doi:10.11887/j.issn.1001-2486.25120009 http://journal.nudt.edu.cn

几乎完全非线性函数研究进展

施晨苗,李康荃,屈龙江*
(国防科技大学 理学院,湖南 长沙 410073)

摘 要:几乎完全非线性(almost perfect nonlinear, APN)函数因差分性质最优,成为密码函数领域研究重点。本文系统综述了APN函数研究进展:一是总结APN算例的一般生成方法;二是提炼已有APN无限类的构造技术,并明确其具体构造;三是介绍APN无限类与算例的等价分类结果;四是梳理APN函数在置换性质、代数次数、非线性度等方面的研究结论;五是回顾APN函数在编码理论和组合设计中的一些应用;六是对APN函数的研究前景进行展望。目前,APN函数的构造仍以二次函数为主,尚未发现高次多项式无限类;"大APN问题"等重要难题仍未解决。未来研究可着力于构造非经典Walsh谱APN多项式、发掘高次APN多项式等,并拓展其在编码与组合设计中的新应用。

关键词:几乎完全非线性函数;构造;等价性;置换;代数次数;非线性度
中图分类号:TP309.7 **文献标志码**:A **文章编号**:1001-2486(2026)03-368-17

Research progress of almost perfect nonlinear functions

*SHI Chenmiao, LI Kangquan, QU Longjiang**
(College of Science, National University of Defense Technology, Changsha 410073, China)

Abstract: APN (almost perfect nonlinear) functions, renowned for their optimal differential properties, have become a research focus in the field of cryptographic functions. This paper systematically reviewed the research progress of APN functions: first, it summarized the general methods for generating APN function examples; second, it refined the construction techniques of existing infinite families of APN functions and clarifies their specific constructions; third, it introduced the equivalence classification results of APN function examples and infinite families; fourth, it combed through the research conclusions on the cryptographic properties of APN functions, such as permutation property, algebraic degree, and nonlinearity; fifth, it reviewed some applications of APN functions in coding theory and combinatorial design; finally, the research prospects of APN functions were prospected. Currently, the construction of APN functions is still dominated by quadratic ones, and no infinite families of polynomials with higher algebraic degree have been found. Major challenges, such as the "big APN problem", remain unsolved. Future research may focus on constructing APN polynomials with non-classical Walsh spectra, discovering APN polynomials with higher degree, among others, and exploring their applications in coding theory and combinatorial design.

Keywords: almost perfect nonlinear functions; constructions; equivalence; permutation; algebraic degree; nonlinearity

在人工智能和量子信息科技飞速发展的时代背景下,密码学已经从一项前沿科技,全面演进为维护国家安全的战略基石与核心支柱。分组密码算法作为众多密码系统的关键组成部分,在保障信息机密性与完整性方面发挥着不可替代的作用。在分组密码中,S盒(substitution boxes)是最常见且至关重要的非线性组件,其本质是有限域上的函数[1],承担着算法所必需的混淆功能。S盒的设计质量好坏主要取决于其抵抗各类密码攻击的密码学指标的性能优劣。

分组密码S盒的主要密码学指标是根据已知的密码分析方法所设定的[2-3],差分攻击[4]是分组密码分析中最有效的密码攻击之一,其基本原理是通过分析具有特定输入差分的明文对经过加密后得到的密文对的差分特征来恢复部分密钥的信息。一个密码函数的抗差分攻击能力由其差分

收稿日期:2025-12-04
基金项目:国家重点研发计划资助项目(2024YFA1013000);国家自然科学基金资助项目(12525115,12571579);湖南省自然科学基金资助项目(2026JJ40001)
第一作者:施晨苗(1996—),男,浙江湖州人,博士,E-mail:cmshi8300@163.com
***通信作者**:屈龙江(1980—),男,河南信阳人,教授,博士,博士生导师,E-mail:ljqu_happy@hotmail.com
引用格式:施晨苗,李康荃,屈龙江. 几乎完全非线性函数研究进展[J]. 国防科技大学学报,2026,48(3):368-384.
Citation:SHI C M, LI K Q, QU L J. Research progress of almost perfect nonlinear functions[J]. Journal of National University of Defense Technology, 2026, 48(3): 368-384.

均匀度决定[5]。差分均匀度越低,函数抵抗差分攻击的能力就越强。低差分函数的相关研究可参见文献[6]。在偶特征有限域上,任意一个函数的差分均匀度至少为 2,若其差分均匀度等于 2,则称该函数为几乎完全非线性(almost perfect nonlinear,APN)函数。因此,APN 函数具有最优的抗差分攻击能力。

APN 函数自 20 世纪 90 年代初被提出以来,因其优良的密码学性质,受到了国内外学者的广泛关注和研究,并在编码理论、组合设计等领域也有重要应用。2006 年之前,已知的 APN 函数主要是单项式。此后,学者陆续发现了非单项式的 APN 算例并构造了无限类。尽管如此,APN 函数仍显得十分稀少,尤其是无限类构造类别至今有限。目前,已知的 APN 单项式无限类仅有 6 类,而多项式无限类也不过 20 类,且后者的代数次数全部为 2 次。

近年来,关于 APN 函数生成与构造的研究已取得显著进展,同时其各类密码性质的研究也成果丰富,一些进展可参见文献[7 - 15]。本文系统梳理了国内外学者针对 APN 函数的生成和构造提出的研究方法,归纳了目前已发现的 APN 函数无限类,总结了 APN 函数之间的等价性结果,汇总了 APN 函数其他密码性质方面的已有结果,回顾了 APN 函数在编码和组合设计中的应用。

1　预备知识

1.1　基本概念

设 n 是一个正整数。F_{2^n}表示包含 2^n 个元素的有限域。对$m\mid n$,用 $Tr_m^n(\cdot)$表示从有限域 F_{2^n}到 F_{2^m}的迹函数,即 $Tr_m^n(x)=\sum_{i=0}^{n/m-1}x^{2^{mi}}$。当 $m=1$ 时,$Tr_1^n(\cdot)$也被称为绝对迹函数。任意一个函数 $G:F_{2^n}\to F_{2^n}$在有限域 F_{2^n}上存在唯一一个次数至多是 2^n-1 的多项式表示:

$$G(x)=\sum_{i=0}^{2^n-1}a_ix^i,\ a_i\in F_{2^n} \tag{1}$$

代数次数是衡量函数抵抗高阶差分攻击[16-17]能力的密码学指标,其定义如下:

定义 1(代数次数)　G 的代数次数 $\deg(G)$,定义为满足式(1)中 $a_i\neq 0$ 的指数 i 的最大二进制重量(也称为 2-重),其中 i 的 2-重是其二进制表示中“1”的个数。代数次数为 1 的函数称作仿射函数,代数次数为 2 的函数称作二次函数。一个仿射函数 G 满足 $G(0)=0$ 称作线性函数。

为评估密码函数抵抗差分攻击的能力,Nyberg 首次给出了差分均匀度的定义[2]:

定义 2(差分均匀度[5])　对任意一个函数 $G:F_{2^n}\to F_{2^n}$,$\Delta_G(a,b)$表示方程 $G(x+a)+G(x)=b$ 在 F_{2^n}中解的个数。称多重集$\{\Delta_G(a,b):a\in F_{2^n}^*,b\in F_{2^n}\}$为 G 的差分谱,G 的差分均匀度 Δ_G 定义为

$$\Delta_G=\max\{\Delta_G(a,b):a\in F_{2^n}^*,b\in F_{2^n}\} \tag{2}$$

如果 $\Delta_G=2$,则称 G 是 APN 函数。

Walsh 变换是分析密码函数性质的重要工具,其定义如下:

定义 3(Walsh 变换)　函数 $G:F_{2^n}\to F_{2^n}$在(a,b)点的 Walsh 变换 $W_G(a,b):F_{2^n}^*\times F_{2^n}\to\mathbb{C}$ 定义为

$$W_G(a,b)=\sum_{x\in F_{2^n}}(-1)^{Tr_1^n(ax+bG(x))} \tag{3}$$

多重集 $W_G=\{W_G(a,b):a,b\in F_{2^n},\ a\neq 0\}$称为 G 的 Walsh 谱,由 G 的 Walsh 变换值的绝对值构成的多重集$\{|W_G(a,b)|:a,b\in F_{2^n},\ a\neq 0\}$称为 G 的扩展 Walsh 谱。

非线性度[18]是衡量密码函数抵抗线性攻击能力的密码指标,其本质是分支函数与所有仿射函数之间的最小汉明距离中的最小值,可以通过汉明距离与 Walsh 变换的关系给出:

定义 4(非线性度[18])　函数 $G:F_{2^n}\to F_{2^n}$的非线性度 $N(G)$定义为

$$N(G)=2^{n-1}-\frac{1}{2}\max_{x\in W_G}|x| \tag{4}$$

当 n 是奇数时,$N(G)$的上界是 $2^{n-1}-2^{(n-1)/2}$,取得这一上界的函数称为 AB(almost bent)函数。显然,AB 函数只可能在奇数次扩张的有限域上存在。当 n 是偶数时,$N(G)$的已知上界是 $2^{n-1}-2^{n/2}$。

1.2　函数的等价性

构造“新”的 APN 函数是密码函数研究中的一个核心问题,其关键在于证明新函数与所有已知 APN 函数均不等价。扩展仿射[5](extended affine, EA)等价和 CCZ(Carlet-Charpin-Zinoviev)等价[19]是保持函数差分均匀度最常见的两个等价关系,特别地,二者都保持函数的 APN 性质。因此,判别新构造的 APN 函数与已知函数的 EA 或 CCZ 等价关系,已成为该领域的一个关键问题。EA 等价和 CCZ 等价的定义如下:

定义 5(EA 等价[5])　设 G、H: $F_{2^n}\to F_{2^n}$,如果存在两个仿射置换 A_1、A_2, 以及一个仿射函数 A_3,使得式(5)成立,则称 G、H 是 EA 等价的。

$$G \circ A_1 = A_2 \circ H + A_3 \tag{5}$$

如果 G、H 是 EA 等价的，并且式(5)中 A_1、A_2、A_3 是线性的，那么称 G、H 是扩展线性(extended linear，EL)等价的。如果 G、H 是 EA 等价的，并且式(5)中 $A_3=0$，那么称 G、H 是仿射等价的，特别地，如果 A_1、A_2 是线性的，则称 G、H 是线性等价的。

定义 6(CCZ 等价[19]) 设 G、H：$F_{2^n}\to F_{2^n}$，$\Gamma_G=\{(x,G(x)):x\in F_{2^n}\}$ 表示函数 G 的图。若存在 $F_{2^n}^2$ 上的一个仿射置换 A，将 G 的图映射到 H 的图，即 $A(\Gamma_G)=\Gamma_H$，则称 G、H 是 CCZ 等价的。

事实上，EA 等价是 CCZ 等价的一个特殊情形[19]。Budaghyan 等[20]证明了对于 F_{2^n} 上的 Gold 函数 $G(x)=x^{2^i+1}$，存在 CCZ 等价但 EA 不等价于 G 的函数。因此，CCZ 等价严格广泛于 EA 等价。进一步地，文献[21]中提出了一个构造 CCZ 等价但 EA 不等价于一个特定函数的方法。

2 生成 APN 算例的一般方法

APN 算例的生成方法可分为两类：一是直接生成法，即直接生成或产生 APN 算例；二是间接生成法，即从已知函数(APN 函数、向量 Bent 函数等)出发生成或产生新的 APN 算例。

2.1 直接生成法

1999 年，Canteaut 通过计算机搜索给出了当 $n\leqslant 25$ 时，有限域 F_{2^n} 上所有的 APN 单项式算例；之后，Edel 将搜索范围扩大到 $n\leqslant 34$ 以及 $n=36$，38，40，42[22]。2006 年，Edel 等[23]首次发现了两个分别定义在 $F_{2^{10}}$ 和 $F_{2^{12}}$ 上的与单项式 CCZ 不等价的二次 APN 二项式算例。

2014 年前后，翁国标等[24]和余玉银等[25]提出了生成二次 APN 算例的矩阵构造法(matrix construction approach)，并发现了在 $n\leqslant 8$ 的情况下有限域 F_{2^n} 上有大量 APN 算例。例如余玉银等在 F_{2^7} 和 F_{2^8} 上分别生成了 487 个和 8 157 个新的二次 APN 算例。2022 年，余玉银等[26]提出正交差分法(ortho-derivative method)，进一步发展矩阵构造法，找到了 F_{2^8} 上 5 412 个新的二次 APN 算例。一种与矩阵构造法相似的方法是熊海等[27]和 Suder[28]提出的反向差分法(antiderivative method)。利用反向差分法构造 APN 算例的关键在于寻找一个满足相容性条件的 2 到 1 映射族 Ω，即 Ω 中的任意两个 2 到 1 映射的线性组合依旧是 2 到 1 的。特别地，当反向差分法中的 2 到 1 映射是线性的(此时生成的 APN 算例是二次的)时，该方法等价于矩阵构造法。此外，Suder 指出找到满足相容性条件的非线性 2 到 1 映射族是困难的。

2022 年，Beierle 等[29]提出递归树搜索(recursive tree search)的方法，结合代数次数为 2 以及线性自等价(linear self-equivalence)这两个特殊性质，发现了 F_{2^8} 上 12 733 个新的二次 APN 算例，其中包括 4 个首次被发现的具有最高线性度的算例，以及有限域 F_{2^9} 上 35 个新的二次 APN 算例。

2.2 间接生成法

2009 年，Edel 等[30]提出了转换构造法(switching construction method)，该方法的思想是通过改变已有 APN 算例的部分坐标函数来生成新的 APN 函数。利用该方法，Edel 等发现了有限域 F_{2^n}($n\leqslant 8$)上一些新的 APN 算例，其中包括 F_{2^6} 上一个非二次的 APN 算例以及一个具有最高线性度的二次 APN 算例。

在已有 APN 算例的基础上，通过增加若干项，生成新的 APN 算例也是一种常用方法，本文将该方法概括为加项构造法。Edel 等提出的转换构造法可以被看成是一种特殊的加项构造法，即在已有 APN 函数的基础上，增加一个布尔函数。加项构造法的另一种特殊应用是加“少项数”多项式。该应用的一个优点是得到的 APN 算例形式简洁。2020 年，Budaghyan 等[31]对 Edel 等发现的 $F_{2^{10}}$ 上的 APN 二项式算例进行加项，发现了 $F_{2^{10}}$ 上 3 个 APN 四项式算例。2021 年，Aleksandersen[32]对已知 APN 函数无限类在有限域 F_{2^8} 和 F_{2^9} 上的代表元进行加项，找到了 F_{2^8} 上一个新的 APN 四项式算例，并发现一些形式复杂(项数多)的 APN 算例等价于四项式和五项式。

同痕等价(isotopic equivalence)是有限半域中的概念。2021 年前后，Budaghyan 等[33-34]将同痕引入 APN 函数的研究中，提出了同痕移动(isotopic shift)的构造方法，生成了有限域 F_{2^9} 上 17 个新的二次 APN 算例。

2022 年，Beierle 等[35]提出修剪扩张法(trims and extensions)，其主要思想是通过将 F_{2^n} 上的 APN 算例限制在维数为 $n-1$ 的线性或仿射超平面上，或者增加两个 n 元布尔函数和一个 F_{2^n} 上向量值函数，利用有限域 F_{2^n} 上的 APN 算例构造 $F_{2^{n-1}}$ 或者 $F_{2^{n+1}}$ 上的二次 APN 算例。基于该方法，Beierle 等发现了 F_{2^8} 上 6 368 个新的二次 APN 算例。

2025 年,Taniguchi 等[36]提出了一个二次 APN 函数的间接构造方法,即对已有二次 APN 函数添加形如 $Tr_1^n(x)L(x)$ 的项,其中 $L(x)$ 是一个线性函数。运用该方法,Taniguchi 等在 F_{2^8} 上利用 APN 函数 x^3 构造了一个与之 CCZ 不等价的二次 APN 算例。

2025 年,Beierle 等[37]结合增加坐标函数和逐步扩大输入空间维数两种方法,生成了 F_{2^8} 上 3 775 599个不等价的二次 APN 算例。这一结果首次将 F_{2^8} 上的 APN 函数个数提升到了百万级。

此外,基于已知的等价类,并利用均匀抽样的测验方法,Beierle 等[37]估计 F_{2^8} 上不等价的 APN 函数的总数大约为 600 万。所以,设计搜索低维有限域上新的 APN 算例的有效方法是一个有重要理论价值的研究课题。

3　APN 函数无限类的构造

构造 CCZ 等价意义下新的 APN 函数无限类是极其困难的。到目前为止,APN 函数无限类构造包括单项式、单变元表示的多项式、双变元表示的多项式以及三变元表示的多项式。

2006 年之前,学者主要通过分析小域上的 APN 算例,然后进行归纳总结,在有限域 F_{2^n} 上得到了 6 类 APN 单项式无限类(CCZ 等价的意义下),其构造如表 1 所示。Dobbertin 猜想已知的单项式形式的 APN 函数无限类是完全的,即除了已有的 6 类,偶特征有限域上不存在其他的 APN 单项式[38]。

表 1　F_{2^n} 上已知的 APN 单项式无限类

Tab. 1　Known infinite families of APN monomials over F_{2^n}

类别	函数	条件	文献
Gold	x^{2^i+1}	$\gcd(i,n)=1$	[5,39]
Kasami	$x^{2^{2i}-2^i+1}$	$\gcd(i,n)=1$	[40-41]
Welch	x^{2^t+3}	$n=2t+1$	[42]
Niho	$x^{2^t+2^{t/2}-1}$, t 为偶数 $x^{2^t+2^{(3t+1)/2}-1}$, t 为奇数	$n=2t+1$	[38]
Inverse	$x^{2^{2t}-1}$	$n=2t+1$	[5,43]
Dobbertin	$x^{2^{4i}+2^{3i}+2^{2i}+2^i-1}$	$n=5i$	[44]

近年来,人们在二次 APN 多项式无限类的构造上取得了较大进展。2008 年,通过对 Edel 等发现的 $F_{2^{12}}$ 上一个 APN 二项式算例进行归纳总结,Budaghyan 等[45]首次得到了两个 APN 多项式无限类。2009 年,Browning 等[46]指出,从形如 $f(x)=x(Ax^2+Bx^q+Cx^{2q})+x^2(Dx^q+Ex^{2q})+Gx^{3q}$ 的多项式中能够得到大量 APN 函数,其中 $q=2^m$(Bartoli 等[47]在理论研究基础上对该结论进行了一些计算验证)。受此启发,2008 年,Budaghyan 等[48]构造了一个 APN 六项式无限类。加项构造法在构造 APN 多项式无限类的研究中同样展现了不错的效果。2009 年,Budaghyan 等[49-50]通过在 Gold 函数的基础上,增加 3 个特殊的布尔函数,得到了 3 个新的 APN 多项式无限类。Bracken 等对 Budaghyan 等构造的一类 APN 二项式进行“加项”,在 2008 年和 2011 年先后构造了一个新的 APN 三项式[51]和四项式无限类[52]。2020 年,利用同痕移动的构造方法,Budaghyan 等[33]给出了一个 APN 五项式无限类。同年,Budaghyan 等[31]对他们通过加项构造法得到的 3 个 $F_{2^{10}}$ 上的 APN 四项式算例展开分析,发现其中一个算例可以推广至无限类,进而构造了一类新的 APN 四项式无限类。2022 年,郑立景等[53]将 Budaghyan 等构造的一类 APN 四项式进行推广,给出了一种基于迹函数的构造方法,得到了一个新的 APN 四项式无限类。李康荃等[54]提出线性置换替换法,对 Bracken 等构造的 APN 四项式无限类进行推广,构造了一个新的 APN 多项式无限类。有限域 F_{2^n} 上单变元二次 APN 多项式无限类的构造有 11 类(CCZ 等价的意义下),如表 2 所示。

当 $n=2m$ 时,有限域 F_{2^n} 可以视作 $F_{2^m}\times F_{2^m}$,于是 F_{2^n} 上的多项式函数可表示为双变元的形式。双变元构造法是一种十分有效的方法。2011 年前后,周悦等[55]和 Carlet[56]利用向量 Bent 函数构造了 $F_{2^m}^2$ 上形如 $(xy,G(x,y))$ 的双变元表示的 APN 函数无限类。之后,多位学者通过选择不同的多项式 G,得到了新的 APN 函数无限类。2022 年,Göloğlu[57]利用射影多项式,提出双射影构造法,即考虑 $F_{2^m}^2$ 上形如 $(G_1(x,y),G_2(x,y))$ 的 APN 函数,其中 G_1 和 G_2 都是射影多项式,并得到了两个新的 APN 函数无限类。2021 年,李康荃等[54]对Göloğlu构造的双射影 APN 函数无限类应用加项构造法,构造了 $F_{2^m}^2$ 上一个新的 APN 函数无限类。2024 年,孙欢等[58]利用该方法得到了一类 CCZ 等价于 APN 函数无限类 C3 的双变元表示的 APN 函数。之后,施晨苗等[59]继续利用该方法构造了 $F_{2^m}^2$ 上一个新的 APN 函数无限类。2025 年,Göloğlu等[60]利用双射影构造法,得到了一个包含更多 CCZ 等价类的 APN 函数无限

表 2 F_{2^n}上已知的单变元表示的二次 APN 多项式无限类

Tab. 2 Known infinite families of quadratic APN polynomials over F_{2^n} in univariate form

类别	函数	条件	文献
C1、C2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk}+s}$	$n=pk$, $\gcd(k,p)=\gcd(s,pk)=1$, $p\in\{3,4\}$($p=3$ 时为 C1 类,$p=4$ 时为 C2 类), $i=sk \bmod p$, $m=p-i$, $n\geqslant 12$, $u\in F_{2^n}^*$ 为本原元	[45]
C3	$sx^{2^i(q+1)}+x^{2^i+1}+x^{q(2^i+1)}+cx^{2^iq+1}+c^qx^{2^i+q}+x^{q+1}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$, $c\in F_{2^n}$, $s\in F_{2^n}\setminus F_q$, $x^{2^i+1}+cx^{2^i}+c^qx+1$ 不存在解 x 使得 $x^{q+1}=1$	[48]
C4	$x^3+a^{-1}Tr_1^n(a^3x^9)$	$a\neq 0$	[49]
C5	$x^3+a^{-1}Tr_3^n(a^3x^9+a^6x^{18})$	$3\mid n$, $a\neq 0$	[50]
C6	$x^3+a^{-1}Tr_3^n(a^6x^{18}+a^{12}x^{36})$	$3\mid n$, $a\neq 0$	[50]
C7	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k$, $\gcd(k,3)=\gcd(s,3k)=1$, $v,w\in F_{2^k}$, $vw\neq 1$, $3\mid(k+s)$, u 是 $F_{2^n}^*$中的本原元	[51-52]
C8	$a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+ax^{2^{2m}+2}+bx^{2^m+2}+(c^2+c)x^3$	$n=3m$, m 为奇数, $d=\gcd(2^m-1,2^{2m}+2^m+1)$, $U=\langle u^{d'(2m-1)}\rangle$, $u\in F_{2^n}$为本原元, d'、d 素数因子相同且与 $2^{2m}+2^m+1$ 素数因子幂次相同。$W=\{yu^j: 0\leqslant j\leqslant d'-1, y\in U\}$。$L(x)=ax^{2^{2m}}+bx^{2^m}+cx$ 满足: $\forall w\in W$, $L(w)\notin\{0,w\}$; 对不同的 v、$w\in W$, 若 $v^{2^i}L(w)+wL(v)^{2^i}\neq 0$, 有 $\frac{w^{2^i}L(v)+vL(w)^{2^i}}{v^{2^i}L(w)+wL(v)^{2^i}}\notin F_{2^m}^*$成立; n 为偶数时, $\lvert\{w^{-1}L(w): w\in W\}\cap F_{2^2}\rvert\leqslant 1$	[33]
C9	$x^3+a(x^{2^s+1})^{2^k}+bx^{3q}+c[x^{(2^s+1)q}]^{2^k}$	$n=2m=10$, $q=2^m$, $(a,b,c)=(\beta,1,0)$, $s=3$, $k=2$, $\beta\in F_{2^2}$ 为本原元; $n=2m$, $q=2^m$, m 为奇数, $3\nmid m$, $(a,b,c)=(\beta,\beta^2,1)$, $\beta\in F_{2^2}$为本原元, $s\in\{m-2,m,2m-1,(m-2)^{-1} \bmod n\}$	[30]
C10	$aTr_m^n(bx^{2^i+1})+a^qTr_m^n(cx^{2^s+1})$	$n=2m$, m 为奇数, $q=2^m$, $a\notin F_q$, $\gcd(i,n)=1$。①$s=n-i$, $c^{2^i}b^{-1}\notin F_{2^m}$; ②$s=3i$, b 为非立方元, $cb^{-2^{2i}+2^i-1}\in F_{2^m}^*$; ③$s=m-2i$, b 为非立方元, $c^{2^{2i}}b^{2^i-1}\in F_{2^m}^*$; ④$s=m+2i$, b 为非立方元, $cb^{2^i-1}\in F_{2^m}^*$; ⑤$s=m$, b 为非立方元, $c\notin F_{2^m}$; ⑥$i=1$, b 为非立方元, $s=(m-2)^{-1}\bmod n$, $c^{2^s-1}b^{-2^{2s}}\in F_{2^m}^*$	[53]
C11	$L(x)^{2^m+1}+vx^{2^m+1}$	$\gcd(s,m)=1$, $v\in F_{2^m}^*$, $\mu\in F_{2^{3m}}^*$, $L(x)=x^{2^{m+s}}+\mu x^{2^s}+x$ 置换 $F_{2^{3m}}$	[54]

类。F_{2^n}上双变元表示的二次 APN 多项式无限类的构造有 8 类(CCZ 等价的意义下),如表 3 所示。

类似地,当 $n=3m$ 时,有限域 F_{2^n}可以视作 $F_{2^m}\times F_{2^m}\times F_{2^m}$,于是 F_{2^n}上的多项式函数可表示为三变元的形式。2024 年,李康荃等[64]运用三射影构造法构造了一类新的 APN 函数无限类,如表 4 所示。

线性置换替换法本质上是先将已有的无限类表示为含线性置换的形式,再将其替换为其他的线性置换,从而得到新的无限类。通过选取不同的线性置换(或对一类线性置换取不同参数),这一方法可能生成较多不等价的算例,但从理论上完全确定符合条件的线性置换(或一类线性置换的具体参数)一般是困难的。

从已有的无限类构造结果可以看出,对于单变元及多变元表示的 APN 函数,利用加项构造法进行间接构造均具有一定的适用性。而双变元构造法中基于 Bent 函数构造 APN 无限类的结果仅局限于双变元表示的情形,对于更一般的多变元表示的情形,尚未有相关结果。

此外,基于双射影构造法的思想,通过三射影

表 3　F_{2^n}上已知的双变元表示的二次 APN 多项式无限类

Tab. 3　Known infinite families of quadratic APN polynomials over F_{2^n} in bivariate form

类别	函数	条件	文献
C12	$(xy, x^{2^k+1}+\alpha y^{(2^k+1)2^i})$	$\gcd(k,m)=1$, m 是偶数, α 是非立方元	[55]
C13	$(xy, x^{3\cdot 2^k+2^{2k}}+ax^{2^{2k}}y^{2^k}+by^{2^k+1})$	$\gcd(k,m)=1$, $x^{2^k+1}+ax+b$ 在 F_{2^m}中没有根	[61]
C14	$(xy, x^{2^i+1}+x^{2^{i+m/2}}y^{2^{m/2}}+bxy^{2^i}+cy^{2^i+1})$	m 是偶数, $\gcd(i,m)=1$, $(cx^{2^i+1}+bx^{2^i}+1)^{2^{m/2}+1}+x^{2^{m/2}+1}$在 F_{2^m}中没有根	[62]
C15	$(x^{q+1}+xy^q+\alpha y^{q+1}, x^{q^2+1}+\alpha x^{q^2}y+(1+\alpha)^q xy^{q^2}+\alpha y^{q^2+1})$	$k、m>0$, $\gcd(k,m)=1$, $q=2^k$, $\alpha\in F_{2^m}$, $x^{q+1}+x+\alpha$ 在 F_{2^m}中没有根	[57,63]
C16	$(x^{2^i+1}+xy^{2^i}+y^{2^i+1}, x^{2^{3i}}y+xy^{2^{3i}})$	$\gcd(3i,m)=1$, m 是奇数	[57]
C17	$(x^3+xy+xy^2+\alpha y^3, x^5+xy+\alpha x^2y^2+\alpha x^4y+(1+\alpha)^2xy^4+\alpha y^5)$	$\alpha\in F_{2^m}$, $x^3+x+\alpha$ 在 F_{2^m}中没有根	[54,63]
C18	$(x^{q+1}+By^{q+1}, x^ry+\frac{a}{B}xy^r)$	$0<k<m$, $q=2^k$, $r=2^{k+m/2}$, $m\equiv 2 \pmod 4$, $\gcd(k,m)=1$, $a\in F_{2^{m/2}}^*$, $B\in F_{2^m}$, B 是非立方元, $B^{q+r}\neq a^{q+1}$	[60]
C19	$(x^{q+1}+xy^q+y^{q+1}+\sum_{i=0}^{k-1}(xy)^{2^i}, x^{q^2+1}+x^{q^2}y+y^{q^2+1}+\sum_{i=0}^{k-1}[xy+(xy)^q]^{2^i})$	$q=2^k$, $\gcd(3k,m)=1$, 满足对 $a、b\in F_{2^m}^*$, $c=ab^{-1}+1$, $d=(ab^{-1})^{q+1}+ab^{-1}+1$, $e=(ab^{-1})^{q^2}+(ab^{-1})^{q^2+1}+1$, $P(x)=(c^qd^{-q}e+1)x^{q^2-1}+(b^{-q^2-q}\cdot d^{-q}e+1)\sum_{i=0}^{k-1}(ab)^{2^{i+k}}x^{2^{i+k}-1}+e(cd^{-1}+d^{-q})x^{q-1}+(b^{-q-1}d^{-1}e+1)\sum_{i=0}^{k-1}(ab)^{2^i}x^{2^i-1}+(ab^{-1})^{q^2}+d^{-1}e+1$ 在 F_{2^m}中没有根	[59]

表 4　F_{2^n}上已知的三变元表示的二次 APN 多项式无限类

Tab. 4　Known infinite families of quadratic APN polynomials over F_{2^n} in trivariate form

类别	函数	条件	文献
C20	$(x^{q+1}+x^qz+yz^q, x^qz+y^{q+1}, xy^q+y^qz+z^{q+1})$	$q=2^i$, $\gcd(7i,m)=1$, 多项式 $P(x,y)=x^{q^2+q+1}+xy^{q^2+q}+xy^q+x^{q^2+q}+x^qy^{q^2}+x^{q^2}y+y^{q^2+q+1}+y^{q^2+q}+y^{q^2}+y^q+1$ 在 $F_{2^m}^2$中没有根	[64]

构造法构造无限类是自然的。学者可类似推广得到四(多)射影构造法,需要注意的是,即使仅考虑平凡系数情形,在此构造方法下搜索 APN 算例的空间大小也将达到 2^{64}(超过 2^{64}),这使得在 F_{2^8}上进行完全搜索极为困难。

4　APN 函数的等价性

APN 函数的等价分类问题是其研究中的一个基础性重要课题。本节介绍低维有限域上算例的等价分类、无限类之间以及无限类内部函数的等价分类。

4.1　APN 算例的等价分类

2008 年,Brinkmann 等[65]对 $n\leqslant 5$ 时,有限域 F_{2^n}上的所有 APN 算例(都 CCZ 等价于一个幂函数)进行了完整分类。2020 年,余玉银等[66]利用矩阵构造法给出了当 $n\leqslant 9$ 时,有限域 F_{2^n}上系数落在 F_2 中的二次 APN 算例的完整分类。2009 年,Browning 等[46]给出了 F_{2^6}上所有二次 APN 算例。2012 年,Langevin 等[67]进一步对 F_{2^6}上所有代数次数不超过 3 的 APN 算例进行分类(CCZ 等价意义下一共 14 个,包含 13 个二次 APN 算例、1 个三次 APN 算例)。2023 年,Kalgin 等[68]利用二次函数的矩阵表示找到了 F_{2^7}上一个新的二次 APN 算例,并且证明他们的结果完成了有限域 F_{2^7}上所有二次 APN 算例的分类(CCZ 等价意义下一共488 个)。2022 年,Beierle 等[35]利用修剪扩张法以及 F_{2^7}上所有二次 APN 算例的分类结果,给出了 F_{2^8}

上所有具有最高线性度的二次 APN 算例的分类。2022 年，Beierle 等[69]分析了 F_{2^9} 上已知的二次 APN 置换算例的 CCZ 等价分类，得到了它们的 EA 等价类个数的下界。

4.2 CCZ 等价不变量

一般而言，理论上证明两个函数之间的 CCZ 等价关系是非常困难的。常用的方法是利用计算机测试两个函数在低维有限域上是否 CCZ 等价。其中判定码等价是常用的方法之一：设 α 是 F_{2^n} 的一个本原元，G、H 是 F_{2^n} 上任意两个函数，当且仅当 C_G 与 C_H 同构时，G 与 H CCZ 等价[46,51]，其中 C_G 是 G 所对应的线性码，校验矩阵为

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 0 & \alpha & \cdots & \alpha^{2^n-1} \\ G(0) & G(\alpha) & \cdots & G(\alpha^{2^n-1}) \end{bmatrix} \tag{6}$$

另一种主要的方法是利用计算机计算低维有限域上算例的 CCZ 等价不变量并进行比较。如果两个函数的 CCZ 等价不变量不相同，那么它们 CCZ 不等价；反之如果它们的 CCZ 等价不变量相同，则不能说明这两个函数之间的 CCZ 等价关系。

当前，已有不少 CCZ 等价不变量被提出，但不是所有不变量都有效，例如，差分谱显然无法用于判断两个 APN 函数之间的等价性。扩展 Walsh 谱也是一个常见的 CCZ 等价不变量，但它通常也不是一个高效的不变量。

2009 年，Edel 等[30]在研究有限域上 APN 幂函数无限类中的算例是否都不等价这一问题时，提出了两个 CCZ 等价不变量：Γ - 秩，Δ - 秩。其定义如下：

定义 7（Γ - 秩[30]） 设 G 是 F_{2^n} 上任意一个 APN 函数。对 a、$b\in F_{2^n}$，定义

$$\Gamma_G\cdot(a,b)=\{(x+a,G(x)+b):x\in F_{2^n}\} \tag{7}$$

$\mathrm{dev}(\Gamma_G)$ 是一个设计，其中点集是 $F_{2^n}^2$，区块集是 $\{\Gamma_G\cdot(a,b):a,b\in F_{2^n}\}$，称设计 $\mathrm{dev}(\Gamma_G)$ 关联矩阵的秩为 Γ - 秩。

定义 8（Δ - 秩[30]） 设 G 是 F_{2^n} 上任意一个 APN 函数。定义

$$D_G=\{(x+y,\ G(x)+G(y)):x,y\in F_{2^n}\} \tag{8}$$

$\mathrm{dev}(D_G)$ 是一个设计，其中点集是 $F_{2^n}^2$，区块集是 $\{D_G\cdot(a,b):a,b\in F_{2^n}\}$，称设计 $\mathrm{dev}(D_G)$ 关联矩阵的秩为 Δ - 秩。

不幸的是，计算 Γ - 秩和 Δ - 秩所需要消耗的内存非常高。当维数达到 10 时，计算 Γ - 秩需要大约 500 GB 的可用内存。需要注意的是，如果使用 MAGMA 编程实现这个方法，其计算结果在高维有限域上不一定准确。

2020 年，Budaghyan 等[70]给出了 APN 函数的另一个 CCZ 等价不变量，并且当函数是二次时，这一不变量的计算特别高效。其定义如下：

定义 9（Π_G[70]） 设 G 是 F_{2^n} 上任意一个 APN 函数。对任意 b、$c\in F_{2^n}$，定义

$$\Pi_G(b,c)=\{a\in F_{2^n}:\exists\ x\in F_{2^n}\quad \text{s.t. } D_a^cG(x)=b\} \tag{9}$$

其中，$D_a^cG(x)=G(x)+G(x+a)+G(a+c)$。多重集 $\Pi_G=\{|\Pi_G(b,c)|:b,c\in F_{2^n}\}$ 是一个 CCZ 等价不变量。

对于 n 最大到 11，Π_G 的计算是非常迅速的。然而，对于奇数 n，该不变量在区分不等价的函数时的效果较差：n 取 5、7、9、11 时，Π_G 只取两个不同的可能值[70]。

2025 年，周子健等[71]通过运用拓扑数据分析中的持续同调和图论工具，提出了 APN 函数的若干新 CCZ 等价不变量。其中部分不变量能够有效区分多个已知的 APN 函数，包括 F_{2^7} 上的 x^3 和 x^9 以及 F_{2^9} 上的 x^3 和 x^{33}（在此之前已有的 CCZ 等价不变量均无法区分这些函数），例如等价不变量 $\Sigma_{4,C}$。

定义 10（$\Sigma_{4,C}$[71]） 设 G 是 F_{2^n} 上任意一个 APN 函数，C_G 是 G 所对应的线性码，d_1 是 C_G 的极小重量。$V_{C,m}$ 表示 C_G 中由极小重量的码字构成的子集，即

$$V_{C,m}=\{c\in C_G:\ w_H(c)=d_1\} \tag{10}$$

$K_{C,m}$ 表示子集 $V_{C,m}$ 的关联单纯复形，$\Sigma_{4,C}$ 表示 $K_{C,m}$ 中所有长度为 4 的环的（顶点个数为 4 的完全子图）个数。

除了上述 CCZ 等价不变量，EA 等价的意义下还有许多不变量，参考文献[72 - 73]。

实际上，在区分不等价的二次 APN 函数时，将差分谱和扩展 Walsh 谱应用于对应的正交导数[74]变得有效。

定义 11（正交导数[74]） 设 $G:F_{2^n}\to F_{2^n}$，G 的正交导数定义为一个唯一的函数 $\pi_G:F_{2^n}\to F_{2^n}$，$\pi_G(0)=0$，满足对任意的 $a\in F_{2^n}\setminus\{0\}$，都有 $\pi_G(a)\neq 0$ 成立，并且对任意的 $x\in F_{2^n}$，都满足

$$Tr_1^n(\pi_G(a)D_a(x))=0 \tag{11}$$

其中，$D_a(x)=G(x)+G(x+a)+G(a)+G(0)$。

对于两个二次 APN 函数 g、h，如果它们是 CCZ 等价的，那么它们的正交导数 π_g 和 π_h 是仿

射等价的[74]。实际上,仿射等价(或者更一般的,CCZ 等价)能保持函数的差分谱。因此,如果 F_{2^n} 上的两个函数对应正交导数的差分谱不同,或者对应正交导数的扩展 Walsh 谱不同,那么这两个函数 CCZ 不等价。

计算正交导数的经典方法是试错(trial and error)法,该计算方法在 sboxU 的最新版本中已被实现[75](在 Linux 系统中使用 sage-math 运行)。但该算法的计算效率较低,其计算量随着维数的增加快速增大,因此如何提升正交导数的计算效率是研究高维数 APN 函数等价性的关键问题。

表 5 列出了 $F_{2^{10}}$ 上所有来自已知二次 APN 函数无限类中的算例对应正交导数的差分谱。

表 5　$F_{2^{10}}$ 上已知二次 APN 函数无限类中所有算例对应正交导数的差分谱

Tab. 5　Differential spectra of the corresponding ortho-derivatives of all instances from known infinite families of quadratic APN functions over $F_{2^{10}}$

类别	正交导数的差分谱
Gold – 1	{0: 595 386, 2: 416 361, 6: 35 805}
Gold – 2	{0: 713 031, 2: 211 761, 4: 92 070, 6: 15 345, 8: 5 115, 12: 10 230}
C3 – 1	{0: 629 331, 2: 330 336, 4: 72 540, 6: 13 020, 8: 2 325}
C3 – 2	{0: 628 401, 2: 329 871, 4: 75 330, 6: 12 555, 8: 1 395}
C4 – 1	{0: 633 636, 2: 322 701, 4: 75 045, 6: 13 980, 8: 1 905, 10: 285}
C4 – 2	{0: 630 216, 2: 327 081, 4: 76 215, 6: 12 150, 8: 1 665, 10: 195, 12: 30}
C9 – 1	{0: 636 306, 2: 315 018, 4: 82 335, 6: 11 715, 8: 2 145, 10: 33}
C9 – 2	{0: 637 701, 2: 313 131, 4: 80 910, 6: 14 415, 8: 1 395}
C9 – 3	{0: 626 541, 2: 330 336, 4: 79 515, 6: 10 230, 8: 930}
C10 – 1	{0: 640 491, 2: 304 296, 4: 89 280, 6: 13 020, 8: 465}
C10 – 2	{0: 624 216, 2: 334 986, 4: 76 725, 6: 11 160, 8: 465}
C13 – 1	{0: 635 314, 2: 317 626, 4: 80 290, 6: 11 780, 8: 2 480, 10: 62}
C13 – 2	{0: 631 811, 2: 322 617, 4: 80 197, 6: 11 098, 8: 1 674, 10: 155}
C13 – 3	{0: 633 733, 2: 320 695, 4: 78 399, 6: 12 803, 8: 1 736, 10: 186}
C13 – 4	{0: 641 514, 2: 307 706, 4: 81 375, 6: 14 880, 8: 1 705, 10: 372}
C13 – 5	{0: 634 260, 2: 321 036, 4: 76 353, 6: 13 857, 8: 1 767, 10: 279}
C13 – 6	{0: 630 664, 2: 324 942, 4: 78 647, 6: 11 842, 8: 1 364, 10: 31, 12: 31, 14: 31}
C15 – 1	{0: 637 701, 2: 313 131, 4: 80 910, 6: 14 415, 8: 1 395}
C15 – 2	{0: 626 541, 2: 330 336, 4: 79 515, 6: 10 230, 8: 930}
C16 – 1	{0: 624 216, 2: 334 986, 4: 76 725, 6: 11 160, 8: 465}
C16 – 2	{0: 640 491, 2: 304 296, 4: 89 280, 6: 13 020, 8: 465}
C17	{0: 634 041, 2: 320 166, 4: 78 420, 6: 13 020, 8: 1 830, 10: 60, 12: 15}
C19 – 1	{0: 631 911, 2: 323 421, 4: 78 495, 6: 11 775, 8: 1 725, 10: 210, 12: 15}
C19 – 2	{0: 632 286, 2: 322 566, 4: 78 540, 6: 12 675, 8: 1 320, 10: 165}
C19 – 3	{0: 636 591, 2: 316 371, 4: 78 720, 6: 13 740, 8: 1 935, 10: 165, 12: 30}

注意到 C9 中的两个 APN 算例与 C15 中两个 APN 算例对应正交导数的差分谱相同,C10 中的两个 APN 算例与 C16 中两个 APN 算例对应正交导数的差分谱相同,表 6 进一步给出这几个 APN 算例对应的正交导数的扩展 Walsh 谱。

显然,从表 5 ~ 6 中给出的实验数据可以看出,Gold 函数,APN 函数无限类 C3、C4、C9、C10、C13、C15、C16、C17、C19 属于不同的 CCZ 等价类。进一步,表 7 列出了 F_{2^9} 上所有来自已知二次 APN 函数无限类中的算例对应的正交导数的差分谱。

表6 $F_{2^{10}}$上已知二次 APN 函数无限类中对应正交导数差分谱相同的算例的对应正交导数扩展 Walsh 谱

Tab. 6 Extended Walsh spectra of the corresponding ortho-derivatives of those instances from known infinite families of quadratic APN functions over $F_{2^{10}}$ whose corresponding ortho-derivatives share the same differential spectra

类别	正交导数的扩展 Walsh 谱
C9 – 2	{0: 111 135, 8: 193 068, 16: 184 605, 24: 158 100, 32: 126 232, 40: 104 253, 48: 65 193, 56: 45 105, 64: 21 731, 72: 17 670, 80: 12 090, 88: 3 720, 96: 2 790, 104: 1 395, 120: 465}
C9 – 3	{0: 113 460, 8: 194 928, 16: 184 605, 24: 154 845, 32: 118 792, 40: 98 208, 48: 68 820, 56: 52 545, 64: 28 706, 72: 18 135, 80: 7 905, 88: 3 720, 96: 930, 104: 1 395, 112: 558}
C10 – 1	{0: 93 000, 8: 212 040, 16: 182 280, 24: 158 565, 32: 139 717, 40: 83 793, 48: 66 123, 56: 51 150, 64: 26 846, 72: 15 345, 80: 12 090, 88: 2 418, 96: 2 325, 112: 1 395, 120: 465}
C10 – 2	{0: 106 485, 8: 200 415, 16: 175 770, 24: 170 655, 32: 115 072, 40: 91 698, 48: 77 283, 56: 44 640, 64: 37 541, 72: 13 485, 80: 8 370, 88: 1 953, 96: 2 790, 104: 930, 112: 465}
C15 – 1	{0: 111 135, 8: 193 068, 16: 184 605, 24: 158 100, 32: 126 232, 40: 104 253, 48: 65 193, 56: 45 105, 64: 21 731, 72: 17 670, 80: 12 090, 88: 3 720, 96: 2 790, 104: 1 395, 120: 465}
C15 – 2	{0: 113 460, 8: 194 928, 16: 184 605, 24: 154 845, 32: 118 792, 40: 98 208, 48: 68 820, 56: 52 545, 64: 28 706, 72: 18 135, 80: 7 905, 88: 3 720, 96: 930, 104: 1 395, 112: 558}
C16 – 1	{0: 106 485, 8: 200 415, 16: 175 770, 24: 170 655, 32: 115 072, 40: 91 698, 48: 77 283, 56: 44 640, 64: 37 541, 72: 13 485, 80: 8 370, 88: 1 953, 96: 2 790, 104: 930, 112: 465}
C16 – 2	{0: 93 000, 8: 212 040, 16: 182 280, 24: 158 565, 32: 139 717, 40: 83 793, 48: 66 123, 56: 51 150, 64: 26 846, 72: 15 345, 80: 12 090, 88: 2 418, 96: 2 325, 112: 1 395, 120: 465}

从表7的实验数据可以看出，Gold 函数，APN 函数无限类 C4、C5、C6、C8、C11、C20 属于不同的 CCZ 等价类。

表7 F_{2^9}上已知二次 APN 函数无限类中所有算例对应正交导数的差分谱

Tab. 7 Differential spectra of the corresponding ortho-derivatives of all instances from known infinite families of quadratic APN functions over F_{2^9}

类别	正交导数的差分谱
Gold – 1	{0: 153 811, 2: 96 579, 6: 10 731, 8: 511}
Gold – 2	{0: 159 943, 2: 78 183, 4: 18 396, 6: 4 599, 8: 511}
C4	{0: 159 016, 2: 79 389, 4: 19 089, 6: 3 483, 8: 493, 10: 144, 12: 18}
C5	{0: 159 226, 2: 78 813, 4: 19 683, 6: 3 201, 8: 529, 10: 162, 12: 18}
C6	{0: 160 525, 2: 77 058, 4: 19 467, 6: 3 792, 8: 589, 10: 126, 12: 45, 14: 12, 16: 9}
C8	{0: 160 097, 2: 79 128, 4: 17 808, 6: 3 269, 8: 700, 10: 357, 12: 231, 14: 42}
C11 – 1	{0: 168 994, 2: 68 712, 4: 15 141, 6: 6 279, 8: 1 659, 10: 336, 12: 21, 14: 21, 16: 105, 18: 147, 20: 189, 24: 21, 26: 7}
C11 – 2	{0: 169 022, 2: 68 341, 4: 16 093, 6: 5 621, 8: 1 561, 10: 364, 12: 91, 14: 63, 16: 140, 18: 196, 20: 84, 22: 35, 24: 7, 26: 14}
C11 – 3	{0: 169 428, 2: 68 040, 4: 15 561, 6: 6 034, 8: 1 533, 10: 420, 12: 126, 14: 21, 16: 84, 18: 189, 20: 126, 22: 63, 26: 7}
C11 – 4	{0: 169 484, 2: 68 159, 4: 15 463, 6: 5 719, 8: 1 736, 10: 420, 12: 105, 14: 63, 16: 133, 18: 175, 20: 126, 22: 28, 24: 21}
C11 – 5	{0: 170 079, 2: 66 297, 4: 16 737, 6: 6 160, 8: 1 407, 10: 420, 12: 21, 14: 42, 16: 63, 18: 210, 20: 133, 22: 63}
C11 – 6	{0: 170 100, 2: 67 529, 4: 15 232, 6: 5 628, 8: 1 848, 10: 553, 12: 98, 14: 98, 16: 126, 18: 189, 20: 126, 22: 28, 24: 14}
C11 – 7	{0: 170 667, 2: 66 297, 4: 15 911, 6: 5 705, 8: 1 947, 10: 385, 12: 140, 14: 84, 16: 168, 18: 147, 20: 63, 22: 63, 24: 21, 26: 7}
C11 – 8	{0: 171 430, 2: 64 617, 4: 16 842, 6: 5 733, 8: 1 932, 10: 483, 12: 105, 14: 21, 16: 147, 18: 105, 20: 154, 22: 21, 24: 42}
C20 – 1	{0: 164 199, 2: 76 734, 4: 13 524, 6: 4 312, 8: 2 205, 12: 147, 16: 294, 18: 147, 20: 49, 22: 21}
C20 – 2	{0: 172 557, 2: 68 355, 4: 12 201, 6: 3 871, 8: 1 638, 10: 735, 12: 1 470, 14: 49, 16: 147, 18: 441, 20: 147, 42: 21}

4.3　APN 函数无限类的等价性理论证明

在 2008 年以前,学者对 APN 函数之间的 CCZ 等价性的理论研究主要集中在幂函数上。2016 年,Yoshiara[76] 利用 APN 幂函数的自同构群中的某些循环子群的共轭性质刻画了偶特征有限域上任意两个 APN 幂函数之间 CCZ 等价的充要条件。2008 年,Budaghyan 等[45] 首先证明了若 APN 函数无限类 C1、C2 与 Gold 函数(Kasami 函数)CCZ 等价,则它们与 Gold 函数(Kasami 函数)EA 等价;然后基于此结论,在理论上证明了 C1、C2 CCZ 不等价于已知的 APN 幂函数无限类。2009 年,Budaghyan 等[49] 通过证明当 $n \geqslant 7$ 时,F_{2^n} 上的 APN 多项式 $f(x) = x^3 + Tr_1^n(x^9)$ 与 Gold 函数 EA 不等价,理论上证明了其与 Gold 函数 CCZ 不等价,同时证明了 $f(x)$ 在 F_{2^7} 上与任意幂函数 CCZ 不等价,他们猜想当 $n \geqslant 7$ 时,$f(x)$ 仍然具有这一性质。之后,Budaghyan 等将 $f(x)$ 进行推广得到了 C4。2016 年,Yoshiara[76] 利用自同构群在图像上的双传递性质证明了如果一个二次 APN 函数与一个 APN 幂函数 CCZ 等价,那么它 EA 等价于某个 Gold 函数。此外,Yoshiara[77] 利用群理论证明了对于两个二次 APN 函数,CCZ 等价当且仅当 EA 等价。观察到 Yoshiara 的这两个结果可以将一个二次 APN 多项式函数与 APN 幂函数间的 CCZ 等价性问题转化为这个二次 APN 多项式函数与一个 Gold 函数之间的 EA 等价性问题。万前红等[78-79] 给出了 C1 ~ C7、C9 与任意 APN 幂函数 CCZ 不等价的理论证明,值得注意的是这证明了 Budaghyan 等提出的猜想。之后,施晨苗等[80-81] 继续利用这一观察给出了 C10、C19 与任意幂函数之间 CCZ 不等价的理论结果。

2022 年,Kaspers 等[82] 刻画了双变元表示的 APN 函数无限类 C12 内部函数 CCZ 等价的充要条件,首次给出了有限域 $F_{2^{2m}}$(m 是偶数)上 CCZ 不等价的 APN 函数总数的下界。此外,Kaspers 等[83] 刻画了 $F_{2^{2m}}$ 上的双变元表示的 APN 函数无限类 C13 内部函数 CCZ 等价的充要条件,首次从理论上证明了 $F_{2^{2m}}$ 上 CCZ 不等价的 APN 函数个数的下界随着维数的增加呈指数增长,这是一个非常有趣且重要的结果。2025 年,Göloğlu 等[60] 进一步发展双变元表示的 APN 函数之间的 CCZ 等价理论,借助群论框架刻画了在一定条件下,两个双射影 APN 函数 CCZ 等价的充要条件。Göloğlu 等进一步对双变元表示的 APN 函数无限类 C12、C13、C15、C16、C18 以及 Gold 函数完成了等价分类。此外,Göloğlu[84] 给出了在由自然群作用定义的一类等价关系意义下,(q,q) 双射影函数的分类理论结果。2024 年,Kölsch[85] 证明了当 3 不整除 m 时,$F_{2^{2m}}$ 上的双变元表示的 APN 函数无限类 C15 中非平凡系数的函数与平凡系数的函数 CCZ 等价,进一步利用双变元表示的 APN 函数等价性框架给出了 3 整除 m 的情况下,无限类 C15 内部函数的 CCZ 等价分类结果。2025 年,施晨苗等[86] 理论证明了李康荃等[64] 构造的两类三变元表示的 APN 函数无限类 CCZ 等价,并将判断双射影 APN 函数之间 CCZ 等价性的理论框架推广到三射影 APN 函数,进一步完成了无限类 C20 内部函数的 CCZ 等价分类。

尽管 APN 函数的等价性理论已经取得了丰硕成果,但目前仍缺乏针对单变元表示的 APN 多项式函数之间等价性判断的通用框架。此外,在多变元表示形式下,现有的等价性理论仅适用于双射影与三射影函数,因此进一步发展与完善现有的等价性理论,具有重要研究意义。

5　APN 函数的密码学性质

为保证加解密可行性并避免熵漏,密码函数通常须具备置换性质。代数次数和非线性度是衡量密码函数安全性的两个重要指标:代数次数反映函数抵抗高阶差分攻击的能力,在实际应用中应避免取值过低;而非线性度则用于评估函数抵抗线性攻击的能力,其值越高越好。因此,对 APN 函数的置换性质、代数次数和非线性度的研究,一直是密码函数研究中的重要课题,学者也已在此方向上取得了丰富的成果。

5.1　置换性质

在 CCZ 等价意义下构造新的 APN 置换无限类尤其困难。容易验证,当 n 是奇数时,F_{2^n} 上 6 类已知的 APN 单项式无限类皆为置换。而在非单项式 APN 置换的无限类构造方面,迄今仅有两类被提出。2008 年,Budaghyan 等[45] 首次构造出一类二项式 APN 置换无限类,即 C1。2022 年,Beierle 等[35] 运用修剪扩张法找到了 F_{2^9} 上两个二次 APN 置换算例。随后,Beierle 等[69] 在后续研究中将这两个算例统一表示为单一的三变元形式,即 $f(x,y,z) = (x^3 + uy^2z,\ y^3 + uxz^2,\ z^3 + ux^2y)$。然而,Bartoli 等[87] 利用有限域上代数几何的工具证明了当 $n > 9$ 时,该函数在有限域 F_{2^n} 上不包含 APN 置换。2024 年,李康荃等[64] 利用三射影构造法提出了另一类非单项式 APN 置换

无限类的构造,即C20(当 m 是奇数时)。值得注意的是,C20在 F_{2^9} 上的二次APN置换算例与Beierle等发现的两个二次APN置换算例在CCZ等价意义下是一致的。

当 n 是偶数时,F_{2^n} 上6类已知的APN单项式无限类都不是置换[88];此外,已知的APN多项式无限类在 F_{2^n} 上也都不是置换。

实际上,当有限域扩张次数为偶数时,APN置换的存在性问题即为著名的"大APN问题"——当 n 为偶数时,是否存在 F_{2^n} 上的APN置换?该问题自1993年被提出以来,就受到了学者的关注和研究,至今已公开30余年。

2006年,侯向东[89]利用群论知识证明了以下结果:

引理[89] 设 n 是偶数,给定 F_{2^n} 上一个置换 G,如果以下条件之一成立,则 G 不是APN。

1) $n\leqslant 4$;

2) G 是二次置换;

3) G 的系数在子域 $F_{2^{n/2}}$ 上。

定义12(组件函数[90]) 设函数 $G:F_{2^n}\to F_{2^n}$。函数 $G_b(x)=Tr_1^n(bG(x))$ 称为 G 的组件函数,其中 $b\in F_{2^n}$。

定义13(高原函数[91-92]) 设函数 $G:F_{2^n}\to F_{2^n}$。如果对固定的 $b\in F_{2^n}$,满足 $W_G(a,b)\in\{0,\pm 2^s\}$,其中 $s\geqslant n/2$,则称组件函数 $G_b(x)=Tr_1^n(bG(x))$ 是高原函数。

2006年,Berger等[90]证明了不存在组件函数都是高原函数的APN置换。2011年前后,Pasalic等[93]、李永强等[94-95]证明了某些幂函数加上线性函数形式的函数一定不是APN置换。2017年,Calderini等[96]发现只要函数的组件函数中包含二次函数,则该函数一定不是APN置换。因此,这样的APN置换的代数次数最低只可能是3次。当然,也可能不存在3次APN置换。2018年,Carlet[97]证明了偶扩张上的幂函数一定不是APN置换。2024年,Musukwa等[98]利用二阶导给出了 F_{2^8} 上3次APN置换存在的必要条件。

关于"大APN问题"唯一一个正面结果是2010年,Dillon等[99]找到了一个 F_{2^6} 上的APN置换,这引起学者的广泛关注,其一元多项式表示为:$u^{45}x^{60}+u^{41}x^{58}+u^{43}x^{57}+u^{4}x^{56}+u^{50}x^{54}+u^{20}x^{53}+u^{45}x^{52}+u^{20}x^{51}+u^{23}x^{50}+u^{36}x^{49}+u^{56}x^{48}+u^{21}x^{46}+u^{5}x^{45}+u^{21}x^{44}+u^{28}x^{43}+u^{3}x^{42}+u^{59}x^{41}+u^{58}x^{40}+u^{57}x^{39}+u^{53}x^{38}+u^{37}x^{37}+u^{40}x^{36}+u^{18}x^{35}+u^{41}x^{34}+u^{54}x^{33}+u^{3}x^{32}+u^{49}x^{30}+u^{41}x^{29}+u^{42}x^{28}+u^{50}x^{27}+u^{53}x^{26}+u^{58}x^{25}+u^{9}x^{24}+x^{23}+u^{28}x^{22}+u^{3}x^{21}+u^{21}x^{20}+u^{52}x^{19}+u^{60}x^{17}+u^{59}x^{16}+u^{10}x^{15}+u^{42}x^{13}+u^{8}x^{12}+u^{35}x^{11}+u^{44}x^{10}+u^{45}x^{8}+u^{8}x^{7}+u^{61}x^{6}+u^{59}x^{5}+u^{20}x^{4}+u^{12}x^{3}+u^{37}x^{2}+u^{2}x$。其中 u 是本原多项式 $x^6+x^4+x^3+x+1$ 在 F_{2^6} 上的根。该APN置换现在被称为"Dillon置换"。Dillon置换CCZ等价于一个被称为"Kim函数"的APN三项式,即 $x^3+x^{10}+ux^{24}$。到目前为止,$n>6$ 情况下的"大APN问题"仍然没有解决。2012年,Langevin等[67]结合计算机程序指出,F_{2^6} 上的所有二次APN置换一定CCZ等价于Dillon置换。2016年,Perrin等[100]通过逆向工程对Dillon置换进行分析,提出了"蝴蝶结构"的概念。之后,Canteaut等[101]将其推广至"广义蝴蝶结构":

定义14(广义蝴蝶结构[101]) 设 R 是 F_{2^n} 上双变元表示的多项式,满足对 F_{2^n} 中所有 y,$R_y:x\mapsto R(x,y)$ 都是 F_{2^n} 上的置换,$F_{2^n}^2$ 的闭蝴蝶结构 V_R 定义为

$$V_R(x,y)=(R(x,y),R(y,x)) \tag{12}$$

$F_{2^n}^2$ 的开蝴蝶结构 H_R 定义为

$$H_R(x,y)=(R_{R_y^{-1}(x)}(y),R_y^{-1}(x)) \tag{13}$$

其中,$R_y(x)=R(x,y)$,$R_y^{-1}(R_y(x))=x$。

2019年,Canteaut等[102]证明了从广义蝴蝶结构中无法得到新的APN置换。2021年,李康荃等[103]利用Hasse-Weil界给出了Kim函数一个推广形式(广义Kim函数)APN性质的完全刻画。在此基础上,Chase等[104]证明了从广义Kim函数中无法得到新的APN置换。2021年,Beierle等[105]发现所有已知的APN置换均满足"线性自等价"这一特殊性质(即对于APN置换 F,存在非平凡线性置换 A 和 B 使得 $F\circ A=B\circ F$)。结合递归树搜索方法,他们利用计算机程序说明了有限域 F_{2^6} 上满足线性自等价性质的APN置换均等价于Dillon置换。

因为Dillon置换是从一个已知APN函数通过CCZ等价得到的,所以研究"大APN问题"的一种途径是在已有APN函数的CCZ等价类中寻找APN置换。2020年前后,Göloğlu等[106-107]利用指数和等理论,证明了当扩张次数是偶数时,Gold函数和Kasami函数无法CCZ等价于置换。2023年,Budaghyan等[88]证明了3到1的二次APN函数在双偶维数的有限域上无法CCZ等价于置换。2025年,Bénéteau等[108]基于APN函数的Bent分支数给出了其CCZ等价于置换的一个必要条件。

5.2　代数次数

在 6 类已知的 APN 单项式无限类中,Gold 函数的代数次数是 2;Kasami 函数的代数次数是 $i+1$;Welch 函数的代数次数是 3;t 是偶数时,Niho 函数的代数次数是$(t+2)/2$, t 是奇数时,其代数次数是 $t+1$;Inverse 函数的代数次数是 $n-1$;Dobbertin 函数的代数次数是$i+3$。所有已知的 APN 多项式无限类的代数次数都是 2。对于小域上的 APN 函数算例,非二次的 APN 函数仅仅只有 2009 年 Edel 等[30]利用转换构造法找到的 F_{2^6} 上 1 个三次 APN 函数算例。

2018 年,Budaghyan 等[109]猜想 F_{2^n} 上不存在代数次数为 n 的 APN 函数,并利用转换构造法的思想,证明了特殊情况下该猜想的正确性。

有限域 F_{2^n} 上已知 APN 函数的代数次数最大值为

$$\deg(n)=\begin{cases} n-1 & \gcd(n,2)=1 \\ \dfrac{n}{2} & \gcd(n,4)=4,\ n\geqslant 8 \text{ 或 } n=10 \\ \dfrac{n}{2}-1 & \gcd(n,4)=2,\ n\geqslant 12 \\ \dfrac{n}{2}+1 & n\leqslant 6 \end{cases} \tag{14}$$

特别地,所有已知的 APN 函数无限类(非单项式)都是 2 次的。一个自然的问题是:对于非单项式的 APN 函数,其代数次数最大能达到多少。另外,能否构造出代数次数大于 2 的 APN 函数无限类也是一个值得研究的困难问题。

5.3　非线性度

学者普遍认为 APN 函数的非线性度不会太差,但无法从理论上证明或者解释该现象。也就是说,给出 APN 函数非线性度的一个下界应该是一件困难的事情。2021 年,Carlet[110]利用 Walsh 变换得到了 F_{2^n} 上包括单项式 APN 函数无限类在内的满足特定条件的 APN 函数 G 的非线性度下界的一个结果:

$$N(G)\geqslant 2^{n-1}-\frac{1}{2}\sqrt[4]{2^{4n-1}-2^{3n}} \tag{15}$$

对于有限域 F_{2^n} 到自身的映射,AB 函数是非线性度最优的函数。不过 AB 函数仅仅存在于 n 是奇数的情形。可以证明[111] AB 函数一定是 APN 函数,反之未必。但当 n 是奇数时,所有的二次 APN 函数都是 AB 函数,也就是说,此时所有二次 APN 函数是同时抵抗差分攻击和线性攻击最优的密码函数。

计算已有 APN 函数无限类的非线性度,尤其是 Walsh 谱分布一般是一件困难的事情。目前已知的 APN 函数无限类的 Walsh 谱分布大多与 Gold 函数的 Walsh 谱分布一致。因此称 Walsh 谱分布与 Gold 函数一致的 APN 函数为经典的。在 APN 单项式中,偶扩张有限域上只有 3 类,即 Gold 函数、Kasami 函数和 Dobbertin 函数,其中 Gold 函数和 Kasami 函数都是经典的。2022 年,Budaghyan 等[112]根据实验数据猜测了 Dobbertin 函数的 Walsh 谱分布,显示 Dobbertin 函数不是经典的。对于 APN 多项式,2007 年至 2019 年,Bracken 等[113-115]、屈龙江等[116-117]、Anbar 等[118]陆续计算出一些已有 APN 函数无限类的 Walsh 谱分布,发现已有 APN 函数无限类(非单项式)都是经典的。2023 年,Kölsch 等[119]证明所有 3 到 1 的 APN 函数都是经典的,这为计算 APN 函数无限类的非线性度提供了便利。2020 年之后构造的非 3 到 1 的 APN 函数无限类的非线性度取值问题到目前为止还没有被解决。不过从实验数据上来看,这些 APN 函数无限类都是经典的。也就是说,在偶扩张有限域上所有的 APN 函数无限类(非单项式)都是经典的。对于小域上的 APN 算例,非经典的结果也很少。2009 年,Edel 等[30]利用转换构造法找到了 F_{2^6} 上 1 个非经典的 APN 算例。2022 年,Beierle 等[29]利用递归树搜索找到了 F_{2^8} 上 4 个非经典的算例。一个值得探究的问题是能否构造非经典谱的 APN 多项式无限类。

6　APN 函数的应用

本节简单介绍 APN 函数在编码理论和组合设计中的一些应用,包括由 APN 函数构造参数良好的线性码和 t-设计。

6.1　由 APN 函数构造线性码

在编码理论中,APN 函数可以用来构造性质优良的线性码。1998 年,Carlet 等[19]首次介绍了 APN 性质在纠错码构造上的应用:设 G 是 F_{2^m} 上的一个 APN 函数,满足 $G(0)=0$,利用 G 的图作为校验矩阵的组成部分,即:

$$\boldsymbol{P}_G=\begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ G(1) & G(\alpha) & G(\alpha^2) & \cdots & G(\alpha^{n-1}) \end{bmatrix} \tag{16}$$

其中,$n=2^m-1$。由 $\boldsymbol{P}_G$ 定义的线性码 C_G 的参数为$[2^n-1,2^n-2n-1,5]$。该线性码可以检测最多 4 个错误,纠正最多 2 个错误。

利用 APN 幂函数,并选择合适的定义集可以

构造线性码。2016 年,丁存生[120]利用 F_{2^n} 上的 Gold APN 函数 $G(x)=x^{2^i+1}$,其中 $\gcd(i,n)=1$,通过定义集 $D=\{G(x)+G(x+1)+1:x\in F_{2^n}\}$ 给出了一个 1-重二进制线性码,其参数为 $[2^{n-1},n-1,2^{n-2}]$。

此外,利用 APN 幂函数,可以通过迹函数定义以下形式的长为 2^n 的线性码:$\{(Tr_1^n(aG(x)+bx))_{x\in F_{2^n}}:a,b\in F_{2^n}\}$。

2020 年,丁存生等[121]利用 F_{2^n}(n 为奇数)上的 Gold APN 函数和 Kasami APN 函数等定义了如下线性码:$\{(Tr_1^n(aG(x)+bx)+c)_{x\in F_{2^n}}:a,b\in F_{2^n},c\in F_2\}$。该线性码的参数是 $[2^n,2n+1,2^{n-1}-2^{(n-1)/2}]$,其对偶码参数是 $[2^n,2^n-n-1,6]$。2022 年,项灿等[122]对由 Gold APN 函数生成的线性码 $\{(Tr_1^n(aG(x)+bx+c))_{x\in F_{2^n}}:a,b,c\in F_{2^n}\}$,运用缩短技术的方法,得到了一些参数是已知最优的二进制线性码,例如 $[28,7,12]$ 线性码、$[13,6,4]$ 线性码以及 $[13,7,4]$ 线性码等。

利用 APN 函数,通过迹函数构造线性码的一些进展可参见文献[123-127]。

近年来,APN 函数构造研究取得了较大进展,在此基础之上,利用新的 APN 函数构造具有更优参数的线性码已成为一个有价值的研究方向。

6.2 由 APN 函数构造 t-设计

在组合设计中,可通过相对差分集将 APN 函数用于构造一类重要的组合设计——半对称设计:设 G 是 F_{2^m} 上的一个 APN 函数,由点集 $F_{2^n}\times F_{2^n}$ 和区块集 $\{\{(x+a,G(x)+b):x\in F_{2^n}\}:a,b\in F_{2^n}\}$ 可定义一个 2-$(2^{2n},2^n,\lambda)$ 设计,该设计具有对称性和可计算性。

以有限域为点集,利用 APN 幂函数构造合适的区块集,其关联结构可给出一些 t-设计。2020 年,唐春明[128]利用 APN 函数给出了 3-设计的两种构造。第一类由 Kasami APN 函数得到:设 $x^{2^{2i}-2^i+1}$ 是 F_{2^n}(n 为奇数)上的 Kasami 函数,其中 $\gcd(i,n)=1$。定义

$$B=F_{2^n}\setminus\{((x+1)^s+x^s+1)^{\frac{1}{2^i+1}}:x\in F_{2^n}\} \tag{17}$$

其中,$s=2^{2i}-2^i+1$,则关联结构 $(F_{2^n},GA_1(B))$ 是一个 3-$(2^n,2^{n-1},2^{2n-3}-2^{n-1})$ 设计,其中 GA_1 是 F_{2^n} 上的一次一般仿射群。第二类 3-设计由 Gold APN 函数导出:设 x^{2^i+1} 是 F_{2^n}(n 是大于等于 4 的奇数)上的 Gold 函数,其中 $\gcd(i,n)=1$。定义

$$B_s=\{(x+1)^s+x^s:x\in F_{2^n}\} \tag{18}$$

其中,$s=2^i+1$,则关联结构 $(F_{2^n},GA_1(B_s))$ 是 3-$(2^n,2^{n-1},2^{n-2}-1)$ 设计。

实际上,一些 t-设计可由线性码导出。2020 年,丁存生等[121]通过由 APN 函数构造的参数为 $[2^n,2n+1,2^{n-1}-2^{(n-1)/2}]$($n$ 为奇数)的线性码及参数为 $[2^n,2^n-n-1,6]$ 的对偶码,运用 Assmus-Mattson 定理给出了 3-$(2^n,k,\lambda)$ 设计的构造。2020 年,唐春明等[129]推广了 Assmus-Mattson 定理,在此基础上证明了以下结果:设 G 是 F_{2^n} 上 2-值差分的且振幅是 s 的 Plateaued 函数,则线性码 $C_G=\{(Tr_1^n(aG(x)+bx)+c)_{x\in F_{2^n}}:a,b\in F_{2^n},c\in F_2\}$ 及其对偶码 $C_G^\perp$ 支持 2-设计。这一结果表明当 G 是 AB 函数时(n 为奇数),即当 G 是具有经典 Walsh 谱的 APN 函数时,C_G 和 $C_G^\perp$ 支持 2-设计。2023 年,Meidl 等[130]证明了对于 F_{2^n}(n 为偶数)上具有经典 Walsh 谱的 APN 函数 G,若 G CCZ 等价于一个二次函数,则由式(6)生成的线性码 C_G 和 $C_G^\perp$ 支持 2-设计。

利用 APN 函数构造线性码再得到 t-设计的一些进展可参见文献[125,131]。

基于 APN 函数构造的丰富成果,如何进一步构造更多结构复杂、类型丰富的组合设计(例如 t-设计,$t>2$)是一个值得深入探究的重要课题。

7 总结与展望

总体而言,国内外学者在 APN 函数研究领域取得了显著进展,通过多种不同的生成和构造方法得到了许多新的 APN 函数(无限类),并解决了 APN 函数的一系列相关问题,包括 APN 函数的等价性以及密码性质等。然而,该领域仍有许多关键问题未被解决,例如“大 APN 问题”,即当偶数 $n\geqslant 8$ 时,是否存在 F_{2^n} 上的 APN 置换? Dobbertin 关于偶特征有限域上不存在其他 APN 单项式的猜想是否正确? 能否从理论上给出 APN 函数个数的渐进界? 如何构造高次(如三次、四次)APN 多项式无限类? 此外,如何构造非经典谱的 APN 多项式无限类也是亟待解决的问题。进一步解决这些问题仍然具有重要的理论价值与实际意义。

参考文献(References)

[1] 李超, 屈龙江, 周悦. 密码函数的安全性指标分析[M]. 北京: 科学出版社, 2011.
LI C, QU L J, ZHOU Y. Analysis of security indicators for cryptographic functions[M]. Beijing: Science Press, 2011. (in Chinese)

[2] 冯登国, 吴文玲. 分组密码的设计与分析[M]. 北京: 清

华大学出版社, 2000.
FENG D G, WU W L. Designs and analysis of block ciphers[M]. Beijing: Tsinghua University Press, 2000. (in Chinese)
[3] 李超, 孙兵, 李瑞林. 分组密码的攻击方法与实例分析[M]. 北京: 科学出版社, 2010.
LI C, SUN B, LI R L. Attack methods and case analysis of block ciphers[M]. Beijing: Science Press, 2010. (in Chinese)
[4] BIHAM E, SHAMIR A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991, 4(1): 3 – 72.
[5] NYBERG K. Differentially uniform mappings for cryptography[C]// Proceedings of Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, 1994: 55 – 64.
[6] 屈龙江, 陈玺, 牛泰霖, 等. 有限域上低差分函数研究进展[J]. 计算机研究与发展, 2018, 55(9): 1931 – 1945.
QU L J, CHEN X, NIU T L, et al. Recent progress in low differential uniformity functions over finite fields[J]. Journal of Computer Research and Development, 2018, 55(9): 1931 – 1945. (in Chinese)
[7] BARTOLI D, STANICA P. Infinite families of APN permutations in constrained trivariate classes over $\mathbb{F}_{2^m}$[EB/OL]. (2026 – 03 – 16)[2026 – 03 – 25]. https://arxiv.org/abs/2603.15146.
[8] CZERWINSKI I, POTT A. On large Sidon sets[J]. Journal of Combinatorial Theory, Series A, 2026, 220: 106129.
[9] THORNBURGH D. Uniform exclude distributions of Sidon sets[EB/OL]. (2024 – 07 – 16)[2025 – 11 – 20]. https://arxiv.org/abs/2407.11783.
[10] BARTOLI D, CALDERINI M, MARINO G, et al. Zeros of special polynomials and their impact on a class of APN functions[EB/OL]. (2025 – 11 – 06)[2025 – 11 – 20]. https://arxiv.org/html/2511.04193v1.
[11] MIHAILA M, THORNBURGH D. On lower bounds for the distances between APN functions[EB/OL]. (2025 – 09 – 02)[2025 – 11 – 20]. https://arxiv.org/abs/2509.02280.
[12] NAGY G P. On the minimum Hamming distance between vectorial Boolean and affine functions[J]. Cryptography and Communications, 2025, 17(6): 1703 – 1720.
[13] CARLET C, PICEK S. On the exponents of APN power functions and Sidon sets, sum-free sets, and Dickson polynomials[J]. Advances in Mathematics of Communications, 2023, 17(6): 1507 – 1525.
[14] NAGY G P. Sidon sets, thin sets, and the nonlinearity of vectorial Boolean functions[J]. Journal of Combinatorial Theory, Series A, 2025, 212: 106001.
[15] THORNBURGH D. On generalizing cryptographic results to Sidon sets in $\mathbb{F}_2^n$[EB/OL]. (2025 – 01 – 19)[2025 – 11 – 20]. https://arxiv.org/abs/2501.11184.
[16] MASSEY J. Shift-register synthesis and BCH decoding[J]. IEEE Transactions on Information Theory, 1969, 15(1): 122 – 127.
[17] RONJOM S, HELLESETH T. A new attack on the filter generator[J]. IEEE Transactions on Information Theory, 2007, 53(5): 1752 – 1758.
[18] MATSUI M. Linear cryptanalysis method for DES cipher[C]// Proceedings of Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, 1994: 386 – 397.
[19] CARLET C, CHARPIN P, ZINOVIEV V. Codes, bent functions and permutations suitable for DES-like cryptosystems[J]. Designs, Codes and Cryptography, 1998, 15(2): 125 – 156.
[20] BUDAGHYAN L, CARLET C, POTT A. New classes of almost bent and almost perfect nonlinear polynomials[J]. IEEE Transactions on Information Theory, 2006, 52(3): 1141 – 1152.
[21] JEONG J, KOO N, KWON S. On the functions which are CCZ-equivalent but not EA-equivalent to quadratic functions over $\mathbb{F}_p^n$[J]. Finite Fields and Their Applications, 2025, 103: 102574.
[22] CARLET C. Boolean functions for cryptography and coding theory[M]. Cambridge: Cambridge University Press, 2020.
[23] EDEL Y, KYUREGHYAN G, POTT A. A new APN function which is not equivalent to a power mapping[J]. IEEE Transactions on Information Theory, 2006, 52(2): 744 – 747.
[24] WENG G B, TAN Y, GONG G. On quadratic almost perfect nonlinear functions and their related algebraic object[EB/OL]. (2013 – 06 – 06)[2025 – 11 – 20]. https://cacr.uwaterloo.ca/techreports/2013/cacr2013 – 18.pdf.
[25] YU Y Y, WANG M S, LI Y Q. A matrix approach for constructing quadratic APN functions[J]. Designs, Codes and Cryptography, 2014, 73(2): 587 – 600.
[26] YU Y Y, PERRIN L. Constructing more quadratic APN functions with the QAM method[J]. Cryptography and Communications, 2022, 14(6): 1359 – 1369.
[27] XIONG H, QU L J, LI C, et al. Some results on the differential functions over finite fields[J]. Applicable Algebra in Engineering, Communication and Computing, 2014, 25(3): 189 – 195.
[28] SUDER V. Antiderivative functions over $\mathbb{F}_{2^n}$[J]. Designs, Codes and Cryptography, 2017, 82(1/2): 435 – 447.
[29] BEIERLE C, LEANDER G. New instances of quadratic APN functions[J]. IEEE Transactions on Information Theory, 2022, 68(1): 670 – 678.
[30] EDEL Y, POTT A. A new almost perfect nonlinear function which is not quadratic[J]. Advances in Mathematics of Communications, 2009, 3(1): 59 – 81.
[31] BUDAGHYAN L, HELLESETH T, KALEYSKI N. A new family of APN quadrinomials[J]. IEEE Transactions on Information Theory, 2020, 66(11): 7081 – 7087.
[32] ALEKSANDERSEN M H. Experimental construction of optimal cryptographic functions by expansion[D]. Bergen: The University of Bergen, 2021.
[33] BUDAGHYAN L, CALDERINI M, CARLET C, et al. Constructing APN functions through isotopic shifts[J]. IEEE Transactions on Information Theory, 2020, 66(8): 5299 – 5309.
[34] BUDAGHYAN L, CALDERINI M, CARLET C, et al. Generalized isotopic shift construction for APN functions[J]. Designs, Codes and Cryptography, 2021, 89(1): 19 – 32.
[35] BEIERLE C, LEANDER G, PERRIN L. Trims and extensions of quadratic APN functions[J]. Designs, Codes and Cryptography, 2022, 90(4): 1009 – 1036.
[36] TANIGUCHI H, POLUJAN A, POTT A, et al. Changing almost perfect nonlinear functions on affine subspaces of small codimensions[EB/OL]. (2025 – 01 – 07)[2025 – 11 –

20]. https://arxiv.org/abs/2501.03922.

[37] BEIERLE C, LANGEVIN P, LEANDER G, et al. Millions of inequivalent quadratic APN functions in eight variables[EB/OL]. (2025-08-06)[2025-11-20]. https://arxiv.org/abs/2508.04644.

[38] DOBBERTIN H. Almost perfect nonlinear power functions on GF(2^n): the niho case[J]. Information and Computation, 1999, 151(1/2): 57-72.

[39] GOLD R. Maximal recursive sequences with 3-valued recursive cross-correlation functions[J]. IEEE Transactions on Information Theory, 1968, 14(1): 154-156.

[40] JANWA H, WILSON R M. Hyperplane sections of fermat varieties in P^3 in char. 2 and some applications to cyclic codes[C]//Proceedings of the 10th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 1993: 180-194.

[41] KASAMI T. The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes[J]. Information and Control, 1971, 18(4): 369-394.

[42] DOBBERTIN H. Almost perfect nonlinear power functions on GF(2^n): the Welch case[J]. IEEE Transactions on Information Theory, 1999, 45(4): 1271-1275.

[43] BETH T, DING C. On almost perfect nonlinear permutations[C]//Proceedings of Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, 1994: 65-76.

[44] DOBBERTIN H. Almost perfect nonlinear power functions on GF(2^n): a new case for n divisible by 5[C]//Proceedings of the fifth International Conference on Finite Fields and Applications, 2001: 113-121.

[45] BUDAGHYAN L, CARLET C, LEANDER G. Two classes of quadratic APN binomials inequivalent to power functions[J]. IEEE Transactions on Information Theory, 2008, 54(9): 4218-4229.

[46] BROWNING K A, DILLON J K, KIBLER R E, et al. APN polynomials and related codes[J]. Journal of Combinatorics, Information & System Sciences: A Quarterly International Scientific Journal, 2009, 34(1/2/3/4): 135-159.

[47] BARTOLI D, GRIMALDI G G, STANICA P. On the classification of Dillon's APN hexanomials[EB/OL]. (2025-11-02)[2025-11-20]. https://arxiv.org/abs/2511.01003.

[48] BUDAGHYAN L, CARLET C. Classes of quadratic APN trinomials and hexanomials and related structures[J]. IEEE Transactions on Information Theory, 2008, 54(5): 2354-2357.

[49] BUDAGHYAN L, CARLET C, LEANDER G. Constructing new APN functions from known ones[J]. Finite Fields and Their Applications, 2009, 15(2): 150-159.

[50] BUDAGHYAN L, CARLET C, LEANDER G. On a construction of quadratic APN functions[C]//Proceedings of the IEEE Information Theory Workshop, 2009: 374-378.

[51] BRACKEN C, BYRNE E, MARKIN N, et al. New families of quadratic almost perfect nonlinear trinomials and multinomials[J]. Finite Fields and Their Applications, 2008, 14(3): 703-714.

[52] BRACKEN C, BYRNE E, MARKIN N, et al. A few more quadratic APN functions[J]. Cryptography and Communications, 2011, 3(1): 43-53.

[53] ZHENG L J, KAN H B, LI Y J, et al. Constructing new APN functions through relative trace functions[J]. IEEE Transactions on Information Theory, 2022, 68(11): 7528-7537.

[54] LI K Q, ZHOU Y, LI C L, et al. Two new infinite classes of APN functions[EB/OL]. (2021-05-18)[2025-11-20]. https://arxiv.org/abs/2105.08464.

[55] ZHOU Y, POTT A. A new family of semifields with 2 parameters[J]. Advances in Mathematics, 2013, 234: 43-60.

[56] CARLET C. Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions[J]. Designs, Codes and Cryptography, 2011, 59(1): 89-109.

[57] GÖLOĞLU F. Biprojective almost perfect nonlinear functions[J]. IEEE Transactions on Information Theory, 2022, 68(7): 4750-4760.

[58] SUN H, YUE Q, JIA X. Note on Budaghyan and Carlet's almost perfect nonlinear functions[J]. Finite Fields and Their Applications, 2024, 93: 102339.

[59] SHI C M, PENG J, ZHENG L J. A new infinite family of bivariate APN multinomials[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2025, E108.A(9): 1327-1330.

[60] GÖLOĞLU F, KÖLSCH L. Equivalences of biprojective almost perfect nonlinear functions[J]. Combinatorial Theory, 2025, 5(3): 7.

[61] TANIGUCHI H. On some quadratic APN functions[J]. Designs, Codes and Cryptography, 2019, 87(9): 1973-1983.

[62] CALDERINI M, BUDAGHYAN L, CARLET C. On known constructions of APN and AB functions and their relation to each other[J]. Rad HAZU, Matematičke Znanosti, 2021, 25: 79-105.

[63] CALDERINI M, LI K Q, VILLA I. Extending two families of bivariate APN functions[J]. Finite Fields and Their Applications, 2023, 88: 102190.

[64] LI K Q, KALEYSKI N. Two new infinite families of APN functions in trivariate form[J]. IEEE Transactions on Information Theory, 2024, 70(2): 1436-1452.

[65] BRINKMANN M, LEANDER G. On the classification of APN functions up to dimension five[J]. Designs, Codes and Cryptography, 2008, 49(1): 273-288.

[66] YU Y Y, KALEYSKI N, BUDAGHYAN L, et al. Classification of quadratic APN functions with coefficients in $\mathbb{F}_2$ for dimensions up to 9[J]. Finite Fields and Their Applications, 2020, 68: 101733.

[67] LANGEVIN P, SAYGI Z, SAYGI E. Classification of APN cubics in dimension 6 over GF(2)[EB/OL]. (2012-02-21)[2025-11-20]. https://langevin.univ-tln.fr/project/apn-6/apn-6.html.

[68] KALGIN K, IDRISOVA V. The classification of quadratic APN functions in 7 variables and combinatorial approaches to search for APN functions[J]. Cryptography and Communications, 2023, 15(2): 239-256.

[69] BEIERLE C, CARLET C, LEANDER G, et al. A further study of quadratic APN permutations in dimension nine[J]. Finite Fields and Their Applications, 2022, 81: 102049.

[70] BUDAGHYAN L, CARLET C, HELLESETH T, et al. On the distance between APN functions[J]. IEEE Transactions on Information Theory, 2020, 66(9): 5742-5753.

[71] ZHOU Z J, LI K Q, ZHOU Y. Topological invariants for linear codes and APN functions[J]. IEEE Transactions on Information Theory, 2025, 71(9): 6771 – 6784.

[72] KALEYSKI N S. Invariants for EA- and CCZ-equivalence of APN and AB functions[J]. Cryptography and Communications, 2021, 13(6): 995 – 1023.

[73] GILLOT V, LANGEVIN P. On known APNs[EB/OL]. (2026 – 01 – 16)[2026 – 03 – 25]. https://arxiv.org/abs/2601.11247.

[74] CANTEAUT A, COUVREUR A, PERRIN L. Recovering or testing extended-affine equivalence[J]. IEEE Transactions on Information Theory, 2022, 68(9): 6187 – 6206.

[75] lpp-crypto. sboxU[EB/OL]. [2025 – 11 – 20]. https://github.com/lpp-crypto/sboxU.

[76] YOSHIARA S. Equivalences of power APN functions with power or quadratic APN functions[J]. Journal of Algebraic Combinatorics, 2016, 44(3): 561 – 585.

[77] YOSHIARA S. Equivalences of quadratic APN functions[J]. Journal of Algebraic Combinatorics, 2012, 35(3): 461 – 475.

[78] WAN Q H, QU L J, LI C. On equivalence between known polynomial APN functions and power APN functions[J]. Finite Fields and Their Applications, 2021, 71: 101762.

[79] WAN Q H, LI C. On equivalence between two known families of APN polynomial functions and APN power functions[J]. Cryptography and Communications, 2022, 14(1): 161 – 182.

[80] SHI C M, PENG J, ZHENG L J, et al. On the equivalence between a new family of APN quadrinomials and the power APN functions[J]. Cryptography and Communications, 2023, 15(2): 351 – 363.

[81] SHI C M. On CCZ-equivalence between a family of brivariate APN polynomials and power functions[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2025, E108.A(9): 1275 – 1280.

[82] KASPERS C, ZHOU Y. A lower bound on the number of inequivalent APN functions[J]. Journal of Combinatorial Theory, Series A, 2022, 186: 105554.

[83] KASPERS C, ZHOU Y. The number of almost perfect nonlinear functions grows exponentially[J]. Journal of Cryptology, 2021, 34(1): 4.

[84] GÖLOĞLU F. Classification of (q, q)-biprojective APN functions[J]. IEEE Transactions on Information Theory, 2023, 69(3): 1988 – 1999.

[85] KÖLSCH L. On a recent extension of a family of biprojective APN functions[J]. Finite Fields and Their Applications, 2024, 99: 102494.

[86] SHI C M, PENG J, KAN H B, et al. On CCZ-equivalence of two new APN functions in trivariate form[J]. Designs, Codes and Cryptography, 2025, 93(10): 4595 – 4625.

[87] BARTOLI D, TIMPANELLA M. On a conjecture on APN permutations[J]. Cryptography and Communications, 2022, 14(4): 925 – 931.

[88] BUDAGHYAN L, IVKOVIC I, KALEYSKI N. Triplicate functions[J]. Cryptography and Communications, 2023, 15(1): 35 – 83.

[89] HOU X D. Affinity of permutations of $\mathbf{F}_{2^n}$[J]. Discrete Applied Mathematics, 2006, 154(2): 313 – 325.

[90] BERGER T P, CANTEAUT A, CHARPIN P, et al. On almost perfect nonlinear functions over $\boldsymbol{F}_{2^n}$[J]. IEEE Transactions on Information Theory, 2006, 52(9): 4160 – 4170.

[91] CANTEAUT A, CARLET C, CHARPIN P, et al. Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions[C]//Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques, 2000: 507 – 522.

[92] ZHANG X M, ZHENG Y L. GAC: the criterion for global avalanche characteristics of cryptographic functions[M]// MAURER H, CALUDE C, SALOMAA A. The Journal of Universal Computer Science. Berlin: Springer, 1996: 320 – 337.

[93] PASALIC E, CHARPIN P. Some results concerning cryptographically significant mappings over GF(2^n)[J]. Designs, Codes and Cryptography, 2010, 57(3): 257 – 269.

[94] LI Y Q, WANG M S. On EA-equivalence of certain permutations to power mappings[J]. Designs, Codes and Cryptography, 2011, 58(3): 259 – 269.

[95] LI Y Q, WANG M S. Permutation polynomials EA-equivalent to the inverse function over GF(2^n)[J]. Cryptography and Communications, 2011, 3(3): 175 – 186.

[96] CALDERINI M, SALA M, VILLA I. A note on APN permutations in even dimension[J]. Finite Fields and Their Applications, 2017, 46: 1 – 16.

[97] CARLET C. Characterizations of the differential uniformity of vectorial functions by the Walsh transform[J]. IEEE Transactions on Information Theory, 2018, 64(9): 6443 – 6453.

[98] MUSUKWA A, SALA M, VILLA I, et al. On second-order derivatives of Boolean functions and cubic APN permutations in even dimension[J]. Mediterranean Journal of Mathematics, 2024, 21(3): 116.

[99] BROWNING K A, DILLON J F, MCQUISTAN M T, et al. An APN permutation in dimension six[J]. International Conference on Finite Fields and Applications; Finite Fields: Theory and Applications, 2010, 518: 33 – 42.

[100] PERRIN L, UDOVENKO A, BIRYUKOV A. Cryptanalysis of a theorem: decomposing the only known solution to the big APN problem[C]//Advances in Cryptology – CRYPTO 2016, 2016: 93 – 122.

[101] CANTEAUT A, DUVAL S, PERRIN L. A generalisation of Dillon's APN permutation with the best known differential and nonlinear properties for all fields of size 2^{4k+2}[J]. IEEE Transactions on Information Theory, 2017, 63(11): 7575 – 7591.

[102] CANTEAUT A, PERRIN L, TIAN S Z. If a generalised butterfly is APN then it operates on 6 bits[J]. Cryptography and Communications, 2019, 11(6): 1147 – 1164.

[103] LI K Q, LI C L, HELLESETH T, et al. A complete characterization of the APN property of a class of quadrinomials[J]. IEEE Transactions on Information Theory, 2021, 67(11): 7535 – 7549.

[104] CHASE B, LISOŇĚK P. Kim-type APN functions are affine equivalent to gold functions[J]. Cryptography and Communications, 2021, 13(6): 981 – 993.

[105] BEIERLE C, BRINKMANN M, LEANDER G. Linearly self-equivalent APN permutations in small dimension[J]. IEEE Transactions on Information Theory, 2021, 67(7): 4863 – 4875.

[106] GÖLOĞLU F, LANGEVIN P. Almost perfect nonlinear

families which are not equivalent to permutations[J]. Finite Fields and Their Applications, 2020, 67: 101707.

[107] GÖLOĞLU F, PAVLŮ J. On CCZ-inequivalence of some families of almost perfect nonlinear functions to permutations[J]. Cryptography and Communications, 2021, 13(3): 377 – 391.

[108] BÉNÉTEAU S H, GOLUBOFF N, KÖLSCH L, et al. On the Walsh spectra of quadratic APN functions[EB/OL]. (2025 – 10 – 22)[2025 – 11 – 20]. https://arxiv.org/abs/2510.12008.

[109] BUDAGHYAN L, CARLET C, HELLESETH T, et al. On upper bounds for algebraic degrees of APN functions[J]. IEEE Transactions on Information Theory, 2018, 64(6): 4399 – 4411.

[110] CARLET C. On the properties of the Boolean functions associated to the differential spectrum of general APN functions and their consequences[J]. IEEE Transactions on Information Theory, 2021, 67(10): 6926 – 6939.

[111] BUDAGHYAN L. Construction and analysis of cryptographic functions[M]. Switzerland: Springer, 2014.

[112] BUDAGHYAN L, CALDERINI M, CARLET C, et al. On two fundamental problems on APN power functions[J]. IEEE Transactions on Information Theory, 2022, 68(5): 3389 – 3403.

[113] BRACKEN C, BYRNE E, MARKIN N, et al. On the Walsh spectrum of a new APN function[C]//Proceedings of IMA International Conference on Cryptography and Coding, 2007: 92 – 98.

[114] BRACKEN C, BYRNE E, MARKIN N, et al. Determining the nonlinearity of a new family of APN functions[C]// Proceedings of International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, 2007: 72 – 79.

[115] BRACKEN C, ZHA Z B. On the Fourier spectra of the infinite families of quadratic APN functions[J]. Advances in Mathematics of Communications, 2009, 3(3): 219 – 226.

[116] TAN Y, QU L J, LING S, et al. On the Fourier spectra of new APN functions[J]. SIAM Journal on Discrete Mathematics, 2013, 27(2): 791 – 801.

[117] QU L J, TAN Y, LI C. On the Walsh spectrum of a family of quadratic APN functions with five terms[J]. Science China Information Sciences, 2014, 57(2): 1 – 7.

[118] ANBAR N, KALAYCI T, MEIDL W. Determining the Walsh spectra of Taniguchi's and related APN-functions[J]. Finite Fields and Their Applications, 2019, 60: 101577.

[119] KÖLSCH L, KRIEPKE B, KYUREGHYAN G M. Image sets of perfectly nonlinear maps[J]. Designs, Codes and Cryptography, 2023, 91(1): 1 – 27.

[120] DING C S. A construction of binary linear codes from Boolean functions[J]. Discrete Mathematics, 2016, 339(9): 2288 – 2303.

[121] DING C S, TANG C M. Combinatorial t-designs from special functions[J]. Cryptography and Communications, 2020, 12(5): 1011 – 1033.

[122] XIANG C, TANG C M, DING C S. Shortened linear codes from APN and PN functions[J]. IEEE Transactions on Information Theory, 2022, 68(6): 3780 – 3795.

[123] DING C S. Linear codes from some 2-designs[J]. IEEE Transactions on Information Theory, 2015, 61(6): 3265 – 3275.

[124] TANG D, CARLET C, ZHOU Z C. Binary linear codes from vectorial Boolean functions and their weight distribution[J]. Discrete Mathematics, 2017, 340(12): 3055 – 3072.

[125] OLMEZ O. A link between combinatorial designs and three-weight linear codes[J]. Designs, Codes and Cryptography, 2018, 86(4): 817 – 833.

[126] DING C S, LI C L, LI N, et al. Three-weight cyclic codes and their weight distributions[J]. Discrete Mathematics, 2016, 339(2): 415 – 427.

[127] ZENG X Y, SHAN J Y, HU L. A triple-error-correcting cyclic code from the Gold and Kasami-Welch APN power functions[J]. Finite Fields and Their Applications, 2012, 18(1): 70 – 92.

[128] TANG C M. Infinite families of 3-designs from APN functions[J]. Journal of Combinatorial Designs, 2020, 28(2): 97 – 117.

[129] TANG C M, DING C S, XIONG M S. Codes, differentially δ-uniform functions, and t-designs[J]. IEEE Transactions on Information Theory, 2020, 66(6): 3691 – 3703.

[130] MEIDL W, POLUJAN A A, POTT A. Linear codes and incidence structures of bent functions and their generalizations[J]. Discrete Mathematics, 2023, 346(1): 113157.

[131] DING C S, LI C J. Infinite families of 2-designs and 3-designs from linear codes[J]. Discrete Mathematics, 2017, 340(10): 2415 – 2431.