密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2017, 4(3): 262–272

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

布尔函数的 (快速) 代数免疫性质研究进展*

唐 灯

西南交通大学数学学院, 成都 611756
通讯作者: 唐灯, E-mail: dtang@foxmail.com

摘 要: 布尔函数是流密码算法中伪随机密钥流序列生成器的核心部件之一. 为了抵抗已知的密码攻击手段, 基于线性反馈移位寄存器的流密码算法中所使用的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. 在 2003 年之前, 为了避免密码系统遭受基于统计分析的概率攻击, 布尔函数应满足平衡性; 为了抵抗最佳仿射逼近和快速相关攻击, 布尔函数应具有高的非线性度; 为了抵抗 Berlekamp-Massey 算法攻击和 Rønjom-Helleseth 攻击, 布尔函数应具高的代数次数; 为了减少布尔函数的输出比特与输入变量分量之间的统计相关性, 为密码系统提供扩散特性, 布尔函数应具有良好的自相关性质; 为了抵抗分别征服攻击和相关攻击, 应用于组合模式中的布尔函数还应当满足高阶弹性. 2003 年, Courtois 和 Meier 在欧洲密码学年会上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 在国际密码学年会上提出快速代数攻击方法. 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. 本文总结了近十余年来国内外学者在构造最优代数免疫布尔函数相关方面的主要研究进展.

关键词: 布尔函数; 非线性度; 代数免疫度; 快速代数免疫度
中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000180

中文引用格式: 唐灯. 布尔函数的 (快速) 代数免疫性质研究进展[J]. 密码学报, 2017, 4(3): 262–272.
英文引用格式: TANG D. Recent progress in (fast) algebraic immunity of Boolean functions[J]. Journal of Cryptologic Research, 2017, 4(3): 262–272.

Recent Progress in (Fast) Algebraic Immunity of Boolean Functions

TANG Deng

School of Mathematics, Southwest Jiaotong University, Chengdu 611756, China
Corresponding author: TANG Deng, E-mail: dtang@foxmail.com

Abstract: Boolean functions are the building blocks of symmetric cryptographic systems. In order to have resistance against the known attacks on each model of stream cipher, Boolean functions should meet various criteria. Before 2003, the following criteria for Boolean functions used in stream ciphers with linear feedback are mandatory: balancedness (to avoid statistical dependence between the plaintext and the ciphertext), high nonlinearity (to withstand the best affine approximation and fast correlation attack), high algebraic degree (to withstand the Berlekamp-Massey and the Rønjom-Helleseth attacks), good autocorrelation properties (to provide the property of diffusion to the cryptosystems), and high order resiliency (to resist the Siegenthaler correlation attack in the case of the combiner model). At Eurocrypt 2003, Courtois and Meier successfully proposed an algebraic attack on

* 基金项目: 国家自然科学基金青年科学基金项目 (61602394); 中央高校基本科研业务费专项资金资助 (2682016CX113)
收稿日期: 2017-03-12 定稿日期: 2017-04-06

several stream ciphers which were previously believed to be secure. The attack was further improved by Courtois at Crypto 2003 where the technique of fast algebraic attack was introduced. To resist the algebraic and fast algebraic attacks, Boolean functions used in stream ciphers with linear feedback should have (almost) optimal algebraic immunity and high fast algebraic immunity. In this paper, we present a survey on the recent progress in the constructions of Boolean functions with optimal algebraic immunity and high fast algebraic immunity.

Key words: Boolean functions; nonlinearity; algebraic immunity; fast algebraic immunity

1 引言

随着计算机信息技术的飞速发展和人们对信息保密的重要性认识不断提升, 数据加密在国家的政治、军事、外交和金融的发展以及个人的工作和生活中占据着越来越重要的作用. 流密码因其实现代价低、加密速度快、安全性强度较高等优势, 在数据加密中具有广泛的实际应用. 流密码算法安全性的核心问题是伪随机密钥流序列生成器的设计, 使其能够产生具有大周期和良好统计特性的伪随机密钥流序列. 在基于线性反馈移位寄存器的流密码算法中, 伪随机密钥流序列生成器的基本设计方式是用非线性布尔函数对若干个大周期线性反馈移位寄存器进行滤波或者组合. 因此, 流密码算法的安全性在很大程度上依赖于其所使用的非线性布尔函数的特性, 布尔函数由此成为流密码算法中伪随机密钥流序列生成器的核心部件之一.

为了抵抗已知的密码攻击手段, 基于线性反馈移位寄存器的流密码算法中所使用的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. 在 2003 年之前, 布尔函数应主要兼具平衡性 (避免系统遭受基于统计分析的概率攻击)、高非线性度 (为了抵抗最佳仿射逼近 [1] 和快速相关攻击 [2])、高代数次数 (为了抵抗 Berlekamp-Massey 算法攻击 [3,4] 和 Rønjom-Helleseth 攻击 [5]) 和良好的自相关性质 (减少布尔函数的输出比特与输入变量分量之间的统计相关性, 为密码系统提供扩散性能). 此外, 应用于组合模式中的布尔函数还应当满足高阶弹性 (为了抵抗分别征服攻击 [6] 和相关攻击 [7]; 如果布尔函数是用于滤波模式中, 则弹性阶数为 1 就已足够). 2003 年, Courtois 和 Meier [8] 在欧洲密码学年会 (Eurocrypt 2003) 上将代数攻击方法应用于基于线性反馈移位寄存器的流密码算法; Courtois 在国际密码学年会 (Crypto 2003) 上提出了针对基于线性反馈移位寄存器的流密码算法的快速代数攻击方法 [9]. 代数和快速代数攻击方法对基于线性反馈移位寄存器的流密码算法构成了极大的威胁, 如 Courtois 和 Meier 利用代数攻击方法有效攻击了日本政府 Cryptrec 计划中提交的 Toyocrypt 流密码算法和欧洲 NESSIE 工程的候选流密码算法 LILI-128. 快速代数攻击不但比代数攻击对 Toyocrypt 和 LILI-128 攻击更为有效, 同时还有效攻击了蓝牙通信中的 E0 算法. 因此, 基于线性反馈移位寄存器的流密码算法中所使用的非线性布尔函数还必须具有抵抗代数和快速代数攻击的能力, 即具有高的代数免疫度 [10] 和快速代数免疫度 [11,12].

本文总结了近十余年来国内外学者在构造具有最优代数免疫度和高快速代数免疫度相关方面的主要研究进展. 第 2 节主要介绍布尔函数的基本概念和其主要密码学性质, 第 3 节总结国内外学者在构造最优代数免疫布尔函数方面的主要研究进展, 第 4 节是本文的总结和展望.

2 预备知识

设 n 是任一正整数, $\mathbb{F}_2$ 为二元有限域. n 维向量空间 $\mathbb{F}_2^n$ 中的任一向量 $a=(a_1,\cdots,a_n)$, 其支撑集 $\mathrm{supp}(a)$ 定义为集合 $\{1\le i\le n|a_i\neq 0\}$, 其汉明重量 $\mathrm{wt}(a)$ 定义为支撑集的势, 即 $\mathrm{wt}(a)=|\mathrm{supp}(a)|$. 设 $a=(a_1,a_2,\cdots,a_n)$ 和 $x=(x_1,x_2,\cdots,x_n)$ 是 $\mathbb{F}_2^n$ 中的任意两个向量, 本文中它们的内积定义为 $a\cdot x=a_1x_1\oplus a_2x_2\oplus\cdots\oplus a_nx_n$. 任一从 n 维向量空间 $\mathbb{F}_2^n$ 到 $\mathbb{F}_2$ 上的映射称作一个 n 元布尔函数. 显然, 所有 n 元的布尔函数的个数为 2^{2^n} 个, 我们将全体 n 元布尔函数的集合记为 $\mathcal{B}_n$. 任一 n 元布尔函数 f 都可以用一个长为 2^n 的行矢量

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

来唯一表示. f 的支撑集 $\mathrm{supp}(f)$ 定义为 $\{x \in \mathbb{F}_2^n | f(x) \neq 0\}$. f 的汉明重量定义为其真值表中非零函数值出现的次数, 即其支撑集的势. 若布尔函数 $f \in \mathcal{B}_n$ 的汉明重量为 2^{n-1}, 则称其是平衡的. 任一 n 元布尔函数 $f \in \mathcal{B}_n$ 都可以用一个定义在 $\mathbb{F}_2[x_1, \cdots, x_n]/(x_1^2 \oplus x_1, \cdots, x_n^2 \oplus x_n)$ 上的多项式表示:

$$f(x_1, \cdots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} a_u (\sum_{j=1}^{n} x_j^{u_j}) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u$$

其中 $a_u \in \mathbb{F}_2$ 并且 $x^u = \sum_{j=1}^{n} x_j^{u_j}$, 这里 x^u 称作单项式. 我们称这种表示方法为布尔函数的代数正规型表示. 任一布尔函数的代数正规型表示具有存在性和唯一性. 布尔函数 $f \in \mathcal{B}_n$ 的代数次数 $\deg(f)$ 定义为所有满足 $a_u \neq 0$ 的元素 u 的汉明重量的最大值. 若 f 的代数次数不超过 1, 则称 f 是仿射函数. 布尔函数除了真值表和代数正规型这两种表示方法外, 还可以用有限域 $\mathbb{F}_{2^n}$ 上的一元多项式表示. 任一 n 元布尔函数都可以唯一地表示成 $\mathbb{F}_{2^n}[x]/(x^{2^n} - x)$ 中的一个一元多项式:

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

其中 $f(x)^2 \equiv f(x) \mod (x^{2^n} - x)$. 当 n 为偶数时, 有限域 $\mathbb{F}_{2^n}$ 可以分解为 $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$, 于是, 布尔函数 $f \in \mathcal{B}_n$ 可以看成是定义在 $\mathbb{F}_{2^{n/2}}^2$ 上的函数, 可以用二元多项式唯一表示:

$$f(x, y) = \sum_{i,j=0}^{2^{n/2} - 1} f_{i,j} x^i y^j$$

其中 $f(x, y)^2 \equiv f(x, y) \mod (x^{2^{n/2}} - x, y^{2^{n/2}} - y)$.

布尔函数的绝大部分密码学准则都可以用布尔函数的 Walsh 变换来刻画. 任一布尔函数 $f \in \mathcal{B}_n$ 在元素 $a \in \mathbb{F}_x^n$ 点的 Walsh 变换定义为:

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + a \cdot x}$$

布尔函数 f 在 $\mathbb{F}_2^n$ 中所有点的 Walsh 变换的值构成的多重集称为 f 的 Walsh 谱.

现在我们简要介绍基于线性反馈移位寄存器的流密码算法中非线性布尔函数应当满足的几个主要密码学准则.

平衡性: 密码算法中所使用的布尔函数必须是平衡的, 否则由于布尔函数的输出序列中 0 和 1 出现的次数不相等, 会使得密码系统遭受基于统计分析的概率攻击. 平衡性是布尔函数的基本设计准则之一.

代数次数: 高的代数次数亦为布尔函数的基本设计准则之一. 事实上, 如果密码算法中所使用的布尔函数的代数次数过低, 则可能遭受 Berlekamp-Massey 算法攻击 [3,4] 和 Rønjom-Helleseth 攻击 [5]. 应当注意的是, n 元平衡布尔函数的代数次数上界是 $n - 1$.

非线性度: 为了使得密码算法中所使用的布尔函数能够抵抗最佳仿射逼近 [1] 和快速相关攻击 [2], 密码算法中所使用的布尔函数必须和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. 设 f 是任一 n 元布尔函数, 称非负整数 $nl(f) = \min_{l \in A_n} d_H(f, l)$ 为布尔函数 f 的非线性度, 其中 A_n 为 n 元仿射函数的集合, $d_H(f, l)$ 表示布尔函数 f 和 l 之间的汉明距离, 即 $d_H(f, l) = |\{x \in \mathbb{F}_x^n | f(x) \neq l(x)\}|$. 根据布尔函数的 Walsh 谱及非线性度定义之间的关系, 由 Parseval 等式 [13] 易得布尔函数非线性度的一个上界. 其中偶数变元时该上界是紧的, 达到该上界的函数称为 Bent 函数; 而对于较大的奇数变元 (平衡) 布尔函数而言, 该上界是否是紧的仍然是一个公开问题.

由于 Bent 函数不平衡, 因此其不能直接用于流密码算法设计, 但可以通过修改 Bent 函数得到高非线性平衡布尔函数. 1994 年, 德国国家安全局的 Dobbertin 研究员在文献 [14] 中给出了一个利用 Bent

函数构造高非线性平衡布尔函数的方法, 并猜想该方法得到的平衡布尔函数的非线性度为平衡布尔函数非线性度的可能最大值. 当奇数变元个数小于等于 7 时, 已经证明 (平衡)Semi-bent 函数的非线性度值 (称为 Bent 级联界) 为最大非线性度; 当奇数变元个数不小于 9 时, 存在非线性度值严格大于 Bent 级联界的非平衡布尔函数, 参见文献 [15–17]. 对于变元个数为 9 和 11, 目前还没有非线性度超过 Bent 级联界的平衡布尔函数的已知结果. 当变元个数为 13 时, 文献 [18] 中得到的结果是目前关于平衡布尔函数非线性度超过 Bent 级联界的最好结果. 当奇数变元个数大于等于 15 时, Patterson-Wiedemann 函数 [17] 及其与 Bent 函数的直和得到的函数是目前已知的最好结果. 总而言之, 对于奇数变元个数大于等于 9 的 (平衡) 布尔函数的最大非线性度实际值目前仍然是一个公开问题.

(快速) 代数免疫度: 2003 年, Courtois 和 Meier [8] 在 Eurocrypt 2003 上将代数攻击 (代数攻击的基本方法是将密码系统表示成一个多变量方程组, 该思想起源于 Shannon [19]) 应用于基于线性反馈移位寄存器的流密码算法, 此方法对已认为安全的流密码算法构成了极大的威胁, 如 Courtois 和 Meier 有效攻击了日本政府 Cryptrec 计划中提交的 Toyocrypt 流密码算法和欧洲 NESSIE 工程的候选流密码算法 LILI-128. 同年, Courtois 基于代数攻击在 Crypto 2003 上提出了针对基于线性反馈移位寄存器的流密码算法的快速代数攻击方法 [9], 快速代数攻击方法不但比代数攻击方法对 Toyocrypt 和 LILI-128 攻击更为有效, 同时还有效攻击了蓝牙通信中的 E0 算法.

为了衡量应用于流密码算法中布尔函数抵抗代数攻击的能力, Meier 等 [10] 提出用代数免疫度衡量布尔函数抵抗代数攻击的能力. 设 f 和 h 是任意两个元布尔函数, 若有 $fh = 0$, 则称 h 是 f 的一个零化子. 布尔函数 f 的代数免疫度 $\mathrm{AI}(f)$ 定义为 f 与 $f+1$ 的非零零化子的最低代数次数. Courtois 和 Meier 在文献 [8] 中证明了 n 元布尔函数的代数免疫度上界是 $\lceil n/2 \rceil$. 若一个 n 元布尔函数 f 的代数免疫度达到上界, 我们则称 f 是最优代数免疫的, 若其代数免疫度比上界小 1, 则称其是几乎最优代数免疫的. 代数攻击方法对流密码算法具有很强的威胁, 此后, 最优代数免疫度便成为布尔函数的一个重要密码设计准则.

代数攻击的时间复杂度小于快速代数攻击的时间复杂度, 但对于最优代数免疫布尔函数而言, 当代数攻击无法成功时, 快速代数攻击则可能有效. 刘美成等在文献 [11] 的早期 arXiv 版本中提出了快速代数免疫度的概念, 并用其衡量布尔函数抵抗快速代数攻击的能力 (文献 [11] 中作者删去了快速代数免疫度的定义; 后来我们在文献 [12] 中重新解释了该定义的合理性和必要性并再次使用该定义). 设 f 是任一 n 元布尔函数, 则 f 的快速代数免疫度定义为:

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

Courtois 在文献 [9] 中的结论表明任一 n 元布尔函数 f 的快速代数免疫度上界为 n. 若 f 的快速代数免疫度达到该上界, 则称 f 具有最优快速代数免疫度 (该类布尔函数在文献 [20] 中亦称作完全代数免疫函数), 若 f 的快速代数免疫度为 $n-1$, 则称 f 具有几乎最优快速代数免疫 (该类布尔函数在文献 [20] 中亦称作几乎完全代数免疫函数). 近十余年来, 国内外学者构造了大量最优代数免疫布尔函数, 并积极研究这些函数的快速代数免疫度, 我们将在下一节中对这些工作作一个系统总结.

相关免疫和弹性: 为了使得密码算法中所使用的布尔函数能够抵抗分别征服攻击 [6] 和相关攻击 [7], 布尔函数应当满足高的相关免疫阶. 相关免疫布尔函数最早是由 Siegenthaler 在研究流密码算法的安全性时提出的, 它在抵抗相关攻击时发挥着巨大作用. 相关免疫性的最早定义是从信息论的角度 (互信息为 0) 给出的, 后来学者研究表明它有很多等价的刻画方法, 其中最经典的方法是肖国镇和 Massey 在文献 [21] 中用布尔函数的 Walsh 谱来刻画的: 对任一 n 元布尔函数 f, 若对任意 $1 \le \mathrm{wt}(a) \le m$ 均有 $W_f(a) = 0$, 则称 f 是 m 阶相关免疫的; 若 f 还满足平衡性, 则称 f 是 m 阶弹性函数. 当布尔函数用于流密码组合模式中时, 为了抵抗相关攻击, 布尔函数应尽可能地具有高的弹性阶, 但是高阶弹性函数的代数次数必然会降低, 因此在实际应用中应当折中考虑. 应当注意的是, 相关攻击并不针对流密码的滤波模式, 一般而言, 滤波模式中使用的布尔函数只需要满足阶弹性就可以了. 关于弹性布尔函数的性质及构造可参见文献 [7, 22–27] 及其参考文献; 特别地, 文献 [28] 对基于修改 Maiorana-McFarland 类 Bent 函数得到的弹性函数的快速代数免疫度进行了分析并给出一个上界.

自相关性质: 对任一布尔函数 $f \in \mathcal{B}_n$, 其在 $a \in \mathbb{F}_2^n$ 处的自相关函数 $C_f(a)$ 定义为:

$$C_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+a)}$$

为了减少布尔函数的输出比特与输入变量分量的统计相关性, 并为密码系统提供扩散性能, 需要算法中所使用的布尔函数在非零点具有低的自相关绝对值. 1985 年, Webster 和 Tavares [29] 在研究分组密码的设计准则时提出了严格雪崩准则这一概念, 即要求 $C_f(a) = 0$ 对任意 $\mathrm{wt}(a) = 1$. 严格雪崩准则不仅适用于分组密码的设计, 而且在流密码中布尔函数的设计和在 Hash 函数的设计中都具有重要地位. 1995 年, Zhang 和 Zheng 在文献 [30] 中指出严格雪崩准则只能衡量布尔函数局部点的自相关值大小, 具有一定的局限性. 因此, 他们提出了整体扩散特征这一概念, 用来衡量布尔函数在定义域上的所有点的自相关值特性. 布尔函数的整体扩散特征包含自相关绝对值指标和自相关平方和指标. 关于布尔函数自相关性质的研究工作可参见文献 [15, 31–37] 及其参考文献.

综上所述, 为了抵抗已知和潜在的各种密码攻击手段, 基于线性反馈移位寄存器的流密码设计中所使用的非线性布尔函数应兼具平衡性 (避免密码系统遭受基于统计分析的概率攻击)、高非线性度 (为了抵抗最佳仿射逼近 [1] 和快速相关攻击 [2])、最优代数免疫度和良好的快速代数免疫度 (为了分别抵抗代数攻击 [8] 和快速代数攻击 [9])、高代数次数 (为了抵抗 Berlekamp-Massey 算法攻击 [3,4] 和 Ronjom-Helleseth 攻击 [5]) 以及良好的自相关性质 (减少布尔函数的输出比特与输入变量分量的统计相关性, 为密码系统提供扩散特性). 此外, 应用于组合模式中的布尔函数还应当满足高阶弹性 (为了抵抗分别征服攻击 [6] 和相关攻击 [7]; 如果布尔函数是用于流密码的滤波模式中, 则阶数为 1 就可以了).

3 (快速) 代数免疫性质研究进展

近十余年来, 国内外诸多学者构造了大量最优代数免疫布尔函数, 并积极研究这些函数的快速代数免疫度. 到目前为止, 构造最优代数免疫布尔函数的方法大致可以分为以下三类: 基于对称布尔函数的研究, 基于布尔函数有限域表示的研究, 基于递归构造. 此外, 国内外学者也构造了几类具有较好 (快速) 代数免疫性质的高非线性和最优代数次数的高阶弹性函数.

3.1 基于对称布尔函数的研究

择多逻辑函数是丁存生等 [1] 在 1991 年提出的一类特殊的对称布尔函数. 2006 年, 印度学者 Dalai 等 [38] 以及比利时学者 Braeken 等 [39] 最早独立证明了择多逻辑函数具有最优代数免疫度. 并且, Dalai 等 [38] 确定了择多逻辑函数的代数次数和非线性度, 研究结果表明择多逻辑函数的非线性度非常低, 不能够抵抗最佳仿射逼近和快速相关攻击. 事实上, 择多逻辑函数的非线性度近似等于代数免疫最优布尔函数的非线性度下界 (关于布尔函数的代数免疫度确定时的一个非线性度下界参见文献 [40], 之后, Mesnager 和 Lobanov 分别在文献 [41] 和 [42] 中独立地将这一结果推广到了高阶非线性度的情形). 2006 年, Armknecht 等 [43] 证明了择多逻辑函数具有很低的快速代数免疫度. 2016 年, 我们在文献 [44] 中确定了两类择多逻辑函数的快速代数免疫度. 当对称布尔函数的变元个数为奇数时, 屈龙江等 [45] 证明仅有两个最优代数免疫对称布尔函数, 它们是择多逻辑函数及其补函数. 当对称布尔函数的变元个数为偶数时, 除择多逻辑函数及其补函数外, 存在着其它最优代数免疫对称布尔函数 (参见文献 [46–48] 等). 2011 年, 彭杰等 [49] 完全解决了偶数变元对称布尔函数具有最优代数免疫度的充分必要条件. 同年, 刘美成等 [11] 证明几乎所有最优代数免疫对称布尔函数的快速代数免疫度都较低.

近年来, 国内外诸多学者尝试通过修改最优代数免疫对称布尔函数得到具有更高非线性度和更好快速代数免疫度的最优代数免疫平衡布尔函数, 并且在这方面取得了一系列研究成果, 例如文献 [38, 50–58]. 其中苏为等在文献 [58] 中给出的布尔函数经过仿射变换后可以得到 1 阶弹性函数 (仿射变换不改变布尔函数的代数免疫度). 然而, 目前通过修改最优代数免疫对称布尔函数得到的最优代数免疫函数的非线性度均与择多逻辑函数的非线性度接近, 因此不能够抵抗最佳仿射逼近和快速相关攻击.

3.2 基于布尔函数有限域表示的研究

2008 年, Carlet 和冯克勤 [59] 研究由冯克勤、廖群英和杨晶在文献 [60] 中给出的一类特殊多输出布尔函数, 构造了一类支撑集定义在偶特征有限域上的布尔函数 (下称 Carlet-Feng 函数). Carlet 和冯克勤证明了 Carlet-Feng 函数兼具平衡性, 最优代数免疫度, 最大代数次数以及高的非线性度下界. Carlet-Feng 函数的非线性度下界超过任何修改对称布尔函数得到的代数免疫最优布尔函数的非线性度, 但这个下界不足以使得布尔函数抵抗最佳仿射逼近和快速相关攻击. 2012 年, 刘美成等在文献 [20] 中给出了 (平衡) 布尔函数快速代数免疫度紧的上界, 并且证明了 Carlet-Feng 函数在变元个数为 2 的次幂加 1 时具有最优快速代数免疫度, 当变元个数为其他情形时具有几乎最优快速代数免疫度.

2010 年, 王启春等 [61] 用线性反馈移位寄存器中每个时钟周期的状态与有限域元素间的对应关系重新构造了 Carlet-Feng 函数, 并给出一个略微提高的非线性度下界. 其后, Rizomiliotis [62] 基于布尔函数的一元多项式表示, 用二元矩阵的秩刻画出布尔函数的代数免疫度大小, 基于此, Rizomiliotis 通过修改 Carlet-Feng 函数构造了一类新的最优代数免疫平衡布尔函数. 随后, 曾祥勇等 [63] 基于 Rizomiliotis 的研究方法, 修改 Carlet-Feng 函数得到三类最优代数免疫平衡布尔函数, 该三类布尔函数的非线性度下界和 Carlet-Feng 函数的非线性度下界几乎相等, 亦具有最大的代数次数. 其后, 李娇等 [64] 基于文献 [62, 63] 的研究结果进一步修改 Carlet-Feng 函数得到两类新的最优代数免疫平衡布尔函数, 该函数亦具有最大的代数次数以及和 Carlet-Feng 函数类似的非线性度下界. 计算机实验结果表明, 文献 [62–64] 中通过修改 Carlet-Feng 函数得到的布尔函数在变元个数较小时的快速代数免疫度与 Carlet-Feng 函数的快速代数免疫度相等或差 1.

2011 年, 涂自然和邓映蒲 [65] 利用 BCH 界 [13] 以及假设他们提出的一个组合猜想 (下称 Tu-Deng 猜想) 正确, 证明一类 Partial Spread (PS) bent 函数具有最优代数免疫度. 通过修改该类 Bent 函数, 涂自然和邓映蒲得到一类最大代数次数的高非线性平衡布尔函数 (下称 Tu-Deng 函数). 若假设 Tu-Deng 猜想正确, 则涂自然和邓映蒲能够证明 Tu-Deng 函数是代数免疫最优的. 然而, Carlet 在文献 [66] 中证明 Tu-Deng 函数具有非常低的快速代数免疫度, 并尝试通过修改 Tu-Deng 函数得到高快速代数免疫度的最优代数免疫平衡布尔函数. 其后, 王启春和 Johansson 在文献 [67] 中给出了布尔函数的高阶非线性度和其快速代数免疫度的一个关系, 基于此得出 Tu-Deng 函数的快速代数免疫度很低是因为其高阶非线性度很低, 并指出很难将 Tu-Deng 函数修改成具有高快速代数免疫度的布尔函数. 2012 年, Pasalic 和韦永壮在文献 [68] 中利用射影空间理论进一步研究 PS bent 函数并得到几类具有潜在最优代数免疫度的布尔函数. 在文献 [69] 中, 涂自然和邓映蒲通过修改 Tu-Deng 函数得到一类高非线性 1 阶弹性函数. 若假设 Tu-Deng 猜想和一个附加的组合假设都正确, 他们证明该类 1 阶弹性函数是代数免疫最优的. 基于 Tu-Deng 函数, 我们利用 Dobbertin 迭代构造方法, 得到一类具有良好密码学性质的偶数变元平衡布尔函数 [70]. 这类函数具有平衡布尔函数的最大代数次数和平衡布尔函数的已知最大非线性度; 若假设 Tu-Deng 猜想正确, 则可证明这类函数是代数免疫最优的. 同时我们也构造了一类具有已知最大非线性度下界的 1 阶弹性布尔函数, 若假设 Tu-Deng 猜想正确, 则可证明这类函数是几乎代数免疫最优的.

2013 年, 受到 Tu-Deng 函数研究方法的启发, 我们在文献 [71] 中给出一类具有最大代数次数和最优代数免疫度的高非线性平衡布尔函数 (下称 Tang-Carlet-Tang 函数). 与 Carlet-Feng 函数的非线性度下界相比, Tang-Carlet-Tang 函数具有可证明的更高的非线性度下界以及具有和 Carlet-Feng 函数几乎相同的实际非线性度, 但这个下界仍不足以使得布尔函数能够抵抗最佳仿射逼近和快速相关攻击. 2014 年, 刘美成等在文献 [72] 中推广了 Tang-Carlet-Tang 函数, 并证明 Tang-Carlet-Tang 函数及其推广均具有几乎最优快速代数免疫度. 后来, 基于文献 [65, 71] 的工作, 吴保峰等利用有限域的加法分解和有限域循环群的乘法分解分别得到了若干类 (几乎) 最优代数免疫平衡布尔函数 [73–75], 并且, 这些函数具有最大的代数次数和较高的非线性度下界, 其快速代数免疫度是未知的. 通过修改 Tang-Carlet-Tang 函数, 王天择等在文献 [76] 中得到了一类代数免疫度至少为几乎最优的 1 阶弹性函数; 文献 [77] 以及我们在文献 [78] 中亦通过修改 Tang-Carlet-Tang 函数分别构造了一类具有可证明的最优代数免疫度的 1 阶弹性布尔函数. 这些弹性函数均具有最优的代数次数和高的非线性度下界, 小变元计算机实验结果表明这些函数是几乎快速代数免疫的.

3.3 递归构造

最优代数免疫布尔函数可以通过递归级联构造或者递归算法得到. 文献 [79] 给出一种递归级联构造最优代数免疫布尔函数的方法, 但此类函数具有较低的非线性度和快速代数免疫度. 2008 年, 李娜等在文献 [80] 中提出交换基技术, 这种方法理论上可以由任意一个代数免疫最优布尔函数经过有限次地交换基得到相同变元个数的其他所有代数免疫最优布尔函数. 2013 年, 涂自然等 [81] 利用 Carlet-Feng 函数递归级联构造了一类奇数变元的代数免疫最优平衡布尔函数, 并且这类函数具有较高的非线性度下界和最优的代数次数.

3.4 高阶弹性函数的多种密码指标优化折中

前文提到, 为了抵抗各种密码攻击方法, 要求应用于基于线性反馈移位寄存器的流密码算法中的布尔函数必须具有高非线性度、适当的弹性阶、高代数次数、高代数免疫度和良好快速代数免疫度. 然而, 在所有上述密码指标之间进行优化折中是非常困难的问题, 尤其是当布尔函数的弹性阶数较高时.

以上三小节内容所提及的布尔函数最多具有 1 阶弹性, 仅适用于流密码滤波模式下. 对于流密码组合模式而言, 布尔函数应首先具有高阶弹性. 具有优良 (快速) 代数免疫性质的高阶弹性布尔函数的构造及相关研究结论较少. 2014 年, 张卫国和 Pasalic 提出一种新型密码函数设计方法——Generalized Maiorana-McFarland (GMM) 构造法 [24]. 采用这种构造方法可以得到同时兼具多种密码学性质的布尔函数, 这些性质包括: 严格几乎最优非线性度、高阶弹性、最优代数次数、良好代数免疫度和较好快速代数免疫度. 值得一提的是, GMM 型布尔函数还便于硬件实现 [82]. 这种构造方法借助不相交线性码可以推广到向量布尔函数的情形, 其仍然可以同时满足多种密码学性质 [83]. 近期, 张卫国和 Pasalic [27] 通过修改 PS 类 Bent 函数, 得到一类具有良好折中密码学性质的布尔函数. 上述两类布尔函数的代数免疫度和快速代数免疫度结论主要基于计算机仿真结果, 作者并没有给出理论上的证明.

此外, 通过设计良好的算法也可以利用计算机搜索到兼具多种良好密码学性质的弹性布尔函数. 例如: 杨俊坡和张卫国在文献 [26] 中给出一种算法, 可以得到具有如下指标参数的布尔函数: (8, 1, 6, 116, 4, 7); (9, 1, 7, 236, 4, 8); (10, 1, 8, 484, 5, 9); (11, 1, 9, 984, 5, 10); (12, 1, 10, 1988, 6, 11); (13, 1, 11, 4012, 6, 12); (14, 1, 12, 8072, 7, 13). 上述函数的 7 个指标依次分别是: 变元个数, 弹性阶, 代数次数, 非线性度, 代数免疫度, 快速代数免疫度.

4 总结与展望

代数和快速代数攻击对基于线性反馈移位寄存器的流密码算法中所使用的布尔函数具有很强的威胁. 虽然近十余年来国内外学者构造了大量代数免疫最优布尔函数, 但仅有若干类函数具有可证明或潜在的高快速代数免疫度, 且这几类函数的非线性度下界都很低, 无法抵抗最佳仿射逼近和快速相关攻击. 目前, 兼具多种良好密码学性质的布尔函数在基于线性反馈移位寄存器的流密码算法中仍有许多亟待解决的问题, 例如:

研究问题 1: 如何构造兼具可证明的高快速代数免疫度和高非线性度下界的最优代数免疫平衡或 1 阶弹性布尔函数?

研究问题 2: 如何分析布尔函数的代数和快速代数免疫度与其它密码学性质之间的内在联系?

研究问题 3: 如何构造兼具多种较好密码学性质的适用于基于线性反馈移位寄存器的轻量级流密码算法中的布尔函数?

总而言之, 布尔函数在流密码算法设计方面的理论和应用研究还需深入, 还有许多问题值得我们继续探讨.

References

[1] DING C, XIAO G, SHAN W. The Stability Theory of Stream Ciphers[M]. Springer Science & Business Media, 1991: vol. 561.

[2] MEIER W, STAFFELBACH O. Fast correlation attacks on stream ciphers[C]. In: Advances in Cryptology—EUROCRYPT 1988. Springer Berlin Heidelberg, 2004: 301–314.

[3] Massey J. Shift-register synthesis and BCH decoding[J]. IEEE Transactions on Information Theory, 1969, 15(1): 122–127.

[4] RUEPPEL R, Staffelbach O. Products of linear recurring sequences with maximum complexity[J]. IEEE Transactions on Information Theory, 1987, 33(1): 124–131.
[5] RONJOM S, HELLESETH T. A new attack on the filter generator[J]. IEEE Transactions on Information Theory, 2007, 53(5): 1752–1758.
[6] SIEGENTHALER T. Decrypting a class of stream ciphers using ciphertext only[J]. IEEE Transactions on Computers, 1985, 100(1): 81–85.
[7] SIEGENTHALER T. Correlation-immunity of nonlinear combining functions for cryptographic applications (corresp.)[J]. IEEE Transactions on Information Theory, 1984, 30(5): 776–780.
[8] COURTOIS N T, MEIER W. Algebraic attacks on stream ciphers with linear feedback[C]. In: Advances in Cryptology—EUROCRYPT 2003. Springer Berlin Heidelberg, 2003: 345–359.
[9] COURTOIS N T. Fast algebraic attacks on stream ciphers with linear feedback[C]. In: Advances in Cryptology-CRYPTO 2003. Springer Berlin Heidelberg, 2003: 176–194.
[10] MEIER W, PASALIC E, CARLET C. Algebraic attacks and decomposition of Boolean functions[C]. In: Advances in Cryptology—EUROCRYPT 2004. Springer Berlin Heidelberg, 2004: 474–491.
[11] LIU M, LIN D, PEI D. Fast algebraic attacks and decomposition of symmetric Boolean functions[J]. IEEE Transactions on Information Theory, 2011, 57(7): 4817–4821.
[12] CARLET C, TANG D. Enhanced Boolean functions suitable for the filter model of pseudo-random generator[J]. Designs, Codes and Cryptography, 2015, 76(3): 571–587.
[13] MACWILLIAMS F J, SLOANE N J A. The Theory of Error-correcting Codes[M]. Elsevier, 1977: vol. 16.
[14] DOBBERTIN H. Construction of bent functions and balanced Boolean functions with high nonlinearity[C]. In: Fast Software Encryption 1995. Springer Berlin Heidelberg, 1995: 61–74.
[15] KAVUT S, MAITRA S, YUCEL M D. Search for Boolean functions with excellent profiles in the rotation symmetric class[J]. IEEE Transactions on Information Theory, 2007, 53(5): 1743–1751.
[16] KAVUT S, YÜCEL M D. 9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class[J]. Information and Computation, 2010, 208(4): 341–350.
[17] PATTERSON N, WIEDEMANN D. The covering radius of the Reed-Muller code is at least 16276[J]. IEEE Transactions on Information Theory, 1983, 29(3): 354–356.
[18] MAITRA S, KAVUT S, YÜCEL M D. Balanced Boolean function on 13-variables having nonlinearity greater than the bent concatenation bound[C]. In: Proceedings of the Fourth International Workshop on Boolean Functions: Cryptography and Applications, BFCA. 2008, 8: 109–118.
[19] SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656–715.
[20] LIU M, ZHANG Y, LIN D. Perfect algebraic immune functions[C]. In: International Conference on the Theory and Application of Cryptology and Information Security. Springer Berlin Heidelberg, 2012: 172–189.
[21] XIAO G., MASSEY J L. A spectral characterization of correlation-immune combining functions[J]. IEEE Transactions on Information Theory, 1988, 34(3): 569–571.
[22] CARLET C. A larger class of cryptographic Boolean functions via a study of the Maiorana-Mcfarland construction[C]. In: Advances in Cryptology—CRYPTO 2002. Springer Berlin Heidelberg, 2002: 549–564.
[23] SARKAR P, MAITRA S. Nonlinearity bounds and constructions of resilient Boolean functions[C]. In: Advances in Cryptology–CRYPTO 2000. Springer Berlin Heidelberg, 2000: 515–532.
[24] ZHANG W G, PASALIC E. Generalized Maiorana–McFarland construction of resilient Boolean functions with high nonlinearity and good algebraic properties[J]. IEEE Transactions on Information Theory, 2014, 60(10): 6681–6695.
[25] ZHANG W, XIAO G. Constructions of almost optimal resilient Boolean functions on large even number of variables[J]. IEEE Transactions on Information Theory, 2009, 55(12): 5822–5831.
[26] YANG J P, ZHANG W G. Generating highly nonlinear resilient boolean functions resistance against algebraic and fast algebraic attacks[J]. Security and Communication Networks, 2015, 8(7): 1256–1264.
[27] ZHANG W G, PASALIC E. Improving the lower bound on the maximum nonlinearity of 1-resilient Boolean functions and designing functions satisfying all cryptographic criteria[J]. Information Sciences, 2017, 376: 21–30.
[28] WEI Y, YIN W, PASALIC E, et al. On algebraic properties of s-boxes designed by means of disjoint linear codes[J]. International Journal of Computer Mathematics, 2016, 93(1): 55–66.
[29] WEBSTER A, TAVARES S E. On the design of s-boxes[C]. In: Advances in Cryptology—CRYPTO 1985. Springer Berlin Heidelberg, 1986: 523–534.
[30] ZHANG K, ZHENG Y. GAC-the criterion for global avalance characteristics of cryptographic functions[J]. Journal of Universal Computer Science, 1995, 1(5): 320–337.
[31] KAVUT S. Correction to the paper: Patterson–Wiedemann construction revisited[J]. Discrete Applied Mathe-

matics, 2016, 202: 185–187.

[32] MAITRA S. Highly nonlinear balanced Boolean functions with good local and global avalanche characteristics[J]. Information Processing Letters, 2002, 83(5): 281–286.

[33] MAITRA S, SARKAR P. Modifications of Patterson-Wiedemann functions for cryptographic applications[J]. IEEE Transactions on Information Theory, 2002, 48(1): 278–284.

[34] STĂNICĂ P, SUNG S H. Boolean functions with five controllable cryptographic properties[J]. Designs, Codes and Cryptography, 2004, 31(2): 147–157.

[35] TANG D, MAITRA S. Construction of n-variable (n=2 mod 4) balanced Boolean functions with maximum absolute value in autocorrelation spectra 2n/2[J]. IACR Cryptology ePrint Archive 2016, 1078.

[36] TANG D, ZHANG W, TANG X. Construction of balanced Boolean functions with high nonlinearity and good autocorrelation properties[J]. Designs, Codes and Cryptography, 2013, 67(1): 77–91.

[37] ZHOU Y, XIE M, XIAO G. On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity[J]. Information Sciences, 2010, 180(2): 256–265.

[38] DALAI D K, MAITRA S, SARKAR S. Basic theory in construction of Boolean functions with maximum possible annihilator immunity[J]. Designs, Codes and Cryptography, 2006, 40(1): 41–58.

[39] BRAEKEN A, PRENEEL B. On the algebraic immunity of symmetric Boolean functions[C]. In: Progress in Cryptology—INDOCRYPT 2005. Springer Berlin Heidelberg, 2005: 35–48.

[40] LOBANOV M. Tight bound between nonlinearity and algebraic immunity[J]. IACR Cryptology ePrint Archive, 2005: 441.

[41] MESNAGER S. Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity[J]. IEEE Transactions on Information Theor,2008, 54(8): 3656–3662.

[42] LOBANOV M. Tight bounds between algebraic immunity and nonlinearities of high orders[J]. IACR Cryptology ePrint Archive 2007: 444.

[43] ARMKNECHT F, CARLET C, GABORIT P, et al. Efficient computation of algebraic immunity for algebraic and fast algebraic attacks[C]. In: Advances in Cryptology—EUROCRYPT 2006. Springer Berlin Heidelberg, 2006: 147–164.

[44] DENG T, RONG L U O, XIAONI D U. The exact fast algebraic immunity of two subclasses of the majority function[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2016, 99(11): 2084–2088.

[45] QU L, LI C, FENG K. A note on symmetric Boolean functions with maximum algebraic immunity in odd number of variables[J]. IEEE Transactions on Information Theory, 2007, 53(8): 2908–2910.

[46] BRAEKEN A. Cryptographic Properties of Boolean Functions and S-boxes[D]. Catholic University of Louvain, 2006.

[47] CHEN Y, LU P. Two classes of symmetric Boolean functions with optimum algebraic immunity: construction and analysis[J]. IEEE Transactions on Information Theory, 2011, 57(4): 2522–2538.

[48] QU L, FENG K, LIU F, et al. Constructing symmetric Boolean functions with maximum algebraic immunity[J]. IEEE Transactions on Information Theory, 2009, 55(5): 2406–2412.

[49] PENG J, WU Q, KAN H. On symmetric Boolean functions with high algebraic immunity on even number of variables[J]. IEEE Transactions on Information Theory, 2011, 57(10): 7205–7220.

[50] CARLET C, ZENG X, LI C, et al. Further properties of several classes of Boolean functions with optimum algebraic immunity[J]. Designs, Codes and Cryptography, 2009, 52(3): 303–338.

[51] DONG D, FU S, QU L, et al. A new construction of Boolean functions with maximum algebraic immunity[C]. In: Information Security. Springer Berlin Heidelberg, 2009: 177–185.

[52] FU S, LI C, MATSUURA K, et al. Construction of rotation symmetric Boolean functions with maximum algebraic immunity[C]. In: Cryptology and Network Security. Springer Berlin Heidelberg, 2009: 402–412.

[53] FU S, QU L, LI C, et al. Balanced rotation symmetric Boolean functions with maximum algebraic immunity[J]. IET Information Security, 2011, 5(2): 93–99.

[54] LI N, QI W F. Construction and analysis of Boolean functions of $2t + 1$ variables with maximum algebraic immunity[C]. In: International Conference on the Theory and Application of Cryptology and Information Security. Springer Berlin Heidelberg, 2006: 84–98.

[55] SARKAR S, MAITRA S. Construction of rotation symmetric Boolean functions on odd number of variables with maximum algebraic immunity[C]. In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Springer Berlin Heidelberg, 2007: 271–280.

[56] SU S, TANG X. Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity[J]. Designs, Codes and Cryptography, 2014: 1–17.

[57] SU S, TANG X, ZENG X. A systematic method of constructing Boolean functions with optimal algebraic immunity based on the generator matrix of the Reed–Muller code[J]. Designs, Codes and Cryptography, 2014, 72(3): 653–673.
[58] SU W, ZENG X, HU L. Construction of 1-resilient Boolean functions with optimum algebraic immunity[J]. International Journal of Computer Mathematics, 2011, 88(2): 222–238.
[59] CARLET C, FENG K. An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity[C]. In: Advances in Cryptology—ASIACRYPT 2008. Springer Berlin Heidelberg, 2008: 425–440.
[60] FENG K, LIAO Q, YANG J. Maximal values of generalized algebraic immunity[J]. Designs, Codes and Cryptography, 2009, 50(2): 243–252.
[61] WANG Q, PENG J, KAN H, et al. Constructions of cryptographically significant Boolean functions using primitive polynomials[J]. IEEE Transactions on Information Theory, 2010, 56(6): 3048–3053.
[62] RIZOMILIOTIS P. On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation[J]. IEEE Transactions on Information Theory, 2010, 56(8): 4014–4024.
[63] ZENG X, CARLET C, SHAN J, et al. More balanced Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks[J]. IEEE Transactions on Information Theory, 2011, 57(9): 6310–6320.
[64] LI J, CARLET C, ZENG X, et al. Two constructions of balanced Boolean functions with optimal algebraic immunity, high nonlinearity and good behavior against fast algebraic attacks[J]. Designs, Codes and Cryptography, 2015, 76(2): 279–305.
[65] TU Z, DENG Y. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity[J]. Designs, Codes and Cryptography, 2011, 60(1): 1–14.
[66] CARLET C. On a weakness of the tu-deng function and its repair[J]. IACR Cryptology ePrint Archive 2009, 606.
[67] WANG Q, JOHANSSON T. A note on fast algebraic attacks and higher order nonlinearities[C]. In: International Conference on Information Security and Cryptology. Springer Berlin Heidelberg, 2010: 404–414.
[68] PASALIC E, WEI Y. On the construction of cryptographically significant boolean functions using objects in projective geometry spaces[J]. IEEE Trans. Information Theory, 2012, 58(10): 6681–6693.
[69] TU Z, DENG Y. Boolean functions optimizing most of the cryptographic criteria[J]. Discrete Applied Mathematics, 2012, 160(4): 427–435.
[70] TANG X, TANG D, ZENG X, et al. Balanced Boolean functions with (almost) optimal algebraic immunity and very high nonlinearity[J]. IACR Cryptology ePrint Archive 2010, 443.
[71] TANG D, CARLET C, TANG X. Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks[J]. IEEE Transactions on Information Theory, 2013, 59(1): 653–664.
[72] LIU M, LIN D. Almost perfect algebraic immune functions with good nonlinearity[C]. In: 2014 IEEE International Symposium on Information Theory (ISIT). IEEE, 2014: 1837–1841.
[73] WU B, JIN Q, LIU Z, et al. Constructing Boolean functions with potentially optimal algebraic immunity based on additive decompositions of finite fields[C]. In: 2014 IEEE International Symposium on Information Theory. IEEE, 2014: 1361–1365.
[74] WU B, ZHENG J, LIN D. Constructing Boolean functions with (potentially) optimal algebraic immunity based on multiplicative decompositions of finite fields[C]. In: 2015 IEEE International Symposium on Information Theory. IEEE, 2015: 491–495.
[75] ZHENG J, WU B, CHEN Y, et al. Constructing 2m-variable Boolean functions with optimal algebraic immunity based on polar decomposition of F22m[J]. International Journal of Foundations of Computer Science, 2014, 25(5): 537–551.
[76] WANG T, LIU M, LIN D. Construction of resilient and nonlinear Boolean functions with almost perfect immunity to algebraic and fast algebraic attacks[C]. In: International Conference on Information Security and Cryptology. Springer Berlin Heidelberg, 2012: 276–293.
[77] WANG Z, ZHANG X, WANG S, et al. Construction of Boolean functions with excellent cryptographic criteria using bivariate polynomial representation[J]. International Journal of Computer Mathematics, 2016, 93(3): 425–444.
[78] TANG D, CARLET C, TANG X. A class of 1-resilient boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks[J]. International Journal of Foundations of Computer Science, 2014, 25(06): 763–780.
[79] CARLET C, DALAI D K, GUPTA K C, et al. Algebraic immunity for cryptographically significant Boolean functions: analysis and construction[J]. IEEE Transactions on Information Theory, 2006, 52(7): 3105–3121.
[80] LI N, QU L J, QI W F, et al. On the construction of Boolean functions with optimal algebraic immunity[J]. IEEE

Transactions on Information Theory, 2008, 54(3): 1330–1334.
[81] TU Z, JIANG Y, ZENG X. Constructing odd variable Boolean functions with optimal algebraic immunity[J]. International Journal of Foundations of Computer Science, 2013, 24(3): 409–417.
[82] PASALIC E, CHATTOPADHYAY A, ZHANG W. Efficient implementation of generalized Maiorana–Mcfarland class of cryptographic functions[J]. Journal of Cryptographic Engineering (2016), 1–9.
[83] ZHANG W, PASALIC E. Constructions of resilient s-boxes with strictly almost optimal nonlinearity through disjoint linear codes[J]. IEEE Transactions on Information Theory, 2014, 60(3): 1638–1651.

作者信息

唐灯(1984–), 博士, 讲师. 主要研究方向为密码函数.
E-mail: dtang@foxmail.com

~~~~~~

中国密码学会 2017 年密码数学理论学术会议通知

为促进国内外密码数学领域专家的交流与合作, 由中国密码学会密码数学理论专业委员会主办, 内蒙古财经大学和内蒙古数据科学与大数据学会承办的 “中国密码学会 2017 年密码数学理论学术会议” 将于 2016 年 8 月 19 日至 20 日在内蒙古自治区呼和浩特举行. 本次会议拟邀请密码数学领域著名专家学者报告该方向的最新成果与发展趋势, 并就此开展深入的研讨.

会议旨在团结和吸引国内外密码数学理论领域的学者专家、行业精英、在校师生和工程技术人员, 共同交流、探讨密码数学理论领域最新成果和发展趋势, 及在网络空间安全、大数据安全等国家安全战略领域的应用前景. 会议将对提高密码学术研究水平, 加强学术界和产业界的相互了解与合作方面起到积极的推动和促进作用. 现将有关事项通知如下:

主办单位: 中国密码学会密码数学理论专业委员会

承办单位: 内蒙古财经大学、内蒙古数据科学与大数据学会

会议时间: 2017 年 8 月 19 日至 20 日, 2017 年 8 月 18 日 15:00–22:00 报到

报到地点: 内蒙古宾悦大酒店 (地址: 呼和浩特市赛罕区昭乌达路 52 号)

注册费: (通过网银转账、银行汇款或现场刷卡交纳)

8 月 15 日前交费: 密码学会会员 1080 元/880 元 (学生); 非会员 1280 元

8 月 15 日后交费: 密码学会会员 1280 元/1080 元 (学生); 非会员 1480 元

住宿: 会议提供内蒙古宾悦大酒店住宿, 费用自理, 为保证会议期间住房, 请于 2017 年 8 月 1 日前预定 (标准间 (含双早): 450 元/天; 大床房 (含单早): 470 元/天).

联系人: 高老师 (会议注册): 13404801950, gaobonmghhht@163.com

王老师 (财务): 010-59703687, cacr02@cacrnet.org.cn

中国密码学会密码数学理论专业委员会

2017 年 6 月 21 日
~~~~~~