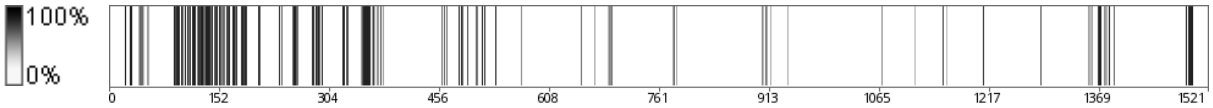
PaperPass旗舰版检测报告
简明打印版

比对结果(相似度):

总　体：34% (总体相似度是指本地库、互联网的综合对比结果)
本地库：34% (本地库相似度是指论文与学术期刊、学位论文、会议论文、图书数据库的对比结果)
期刊库：17% (期刊库相似度是指论文与学术期刊库的比对结果)
学位库：33% (学位库相似度是指论文与学位论文库的比对结果)
会议库： 6% (会议库相似度是指论文与会议论文库的比对结果)
图书库： 7% (图书库相似度是指论文与图书库的比对结果)
互联网： 5% (互联网相似度是指论文与互联网资源的比对结果)

报告编号：5EC0FA53EAFD40JAV
检测版本：旗舰版
论文题目：布尔函数的(快速)代数免疫性相关研究
论文作者：张柳
论文字数：25707字符(不计空格)
段落个数：449
句子个数：1521 句
提交时间：2020-5-17 16:48:19
比对范围：学术期刊、学位论文、会议论文、书籍数据 、互联网资源
查询真伪：http://www.paperpass.com/check

句子相似度分布图:



本地库相似资源列表(学术期刊、学位论文、会议论文、书籍数据):

1.相似度：29% 篇名：《两类优良代数免疫性质布尔函数的构造与分析》
来源：学位论文 汕头大学 2019
2.相似度： 7% 篇名：《流密码设计中布尔函数的构造与分析》
来源：学位论文 西南交通大学 2015
3.相似度： 5% 篇名：《布尔函数的(快速)代数免疫性质研究进展》
来源：学术期刊 《密码学报》 2017年3期
4.相似度： 3% 篇名：《抗代数攻击布尔函数的构造与分析》
来源：学位论文 解放军信息工程大学 2013
5.相似度： 3% 篇名：《几类具有良好密码学性质的布尔函数的构造》
来源：学位论文 西南交通大学 2015
6.相似度： 3% 篇名：《旋转对称布尔函数的快速代数免疫度研究》
来源：学位论文 复旦大学 2013
7.相似度： 2% 篇名：《代数免疫最优的偶数元旋转对称布尔函数构造研究》
来源：学位论文 汕头大学 2015
8.相似度： 2% 篇名：《具有优良密码学性质的布尔函数的构造及其在CDMA系统中的应用》
来源：学位论文 西安电子科技大学 2018
9.相似度： 2% 篇名：《代数免疫最优的旋转对称布尔函数若干构造》
来源：学位论文 汕头大学 2016

10.相似度： 2% 篇名：《旋转对称布尔函数研究综述》
来源：学术期刊 《密码学报》 2017年3期
11.相似度： 2% 篇名：《一类布尔函数的代数免疫度的下界》
来源：学术期刊 《通信学报》 2016年10期
12.相似度： 1% 篇名：《级联函数的扩展代数免疫性》
来源：学术期刊 《密码学报》 2015年3期
13.相似度： 1% 篇名：《几类热点布尔函数的性质分析》
来源：学位论文 解放军信息工程大学 2013
14.相似度： 1% 篇名：《具有良好密码学性质的布尔函数的级联构造》
来源：学术期刊 《密码学报》 2014年1期
15.相似度： 1% 篇名：《布尔函数和向量值函数的代数免疫度》
来源：学位论文 国防科学技术大学 2008
16.相似度： 1% 篇名：《周期序列谱免疫度的性质研究》
来源：学位论文 解放军信息工程大学 2015
17.相似度： 1% 篇名：《代数免疫度最优布尔函数的构造》
来源：学位论文 国防科学技术大学 2011
18.相似度： 1% 篇名：《布尔函数的代数免疫性分析》
来源：学位论文 淮北师范大学 2011
19.相似度： 1% 篇名：《满足多种指标的密码函数的设计》
来源：学位论文 西安电子科技大学 2016
20.相似度： 1% 篇名：《递归构造多个具有最优代数免疫度的平衡布尔函数》
来源：学术期刊 《系统科学与数学》 2012年7期
21.相似度： 1% 篇名：《具有几乎完美代数免疫的偶数元弹性函数构造》
来源：学术期刊 《计算机工程》 2014年12期
22.相似度： 1% 篇名：《弹性布尔函数的构造》
来源：学位论文 国防科学技术大学 2011
23.相似度： 1% 篇名：《布尔函数的代数免疫度和扩展代数免疫度》
来源：学位论文 国防科学技术大学 2010
24.相似度： 1% 篇名：《多输出布尔函数代数免疫度的若干性质》
来源：学术期刊 《信息工程大学学报》 2013年4期
25.相似度： 1% 篇名：《高维守恒律方程基本波的相互作用与演化》
来源：学位论文 汕头大学 2008
26.相似度： 1% 篇名：《基于FPGA的流密码机设计》
来源：学位论文 西安电子科技大学 2010
27.相似度： 1% 篇名：《基于全局优化搜索的良好密码特性布尔函数构造策略》
来源：学位论文 复旦大学 2012
28.相似度： 1% 篇名：《一类级联布尔函数的密码学性质》
来源：学术期刊 《淮北师范大学学报（自然科学版）》 2018年1期
29.相似度： 1% 篇名：《旋转对称布尔函数的密码学性质的研究》
来源：学位论文 解放军信息工程大学 2012
30.相似度： 1% 篇名：《流密码算法的研究与设计》
来源：学位论文 南京航空航天大学 2011
31.相似度： 1% 篇名：《最优代数免疫度弹性布尔函数的构造》
来源：学位论文 湖北大学 2009
32.相似度： 1% 篇名：《密码函数安全性指标的研究进展》
来源：学术期刊 《密码学报》 2014年6期
33.相似度： 1% 篇名：《信息安全中删位纠错码与MAI函数的构造》
来源：学位论文 四川师范大学 2015
34.相似度： 1% 篇名：《布尔函数的代数免疫度与非线性度》
来源：学位论文 华南师范大学 2010
35.相似度： 1% 篇名：《多输出布尔函数与布尔函数代数免疫阶之间的关系》
来源：学术期刊 《电子学报》 2011年1期
36.相似度： 1% 篇名：《密码学中布尔函数及多输出布尔函数的构造》
来源：学位论文 西安电子科技大学 2012
37.相似度： 1% 篇名：《具有K阶代数免疫的布尔函数》
来源：学术期刊 《计算机技术与发展》 2011年3期
38.相似度： 1% 篇名：《具有较低透明阶值S盒的分析与构造》

来源：学位论文 西安电子科技大学 2017
39.相似度： 1% 篇名：《代数免疫度最优的旋转对称布尔函数的构造》
来源：学位论文 汕头大学 2014
40.相似度： 1% 篇名：《一类平衡的最优代数免疫度布尔函数的构造》
来源：学术期刊 《计算机应用与软件》 2018年1期
41.相似度： 1% 篇名：《几类流密码分析技术研究》
来源：学位论文 西安电子科技大学 2011
42.相似度： 1% 篇名：《基于字的流密码算法Dragon的研究》
来源：学位论文 西安电子科技大学 2008
43.相似度： 1% 篇名：《几类对称布尔函数的非线性度、代数次数和代数免疫阶》
来源：学术期刊 《计算机学报》 2014年11期
44.相似度： 1% 篇名：《特殊性质的布尔函数构造与序列设计》
来源：学位论文 西安电子科技大学 2012
45.相似度： 1% 篇名：《最优代数免疫布尔函数构造方法的研究》
来源：会议论文 2008-10-11
46.相似度： 1% 篇名：《流密码的新分析方法研究》
来源：学位论文 桂林电子科技大学 2015
47.相似度： 1% 篇名：《对称布尔函数和Bent函数若干关键问题的研究》
来源：学位论文 西南交通大学 2013
48.相似度： 1% 篇名：《互补对称布尔函数的非线性度》
来源：会议论文 2011-10-15
49.相似度： 1% 篇名：《构造最优代数免疫度的布尔函数》
来源：学位论文 大连理工大学 2014
50.相似度： 1% 篇名：《一类具有最高代数免疫阶的非对称布尔函数构造及分析》
来源：学术期刊 《计算机安全》 2008年10期

互联网相似资源列表：
1.相似度： 3% 标题：《两类基于布尔函数的线性码及其应用》
https://www.doc88.com/p-5774427080225.html

全文简明报告:

硕 士 学 位 论 文

题 目

{83%：布尔函数的(快速)代数免疫性相关研究}

英文题目

Research on the (fast) algebraic immunity of Boolean functions

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.　05.　31

学位论文原创性声明

{100%：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。}　{100%：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。}　{100%：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

{100%：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；}{98%：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；}　{100%：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，　{49%：使用布尔函数是实现这些非线性函数的一种有效途径。}{69%：为了抵抗已知的密码攻击手段，非线性布尔函数必须兼具可证明的能够抵抗已知密码攻击的性能。}　{79%：在2003年之前，为了抵抗各种已知的密码攻击，流密码系统中所使用的布尔函数必须同时满足一下几个性质：}　{68%：平衡性，高非线性度，高代数次数，适当的弹性阶以及良好的自相关性质。}　{74%：2003年，Courtois和Meier提出将代数攻击应用于基于线性反馈移位寄存器的流密码算法，同年，Courtois提出快速代数攻击方法。}　{67%：为了抵抗代数和快速代数攻击，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。}　{54%：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：}

{42%：在使用计算机进行辅助验证的基础上，研究了C-F函数，Tu-Deng函数，T-C-T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（ ），从而能得到大量性质优良的布尔函数。 经研究发现，当参数 {51%：取不同值时，这些布尔函数是具有仿射等价的关系。}

{49%：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。} {42%：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

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 the known cryptographic attack, the nonlinear Boolean function used in the stream cipher algorithm based on the linear feedback shift register must have the provable performance to resist the known cryptographic attack. Before 2003, in order to avoid the probability attack based on statistical analysis, the Boolean function should meet the balance; In order to resist the best affine approximation and fast correlation attack, Boolean functions should have high nonlinearity; In order to resist the attack of Berlekamp-Massey algorithm and the attack of Rønjom-Helleseth, Boolean functions should have high algebraic degree; In order to reduce the statistical correlation between the output bits and the input variables of the Boolean function and provide the spreading characteristics for the cryptosystem, the Boolean function should have good autocorrelation property; In order to resist the conquest attack and correlation attack respectively, the Boolean function applied to the combination mode should also satisfy the high-order resilient.In 2003, Courtois and Meier applied algebraic attack to stream cipher algorithm based on linear feedback shift register at European cipher annual conference. In the same year, Courtois proposed a fast algebraic attack method at international cipher annual conference. In order to resist algebraic and fast algebraic attacks, Boolean functions should have high algebraic immunity and good fast algebraic immunity, respectively.In this paper, affine equivalence relations and fast algebraic immunity of Boolean functions based on finite field representation are studied.

On the basis of computer-aided verification, we study the affine equivalence of C-F function, Tu-Deng function and T-C-T

function. These three kinds of functions based on the finite field representation have the same parameter 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 is different.

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

绪 论

{62%：当今世界已经进入信息化时代，信息安全越来越受到人们的重视。} {100%：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。} {77%：作为信息安全的基石和核心的密码学，在构建安全可靠的信息系统中起到重要作用。}

{85%：布尔函数是许多密码系统的核心组成部分，其密码学性质直接决定密码系统的安全性。} {100%：本章首先介绍布尔函数的研究背景及意义；} {100%：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；} {62%：接着讲述国内外布尔函数(快速)代数免疫度的研究现状；} {85%：最后对本文行文结构和主要工作做了介绍。}

研究背景及意义

{98%：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、传输和破译，} {71%：主要应用于军事方面，只被少数人掌握和控制。} {68%：所以，这一阶段密码学不像是一门学科，反而更像是一门技巧性很强的艺术，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，{100%：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。} {100%：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，} {100%：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，开辟了公钥密码学的研究分支。 {88%：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)，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， {59%：该密码的安全性是基于大整数因式分解的困难性，极大促进了公钥密码的发展。} {93%：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方法，} {87%：使得密码编码学和分析学相互促进，从而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， {97%：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。} {90%：最后，由Daemen

和Rijmen设计的Rijndael算法[6]，在安全性、性能和实现特性等方面获得绝对优势，被选定为AES算法。} {92%：继美国AES计划之后，欧洲相继启动了NESSIE计划[7]和ECRYPT计划[8]，在世界范围内征集密码算法标准。} {100%：近几年，我国也在制定和更新各类密码标准。} {100%：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。}

{97%：根据密钥的特点，Simmons[9]将密码体制分为两大类——对称密码：} 加密密钥和解密密钥相同； 非对称密码： {63%：加解密密钥不同，一个公开发布，另一个用户自己秘密保存。} {83%：对称密码的最大优势是加解密速度快，适于保障大数据量的安全传输，但密钥管理困难。} {100%：非对称密码机制较为灵活，但加解密速度相对较慢。} {77%：按照对明文加密方式的不同，对称密码可分为分组密码和流密码。} {69%：分组密码是将明文分成相同大小的数据块，在每个时钟周期用相同的密钥加密每一个数据块。} {90%：流密码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，在每一个时钟周期分别用一比特密钥加密一比特明文，} 所以要求密钥和明文等长。 {100%：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。} {71%：事实上，对于流密码的研究主要归结为布尔函数的研究。}

{64%：我国在流密码研究方面做出了凸出贡献，由中国科学院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]，} {100%：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，} {100%：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。}

{100%：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。} {100%：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)。} {100%：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；} {100%：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。} {88%：同时，为了抵抗各种已知的密码攻击，密码系统中使用的布尔函数必须同时满足多项密码学性质，} {65%：尤其是近年来提出的代数攻击[22]和快速代数攻击[24]，} 对布尔函数提出了更高的要求。 {100%：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：} {100%：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。}

流密码与布尔函数

{75%：流密码系统中，通常使用布尔函数作为密钥流生成器的非线性部分，与反馈移位寄存器搭配生成具有良好安全性的密钥流。} {81%：此外，布尔函数必须满足多种性质以抵抗已知攻击。}

布尔函数在流密码中的应用

{86%：流密码又称序列密码，加密和解密思想非常简单：} {84%：使用密钥序列与明文序列进行“ 异或 ”生成密文，使用相同的密钥序列与密文“ 异或 ”来恢复明文。} 流密码的模型如图1-1所示。 {88%：当用于加密的序列是由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 ”密码系统。} {84%：Shannon已经证明“ 一次一密 ”密码体制在理论上是不可破解的，也就是说密钥序列是一个随机序列。} {71%：然而随机序列的产生、存储和传送在现实中是非常困难的，因此不适合流密码的加密和解密。} {79%：在实际应用中，使用伪随机序列作为加解和解密序列则更为常见。} {55%：伪随机序列是根据一定的算法生成带有一个短的消息密钥的非常长的序列。} {69%：伪随机序列具有

预先确定和重复实现的性质，也具有随即序列的性质，称为序列的伪随机性。} {89%：序列密码系统的安全性取决于密钥流伪随机性。} {64%：因此，如何设计一个能产生长周期和良好伪随机序列的密钥流生成器成为流密码研究的关键问题。}

图1-1 流密码模型

{80%：在流密码的研究中，人们通常把它分为驱动部分和非线性组合部分。} {88%：驱动部分控制存储器进行状态转移，负责提供多个组合部分使用的周期大、统计特性好的序列；} {79%：非线性组合部分则将驱动部分提供的序列组合起来，生成满足要求且具有良好密码性能的密钥流序列。} {69%：反馈移位寄存器是当前流密码设计的主流，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。} {93%：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)。 {79%：LFSR具有实现简单、速度快、便于分析和计算等优点，广泛应用于各种数字电路中，是密钥算法中关键的密钥流构成部件。}

{89%：图1-2 n级反馈移位寄存器模型}

{89%：从加密角度来说，由LSFR产生的伪随机序列密码学性质极弱，不能作为加密密钥使用。} {79%：在现代密码学中，最常见的方法是使用满足一定密码学性质的非线性布尔函数对大周期的LFSR进行滤波，} {98%：或者将多个具有大周期的LFSR进行组合，即滤波模式(图1-3)和组合模式(图1-4)，} {68%：通过这种方式，不仅可以利用LFSR的周期性来生成较长周期的伪随机序列，} {85%：也可以实现将非线性性质引入到生成的序列中来实现Shannon所提出的混淆和扩散原则，} {84%：确保产生密钥流序列的安全强度。} {97%：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

流密码的(快速)代数攻击

{62%：代数攻击是在已知明文和对应密文的情况下进行的攻击。} {84%：其基本思想起源于Shannon，他认为密码算法可以表示为一个大型的多变元方程组，通过求解这个方程组可以得到密钥。} {97%：根据Kerckhoff原则，密码算法的所有细节完全公开，因此，密码分析学者可以通过明文-密文对应关系以及密码算法的结构，} 建立以密钥为未知变量的方程组。 {77%：事实上，密码研究者正是基于方程组求解的复杂度来保证密码系统的安全。} {80%：代数攻击正是抓住这一关键点，从方程建立的初始阶段寻找突破口——建立一个尽可能次数低的方程组，以降低方程组求解的复杂度。} {98%：在2003年欧密会上，Courtois和Meier[22]成功地将代数攻击用于流密码的分析破译，} {79%：引起国内外密码学者的广泛关注，使用标准代数攻击，成功攻破了一些著名的密码系统，如} {98%：日本政府Cryptrec计划中提出的Toyocrypt流密码算法和欧洲NESSIE工程的候选流密码算法LILI-128等} 。

{100%：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 是LFSR的初始状态(通常与密钥直接相关)， 时刻状态为 ，输出密钥流比特用 表示，密码系统中过滤函数是 元布尔函数 。 在已知密钥流比特 的情况下，从而得到如下方程组

(1-1)

{70%：对于非线性滤波函数生成器，可以给出一个类似的方程。} 理论上，如果知道足够多的 {90%：，就能建立足够多的方程进而求出密钥。} {74%：然而，若非线性滤波函数的代数次数较高，则很难求解这个方程组。} {76%：实际上，代数攻击和快速代数攻击都试图降低上述方程组的求解复杂度。}

{97%：Courtois和Meier[22]提出并证明了布尔函数的低次倍式存在定理：} 对于任意元布尔函数f，存在次数不超过 的非零布尔函数 ，使得 的次数不超过 。 基于该定理，对于高次函数 ，考虑其较低次数的倍式 ，其中 且 的代数次数不超过 。用 乘以 的两边得

，

若 ，则 ； 若 ，则 。 因此，方程组(1-1)能转化为以初始状态 为未知数关于 或 {83%：的低次方程组，很大程度降低了求解复杂度。} {98%：2004年，Meier等[23]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。 {70%：此后，国内外密码学者提出了许多构造具有优良代数免疫度的布尔函数的方法[11-15, 31, 32, 44, 45]。}

{87%：2003年，在美密会上Courtois[24]改进标准代数攻击并提出了快速代数攻击：} 考虑 的倍式 ，其中 且 的代数次数远小于 ， 的代数次数小于 的代数次数。在获取了一些连续的密钥流比特 之后，通过找到关于 的一个线性组合 ，来得到关于 的一个线性组合 。 {72%：显然，快速代数攻击的实施不需要大量的线性无关零化子来建立方程，只需要一个特殊的关于} {91%：的一倍式关系，但是需要更多的明文-密文来获得连续的密钥比特流。} {91%：因此，快速代数攻击对布尔函数提出了更高的要求。} {100%：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。} {93%：为了衡量布尔函数抵抗快速代数攻击的能力，文献[28]引进了快速代数免疫度(Fast Algebraic Immunity，FAI)的概念。} {70%：目前，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被证明是具有高的快速代数免疫度，} {68%：用计算机程序对较小变元的函数进行测试是更为常见的做法，以证明该类函数抵抗快速代数攻击的能力。} {96%：标准代数攻击和快速代数攻击的复杂度比较见表1-1。}

{100%：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

快速代数攻击

注: 表中 ， ， 是线性反馈移位寄存器的级数， 是 的代数免疫度， 是 的代数次数。

安全的布尔函数设计准则

{88%：布尔函数作为序列密码、分组密码和Hash函数的重要组成部分，其密码学性质的好坏直接关系到密码系统的安全性。} {83%：布尔函数的安全性指标是衡量布尔函数密码学

性质的重要参数，这些安全指标的提出和密码分析方法密切相关。} {87%：布尔函数的安全性指标主要包括：} {62%：平衡性、代数次数、非线性度、相关免疫阶、弹性阶、代数免疫度和快速代数免疫度[19]。}

平衡性

{77%：布尔函数可以作为反馈移位寄存器序列中反馈函数、滤波序列中的滤波函数和非线性组合序列中的非线性组合函数的基本组件。} {93%：序列密码产生的密钥流是否具有高的安全强度，取决于它们是否具有良好的伪随机特性。} {74%：高平衡性是保证序列伪随机特性的一个重要特性。} {67%：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。} {91%：例如，周期为偶数的二元序列是平衡的，是指其中0和1的出现个数相同。} 当一个 {70%：元布尔函数的真值表中0和1的个数相同时，它是平衡的，也就是该布尔函数的Hamming重量为} 。

代数次数

{95%：密码系统中所使用的布尔函数应当具有高的代数次数，其同样为布尔函数的基本设计准则之一。} {79%：事实上，如果密码系统中所使用的布尔函数代数次数过低，则可能遭受Berkekamp-Massey算法攻击和Ronjom-Helleseth攻击。}

非线性度

{73%：为抵抗线性密码攻击，密码系统中所使用的布尔函数应该与所有仿射函数具有较大的汉明距离。} 布尔函数 的非线性度 定义为 和所有仿射函数的最小 距离，即 。

也可表示为

。

由 恒等式可知对任意 元布尔函数 ，有

。

达到这个上界的布尔函数称为 函数， 函数的 谱值只能为 或 。 {75%：由于布尔函数的非线性度是一个整数，所以当} 是偶数时， 函数才可能存在。

代数免疫度

代数免疫度(Algebraic Immunity，AI)[21， 23]的提出与代数次数有关， {100%：代数攻击的基本思想是将密码体制的破译问题归结到代数方程组的求解。} {100%：人们在破译LILI-128和Toyocrypt等序列密码时，发现如果密码体制使用的布尔函数} 或者 {100%：具有低次的零化子，那么密码体制可能遭到代数攻击。} 可以证明， {100%：元布尔函数的代数免疫度不超过} {74%：，若达到了此上界，则称该布尔函数是代数免疫度最优的函数。}

快速代数免疫度

{79%：快速代数免疫度(Fast Algebraic Immunity，FAI)[28]是评价布尔函数抵抗快速代数攻击能力的指标，定义为} 与 的较小值，其中 表示 的代数免疫度， 表示 的代数次数。 {80%：密码系统中布尔函数应具备较高的快速代数免疫度。} 若 元布尔函数的FAI达到 (或 {100%：)，则称该函数具有最优(或几乎最优)快速代数免疫度。

}

国内外研究现状

{71%：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·f的代数次数不大于n2，} 那么对f实施快速代数攻击就是比较有效的[24-26]。 {91%：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[27, 28]。} 2012年，刘美成等[29]提出了完美代数免疫(Perfect Algebraic Immune, PAI)的概念，f是n元布尔函数， {52%：e是任意正整数且e<n2，若对于任意次数不小于e的函数g都有g·f的代数次数不小于n-e，} 则称f是完美代数免疫函数。 {75%：并且他们[29]证明了n元布尔函数具有完美代数免疫度当且仅当n=2s或n=2s+1；} {92%：并且仅当变元数量是2s+1，存在平衡完美代数免疫函数，仅当变元数量是2s，存在不平衡完美代数免疫函数。} {92%：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[29]。} {95%：2012年，王启春等[30]给出了快速代数免疫度关于高阶非线性度的一个上界。} {82%：C-F函数[12]和T-C-T函数[32]是目前比较有代表性的两类布尔函数，} {100%：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。} {80%：2012年，刘美成等[29]证明了变元数量为2s+1的C-F函数是完美代数免疫函数；} {93%：2014年，他们[33]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。} {97%：2017年，唐灯等[34]构造了一大类代数免疫最优1阶弹性函数，这类函数兼有最优代数次数和很高的非线性度下界等良好性质，} {88%：且能从理论上证明其快速代数免疫度不小于n-6。} {100%：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。} {100%：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。}

本文内容及结构

{50%：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进行研究，论文的研究内容和组织结构如下：}

{83%：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。}

{44%：第三章研究了C-F函数，Tu-Deng函数，T-C-T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 （ {56%：），使得能达到大量性质优良的布尔函数。} 经研究发现，当参数 {51%：取不同值时，这些布尔函数是具有仿射等价的关系。}

{46%：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快速代数免疫度大于等于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。

{78%：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。}

预备知识

{61%：本章首先介绍布尔函数及其表示的基本概念；} {52%：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。}

布尔函数的基本概念

设 是二元有限域， 为正整数， 是 上的 维向量空间，从 到 的映射 称为 元布尔函数。 记全体 元布尔函数的集合为 ，则 中元素个数为 ，也就是说，共有 个不同的布尔函数。

任意一个 变元布尔函数 都可以用一个长为 的真值表

唯一表示。 的支撑集 定义为： 满足 且 的全体元素的集合。 集合 中所含元素的个数称为 的Hamming重量，记为 。 如果一个 元布尔函数 满足 ，则称该函数是平衡的，即

，

这里 表示集合 中所含元素的个数。

设 ， 和 的Hamming距离定义为

。

由定义可知， 和 的Hamming距离实际上为差函数 的Hamming重量，即

。

一个 元布尔函数 可以用一个 上的含 个变元的多项式表示：

（2-1）

这里， ，+表示 中的加法运算，即模2加运算。 形如式（2-1）的表示称为布尔函数 的小项表示。 在进行合并同类项后可得到多项式：

， (2-2)

这里系数 。

布尔函数 形如式（2-2）的表示形式存在且唯一，该表示形式为 的代数正规型（Algebraic Normal Form，ANF）。 若记集合 ，用 表示 的幂集，即 的所有子集构成的集合，则 的代数正规型还可以表示为

， （2-3）

这里 。

非零布尔函数 {68%：的ANF中系数非零项所含有变元的个数的最大值称为它的代数次数，记为} ，即

，

{67%：规定零函数的代数次数为0. 仿射函数的代数次数不超过1，全体} 元仿射函数的集合记为 ，即

。

{66%：线性函数定义为常数项等于0的仿射函数，} 表示全体 元线性函数的集合，即

。

由于 当且仅当对任意 ，都有 ，于是对任意给定的 ，令 ，则布尔函数 在元素 处的值可以表示为

。 （2-4）

布尔函数的密码学性质

{69%：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，} {100%：高非线性度，高代数次数，较好的(快速)代数免疫度等。}

平衡性

{84%：密钥流生成器产生的密钥流是否为伪随机流，决定流密码系统的安全性。} {90%：平衡性是衡量伪随机性的一个重要属性。} {76%：如果密码系统中使用的布尔函数输出序列中0和1数量不等，那么根据统计分析，密码系统就无法抵抗概率攻击。} {66%：因此，平衡性是布尔函数基本设计要求之一。} 布尔函数平衡性可由Walsh变换来描述。

引理2.1 若布尔函数 是平衡的，则 。

代数次数

{76%：为了抵抗Berlekamp-Massey算法攻击[16， 17]和Rønjom-Helleseth攻击[18]，应用中的布尔函数应具有较高的代数次数。} 对于 元平衡布尔函数 ，其中 ，即 的汉明重量是偶数，由(2-2)式计算 的系数为

因此有如下引理：

引理2.2 若布尔函数 的汉明重量是偶数，则 。

非线性度

{69%：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[19]和快速相关攻击[20]，布尔函数与所有仿射函数具有较大的汉明距离。} 由此产生了非线性度的定义。

{62%：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 ，其非线性度为

.

另外，对 ，由Walsh谱的定义可得

{100%：因此，布尔函数的非线性度可由Walsh变换等价表示为}

(2-6)

(快速)代数免疫度

{87%：代数免疫度[21， 23]是评价布尔函数抵抗代数攻击能力的指标，代数攻击的基本思路是将密码系统破译问题归结为代数方程组的求解问题。} {100%：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2.2 ([23]) 对于两个布尔函数 ，若 ，则称 是 的一个零化子。 元布尔函数 的所有零化子组成的集合记为 。 布尔函数 的代数免疫度 定义为：

若 {100%：元布尔函数的代数免疫度达到了上界} [23]，则称 具有最优代数免疫度。

{89%：布尔函数具有较高的代数免疫度仅仅是抵抗代数攻击的必要条件，而不是充要条件。} 对于 元布尔函数 {100%：，若存在一个代数次数较低的非零函数} 使得 的代数次数远小于 ，那么快速代数攻击对于 就是有效的[24-26]。 {87%：为了抵抗快速代数攻击，密码系统中使用的布尔函数需具有较高的快速代数免疫度[27, 28]。}

定义2.3 ([28]) 布尔函数 的快速代数免疫度为

若 的快速代数免疫度达到 (或)，则称 {100%：具有最优(或几乎最优)快速代数免疫度。}

序列表示和布尔函数的等价性

两个 元布尔函数 和 是仿射等价的当且仅当存在一个 上的 的可逆矩阵 和一个 上的向量 使得：

，

这里 。 {52%：因为仿射等价布尔函数有相同的代数次数，与此同时也拥有相同的代数免疫度。} {55%：因此，布尔函数的代数次数和代数免疫度是仿射不变量。}

令寄存器生成一个周期为 的 序列，并且序列 满足递归关系：

，

这里 。 与此同时， 是它的生成多项式并且是本源的。 （转置）伴随矩阵（我们称它为序列的生成矩阵）是

。

令 为时刻 时寄存器的状态。 然后下一时刻的寄存器状态被确定通过

.

如果寄存器的初始状态是 ，那么序列能被表示为 。 这里 可以是任意非零 维列向量，因此这里有 个 对应于 个不同的 序列。 令 ，序列能够表示为

，

这里 。

因为次数为 的本源多项式的数量是 ，所以这有 个 生成 序列，并且不同的对应不同的序列。 因为，这存在 个 序列，每个序列能够表示为

，

这里 , 是序列的生成矩阵，并且 。 显而易见， 是 的初始状态。

令 。 显而易见，这存在两个 使得 ，这里 是 的一个子集。 我们定义两个函数为 和 。 那么 与 不相同仅当 和 。 给定任意的 ，通过使用 和 作为滤波函数生成的密钥流是相同的。 因此， 和 能够被看成相同的函数。令

。

那么任意的 能够通过它的支撑集表示为如下形式

，

这里 的寄存器的生成军阵，并且 。

Rønjom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 令 {66%：为一个通过过滤生成器残生的密钥流当} 有本源反馈多项式和滤波函数 。 是与 等价的如果这存在一个被 过滤和能产生相同密钥流的 。特别的是，如果这两个 有相同的生成多项式，我们说 和 是线性等价的，并且定义为 。否则， 和 是非线性等价的，并且定义为 。

{51%：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C-F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T-C-T函数支撑集的平移等价关系。

C-F函数支撑集的平移等价关系

{53%：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代数免疫度的布尔函数（C-F函数）。}

构造3.1（[37]）令 为大于1的整数， 为 上的本源元。 当 是一个 元的布尔函数，它的支撑集为

，

这里 是一个整数，布尔函数 有最优代数免疫度 。

在C-F函数的支撑集中存在一个参数 ，当我们对 {43%：取不同值时，C-F函数的支撑集是不相同的，随之对应的布尔函数也是不相同的。} {61%：因此，根据这种构造方法，我们可以得到大量具有最优代数免疫度的布尔函数。} 然而，当参数 {55%：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、代数免疫度和非线性度是不变量。}

随后，王启春利用 {68%：上的本源多项式的伴随矩阵构造了一类具有最优代数免疫度的布尔函数[38]。} 构造1的主要结果完全等价于通过代替二元 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 为大于1的整数， 是长度为 的 序列。 当 是一个 元的布尔函数，它的支撑集为

这里 定义为 上的全零向量，那么布尔函数 有最优代数免疫度 。

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 为大于1的整数， 是 上的次数为 的本源多项式。 如果 是 的一个根，并且 是一个非零序列，这存在一个 上的基 使得

。

引理3.2 （[40]）令 ，并且

，

这里 是序列的生成矩阵， 。 清晰可见，任意 能够 被表示为

，

这里 ， 是一个生成矩阵，并且 。

定理3.1 令 为大于1的整数， 为 上的本源元。 当 是一个 元的布尔函数，它的支撑集为

，

这里 是一个整数。 当参数 {45%：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C-F函数支撑集中的 都有一个非零序列 与之相对应。 令 为 时刻寄存器中的状态。 那么下一时刻的状态为

.

如果寄存器的初始状态是 ，那么这个序列能够表示为

。

因为

，

所以

。

因此，我们能将C-F函数表示为

。

从引理3.2可知给定一个 ，它的生成矩阵为 ，令 ，并且

。

显而易见，任意 能够被表示为

，

这里 是一个生成矩阵， 。 因此，当参数 {48%：取不同值时，所生成的C-F函数是仿射等价的。}

Tu-Deng函数和T-C-T函数支撑集的平移等价关系

{72%：涂自然和邓映蒲构造了一类具有最优代数免疫度的} 函数，它是属于Dillon定义的 类[31]。 {49%：在稍微修改它的真值表后，可以得到一个平衡的布尔函数。} {53%：虽然会稍微降低它的非线性度，但它仍然具有最优代数免疫度。} 但是，在本文中，我们研究的重点是仿射等价关系。

构造3.3（[31]）令 ， 是 上的本源元。 布尔函数 定义如下

。

布尔函数 定义如下

。

定理3.2令 ， 是 上的本源元。 布尔函数 定义如下

，

布尔函数 的支撑集能被定义为

，

这里 ， 是一个整数。

证明 我们假定 是 上的本源元， 是 上的本源元，所以 。 通过构造3.3，我们能假设 ，因此

，

并且 。 令 为 上的任一元素。 是 -向量空间 的一个基。 因此，我们有 。 令 ，所以 。 通过 的支撑集，我们知道当 时， 。 最后，我们知道布尔函数 的支撑集为

。

在Tu-Deng函数的启发下，唐灯将函数 替换为 得到了两类变元为 的具有优良性质的布尔函数。 第一类函数是不平衡的，它的汉明重量为 ，代数次数为 ，并且具有非常高的非线性度。

构造3.4 （[32]）令 ， 为 上的一个本源元。 集合 ，这里 是一个整数。那么布尔函数 定义如下

，

这里布尔函数 的支撑集为 。

定理3.3令 , 是 上的本源元。 布尔函数 定义如下

,

布尔函数 的支撑集能被定义为

,

这里 , 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 取不同值时，T-C-T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T-C-T函数是仿射等价的当参数 取不同值时。 T-C-T函数的支撑集可以写作

。

我们能将T-C-T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 , 。从定理3.1得知当参数 取不同值时，由 得到的布尔函数是仿射等价的。 此外， 的使用仅仅是安排 后的第 个位置的值为1，这样增加了真值表中1的数量。 只要 是确定的，那么 的位置就是在 后不断移动的。 因此 对支撑集的平移等价性是没有影响的。 故当参数 取不同值时，T-C-T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。

本章小结

本章研究了基于 {60%：上的本源元构造的布尔函数的仿射等价关系。} {43%：尽管这三个构造被证明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。} {65%：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。

{69%：一类1阶弹性布尔函数的快速代数免疫度的下界}

{50%：本章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6。} {50%：在之前的研究中，主要是通过计算机辅助计算布尔函数的快速代数免疫度。} 于此同时，我们也证明了一些起源于Tu-Deng猜想的组合事实。

{82%：一类具有几乎最优代数免疫度的布尔函数}

近些年，利用C-F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。 {48%：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 , 是 上的一个本源元, , 这里 。 布尔函数 定义如下：

（4-1）

这里 定义在 上，并且 。

主张4.1 ([32])构造4.1中 变元布尔函数 包括四个密码学性质：

, ;

;

;

。

{48%：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, 的基数是 。 我们会减少 的基数从而获得基数为 的 。

构造 4.2令 , 是 上的一个本源元, , 这里 。 布尔函数 定义如下：

（4-2）

这里 定义在在 上，并且 。

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 , 令

。

那么 。

引理 4.2对于 , 令

。

那么 。

证明 因为移位等价性, 能够被表示为如下的形式：

,

这里 。

如果 , 即 , 令

,

那么 和 。 因此 。

假设现在 ，并且令 ，那么

。

情形1： 是偶数。 令

这里 。 因为

，

所以 存在。 显而易见， ，并且

。

因此 。

情形1： 是奇数。 令

这里 。 因为

，

所以 存在。 显而易见， ，并且

。

因此 。

因此，对于任意的 ，这总是存在至少一个 ，所以 。

引理4.3 对于 ，令

。

那么 。

证明 显而易见，

。

从引理4.1和引理4.2，可知 和 。 因此

.

引理4.4 对于 ，令

。

那么 。

证明 当 ， ，并且 ，即 。

情形1： 是奇数。 我们有 。 所以

，

因为对于奇数 ， 。

情形1： 是偶数。 我们有 。 所以

。

因为对于偶数 ， 。

证明完成。

{58%：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 ，令

。

那么 。

定理4.1 令 为构造4.2中 变元的布尔函数。 那么 是 。

证明 从构造4.2中，我们能看出 。

首先，假定 是 的一个代数次数小于 的零化子，即

对于所有的 ， 。

当 时， 。 这暗示当 时，

。

因此

，

这里

，

当 ， 对于 时， 。

因此，当 ，向量

是一个 码的码字，它的长度为 ，设计距离为 。 此外，当它有元素在 中时，它的码字为零。 由于 {45%：界，当它的码字为非零时，它的汉明重量不少于} 。 但从引理4.5得知，它的汉明重量不超过 。 因为，这个码字不得不为零，即

，

这里 。 因此，我们能得到 当 。 所以， 。

现在讨论 的情况。 假定 是 的一个代数次数小于 的零化子。 相似的，

，

这里 。 因此，向量

是一个 码的码字，它的长度为 ，设计距离为 。 此外，当它有元素在 中时，它的码字为零。 然而由 {52%：界的定义可知，当它的码字为非零时，它的汉明重量至少为} 。 从引理4.5，可以推断它的汉明重量最多 ，产生了一个矛盾。 所以， 。

从以上的讨论可知， 和 {80%：的零化子的代数次数最小值不小于} 。 所以， 。

{69%：一类1阶弹性布尔函数的快速代数免疫度的下界}

{44%：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 ， 是 上的一个本源元， 和 ，这里 。 布尔函数 定义如下；

（4-3）

这里 属于（4-1），并且 包括以下三部分：

；

；

。

换句话说， 包括以下四部分：

；

；

；

。

定理 4.2 （[43]）令 ， 是构造4.3中的 元布尔函数。 那么布尔函数 的代数免疫度是 ，即 。

{48%：我们将会给出构造4.3的一个快速代数免疫度的下界。} 与此同时，我们需要如下的两个引理。

引理 4.6 令 ， 是 上的一个本源元，

这里 。 当布尔函数 有 时， 的代数次数大于等于 ，这里 。

证明 首先，从定理4.1中可知， 有代数免疫度 当 和 是（4-2）中定义的布尔函数。 因此， {81%：的非零零化子的代数次数不小于} 。 其次，很容易看出当

时， 是构造4.2中的 的一个非零零化子。 因此， 的代数次数大于等于 。 证明完毕。

引理 4.7 令 ， 是 上的一个本源元，

这里 和 。 对于每个 ，如果我们选择一个任意元素 ，那么这将会有 个不同的对 使得 等于1如果 ，这里 。

证明 很容易看出 因为 当且仅当 和 ，这里与条件 矛盾。 显而易见，因为 。 那么我们得到 。 换句话说，我们也有 。 因此，为了去证明这存在不同的元素对 使得 等于1，我们必须证明对于任意的 ，这有 不同的元素对 使得 。由于

注意 如果 、 、 。 由以上两个等式可得 ，即 。 的基数是 。也就是说， 。 因此 ，并且 。 当 ，有两种情况需要去考虑：

， 。

， 。

所以这有 个不同的元素对 使得 。 证明完毕。

定理 4.3 令 ， ，构造4.3中的布尔函数 的快速代数免疫度至少为 。

证明 为了证明当 {75%：时，布尔函数的快速代数免疫度至少为} 。 我们应该证明当 和 ， 。 我们将使用反证法证明这个结论。 假设 当这有一个布尔函数 ，并且 。 之后，通过（4-3）我们知道

（4-4）

这里 属于（4-1），并且 的支撑集为

。 这有两种情况需要考虑。

情形1： ，这里 。 通过引理4.6，我们知道 。 因为 是 的一个非零零化子，并且从定理4.2可知 {81%：的非零零化子的代数次数不小于} ，所以 。 在此情况下，我们有 与我们的假设 矛盾。

情形2： 。 那么这必须存在一个元素 使得 。

从引理4.7可知，这有存在元素 使得 等于1当 和 。 我们知道 是非零的，并且 。 在（4-4）的两边分别乘上 得到

。

因为 是 {58%：的一个非零零化子，所以我们得到}

。

从以上证明我们得知这有一个非零函数 使得 ，这里 。 当 ，它是与主张4.1的第四条矛盾的。 当 ，它与 矛盾。

因此，它是不可能的去假设 ，故我们有 。 证明完毕。

本章小结

{52%：在本章中，我们证明了一类1阶弹性布尔函数的快速代数免疫度大于等于} 。{45%：为了证明本节的一个布尔函数的代数免疫度，我们证明了一些来源于Tu-Deng猜想的组合事实。} {41%：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快速代数免疫度下界。} 但是，所得到的下界与实际值还存在一定的差距。 {52%：如果能够找到一个更低代数次数的布尔函数} {45%：，那么我们将能提升快速代数免疫度的下界，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。

总结与展望

{100%：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。}

论文工作总结

{82%：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。} {91%：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性质：} {100%：平衡性，良好的(快速)代数免疫度，高非线性度，高代数次数等。}

{100%：本文完成的研究工作及取得的创新性研究成果主要包括：}

{41%：（1）在计算机辅助验证的基础上，我们研究了C-F函数，Tu-Deng函数，T-C-T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（ {56%：），使得能达到大量性质优良的布尔函数。} 经研究发现，当参数 {51%：取不同值时，这些布尔函数是具有仿射等价的关系。}

{46%：（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快速代数免疫度。} {43%：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快速代数免疫度大于等于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。

后续研究工作展望

{100%：结合本文的研究工作，下一步的研究工作主要包括：}

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快速代数攻击能力的主要方式。 {54%：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快速代数攻击的能力。} 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。

{69%：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。 {44%：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

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

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

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

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.

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

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

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

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

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

http://dacas.cn.

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.

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.

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.

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.

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.

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

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

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

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.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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

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

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.

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.

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

{100%：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。} {100%：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！

{100%：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。}

{100%：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。}

{100%：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。} {100%：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。} {100%：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

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.

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.

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.

Chen Yindong，Zhang Liu，Gong zhangquan，et al. Constructing Two Classes of Boolean Functions with Good Cryptographic Properties. IEEE ACCESS.2019，7：149657-149665.