：

1) $tr_1^k(\lambda z')=1$， $tr_1^k(\mu r')=0$。

2) $tr_1^k(\lambda z')=0$， $tr_1^k(\mu r')=1$。

所以这有$2(2^{k-2}(2^{k-2}-1))$个不同的元素对$(z',r')\in U'$使得$tr_1^k(\lambda z'+\mu r')=1$。证明完毕。

定理 4.3 令$n=2k>10$，$0\le s<2^{k-1}-1$，构造 4.3 中的布尔函数f_s的FAI至少为$n-6$。

证明 为了证明当$0\le s<2^{k-1}-1$时，布尔函数的FAI至少为$n-6$。我们应该证明当$g\in\mathbb{B}_n$和$1\le \deg(g)<k$， $\deg(g)+\deg(f_sg)\ge n-6$。我们将使用反证法证明这个结论。假设$\deg(g)+\deg(f_sg)\le n-7$当这有一个布尔函数$g$，并且$1\le\deg(g)<k$。之后，通过（4-3）我们知道

$$f_sg=(b_s+u_s)g \qquad (4\text{-}4)$$

这里$b_s(x,y)\in\mathbb{B}_n$属于（4-1），并且$u_s(x,y)$的支撑集为

$\{(\alpha^i,\alpha^{s+2^{k-1}-i-1})\mid i\in\{0,\cdots,s+2^{k-1}-1\}\}\cup\{(\alpha^i,\alpha^{s-i-1})\mid s>i\in\overline{\Delta_s}\}\cup\{(0,\alpha^i)\mid i\in\Delta_s\}\cup\{(\alpha^i,0)\mid i\in\Delta_s\}$。这有两种情况需要考虑。

情形 1：$supp(g)\subseteq T_s$，这里

$T_s=\{(0,y):y\in\mathbb{F}_{2^k}\}\cup\{(x,0)\mid x\in\mathbb{F}_{2^k}\}\cup\{(z,\alpha^{s+2^{k-1}-1}z^{2^k-2})\mid z\in\mathbb{F}_{2^k}^*\}\cup\{(\gamma,\alpha^{s-1}\gamma^{2^k-2})\mid\gamma\in F_{2^k}^*\}$。通过引理 4.6，我们知道$\deg(g)\ge k-1$。因为$f_sg$是$f_s+1$的一个非零零化子，并且从定理 4.2 可知$f_s+1$的非零零化子的代数次数不小于$k$，所以$\deg(f_sg)\ge k$。在此情况下，我们有$FAI(f_s)\ge n-1$与我们的假设$FAI(f_s)\le n-7$矛盾。

情形 2：$supp(g)\not\subseteq T_s$。那么这必须存在一个元素$(a,b)\in supp(g)$使得$(a,b)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}\setminus T_s$。从引理 4.7 可知，这有存在元素$(z',r')\in U'$使得$g'(x,y)=tr_1^k(z'\alpha^{2^{k-1}-s}xy+r'\alpha^{2^k-s}xy)$等于 1 当$(x,y)=(a,b)$和$U'=\{z\in\mathbb{F}_{2^k}^*\mid tr_1^k(z)=0\}$。我们知道$gg'$是非零的，并且$\deg(gg')\le\deg(g)+2$。在（4-4）的两边分别乘上$g'$得到

$$f_sgg'=(b_s+u_s)gg'=(b_s+u_s)g'g=b_sgg'。$$

因为g'是u_s的一个非零零化子，所以我们得到

$$\deg(gg')+\deg(f_sgg')=\deg(gg')+\deg(b_sgg')\le FAI(f_s)+4\le n-3。$$

从以上证明我们得知这有一个非零函数gg'使得$\deg(gg')+\deg(b_sgg')\le n-3$，这里

$\deg(gg') < k+2$。当$\deg(ff') < k$，它是与命题 4.1 的第四条矛盾的。当$k \le \deg(gg') < k+2$，它与$\deg(gg') + \deg(b_s gg') \ge n$矛盾。

因此，它是不可能的去假设$FAI(f_s) \le n-7$，故我们有$FAI(f_s) \ge n-6$。证明完毕。

4.3. 本章小结

在本章中，我们证明了一类 1 阶弹性布尔函数的FAI大于等于$n-6$。为了证明本节的一个布尔函数的AI，我们证明了一些来源于Tu-Deng猜想的组合事实。利用该方法，我们同时也能证明一些其他的 1 阶弹性布尔函数有相同的FAI下界。但是，所得到的下界与实际值还存在一定的差距。如果能够找到一个更低代数次数的布尔函数$g'(x,y)$，那么我们将能提升FAI的下界，这也是我们后续研究的方向。

此部分研究工作已整理成文章 A Lower Bound of Fast Algebraic Immunity of A Class of 1-Resilient Boolean Functions，并于 2019 年 12 月在 IEEE ACCESS 期刊发表。

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在维护密码系统的安全性方面起着关键作用。为了有效抵御各种已知密码攻击，在密码系统中使用的布尔函数应同时满足以下性质：平衡性，良好的(快速)代数免疫度，高非线性度，高代数次数等。

本文完成的研究工作及取得的创新性研究成果主要包括：

（1）在计算机辅助验证的基础上，我们研究了Carlet-Feng函数，Tu-Deng函数，Tang-Carlet-Tang函数的仿射等价关系。基于有限域表示的这三类函数，它们的支撑集中都含有共同的参数s（$0 \le s \le 2^n - 2$）,使得能达到大量性质优良的布尔函数。经研究发现，当参数s取不同值时，这些布尔函数是具有仿射等价的关系。

（2）在之前的研究中，主要是通过计算机辅助来计算布尔函数的FAI。在唐灯的方法的启发下，利用数学证明的方法得到了一类一阶弹性函数的FAI大于等于n-6。于此同时，我们也证明了一些起源于Tu-Deng猜想的组合事实。

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） **提升快速代数免疫度的下界**。目前，所证明的FAI的下界与实际值仍有较大差距，计算机辅助计算仍是评价布尔函数抵抗FAA能力的主要方式。我们需要提升下界，以更加严谨和可信的方法来证明一个布尔函数抵抗FAA的能力。此外，当前的研究主要针对一个特定的布尔函数，能否将该证明方法推广到其他布尔函数，仍是一个待证明的问题。

（2） **证明布尔函数快速代数免疫度的精确值。**当我们将布尔函数的FAI的下界提升到足够高时，或者利用已经证明的上界，是否能够证明某些布尔函数FAI的精

确值。毕竟，数学证明是更加严谨和可信的。我们可以尝试选取一些特殊的布尔函数，比如旋转对称布尔函数，做一些尝试性的工作。

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] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

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

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

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

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

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] C. Carlet, K. Feng, An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, Good Immunity to Fast Algebraic Attacks and Good Nonlinearity[C], International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology. Springer-Verlag, 2008:425-440.

[38] Q. Wang, J. Peng, H.Kan, Constructions of Cryptographically Significant Boolean Functions Using Primitive Polynomials[J]. IEEE Transactions on Information Theory, 2010, 56(6):3048-3053.

[39] H. Chen, T. Tian, W. Qi, On the affine equivalence relation between two classes of Boolean functions with optimal algebraic immunity[J]. Designs Codes Cryptography, 2013, 67(2):175-185.

[40] Q. Wang, T. Johansson, On Equivalence Classes of Boolean Functions[M] Information Security and Cryptology - ICISC 2010. Springer Berlin Heidelberg, 2010:311-324.

[41] Rønjom, S., Cid, C.: Nonlinear Equivalence of Stream Ciphers. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 40–54. Springer, Heidelberg (2010), http://www.isg.rhul.ac.uk/~ccid/publications/NL-equivalence.pdf

[42] Q. Jin, Z. Liu, B. Wu, "1-resilient Boolean function with optimal algebraic immunity," Cryptology ePrint Archive, Report 2011/549, http://eprint.iacr.org/.

[43] D. Tang, C. Carlet, X. Tang, "A class of 1-resilient Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks," International Journal of Foundations of Computer Science, vol. 25, no. 6, pp. 763-780, 2014.

[44] 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.

[45] 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.

致谢辞

感谢我的硕士导师陈银冬老师，在他的帮助下，我才能一步步的走进并深入到神奇的密码学世界中，引领并帮助我从事密码学布尔函数的研究工作。陈老师治学严谨，为人又很谦和，从他的身上我学到了很多做人和做事的道理。在此感谢陈老师对我的悉心培养。

感谢科研团队学科负责人蔡伟鸿老师，是他像一个家长一样悉心的照顾我们的生活，是他培养我们良好的科研习惯和素养，并为我们提供了整洁舒适的科研环境。

感谢实验室熊智老师、蔡玲如老师和其他同学给予我的帮助。

感谢我的父母，无条件支持我的决定。他们为我提供了好的家庭氛围，感谢他们对学习的重视，让我无后顾之忧一心追求学术。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。

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，**Zhang Liu**，Tang Deng and Cai Weihong. Translation equivalence of Boolean functions expressed by primitive element. IEICE Transactions on Fundamentals of Electronics Communications and Computer Science, 2019, E102-A(04):672–675.
2. Chen Yindong, **Zhang Liu**, Guo Fei, et al. Fast algebraic immunity of 2m+2 & 2m+3 variables majority function. IEEE ACCESS, 2019,7: 80733-80736.
3. Chen Yindong, **Zhang Liu**, Xu jianlong, et al. A Lower Bound of Fast Algebraic Immunity of A Class of 1-Resilient Boolean Functions. IEEE ACCESS, 2019,7: 90145-90151.
4. Chen Yindong, **Zhang Liu**, Gong zhangquan, et al. Constructing Two Classes of Boolean Functions with Good Cryptographic Properties. IEEE ACCESS.2019,7: 149657-149665.