论文检测全文报告

基本信息

报告编号：20200521358995 49DEFAC4E30

文档名称：布尔函数的(快速)代数免疫性相关研究

文档作者：张柳

提交方式：上传文档检测

提交时间：2020年05月21日

正文字符数：12431

正文字数：10880

检测范围：大雅全文库

总体结论

文献相似度：27.85%

去除参考文献相似度：27.85%

去除本人已发表论文相似度：27.85%

重复字符数：3462

文献原创度：72.15%

单篇最大相似度：3.83%

单篇最大重复数：476

最相似文献题名：一类布尔函数的代数免疫度的下界

相似片段分布

最密集相似段:	0	密集相似段:	18	非密集相似段:	12
前部相似段:	10	中部相似段:	12	尾部相似段:	8

典型相似文献

相似图书

序号	题名	作者	出处	相似度
1	密码函数的安全性指标分析	李超;屈龙江;周悦	北京：科学出版社，2011.02	2.29%
2	布尔函数的设计与分析	周宇;胡予濮;董新锋	北京：国防工业出版社，2015.05	1.87%
3	密码学教程	陈少真	北京：科学出版社，2012.08	1.52%
4	安全的布尔函数构造	阚海斌;彭杰;王启春	北京：科学出版社，2014.05	1.29%
5	实用化的签密技术	AlexanderW.Dent;YuliangZheng	北京：科学出版社，2015.03	0.85%
6	组合网络理论	徐俊明	北京：科学出版社，2007.05	0.81%
7	中国密码学发展报告 2007	中国密码学会组	北京：电子工业出版社，2008.07	0.74%
8	预测控制的理论与方法	丁宝苍	北京：机械工业出版社，2017.05	0.68%
9	未知标题			0.68%
10	南京航空航天大学论文集 2008年 第21册 信息科学与技术学院 第1分册 下	南京航空航天大学科技部	南京航空航天大学科技部，2009.05	0.68%
11	未知标题			0.68%
12	数字助听器信号处理关键技术	邹采荣;梁瑞宇;王青云	北京：科学出版社，2016.06	0.68%
13	未知标题			0.68%

14	节能照明光源新进展	陈育明;陈大华	合肥：安徽科学技术出版社，2016.01	0.68%
15	现代物流与商务发展研究	现代物流与商务湖北省协同创新中心（培育）	北京西安：世界图书出版公司，2015.12	0.68%
16	未知标题			0.68%
17	密码学进展 中国密码学会2007年会论文集	何大可;黄月江	成都：西南交通大学出版社，2007.10	0.61%
18	Visual Basic程序设计教程	亢临生;王金虹	北京：高等教育出版社，2010.08	0.6%
19	未知标题			0.55%
20	信息安全概论	牛少彰;崔宝江;李剑	北京：北京邮电大学出版社，2016.08	0.51%
21	信息安全概论 第2版	牛少彰;崔宝江;李健	北京：北京邮电大学出版社，2007.09	0.51%
22	密码学的基本理论与技术	张文政;陈克非;赵伟	北京：国防工业出版社，2015.11	0.47%
23	现代密码学 第2版	杨波	北京：清华大学出版社，2007.04	0.45%
24	信息和通信安全-CCICS'2007 第五届中国信息和通信安全学术会议论文集	谢冬青;李超	北京：科学出版社，2007.07	0.44%
25	数据通信与计算机网络 第3版	杨心强;陈国友	北京：电子工业出版社，2007.07	0.4%
26	现代商业技术	晏维龙	北京：中国人民大学出版社，2005.12	0.4%
27	数据通信与计算机网络 第4版	杨心强;陈国友	北京：电子工业出版社，2012.05	0.4%
28	计算机网络	杨心强	北京：人民邮电出版社，2010.05	0.4%
29	电子商务安全	唐四薪	北京：清华大学出版社，2013.05	0.38%
30	高非线性度布尔函数的设计与分析	张凤荣	徐州：中国矿业大学出版社，2014.11	0.32%
31	中国电子学会第十五届信息论学术年会暨第一届全国网络编码学术年会论文集 上	杨义先;韦岗;范平志	北京：国防工业出版社，2008.09	0.32%
32	信息编码与加密实践	夏娜;蒋建国;丁志中	合肥：合肥工业大学出版社，2008.10	0.29%
33	密码学及信息安全基础	陈小松	北京：清华大学出版社，2018.09	0.26%
34	环境影响评价实用教程	沈珍瑶	北京：北京师范大学出版社，2007.07	0.24%
35	卫星通信	夏克文	西安：西安电子科技大学出版社，2008.12	0.23%
36	概率论与数理统计	王红蔚;孔波;牧少伯;张宏波;郑喜英	郑州：郑州大学出版社，2015.02	0.2%
37	2012-2013电子信息学科发展报告	中国科学技术协会;中国电子学会	北京：中国科学技术出版社，2014.04	0.2%
38	陈永明讲评数学题 高中习题归类研讨	陈永明;阮夏丽	上海：上海科技教育出版社，2012.11	0.2%
39	判定树理论导引	堵丁柱	长沙：湖南教育出版社，1998.12	0.17%
40	离散数学及其应用 原书第7版	KENNETH H.ROSEN;徐六通;杨娟;吴斌	北京：机械工业出版社，2015.01	0.17%
41	信息论与编码	宋鹏;范锦宏;王恩成;齐建中;王乐	西安：西安电子科技大学出版社，2018.01	0.17%
42	微型计算机原理与接口技术	吴永祥	北京：煤炭工业出版社，1995.10	0.16%
43	信道编码及其识别分析	张永光;楼才义	北京：电子工业出版社，2010.09	0.15%
44	现代密码学 第2版	许春香;李发根;汪小芬;禹勇;聂旭云	北京：清华大学出版社，2015.01	0.15%
45	中国当代商业广告史	黄艳秋;杨栋杰	开封：河南大学出版社，2006.11	0.14%
46	密码学与数论基础	丁秀源;薛昭雄	济南：山东科学技术出版社，1993.03	0.14%
47	网络安全与管理	张素娟;吴涛;朱俊东	北京：清华大学出版社，2012.10	0.14%
48	分组密码的设计与分析	吴文玲;冯登国;张文涛	北京：清华大学出版社，2009.10	0.14%
49	广州大学2008届优秀毕业论文（设计）选集	禹奇才	北京：兵器工业出版社，2008.10	0.13%

50	信息和通信安全 CCICS'2009第六届中国信息和通信安全学术会议论文集	胡爱群	北京：科学出版社，2009.06	0.13%

相似期刊

序号	题名	作者	出处	相似度
1	一类布尔函数的代数免疫度的下界	田叶;张玉清;胡予濮;伍高飞	通信学报，2016，第10期	3.83%
2	布尔函数的(快速)代数免疫性质研究进展	唐灯	密码学报，2017，第3期	3.48%
3	递归构造多个具有最优代数免疫度的平衡布尔函数	叶载良;王学理	系统科学与数学，2012，第7期	3.02%
4	一类平衡的最优代数免疫度布尔函数的构造	王筱琛;陈克非;沈忠华;程慧洁	计算机应用与软件，2018，第1期	1.59%
5	具有良好密码学性质的布尔函数的级联构造	吴保峰;林东岱	密码学报，2014，第1期	1.35%
6	基于先验结果对涂-邓猜想一些情形下的递推证明	黄昆;李超;屈龙江	武汉大学学报(理学版)，2012，第6期	1.22%
7	大函数ISFPRM面积优化方法	瞿婷;王伦耀;罗文强;夏银水	电子学报，2018，第5期	1.1%
8	基于交织技术的最优低碰撞区跳频序列集	凌龙;牛宪华;胡梦婷;吕中	西华大学学报(自然科学版)，2018，第2期	0.98%
9	一类具有新参数的最优低碰撞区跳频序列集	吕中;张永辉	通信电源技术，2018，第2期	0.98%
10	偶数变元代数免疫最优布尔函数的构造方法	陈银冬;陆佩忠	通信学报，2009，第11期	0.95%
11	级联函数的扩展代数免疫性*	刘志高;张福泰	密码学报，2015，第3期	0.94%
12	基于中国剩余定理的最优低碰撞区跳频序列集扩展构造	韩璐;牛宪华;蔡红斌	西华大学学报(自然科学版)，2019，第5期	0.85%
13	兼顾可用性和可靠性的可视密码最佳方案	乔明秋;赵振洲	信息技术与网络安全，2019，第4期	0.81%
14	Constructions for almost perfect binary sequence pairs with even length	PENGXiuping;LINHongbin;RENJiadong;andCHENXiaoyu	Journal of Systems Engineering and Electronics，2018，第2期	0.81%
15	布尔函数的可约性	叶载良	商洛学院学报，2009，第6期	0.8%
16	互补对称布尔函数的非线性度	陈银冬;陆佩忠	计算机工程与科学，2011，第10期	0.79%
17	一种新的安全电子拍卖协议	付剑晶	计算机应用与软件，2006，第6期	0.76%
18	二元2n周期序列谱免疫度的快速算法	王宁;顾聪	佛山科学技术学院学报(自然科学版)，2017，第4期	0.76%
19	基于RM码最优代数免疫度奇元布尔函数的构造	赵庆兰;刘航;郑东	西安邮电大学学报，2017，第4期	0.76%
20	一种提高DCT域水印稳健性的算法	张吉赞	计算机应用与软件，2006，第6期	0.76%
21	基于NetFlow的网络入侵检测系统	黄艳;李家滨	计算机应用与软件，2006，第6期	0.76%
22	一类级联布尔函数的密码学性质	王春侠;卓泽朋	淮北师范大学学报(自然科学版)，2018，第1期	0.75%
23	中国密码学会2015年混沌保密通信学术会议征文通知		密码学报，2015，第3期	0.73%
24	一类特殊布尔函数的代数免疫度研究	欧海文;张玉娟	计算机应用研究，2012，第2期	0.72%
25	布尔函数代数免疫度的研究	马陵勇;崇金凤;卓泽朋	计算机工程与应用，2013，第12期	0.69%
26	Q_Value检测: 一种新的随机数统计检测方法*	庄家;马原;朱双怡;林璟锵;荆继武	密码学报，2016，第2期	0.68%
27	基于预共享密钥的LAN安全关联方案改进与分析	肖跃雷;武君胜;朱志祥	计算机应用，2018，第11期	0.68%
28	车载传感网中基于聚合签名的认证方案	王大星;滕济凯	吉林大学学报(理学版)，2018，第3期	0.68%
29	基于DPA对Gauss形式CRT-RSA的选择明	李增局;史汝辉;王建	密码学报，2016，第2期	0.68%

	文攻击*	新;李超;李海滨;石新凌		
30	基于哈希链的BLE密钥协商方案设计	黄艺波;黄一才;郁滨	系统仿真学报，2016，第6期	0.68%
31	单比特相关器在超声测距中的应用研究	张博轩;赵天白	无线电工程，2019，第9期	0.68%
32	最佳及几乎最佳高斯整数ZCZ序列集的构造	刘凯;陈盼盼	电子学报，2018，第3期	0.68%
33	基于混沌加密对抗窃听的安全网络编码方案	徐光宪;王栋	计算机应用，2019，第5期	0.68%
34	CRT-RSA算法的选择明文攻击*	李增局;彭乾;史汝辉;李超;马志鹏;李海滨	密码学报，2016，第5期	0.68%
35	ESI、InCites和JCR数据库联合提供外文文献馆藏建设数据支持研究*——以东华大学为案例	董政娥;陈磊;陈惠兰	图书馆，2016，第3期	0.68%
36	一类扩展广义Feistel结构抵抗差分和线性密码分析能力评估*	殷勍;王念平	密码学报，2016，第2期	0.68%
37	Identif i cation and PID Control for a Class of Delay Fractional-order Systems	Zhuoyun Nie;Qingguo Wang;Ruijuan Liu;Yonghong Lan	IEEECAA Journal of Automatica Sinica，2016，第4期	0.68%
38	Server-aided access control for cloud computing	WENG Jian; WENG Jia-si; LIU Jia-nan; HOU Lin	网络与信息安全学报，2016，第10期	0.68%
39	MAIORANA-MCFARLAND'S BENT函数零化子空间维数	张凤荣;胡予濮;马华;谢敏;周宇	计算机研究与发展，2012，第6期	0.6%
40	最优代数免疫函数的一个新结果	黄景康;王卓;张椿玲;袁秀娟	西北民族大学学报(自然科学版)，2012，第2期	0.58%
41	T-D猜想上多输出布尔函数构造	陈怡然;周梦	应用数学进展，2014，第2期	0.56%
42	构造具有良好密码学性质的旋转对称布尔函数	熊晓雯;魏爱国;张智军	电子与信息学报，2012，第10期	0.54%
43	时间透镜成像在流密码技术中的应用与研究	郭淑琴;徐大财;刘儒林;蒋佩兰	浙江工业大学学报，2017，第2期	0.54%
44	布尔函数的非零零化子计数	叶载良	西安工程大学学报，2010，第4期	0.5%
45	两类具有最优代数免疫阶的奇变元布尔函数	苏为;曾祥勇	湖北大学学报(自然科学版)，2009，第4期	0.42%
46	具有最优代数免疫阶布尔函数的构造	王帅;王孟	洛阳师范学院学报，2012，第5期	0.41%
47	Bent函数构造方法研究*	杨小龙;胡红钢	密码学报，2015，第5期	0.39%
48	向量值函数的代数免疫度与非线性度	董德帅;屈龙江;付绍静;李超	计算机工程与科学，2009，第8期	0.39%
49	DES的S盒的布尔性质	董军武	通信技术，2012，第12期	0.39%
50	PRESENT算法的改进及仿真设计	汪亚;魏国珩;张玉婷;蔡双进	计算机工程与设计，2017，第9期	0.39%

相似网络文档

序号	题名	作者	相似度
1	布尔函数的几类密码学性质分析	李雪莲	1.61%
2	布尔函数的代数免疫度与非线性度	郭青	1.39%
3	一类代数免疫度达到最优的布尔函数的构造		1.33%
4	基于流密码的代数攻击及代数免疫性研究	罗卫华	1.22%
5	布尔函数和向量值函数的代数免疫度	董德帅	1.21%
6	具有最优代数免疫度的布尔函数		1.13%
7	The Design of Authenticated Telnet Protocol to Enh.....		1.01%
8	未知标题		0.98%

9	代数免疫函数的研究	张毛优	0.81%
10	代数攻击及代数免疫中布尔函数的研究	郑友云	0.71%
11	未知标题		0.68%
12	教师姓名王文俊		0.68%
13	Novel Gaussian Normal Basis Multiplier with Even T.....		0.68%
14	new directions in wireless communication research		0.68%
15	未知标题		0.68%
16	未知标题		0.68%
17	未知标题		0.68%
18	RESEARCH DEGREE AND PROFESSIONAL DOCTORATE		0.68%
19	未知标题		0.68%
20	布尔函数的代数免疫性研究	万鑫	0.65%
21	布尔函数代数免疫性质的研究	孙博	0.54%
22	基于混沌算法的视频加密传输系统的研究	董学洋	0.45%
23	几类代数免疫阶最优的布尔函数的研究	李春雷	0.43%
24	公钥密码系统中底层运算的硬件加速	宋灏龙	0.4%
25	椭圆曲线密码（ECC）算法的FPGA实现及优化设计	黄威	0.4%
26	几类密码函数的二阶非线性度下界	陈新姣	0.39%
27	一种安全应用层组播协议的设计与实现	岳静	0.39%
28	布尔函数零化子构造及对称布尔函数代数免疫性分析	徐春霞	0.39%
29	竹红菌素类光敏剂的设计、合成、光物理、光化学及光生物	何玉英	0.38%
30	基于免疫原理的程序自动保护技术研究	夏方遒	0.35%
31	基于遥感的海洋水产养殖氮磷排放总量测算研究	梁融韬	0.31%
32	网络协商机制在协同商务平台中的研究与应用	韩新冉	0.31%
33	城市化进程中的回族社区变迁与文化传承：以宁夏银川市康居A区为例	杨科	0.31%
34	用于扩频通信的Bent函数序列的研究	吕宏伟	0.3%
35	基于新型离散小波变换的数字通信系统的研究	康凯	0.29%
36	智能客户端技术研究及其在管理信息系统中的应用	刘海波	0.29%
37	DNA序列的比较及RNA二级结构计数	康金慧	0.28%
38	激光诱导模拟体液的实验研究	张文艳	0.27%
39	船舶细水雾喷头设计及灭油池火试验研究	兰红安	0.27%
40	不同抗性大豆品种根系分泌物的化感作用及其组分分析	张俊英	0.27%
41	评价光催化剂性能的动态实验系统的研究	常梦媛	0.27%
42	卷积码的译码算法研究	李校娟	0.25%
43	现代序列密码的设计与分析	尤加勇	0.23%
44	医学图像检索的特征提取算法的开发与应用	王斌	0.23%
45	布尔函数代数免疫性质		0.22%
46	一种改善支撑向量域描述性能的核优化算法		0.22%
47	布尔函数零化子的构造和代数免疫最优布尔函数的构造	冀会芳	0.21%
48	基于决策树的分类算法及实现	黄小兰	0.2%
49	基于移动代理的分布式知识发现系统研究	金剑	0.2%
50	中国农村经济研究会研究	马世荣	0.19%

全文对比

硕 士 学 位 论 文

题 目 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

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在代数攻击的基础上进行了改进从而提出了快速代数攻击。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才能有效的抵抗代数攻击和快速代数攻击。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：

在使用计算机进行辅助验证的基础上，研究了函数，函数，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，当参数取不同值时，这些布尔函数是具有仿射等价的关系。

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.

On the basis of computer-aided verification, we study the affine equivalence of function, function and function. These three kinds of functions based on the finite field representation have the same parameterin 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 parameteris 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 immunity32

目 录

摘要.....I

ABSTRACT.....II

目录.....III

第一章绪论.....1

1.1.研究背景及意义.....1

1.2.流密码与布尔函数.....3

1.3.国内外研究现状.....9

1.4.本文内容及结构.....10

第二章预备知识.....11

2.1.布尔函数的基本概念.....11

2.2.布尔函数的密码学性质.....13

2.3.序列表示和布尔函数的等价性.....15

第三章基于本源元表示的布尔函数的平移等价性.....18

3.1.函数支撑集的平移等价关系.....18

3.2.Tu-Deng函数和T-C-T函数支撑集的平移等价关系.....20

3.3.本章小结.....22

第四章一类1阶弹性布尔函数的快速代数免疫度的下界.....23

4.1.一类具有几乎最优代数免疫度的布尔函数.....23

4.2.一类1阶弹性布尔函数的快速代数免疫度的下界.....29

4.3.本章小结.....32

第五章总结与展望.....33

5.1.论文工作总结.....33

5.2.后续研究工作展望.....33

参考文献.....34

致谢辞.....38

攻读硕士学位期间的科研成果.....39

绪 论

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。在加密过程中使用的序列称为加密密钥，而在解密过程中使用的序列称为解密密钥，它们可以相同，也可以不同。

根据密钥的特点，对称密码体制可分为流密码和分组密码。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。

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。

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，因此并不适用于流密码的加解密过程。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。伪随机序列可根据原始短序列和生成算法预先确定的，并且是可以重复实现的，同时又具有随机序列的特性，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。

图1-1 流密码模型

流密码是由驱动部分和非线性组合部分组成。驱动部分主要是用来控制存储器的状态根据时钟周期进行转移，从而生成大周期、统计性能好的序列提供给组合部分使用。而非线性组合部分的职责是将由驱动部分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来设计流密码，布尔函数是它的基本组件，级反馈移位寄存器模型结构如图1-2所示。LFSR实现过程非常简单，生成序列的速度快，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，成为了密钥算法的重要构成组件。

图1-2 级反馈移位寄存器模型

从加密的角度来说，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

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。那么代数攻击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。在2003年的欧密会上，Courtois和Meier[22] 成功了利用代数攻击破译了一些流密码，这引起了国内外密码学者的广泛关注。

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)

实际上，代数攻击和快速代数攻击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：对于任意元布尔函数，如果存在次数不超过的非零布尔函数，使得的代数次数不超过。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]-, [12], [13], [14], [15], [31], [32],44,45]。

后来在2003年美密会上，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。在得到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。

通过研究发现，对布尔函数发动快速代数攻击并不需要求出大量的线性无关零化子来建立方程，仅需要找到一个关于的特殊倍式关系。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。文献[28]引进了快速代数免疫度(FAI)的概念用来评判布尔函数抵御快速代数攻击的能力。目前对于FAI的研究在处于起步阶段，还没有大量的好的研究成果，通过理论证明的方式来评价布尔函数抵抗快速代数攻击的能力仍然是非常困难的，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，以此来评估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

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

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。因此，安全性指标成为了衡量布尔函数密码学性质的重要参数。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

国内外研究现状

对于元布尔函数，若存在一个代数次数较低的函数使得的代数次数不大于，那么快速代数攻击对于就是有效的[24]-, [25], [26]。为了抵御快

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]。2012年，刘美成等[29]提出了完美代数免疫(PAI)的概念，是元布尔函数，是任意正整数且，若对于任意次数不小于的函数都有的代数次数不小于，则称是PAI函数。他们[29]同时证明了元布尔函数是PAI函数当且仅当或；并且仅当变元数量是，存在平衡PAI函数，仅当变元数量是，存在不平衡PAI函数。实际上，PAI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[29]。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。函数[12]和函数[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]证明了变元数量为的函数是PAI函数；2014年，他们[33]还证明了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。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。

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：

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。

第三章研究了函数，函数，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（），使得能达到大量性质优良的布尔函数。经研究发现，当参数取不同值时，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。

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。

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。定义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,和的距离定义为

。

由定义可知，和的距离实际上为差函数的重量，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，）。若记集合，用表示的幂集，即的所有子集构成的集合，则的还可以表示为

，（2-3）

这里。

非零布尔函数的中系数为非零的项所含有变元个数的最大值称为它的代数次数，记为，即

，

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

。

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

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 若布尔函数是平衡的，则。

代数次数

为了有效抵抗算法攻击[16], [17]和攻击[18]，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，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

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，其非线性度为

.

另外，对，由Walsh谱的定义可得

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

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，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或者具有低次的零化子，那么密码系统对代数攻击的抵抗能力较弱。

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。

布尔函数仅仅具有较高的代数免疫度对于抵抗代数攻击是不够的，这仅仅是必要条件，而不是充要条件。对于元布尔函数，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][25]。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FAI[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。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代数免疫度。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 令为一个通过过滤生成器产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。

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函数和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

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（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。

在函数的支撑集中存在一个参数，当我们对取不同值时，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。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，当参数取不同值时，所生成的函数是仿射等价的。

Tu-Deng函数和T-C-T函数支撑集的平移等价关系

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]。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，函数是仿射等价的。与此同时，函数也是仿射等价的。

证明 我们首先证明函数是仿射等价的当参数取不同值时。函数的支撑集可以写作

。

我们能将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，函数是仿射等价的。相同的证明过程可以得到函数也是仿射等价的。

本章小结

本章研究了基于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。

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快速代数免疫度大于等于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快速代数免疫度。于此同时，我们也证明了一些起源于猜想的组合事实。

一类具有几乎最优代数免疫度的布尔函数

近些年，利用函数作为一个组件，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，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：

，；

；

；

。

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。

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，和的零化子的代数次数最小值不小于。所以，。

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，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。

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，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FAI至少为。

证明 为了证明当时，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

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。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，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。

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。

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，我们研究了函数，函数，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（），使得能达到大量性质优良的布尔函数。经研究发现，当参数取不同值时，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快速代数免疫度。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猜想的组合事实。

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：

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。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。

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

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 [EBOL]. http:www.cryptonessie.org.

European IST. ECRYPT Project [EBOL]. http:www.nist.govaes.

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.orgpdf0910.4632, 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 2011549, 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

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，无条件的支持我的决定。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

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.

说明：

1.文献相似度=送检论文中与检测范围所有文献的相似字数/送检论文正文字符数

2.去除参考文献相似度=送检论文中检测范围所有文献（不包括参考文献）的相似字数/送检论文正文字符数

3.去除本人已发表论文相似度=送检论文中与检测范围所有文献（不包括自引）的相似字数/送检论文正文字符数

4.单篇最大相似度：送检论文与某一文献的相似度高于全部其他文献

5.正文字符数:送检论文正文部分的总字符数，包括汉字、非中文字符、标点符号、阿拉伯数字（不计入空格）

6.正文字数：送检论文正文部分的总字数，正文不包括摘要、关键词、目录、图片、表格、附录、参考文献等

北京大雅因和信息技术有限公司 相似度检测专用章