DOI:10.7544/issn1000-1239.2018.20180159
55(9):1931-1945,2018

有限域上低差分函数研究进展

屈龙江　陈　玺　牛泰霖　李　超
(国防科技大学文理学院　长沙　410073)
(ljqu_happy@hotmail.com)

Recent Progress in Low Differential Uniformity Functions over Finite Fields

Qu Longjiang, Chen Xi, Niu Tailin, and Li Chao
(*College of Liberal Arts and Sciences, National University of Defense Technology, Changsha* 410073)

Abstract　To prevent differential attack on the cipher, cryptographic functions are required to have low differential uniformity. Perfect nonlinear (PN) functions, almost perfect nonlinear (APN) functions and differentially 4-uniform permutations are the most important cryptographic functions with low differential uniformity. Here we survey the recent main research results about cryptographic functions with low differential uniformity such as PN functions, APN functions and differentially 4-uniform permutations. First, we recall the connections between PN functions and the mathematical objects such as the semifield, which survey the known constructions of PN functions and the pseudo-planar functions. Second, the properties and judgement of APN functions are analyzed. We also list the known constructions of APN functions and recall the inequivalent results between them. Third, we summarize the known results on the constructions of differentially 4-uniform permutations and discuss their equivalence. Then, we recall the applications of low differential uniformity functions in the design of actual ciphers. Lastly, we propose some research problems on cryptographic functions with low differential uniformity.

Key words　perfect nonlinear (PN) function; almost perfect nonlinear (APN) function; differentially 4-uniform permutation; low differential uniformity function; S-box

摘　要　为了抵抗差分密码攻击,密码算法设计希望使用低差分函数.完全非线性函数(perfect nonlinear function, PN 函数)、几乎完全非线性函数(almost perfect nonlinear function, APN 函数)和 4 差分置换(differentially 4-uniform permutition)是最重要的几类低差分函数(low differential uniformity function).总结了近年来在 PN 函数、APN 函数和 4 差分置换等低差分函数研究方面的主要进展.1)回顾了 PN 函数与半域等数学对象的联系,梳理了 PN 函数的已有构造以及伪平面函数的构造;2)分析了 APN 函数的性质与判定,总结了 APN 函数的已有构造以及它们之间等价性分析方面的结果;3)对于 4 差分置换,总结了其已有构造及其等价性分析结果;4)介绍了低差分函数在实际密码算法设计中的应用;5)对低差分函数的下一步研究进行了展望.

关键词　完全非线性函数;几乎完全非线性函数;4 差分置换;低差分函数;S-盒

中图法分类号　TP309.7

收稿日期:2018-03-08;**修回日期**:2018-06-13

基金项目:国家重点研发计划项目(2017YFB0802001);国家自然科学基金优秀青年科学基金项目(61722213)
This work was supported by the National Key Research and Development Program of China (2017YFB0802001) and the National Natural Science Foundation of China for Excellent Young Scientists (61722213).

密码学是网络空间安全和信息安全的核心,作为一门综合性学科,其发展与国家安全息息相关,也与政治、军事、外交等国家事务密不可分.对称密码学是密码学的重要分支,主要研究对象包括分组密码、流密码、Hash 函数等.对称密码算法是各国政府、军事和银行等重要部门保护核心敏感信息的主要算法.密码函数包含布尔函数与向量函数(S-盒)两大类,是构成序列密码、分组密码和 Hash 函数等对称密码算法的核心组件,而且往往是唯一的非线性组件,其密码学性质的好坏对基于该组件设计的密码算法的安全性有着至关重要的影响[1-9],相应的密码算法对于各种已知攻击的抵抗性可以由它所使用密码函数的相应密码学指标来衡量.

差分攻击是攻击迭代分组密码最有效的方法之一.差分攻击的基本思想是通过分析明文对差值对密文对差值的影响来恢复某些密钥比特.一个密码算法抵抗差分攻击的能力与其采用的密码函数抵抗差分攻击的能力密切相关,而后者可以用差分均匀度来衡量.一个密码函数的差分均匀度越小,其抵抗差分攻击的能力就越强.有限域 F_q 上的低差分函数主要包括完全非线性函数(perfect nonlinear function, PN 函数)、几乎完全非线性函数(almost perfect nonlinear function, APN 函数)和差分均匀度为 4 的函数(4-uniform function, 4 差分函数)等.当有限域的特征为奇数时,PN 函数、APN 函数分别达到最优、次优的差分均匀度;而在偶特征的有限域上,差分均匀度必然为偶数,此时 APN 函数、4 差分函数分别达到最优、次优的差分均匀度.由于绝大多数密码算法用的密码函数是定义在偶特征有限域上的,所以在密码研究中,APN 函数、4 差分函数受到了更多关注.但是需要注意的是,PN 函数、APN 函数和 4 差分函数等低差分函数之间有着十分紧密的联系,很多构造是相互启发的.

为了抵抗差分攻击、线性攻击和插值攻击等分析方法,一个理想的 S-盒通常应同时具有低差分均匀度,高非线性度和高代数次数等多种良好密码学性质.由于在代替置换网络(substitution-permutation-network, SPN)结构分组密码 S-盒的设计中,为了避免熵泄露,一般要求分组密码中使用的向量函数是置换;而为了软硬件实现时具有较高的效率,又希望其定义在二元域的偶数维扩域上,因此相比一般的 4 差分函数,偶扩张上的 4 差分置换的构造与分析近年来受到了更多研究和关注.另外,由于具有对合性质的函数可以提高硬件实现的效率,这一性质在研究中也受到了较多关注.因此,本文主要总结了 PN 函数、APN 函数和偶扩张上的 4 差分置换方面的研究进展.最后,需要说明的是,低差分函数在编码和通信领域中也有广泛应用,比如满足特定性质的密码函数可以用来构造性能优良的纠错码和跳频码[10],并且所构造的码参数与原有密码函数的非线性度等安全性指标密切相关.

1 基本概念和知识

1.1 基本概念

设 F_q 为 $q=p^n$ 元有限域,其中素数 p 为其特征,则 F_q 可以看作 F_p 上的 n 维向量空间.事实上,设 $f(x)\in F_p[x]$ 是一个 n 次不可约多项式,α 为其在分裂域中的一个根,则:

$$F_{p^n}=\{a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1}\mid a_0,a_1,\cdots,a_{n-1}\in F_p\},$$

于是映射 $\varphi:\sum_{i=0}^{n-1}a_i\alpha^i\rightarrow(a_0,a_1,\cdots,a_{n-1})$ 是从线性空间 F_{p^n} 到线性空间 F_p^n 的同构映射.因此本文接下来将不加说明地把 F_{p^n} 和 F_p^n 交替使用.

如果 F 为有限域 F_{p^n} 到其自身的映射,则它可以表示为 F_{p^n} 上的单变元多项式:

$$F(x)=\sum_{j=0}^{p^n-1}\delta_j x^j.$$

设整数 j 的 p 进制展开为 $j=\sum_{s=0}^{n-1}j_s p^s$,$0\leqslant j_s\leqslant p-1$,定义 j 的 p 重量为 $w_p(j)=\sum_{s=0}^{n-1}j_s$,则 F 的代数次数可以由其单变元表示直接定义.

定义 1. 代数次数.设 F 为有限域 F_{p^n} 到其自身的映射,其单变元表示为

$$F(x)=\sum_{j=0}^{p^n-1}\delta_j x^j,$$

那么 F 的代数次数定义为

$$\deg F=\max\{w_p(j)\mid j=0,1,\cdots,p^n-1,\delta_j\neq 0\}.$$

需要指出的是,这个概念和常见的"多项式次数"的概念有所不同,比如 F_{2^n} 上的单项式 $F(x)=x^3$ 的多项式次数为 3,但它的代数次数为 2(因为 $3=2+1=(11)_2$).如果一个函数的代数次数不超过 1,则称其为仿射函数.不含常数项的仿射函数,称为线性函数或者线性化多项式.

设 F 为有限域 F_{p^n} 到其自身的映射.若 F_{p^n} 中的每一个元素在其像集中都恰好出现一次,则称 F 为 F_{p^n} 上的置换.若函数 G 满足 $G(F(x))=x$,则称 G

为置换 F 的逆.若置换 F 的逆恰为其自身,即有 $F(F(x))=x$,则称 F 是对合函数.

定义 2. 差分均匀度.设 F 为有限域 F_q 到其自身的映射,对于任意 $(a,b)\in F_q^*\times F_q$,F 在 (a,b) 处的差分值定义为

$$\delta_F(a,b)=\sharp\{x\in F_q\mid F(x+a)-F(x)=b\}. \quad (1)$$

多重集 $\{*\delta_F(a,b)\mid(a,b)\in F_q^*\times F_q*\}$ 称为 F 的差分谱.F 的差分均匀度定义为

$$\Delta_F=\max_{(a,b)\in F_q^*\times F_q}\delta_F(a,b),$$

称 F 的差分均匀度为 Δ_F 或称 F 为 Δ_F-差分(一致性)函数.

一个密码函数的差分均匀度越小,其抵抗差分攻击的能力就越强.特别地,若 $\Delta_F=1$,则称其为完全非线性函数(PN 函数);若 $\Delta_F=2$,则称其为几乎完全非线性函数(APN 函数).当有限域的特征为偶数时,注意到若 x_0 是式(1)的解,则 x_0+a 必然也是式(1)的解,这表明式(1)的解必然成对出现,因此差分均匀度必然为偶数.这表明在偶特征的有限域上,APN 函数、4 差分函数分别达到最优、次优的差分均匀度.事实上,若 q 为偶数,则 F_q 上的一个函数的差分均匀度可以取从 2 到 q 的所有可能的偶数;若 q 为奇数,则 F_q 上的一个函数的差分均匀度可以取除 $q-1$ 外,从 1 到 q 的其他任一整数[11].另外,需要说明的是,差分均匀度和完全非线性函数均可以推广定义到一般的交换群上,相关工作这里不再赘述,感兴趣的读者可以参阅文献[12].

定义 3. 非线性度.设 F 为有限域 F_{2^n} 到其自身的映射,其 Walsh 变换 $F^W:F_{2^n}^*\times F_{2^n}\to C$ 定义为

$$F^W(a,b)=\sum_{x\in F_{2^n}}(-1)^{Tr_1^n(aF(x)+bx)},$$

其中,$Tr_1^n(x)=x+x^2+x^{2^2}+\cdots+x^{2^{n-1}}$ 为 F_{2^n} 上的绝对迹函数.

多重集 $\{*F^W(a,b)\mid(a,b)\in F_{2^n}^*\times F_{2^n}*\}$ 称为 F 的 Walsh 谱.而 F 的扩展 Walsh 谱定义为

$$\{*\mid F^W(a,b)\mid\mid(a,b)\in F_{2^n}^*\times F_{2^n}*\}.$$

F 的非线性度定义为

$$NL(F)=2^{n-1}-\max_{(a,b)\in F_{2^n}^*\times F_{2^n}}\{\mid F^W(a,b)\mid\}/2.$$

当 n 为奇数时,非线性度 $NL(F)$ 的上界为 $2^{n-1}-2^{(n-1)/2}$,达到该最大值的函数称为几乎 Bent 函数(almost Bent function, AB 函数);当 n 为偶数时,人们猜想非线性度 $NL(F)$ 的上界为 $2^{n-1}-2^{n/2}$.若能达到该值,则称之为达到已知最优非线性度的函数.

1.2 CCZ 等价与 EA 等价

新的低差分函数的构造是密码函数研究中的重要问题,它涉及到这些函数之间的等价性问题.最主要的等价性有 2 个:CCZ 等价和 EA 等价.

定义 4. 扩展仿射等价.设 F,G 为 2 个 F_q 到自身的函数,若存在仿射置换函数 l_1,l_2 和仿射函数 l_3,使得 $F=l_1\circ G\circ l_2+l_3$,则称 F 和 G 扩展仿射等价(extended affine equivalent, EA 等价).特别地,若 $l_3=0$,则称 F 和 G 仿射等价.

定义 5. CCZ 等价.F_q 上函数 F 的图定义为 $\{(x,F(x)):x\in F_q\}$,若 2 个函数的图仿射等价,则称这 2 个函数 CCZ 等价(Carlet-Charpin-Zinoviev equivalent, CCZ 等价).

容易验证 EA 等价意味着 CCZ 等价;但是反之不然.CCZ 等价保持函数的差分均匀度和非线性度(更准确地说,是保持函数的扩展 Walsh 谱),而 EA 等价还保持代数次数(如果函数的代数次数≥2).一般而言,在理论上证明 2 个无限函数类是否 CCZ 等价是一个非常困难的问题,而判断 EA 等价则要简单许多.

由于在理论上分析不同函数之间的 CCZ 等价性非常困难,实践上人们一般通过计算机计算一些 CCZ 等价不变量,比如差分均匀度、扩展 Walsh 谱、Γ-秩、Δ-秩和各种形式的自同构群等.如果 2 个函数有不同的 CCZ 等价不变量,则它们一定不等价;反之则不能判断.另外,一个无限函数类的差分均匀度、扩展 Walsh 谱等 CCZ 等价不变量的有效计算研究在理论上和应用上都是很有意义的,特别是扩展 Walsh 谱的计算.这不仅是因为由扩展 Walsh 谱可以决定出非线性度,还因为:由 APN 函数可以构造性能优良的线性码,并且 APN 函数的扩展 Walsh 谱对应于该线性码的重量分布,而线性码的重量分布是线性码的一个重要参数,利用其可以有效计算译码算法的错误概率.

2 PN 函数

2.1 性质与判定

PN 函数有一些等价判别准则.

定理 1. 设 $F:F_{p^n}\to F_{p^n}$,则 3 个条件等价:

1) F 为 PN 函数,即对任意 $a,b\in F_{p^n}$,$a\neq0$,方程 $F(x+a)-F(x)=b$ 至多有 1 个解;

2) 对任意的 $0\neq a\in F_{p^n}$,函数 D_aF 为 F_{p^n} 上的置换多项式,其中 $D_aF=F(x+a)-F(x)$;

3) $D=\{(x,F(x))\mid x\in F_{p^n}\}$ 为 $F_{p^n}\times F_{p^n}$ 中的 $(p^n,p^n,p^n,1)$-相对差集.

除此之外,有限域上的 PN 函数还可以用来构造达到 Welch 界的最优码本(codebook),量子测量、量子计算中有重要作用的最优互无偏基(mutually unbiased base, MUB)以及压缩感知中的最优相干矩阵(coherence matrix)等. 由于本文主要是从密码学的角度论述,这些联系就不再赘述了,感兴趣的读者可以参阅文献[13-15].

特别地,对于二次 PN 函数,也称为 Demobowski-Ostrom(DO)型函数,有等价判定准则:

定理 2. 设 $F:F_{p^n}\to F_{p^n}$ 且为二次函数,则 2 个条件等价:

1) F 为 PN 函数,即对任意 $0\neq a\in F_{p^n}$,函数 $D_aF=F(x+a)-F(x)$ 为 F_{p^n} 上的线性化置换多项式;

2) $(F_{p^n},+,*)$ 为有限交换预半域,其中"$*$"为 F_{p^n} 上定义的乘法:

$$x*y=(F(x+y)-F(x)-F(y))/2.$$

预半域与域相比,可能失去结合律且可能不含单位元.

2008 年 Kyureghyan 和 Pott 证明了 2 个 PN 函数 CCZ 等价当且仅当它们 EA 等价[16]. 因此相比于一般函数的 CCZ 等价性判断,PN 函数 CCZ 等价性判断的难度略小一些,但仍很困难.

2012 年翁国标和曾祥勇刻画了 DO 型 PN 函数的映射性质[17].

定理 3[17]. 设 F 为 $F_{p^n}[x]$ 中的 DO 型多项式,则 F 为 PN 函数当且仅当其像集中的每一个非零元均有 2 个原像,即 F 是 2 到 1 的映射.

2.2 已有构造

2005 年以前,有限域 F_{p^n} 上 PN 函数的研究主要集中于幂函数(单项式),包括 2 类(不等价的)PN 幂函数:

1) Demobowski-Ostrom 幂函数[18]:

$$\pi_1(x)=x^{p^t+1},$$

其中,整数 $t\geqslant 0$,$n/\gcd(n,t)$ 为奇数;

2) Coulter-Mattews 幂函数[19]:

$$\pi_2(x)=x^{\frac{3^k+1}{2}},$$

其中,整数 $p=3$,k 为奇数且 n 和 k 的最大公约数 $\gcd(n,k)=1$;

2006 年以后,人们陆续发现了一些多项式形式的二次 PN 函数. 目前 F_{p^n} 上已知的多项式 PN 函数有:

1) Ding-Yuan 多项式[19-20]:

$$\pi_3(x)=x^{10}-\mu x^6-\mu^2x^2,$$

其中,整数 $p=3$,n 为奇数且 $\mu\in F_{p^n}^*$;

2) Zha-Kyureghyan-Wang 多项式[21]:

$$\pi_4(x)=x^{p^s+1}-\mu^{p^k}x^{p^{lk}+p^{-lk+s}},$$

其中,整数 $n=3k$,$(3,k)=1$,$k/\gcd(k,s)$ 为奇数,$s\equiv\pm k \bmod 3$ 且 μ 为 $F_{p^n}^*$ 中本原元;

3) Budaghyan-Helleseth 第 1 类多项式[22]:

$$\pi_5(x)=(bx)^{p^s+1}-((bx)^{p^s+1})^{p^k}+\sum_{i=0}^{k-1}c_ix^{p^i(p^k+1)},$$

其中,$\sum_{i=0}^{k-1}c_ix^{p^i}\in F_{p^k}[x]$ 且置换 F_{p^n},$b\in F_{p^n}^*$,且 $\gcd(p^s+1,p^k+1)\neq\gcd(p^s+1,(p^k+1)/2)$,$\gcd(k+s,2k)=\gcd(k+s,k)$;

4) Budaghyan-Helleseth 第 2 类多项式[22]:

$$\pi_6(x)=bx^{p^s+1}+(bx^{p^s+1})^{p^k}+cx^{p^k+1}+\sum_{i=1}^{k-1}r_ix^{p^i(p^k+1)},$$

其中 $c\in F_{p^n}\backslash F_{p^k}$,$r_i\in F_{p^k}$,$0\leqslant i<k$,$b\in F_{p^n}^*$ 为非平方元,且 $\gcd(k+s,n)=\gcd(k+s,k)$;

5) Bierbrauer 多项式[23]:

$$\pi_7(x)=x^{p^t+1}-\alpha x^{p^{2s}+p^{s+t}},$$

其中,$n=3s$,$q=p^s$,$q'=p^t$,$s'=s/\gcd(s,t)$,$t'=t/\gcd(s,t)$,s' 为奇数,$a\in F_{q^3}$ 且其阶为 q^2+q+1,$s+s'\equiv 0 \bmod 3$ 或 $q\equiv q' \bmod 3$.

如定理 2 所述,上述二次 PN 函数还等价于交换预半域. 人们还构造了一些其他的半域,其对应的多项式较复杂,下面列出这些半域,感兴趣的读者可以自行推导其对应 PN 函数的多项式表达式:

1) Dickson 半域[24]:定义在 $F_{q^{2k}}$ 上,其乘法定义为

$$(a,b)*(c,d)=(ac+\alpha b^qd^q,ad+bc),$$

其中,$\alpha\in F_{q^k}$ 为一个非平方元;

2) Ganley 半域[25]:定义在 $F_{3^{2k}}$ 上,其中 $k\geqslant 3$ 为奇数,其乘法定义为

$$(a,b)*(c,d)=(ac-b^9d-bd^9,ad+bc+b^3d^3)$$

3) Cohen-Ganley 半域[26]:定义在 F_{3^n} 上,其中 $n\geqslant 2$,其乘法定义为

$$(a,b)*(c,d)=(ac+\beta bd+\beta^3(bd)^9,ad+bc+\beta(bd)^3),$$

其中,$\beta\in F_{3^n}$ 为一个非平方元;

4) Zhou-Pott 半域[27]:设 $n=2m$,k 为正整数,且 $m/\gcd(m,k)$ 为奇数,定义 $x\circ_k y=x^{p^k}y+y^{p^k}x$,设 $(a,b)*(c,d)\in F_{p^{2m}}$,乘法定义为

$$(a,b)*(c,d)=(a\circ_k c+\alpha(b\circ_k d)^\delta, ad+bc)$$

其中,$\alpha\in F_{p^m}$ 为一个非平方元;δ 为 F_{p^m} 上的一个自同构.

除此之外,人们还在 F_{3^5},F_{3^8},F_{5^5} 中发现了一些零散半域[28-30].目前还不能把它们推广到无限类.

从上面论述可以看出,除了 Coulter-Mattews 函数外,其他所有已知 PN 函数都是二次的,因此都对应于交换(预)半域.二次 PN 函数的 CCZ 等价性与其对应半域的同痕(isotopy)是一致的.半域同痕的不变量包括核(nucleus)、中心(center)、对应平面的自同构群等.关于上述半域同痕性的讨论,请参阅文献[31]及其引用的参考文献.

定义 6. 非凡完全非线性函数(exceptional perfect nonlinear function).设 $F:F_q\to F_q$,若 F 在 F_q 的无穷多个扩域上为完全非线性函数,则称 F 为非凡完全非线性函数.若 $F(x)=x^d$,则称 d 为非凡完全非线性指数.

利用代数几何的方法,2015 年 Zieve[32] 证明了:

定理 4. 设 p 为奇素数,d 为正整数,单项式 $F(x)=x^d$ 为 F_{p^n} 上的完全非线性函数对无穷多个整数 n 成立当且仅当 d 为下列情形之一:

1) $d=p^i+p^j, i\geqslant j\geqslant 0$;

2) $d=(3^i+3^j)/2, p=3, i\geqslant j\geqslant 0$ 且 $i-j$ 为奇数.

除了上述 2 个非凡完全非线性函数外,容易看出 Ding-Yuan 多项式 $\pi_3(x)=x^{10}-\mu x^6-\mu^2x^2$ 也是一个非凡完全非线性函数.

本节的最后,介绍一下偶特征上的平面函数,也称为伪平面函数(pseudo-planar function)或修改的平面函数(modified planar function).PN 函数仅在奇特征有限域上存在,APN 函数在某种意义上可以视为 PN 函数在偶特征有限域上的推广,但 APN 函数与射影平面、码本等并没有联系.2013 年周悦引入伪平面函数[33]的定义:

定义 7. 伪平面函数.设 $F:F_{2^n}\to F_{2^n}$,若对任意 $0\neq a\in F_{2^n}$,函数

$$D_aF=F(x+a)+F(x)+ax$$

均为 F_{2^n} 上的线性化置换多项式,则称 F 为伪平面函数.

与 PN 函数类似,伪平面函数与射影平面、交换半域等数学对象有着深刻的内在联系,在压缩感知矩阵设计、最优码本设计等领域中有着丰富的应用.目前所有已知伪平面函数都是二次函数,都对应着 F_{2^n} 上的交换半域.周悦在文献[33]中给出了 2 类伪平面函数,分别对应着有限域和 Kantor 半域.随后 Schmidt、周悦[34] 和 Scherr, Zieve[35] 研究了单项式伪平面函数,给出了三类构造.2015 胡思煌等人[36] 构造了三类二项式伪平面函数.2016 年屈龙江[37] 将一大类二次函数为伪平面函数的判定问题转化为一个对应含参 Dickson 行列式是否非零的判定问题,大大降低了判定时间复杂度;利用该 Dickson 行列式系数的特殊性质能够进一步简化计算证明.该方法不仅构造了 5 类新的多项式伪平面函数,而且将所有已知函数都统一归纳到了一个大类中.

3 APN 函数

由于密码学应用主要使用(向量)布尔函数,所以本节主要讨论偶特征域上的 APN 函数.对于奇特征域上 APN 函数感兴趣的,请参阅文献[38-40].

3.1 性质与判定

APN 函数有一些等价判别准则:

定理 5. 设 $F:F_{2^n}\to F_{2^n}$,则 6 个条件等价:

1) F 为 APN 函数,即对任意 $a,b\in F_{2^n}, a\neq 0$,方程 $F(x+a)+F(x)=b$ 至多有 2 个解;

2) 对任意使得 $x+y+z+t=0$ 的两两互异的 $x,y,z,t\in F_{2^n}$,有 $F(x)+F(y)+F(z)+F(t)\neq 0$;

3) 对任意非零 $a\in F_{2^n}$,均有 $|D_a(F)|=2^{n-1}$,其中 $D_a(F)=\{F(x+a)+F(x)\mid x\in F_{2^n}\}$;

4) $wt(\gamma_F)=2^{2n-1}-2^{n-1}$,其中 γ_F 为由 F 定义的 $2n$ 元布尔函数:$\gamma_F(a,b)=1$ 当且仅当 $a\neq 0$,且方程 $F(x+a)+F(x)=b$ 有解[10];

5) 对任意非零 $a\in F_{2^n}$,均有:

$$\sum_{\lambda\in F_{2^n}} F^W(D_a(f_\lambda))^2=2^{2n+1},$$

其中,f_λ 表示 F 的组件函数,$F^W(g)$ 表示布尔函数 g 在 $x=0$ 处的 Walsh 谱[41];

6) $\sum_{\lambda\in F_{2^n}^*} v(f_\lambda)=(2^n-1)2^{2n+1}$,其中 f_λ 表示 F 的组件函数,$v(f)=\sum_{a\in F_{2^n}} F^W(D_af)^2$ 表示布尔函数 f 的平方和指标[41].

2017 年 Carlet 以 Walsh 变换为工具刻画向量函数的差分均匀度,特别地,给出 APN 函数的如下等价判别准则:

定理 6[42]. 设 $F:F_{2^n}\to F_{2^n}$,则 F 为 APN 函数当且仅当下列任一条件成立:

1) $\sum_{u,v\in F_{2^n},u\neq 0} W_F^4(u,v)=2^{3n+1}(2^n-1)$;

2) $\sum_{u_1,v_1,u_2,v_2\in F_{2^n},u_1,u_2\neq 0,u_1\neq u_2} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)=2^{5n}(2^n-1)(2^n-2)$.

APN 函数和 AB 函数具有联系:

定理 7[10,43]. 设 $F:F_{2^n}\to F_{2^n}$. 若 F 为 AB 函数,则 F 为 APN 函数. 反过来,当 n 为奇数时,如果 F 为 APN 函数,且其所有 Walsh 谱值均被 2^{n+1} 整除,那么 F 为 AB 函数;特别地,二次 APN 函数必为 AB 函数.

对于 APN 幂函数,Berger 等完全刻画了它的映射性质.

定理 8[42]. 设 x^d 为 F_{2^n} 上的 APN 函数,则:

$$\gcd(d,2^n-1)=\begin{cases}1, & n\text{ 为奇数},\\ 3, & n\text{ 为偶数}.\end{cases}$$

上述结果表明,F_{2^n}(n 奇)上的 APN 幂函数必然是置换,但 F_{2^n}(n 偶)上的 APN 幂函数则不可能为置换.

2011 年 Leander 和 Rodier[44] 研究了 APN 函数的代数次数上界,证明了 $x^{-1}+g(x)$,其中 g 为非仿射函数,至多对有限个 n 能在 F_{2^n} 上为 APN 函数. 最近 Budaghyan 等人[45] 研究了 F_{2^n} 上代数次数为 n 的 APN 函数的存在性,利用差分、Walsh 谱的幂级数刻画了这些函数,给出了一些不存在性的结果. 特别地,证明了对于 F_{2^n} 上多数已知 APN 函数 $F(x)$,$x^{2^n-1}+F(x)$不是 APN 函数;这意味着,如果改变这些 APN 函数的一个点,得到的是非 APN 函数.

2016 年 Gorodilova[46] 刻画了 APN 函数的子函数,证明了一个 n 元向量函数为 APN 函数当且仅当其 2 个 $n-1$ 元子函数或者为 APN 函数,或者为 4 差分函数,且满足相容性条件.

3.2 已有构造

2005 年以前,有限域 F_{2^n} 上 APN 函数的研究主要集中于幂函数,包括 Gold 函数、Kasami 函数、Welch 函数、Niho 函数、逆函数和 Dobbertin 函数这 6 类 APN 幂函数.

1) Gold 函数[47-48]:x^{2^i+1},其中 $\gcd(i,n)=1$,$1\leqslant i\leqslant\frac{n-1}{2}$;

2) Kasami 函数[49]:$x^{2^{2i}-2^i+1}$,其中 $\gcd(i,n)=1$,$1\leqslant i\leqslant\frac{n-1}{2}$;

3) Welch 函数[50]:x^{2^k+3},其中 $n=2k+1$;

4) Niho 函数[51]:$x^{2^k+2^{k/2}-1}$,当 k 是偶数时;$x^{2^k+2^{(3k+1)/2}-1}$,当 k 是奇数时;其中 $n=2k+1$;

5) Inverse 函数[52,48]:$x^{2^{2k}-1}$,其中 $n=2k+1$;

6) Dobbertin 函数[53]:$x^{2^{4k}+2^{3k}+2^{2k}+2^k-1}$,其中 $n=5k$.

2006 年 Dillon 在 F_{2^6} 上发现了很多不等价于幂函数的多项式 APN 函数[54]. 学者们从这些例子出发,陆续构造了一些与幂函数不等价的多项式二次 APN 函数无限类,它们的形式是通过对不同参数的 Gold 函数进行组合得到新的 APN 函数. 我们将这些函数归纳总结,它们均是定义在 F_{2^n} 上的:

1) Budaghyan-Carlet-Leander 函数[55]:

$$x^{2^s+1}+\alpha^{2^t-1}x^{2^{it}+2^{rt+s}},$$

其中,$n=lt\geqslant 12$,$l\in\{3,4\}$,$\gcd(t,l)=\gcd(s,lt)=1$,$i\equiv st \bmod l$,$r=l-i$,$\alpha\in F_{2^n}$ 为本原元.

2) Bracken-Byrne-Markin-McGuire 第 1 类函数[56]:

$$\alpha x^{2^s+1}+\alpha^m x^{2^{m+s}+2^m}+\beta x^{2^m+1}+\sum_{i=1}^{m-1}\gamma_i x^{2^{m+i}+2^i},$$

其中,$n=2m$,m 为奇数,$\gamma_i\in F_{2^m}$,$\gcd(s,m)=1$,s 为奇数,$\alpha,\beta\in F_{2^n}$ 为本原元;

3) Bracken-Byret-Markin-McGuire 第 2 类函数[57]:

$$\alpha^{2^t}x^{2^{n-t}+2^{t+s}}+\alpha x^{2^s+1}+\beta x^{2^{n-t}+1}+\gamma\alpha^{2^t+1}x^{2^{t+s}+2^s},$$

其中,$n=3t$,$\gcd(s,3t)=\gcd(3,t)=1$,$3\mid t+s$,$\alpha\in F_{2^n}$ 为本原元,$\beta,\gamma\in F_{2^t}$,$\beta\gamma\neq 1$;

4) Budaghyan-Carlet 第 1 类函数[55]:

$$x^{2^{2s}+2^s}+\alpha x^{2^m+1}+\beta x^{2^{2s+m}+2^{s+m}},$$

其中,$n=2m$,$\gcd(i,m)=1$,$\alpha,\beta\in F_{2^n}$ 使得:

$\beta^{2^m+1}=1$,$\beta\notin\{\lambda^{(2^i+1)(2^m-1)},\lambda\in F_{2^n}\}$,$\beta\alpha^{2^m}+\alpha\neq 0$;

5) Budaghyan-Carlet 第 2 类函数[55]:

$$x(x^{2^i}+x^{2^m}+\alpha x^{2^{m+i}})+$$
$$x^{2^i}(\alpha^{2^m}x^{2^m}+\beta x^{2^{m+i}})+x^{2^m(2^i+1)}$$

其中,$n=2m$,$\gcd(i,n)=1$,$\beta\in F_{2^n}\backslash F_{2^m}$,并且 $x^{2^i+1}+\alpha x^{2^i}+\alpha^{2^m}x+1$ 在 F_{2^n} 上没有满足 $x^{2^m+1}=1$ 的解.

2009 年,Budaghyan 等人[58] 从 x^3 出发,构造了一类形式非常简单的在任何 F_{2^n} 上都存在的 APN 函数无限类:

$$x^3+Tr_1^n(x^9),$$

并在文献[59]中构造了更多具有这种形式的 APN 函数无限类. Edel 和 Pott[60] 研究了构造该 APN 函数的方法并提出“交换构造(switching construction)”技术,通过变换已有 APN 函数的坐标函数来构造

新的 APN 函数,得到了目前唯一的一个既 CCZ 不等价于幂函数也 CCZ 不等价于二次函数的 F_{2^6} 上的 APN 函数:

$$F(x)=x^3+\alpha^{17}(x^{17}+x^{18}+x^{20}+x^{24})+$$
$$\alpha^{18}x^9+\alpha^{36}x^{18}+\alpha^9x^{36}+x^{21}+x^{42}+$$
$$Tr_1^6(\alpha^{27}x+\alpha^{52}x^3+\alpha^6x^5+\alpha^{19}x^7+\alpha^{28}x^{11}+\alpha^2x^{13})$$

其中,本原元 α 为 $x^6+x^4+x^3+x+1$ 的一个根.

2011 年 Carlet[61] 以及 2013 年周悦和 Pott 等人[27]分别利用向量 Bent 函数构造 APN 函数,该方法得到的构造涵盖了以往的许多构造.这 2 个构造都使用了双变元表示,即当 $n=2m$ 时,将 F_{2^n} 视为 $F_{2^m}\times F_{2^m}$.

1) Carlet 函数[61]:令 $n=2m$,整数 i,j 满足 $\gcd(n/2,i-j)=1$.令 $\alpha,\beta\neq 0,\gamma,\delta\in F_2^m$,

$$g(x,y)=\alpha x^{2^i+2^j}+\gamma x^{2^i}y^{2^j}+\delta x^{2^j}y^{2^i}+\beta y^{2^i+2^j},$$

则:

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

是 APN 函数当且仅当多项式

$$g(x,1)=\alpha x^{2^i+2^j}+\gamma x^{2^i}+\delta x^{2^j}+\beta$$

在 F_{2^m} 中无根;

2) Zhou-Pott 函数[27]:令 $n=2m$,m 是偶数,$\gcd(k,m)=1$.令 $\alpha\in F_{2^m}^*$,σ 为 F_{2^m} 上的一个自同构,

$$g(x,y)=x^{2^k+1}+\alpha(\sigma(y))^{2^k+1},$$

则:

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

是 APN 函数当且仅当 α 不能写成

$$a^{2^k+1}(t^{2^k}+t)/(\sigma(t^{2^k}+t))$$

的形式,其中 $a,t\in F_{2^m}$.

2014 年,余玉银等人[62]提出了一个通过齐二次函数对应矩阵坐标变换的方法构造二次 APN 函数,在 F_{2^7},F_{2^8} 上分别发现了 471 类和 2252 类 CCZ 不等价的二次 APN 函数.同时,翁国标等人[63]受 DO 函数与半域的对应启发,提出了 APN 代数(APN algebra)的概念来刻画二次 APN 函数,同样在 F_{2^7},F_{2^8} 上发现了大量新的二次 APN 函数.2014 年,Carlet 等人[64]通过寻找特殊形式的二次置换多项式的方法在 F_{2^8} 上找到了 18 类 APN 函数.

介绍一下非凡几乎完全非线性函数(exceptional almost perfect nonlinear function)即在无穷多个扩域上具有几乎完全非线性的函数.利用代数几何的方法,2011 年 Hernando 和 McGuire[65]证明了结果:

定理 9. 设 d 为正整数,单项式 $F(x)=x^d$ 为 F_{2^n} 上的 APN 函数对无穷多个整数 n 成立当且仅当 d 为 Gold 指数或者 Kasami 指数,即 $d=2^i+1$ 或 $d=2^{2i}-2^i+1$.

目前人们仅知道上述 2 个非凡 APN 函数.

3.3 等价性

理论上分析 APN 函数之间的 CCZ 等价性非常困难,人们一般通过计算机在小域上计算一些 CCZ 等价不变量来说明 APN 函数之间的 CCZ 等价性.目前 APN 函数 CCZ 等价性的理论研究主要集中于幂函数之间以及多项式函数与部分幂函数之间.虽然学者们普遍认为 3.2 节中所列出的 APN 幂函数相互之间应该是 CCZ 不等价的,但在很长一段时间里,Gold 函数、Kasami 函数、Welch 函数和 Niho 函数四者之间的等价性以及逆函数和 Dobbertin 函数两者之间的等价性目前都没能给出严格的数学证明[31].直到 2018 年,Dempwolf[66]完全解决了幂函数之间的 CCZ 等价性问题.但各类多项式 APN 函数无限类之间的 CCZ 等价性依旧是公开问题.目前已有的结果可以归结为 6 个方面:

1) 参数不同的 Gold 函数之间是 CCZ 不等价的[67];

2) 逆函数和 Dobbertin 函数这 2 类函数与 Gold 函数,Kasami 函数,Welch 函数和 Niho 函数这四类函数之间 CCZ 不等价[68-69];

3) Budaghyan[55]证明了当 $n\geqslant 12$ 时,论文中构造的 APN 函数 CCZ 不等价于 Gold 函数、Kasami 函数、逆函数和 Dobbertin 函数且 EA 不等价于任何幂函数;

4) 2012 年 Yoshiara[70]证明了 Edel 的猜想:2 个二次 APN 函数 CCZ 等价当且仅当它们 EA 等价;

5) 2017 年 Yoshiara[71]证明了 n 为偶数时,如果有 2 个 plateaued APN 函数且其中一个为幂函数,则它们 CCZ 等价当且仅当它们 EA 等价;

6) Dempwolf[66]证明了 F_{p^n} 上的 2 个幂函数 x^k 和 x^l 是 CCZ 等价的当且仅当存在整数 $0\leqslant a<n$,使得 $l\equiv p^ak\pmod{p^n-1}$ 或者 $lk\equiv p^a\pmod{p^n-1}$.

另外,目前所有二次 APN 函数族的 Walsh 谱都得到了计算,结果表明,这些函数都具有与 Gold 函数相同的 Walsh 谱,即当 n 为奇数时为三谱值,而当 n 为偶数时为五谱值[72-73,58].

3.4 大 APN 问题

为了避免熵泄露,一般要求分组密码中使用的向量函数是个置换;同时为了软硬件实现时具有较高的效率,又希望其定义在二元域的偶数维扩域(偶

数维扩张,以下简称偶扩张)上. 于是寻找偶扩张上的 APN 置换就成为了密码学研究中的一个重要问题,该问题被称为"大APN问题(bigAPNproblem)".

问题 1. 大 APN 问题. 当 n 为偶数时,是否存在 F_{2^n} 上的 APN 置换?

该问题已经公开近 30 年了,是目前密码函数领域里最著名的公开问题. 很长一段时间里,人们只能得到关于该问题的一些负面结果,于是很多密码学家和数学家猜想,F_2 的偶次扩域上不存在 APN 置换. 但 2009 年 Dillon 等人发现了 F_{2^6} 上的一个 APN 置换[74],然而 $n\geqslant 8$ 情况下的"大 APN 问题"目前仍然是公开的. 关于"大 APN 问题",目前已知有 4 个方面结果:

1) 2009 年 Dillon 通过分解一个 APN 函数所对应的线性码,找到了 F_{2^6} 上的一个 APN 置换[74]. 但其表达形式非常复杂. 2016 年,Perrin 等人[75]提出了"蝴蝶结构(butterfly structure)",很好地从理论上诠释了这个 APN 置换,但是,他们的方法并没有发现偶扩张上的其他 APN 置换.

2) F_{2^2} 和 F_{2^4} 上不存在 APN 置换. Langevin 等人[76]结合计算机验证指出,F_{2^6} 上的 3 次 APN 置换一定与 Dillon 等人发现的 APN 置换是 CCZ 等价的.

3) 定理 8 表明偶扩张上的幂函数不可能为 APN 置换. Seberry 等人证明了偶扩张上的二次函数也不可能为 APN 置换. Pasalic[77]、李永强等人[78-79]分别证明了某些形如一个幂函数和一个线性函数的和函数不可能为 APN 置换.

4) Berger 等人[41]证明了如果 $F\in F_{2^{n/2}}[x]$,则该函数不是 APN 置换;如果对于任意的 $\lambda\in F_{2^n}^*$,函数 F 的组件函数 f_λ 均是平原函数,则该函数不是 APN 置换. Calderini 等人[80]证明了如果函数的组件函数中有二次函数,则该函数不是 APN 置换.

APN 函数研究的困难性有 3 个方面:1)一个随机函数是 APN 函数的概率很低,这为其搜索、构造带来很大困难;2)缺乏判断 CCZ 等价的有效工具,研究中人们经常会发现找到的函数 CCZ 等价于已知函数;3)除了单项式(幂函数)和二项式外,已知 APN 函数的表达形式往往比较复杂,例如 Dillon 等人构造的 APN 置换,这也进一步研究带来较大困难. 因此我们对于 APN 函数的认识还不够深刻,亟需更深刻、更有力的研究工具.

4 4 差分置换

4 差分函数是偶特征有限域上具有次优差分均匀度的函数. 4 差分函数的构造并不困难,一种自然的方法是复合一个 APN 函数和一个 2 到 1 的线性函数. 从密码应用角度看,由于缺乏偶扩张上的 APN 置换,密码算法 S-盒设计的一个自然选择就是使用 4 差分置换,比如著名 AES(advanced encryption standard)算法的 S-盒使用了 F_{2^8} 上的逆函数就是一个 4 差分置换. 偶扩张上 4 差分置换的构造与性质对于对称密码设计与分析具有十分重要的意义. 因此接下来本节只论述偶扩张上 4 差分置换.

4.1 已有构造

近年来偶扩张上 4 差分置换的研究受到较多关注,人们给出了一系列新的构造,下面分为具有五谱值的 4 差分置换和从逆函数出发构造的 4 差分置换两大类进行叙述.

4.1.1 具有五谱值的 4 差分置换

已有具有五谱值的 4 差分置换其 Walsh 谱取值均为 $\{0,\pm 2^{n/2},\pm 2^{(n+2)/2}\}$,因此非线性度达到已知最优 $2^{n-1}-2^{n/2}$,其中一些构造的代数次数也不太低,但目前已有的构造均无法达到最优代数次数 $n-1$.

1) 基础构造

2011 年以前,偶扩张上的 4 差分置换无限类只有 Gold 函数、Kasami 函数、逆函数、Bracken-Leander 函数和 Bracken-Tan-Tan 函数 5 类基础构造. 其中除了逆函数外,其余 4 类 Walsh 谱取值均为 $\{0,\pm 2^{n/2},\pm 2^{(n+2)/2}\}$.

① Gold 函数[47]:x^{2^i+1},其中 $n=2k$,k 为奇数且 $\gcd(i,n)=2$;

② Kasami 函数[81-82]:$x^{2^{2i}-2^i+1}$,其中 $n=2k$,k 为奇数且 $\gcd(i,n)=2$;

③ 逆函数:x^{-1},其中定义 $0^{-1}=0$;

④ Bracken-Leander 函数[83]:$x^{2^{2k}+2^k+1}$,其中 $n=4k$,k 为奇数;

⑤ Bracken-Tan-Tan 函数[84]:$\alpha x^{2^s+1}+\alpha^{2^k}x^{2^{-k}+2^{k+s}}$,其中 $n=3k$,k 是偶数,但 $3\nmid k$ 且 $k/2$ 是奇数,$\gcd(i,n)=2$,$3\mid(k+s)$,α 是 F_{2^n} 上的本原元.

其中,前 4 类为幂函数,最后一类为二项式函数. 除了 Kasami 函数和逆函数之外,其他函数的代数次数都是 2 或者 3,且仅有逆函数是对合函数. 容易看出,这里除了 Bracken-Leander 函数以外,其余 3 类都是从 APN 函数修改构造的.

2) Gold 函数收缩构造

2011 年 Carlet 提出了一种利用 $F_{2^{2k+1}}$ 上 APN 置换来构造 $F_{2^{2k}}$ 上 4 差分置换的方法[85]. 李永强等人对该方法进行了进一步研究,从 Gold 函数出发,成功地构造了 2 类偶扩张上的具有已知最优非线性度的 4 差分置换[86]. 其具体形式如下:

① Li-Wang 第 1 类构造[86]:令 $n\geqslant 4$ 为偶数,$\gcd(i,n+1)=1$,$u\in F_{2^{n+1}}^{*}$,$c=0$ 或 1,将 F_{2^n} 上的向量看作是 n 维线性子空间 $H_u=\{ux^{2^i}+u^{2^i}x\mid x\in F_{2^{n+1}}\}$ 中的元素. 定义 F_u 为 $ux^{2^i/(2^i+1)}+u^{2^i}x^{1/(2^i+1)}+cx$ 限制在 H_u 上的函数,其中 $x^{1/(2^i+1)}$ 表示 x^{2^i+1} 在 $F_{2^{n+1}}$ 上的逆函数.

② Li-Wang 第 2 类构造[86]:令 n 为偶数且 $3\mid n+1$,$\gcd(i,n+1)=1$,$s=i \bmod 3$,将 F_{2^n} 上的向量看作是 n 维线性子空间 $T^{(0)}=\{x\in F_{2^{n+1}}\mid Tr_1^{n+1}(x)=0\}$ 中的元素. 定义

$$F'=x^{1/(2^i+1)}+Tr_3^{n+1}(x+x^{2^{2s}})+(x^{1/(2^i+1)}+Tr_3^{n+1}(x+x^{2^{2s}}))^{2^i}$$

限制在 $T^{(0)}$ 上的函数.

这 2 类函数的代数次数为 $(n+2)/2$,但均不是对合函数.

3) 蝴蝶结构

2016 年 Perrin 等人[75]用逆向工程分析 Dillon 等构造的 APN 置换,提出了“蝴蝶结构”. 该结构是由 2 个 F_{2^k} 上双变元函数组成的 $2k$ 元(k 奇)映射,有 2 种 CCZ 等价的表示形式:①“开蝴蝶结构”,$H_R(x,y)=(R_{R_y^{-1}(x)}(y),R_y^{-1}(x))$;②“闭蝴蝶结构”,$V_R(x,y)=(R(x,y),R(y,x))$,其中对于任意 $x,y\in F_{2^k}$,都有 $R_y(x)=R(x,y)$ 且 $R_y^{-1}(R_y(x))=x$. 他们证明了一个具有“开蝴蝶结构”的函数是置换且“开蝴蝶结构”与“闭蝴蝶结构”是 CCZ 等价的. Perrin,Canteaut,Fu 等人先后证明了当 $R(x,y)$ 满足以下条件之一时,$V_R(x,y)$ 的差分均匀度为 4,从而证明了 $H_R(x,y)$ 是 4 差分置换.

① Perrin-Udovenko-Biryukov 构造[75]:

$$R(x,y)=(x+\alpha y)^3+y^3,$$

其中,$\alpha\in F_{2^k}^{*}$.

② Canteaut-Duval-Perrin 构造[87]:

$$R(x,y)=(x+\alpha y)^3+\beta y^3,$$

其中,$\alpha,\beta\in F_{2^k}^{*}$,$\beta\neq(1+\alpha)^3$.

③ Fu-Feng 构造[88-89]:

$$R(x,y)=(x+\alpha y)^{2^t(2^i+1)}+y^{2^t(2^i+1)},$$

其中,$\alpha\in F_{2^k}^{*}$,$\gcd(i,k)=1$,$0\leqslant t\leqslant k-1$.

这些 4 差分置换具有已知最优的非线性度,代数次数为 $n/2$ 或者 $(n+2)/2$,这些函数的“开蝴蝶结构”形式均为对合的. 利用“蝴蝶结构”可以给出 Dillon 等构造 APN 置换的简洁表达形式. 但遗憾的是 Canteaut 等证明在该结构构造的函数中,除了 Dillon 等构造的 APN 置换外,没有其他 APN 置换.

4.1.2 从逆函数出发构造的 4 差分置换

当 n 为偶数时,逆函数 x^{-1} 是对合的 4 差分置换[48,52],具有最优代数次数 $n-1$,其非线性度达到已知最优 $2^{n-1}-2^{n/2}$,Walsh 谱可以取遍 $\pm 2^{(n+2)/2}$ 之间的每一个被 4 整除的整数值. AES,Camellia 等很多标准算法均使用逆函数做 S 盒. 从逆函数出发构造的 4 差分置换普遍具有最优代数次数 $n-1$ 和较高的非线性度,其中一些子类还可以达到已知最优非线性度.

1) 逆函数交换构造

2013 年屈龙江等人通过“交换构造(switching construction)”的技术研究了逆函数,提出了优先函数的概念,并且以此为工具构造为

$$x^{-1}+Tr_1^n(x^{-d}+(x^{-1}+1)^d),$$

其中,$d=2^n-2$ 或者 $3(2^t+1)$,$2\leqslant t\leqslant n/2-1$ 的 2 个简洁的 4 差分置换无限类[90]. 他们又提出优先布尔函数的概念,在偶扩张上构造出了至少 $2^{(2^n+2)/3}$ 个形如 $x^{-1}+f(x^{-1})$ 的具有最优代数次数的 4 差分置换,从而在理论上首次证明了 $F_{2^{2k}}$ 上 4 差分置换的个数是随着变元个数增长而呈双指数增长的[91]. 这些函数都可以看作是在逆函数基础上添加某个布尔函数得到的,我们简称为 BI 函数,这类函数是 4 差分置换的充分必要条件如下[92]:

BI 4 差分置换:令 n 为偶数,ω 是 F_{2^n} 中阶为 3 的元素,f 是 n 元布尔函数. 则 BI 函数是 4 差分置换当且仅当对于任意 $x\in F_{2^n}$ 均有 $f(x)=f(x+1)$ 且对于任意 $z\in F_{2^n}\backslash F_4$,2 个等式中至少有一个成立:

$$f(0)+f\left(z+\frac{1}{z}+1\right)+f\left(\omega z+\frac{1}{\omega z}+1\right)+f\left(\omega^2 z+\frac{1}{\omega^2 z}+1\right)=0,$$

$$f(0)+f\left(z+\frac{1}{z}+1\right)+f\left(\omega\left(z+\frac{1}{z}+1\right)\right)+f\left(\omega^2\left(z+\frac{1}{z}+1\right)\right)=0$$

查正邦等学者[93-94]、彭杰等学者[95]也先后研究了逆函数的交换构造法,并进一步研究了其中一些具有良好密码学性质的子类. BI 4 差分置换具有最优代数次数和较高的非线性度,其中一些子类还具

有已知最优非线性度.BI 4 差分置换是对合函数当且仅当 2 种情况之一成立[96]:

① $n=2k$,k 为奇数,

$Supp(f)=\{0,1\},\{\omega,\omega^2\}$或$\{0,1,\omega,\omega^2\}$;

② $n=2k$,k 为偶数,

$$Supp(f)=\{0,1,\omega,\omega^2\}.$$

2) 逆函数其他修改构造

李永强、查正邦、彭杰、唐灯和 Carlet 等学者也先后通过不同的方法对 F_{2^n} 上的逆函数进行修改,得到了一些新的 4 差分置换,这些 4 差分置换普遍具有最优代数次数和较高的非线性度.具体修改方式为:

① Li-Wang-Yu 构造[97]:

$$F(x)=\begin{cases}a_{i+1}^{-1}, & x=a_i,\\ x^{-1}, & x\notin\{a_i\mid 0\leqslant i\leqslant m\};\end{cases}$$

其中,$\{a_i\mid 0\leqslant i\leqslant m\}$为满足一定条件的圈.

② Zha-Hu-Sun 构造[93]:

$$F(x)=\begin{cases}\beta x^{-1}+\alpha, & x\in F_{2^d},\\ x^{-1}, & x\in F_{2^n}\backslash F_{2^d};\end{cases}$$

其中,d 是偶数,$d\mid n$ 且 n/d 为奇数,$\alpha,\beta\in F_{2^d}$,$Tr_1^d\left(\frac{1}{\alpha}\right)=1$.

③ Peng-Tan 构造[98]:

$$F(x)=\begin{cases}\beta(x+1)^{-1}+\alpha, & x\in F_{2^d},\\ x^{-1}, & x\in F_{2^n}\backslash F_{2^d};\end{cases}$$

其中,$\alpha,\beta\in F_{2^d}$ 满足某些具体条件.

④ Peng-Tan-Wang 第 1 类构造[99]:

$$F(x)=\begin{cases}(\gamma x)^{-1}, & x\in U,\\ x^{-1}, & x\in F_{2^n}\backslash U;\end{cases}$$

其中,$\gamma\in F_{2^n}$,U 是循环群$\langle\gamma\rangle$中一些集合的并.

⑤ Peng-Tan-Wang 第 2 类构造[100]:

$$F(x)=\begin{cases}(x+1)^{-1}+1, & x\in U,\\ x^{-1}, & x\in F_{2^n}\backslash U;\end{cases}$$

其中,U 是 $F_{2^n}\backslash F_4$ 中一些六元集合的并.

⑥ Tang-Carlet-Tang 构造[101]:

$$F(x)=\begin{cases}(x+1)^{-1}, & x\in T,\\ x^{-1}, & x\in F_{2^n}\backslash T;\end{cases}$$

其中,$x\in T$ 当且仅当 $x+1\in T$,且若 $x\in T$ 则有 $Tr_1^n\left(\frac{1}{x}\right)=Tr_1^n\left(\frac{1}{x+1}\right)=1$.

其中,第⑥类函数的逆变换是 BI 4 差分置换,因此它们是 CCZ 等价的.前 5 类函数均包含一些对合的 4 差分置换子类,这里不具体列出相关条件,感兴趣的读者请参阅文献[96].

3) 逆函数扩张构造

2014 年,Carlet 和唐灯等人[102]利用 $F_{2^{2k-1}}$ 上的逆函数是 APN 函数这一特性,构造了 $F_{2^{2k}}$ 上一大类数量至少有 $(2^{n-3}-\lfloor 2^{(n-1)/2-1}\rfloor-1)\times 2^{2^{n-1}}$ 个的新 4 差分置换,这类函数具有最优代数次数以及较高的非线性度,其具体形式如下:

Carlet-Tang-Tang-Liao 函数:令 $n\geqslant 6$ 为偶数,对于任意满足条件 $Tr_1^{n-1}(c)=Tr_1^{n-1}(1/c)=1$ 的$c\in F_{2^{n-1}}\backslash\{0,1\}$,定义 F_{2^n} 上的函数为

$$F(x_1,x_2,\cdots,x_{n-1},x_n)=\begin{cases}(1/x',f(x')), & x_n=0,\\ (c/x',f(x'/c)+1), & x_n=1,\end{cases}$$

其中,$x'\in F_{2^{n-1}}$ 由$(x_1,x_2,\cdots,x_{n-1})\in F_2^{n-1}$ 定义,f 是任意一个 $n-1$ 元布尔函数.这类函数是对合的 4 差分置换当且仅当 $f=0$[96].

4.2 等价性研究

4 差分置换同样可以通过计算差分谱、扩展 Walsh 谱、Γ-秩、Δ-秩和各种形式的自同构群等 CCZ 等价不变量来判断它们之间的等价性,最常见的是计算 Walsh 谱和差分谱.具有五谱值的 4 差分置换和从逆函数出发构造的 4 差分置换这 2 类相互之间的 CCZ 不等价性一般可以通过计算 Walsh 谱来证明或者验证,因为从逆函数出发构造的 4 差分置换一般不是五谱值的.而在每一大类里各自不同构造之间的 CCZ 不等价性多数情况下是通过在小域上计算 Walsh 谱或者差分谱来验证的.接下来我们主要描述该方面的理论结果.

首先,具有五谱值的 4 差分置换之间的等价性研究相对较少.由于函数存在域的不同,Bracken-Leander 函数、Bracken-Tan-Tan 函数与其他 2 类基础构造是 CCZ 不等价的.其次,由于 F_{2^n} 上一个函数的 CCZ 等价类里至多包含 2^{4n^2+2n} 个函数,而 BI 4 差分置换里至少有 $2^{(2^n+2)/3}$ 个函数,因此 BI 4 差分置换里至少含有 $2^{(2^n+2)/3-4n^2-2n}$ 个不同的 CCZ 等价类[91].再次,唐灯和 Carlet 等人通过差分谱证明了 BI 4 差分置换与 Carlet-Tang-Tang-Liao 函数这两大类 4 差分置换分别与二次函数是 CCZ 不等价的,并分别从这 2 类 4 差分置换中找出了一些子类在理论上证明了这些子类与逆函数是 CCZ 不等价的[101].最后,陈玺等人提出投影差分谱的概念,将所研究的函数投影到低维空间上,检验其投影函数的投影差分谱是否满足 2 个 CCZ 等价函数投影差分谱所满足的必要条件,并通过该方法证明了所有 Carlet-Tang-Tang-Liao 函数与逆函数是 CCZ 不等价的[103].

5 应 用

本节简单地回顾低差分函数在实际密码算法中的应用.

在 Nyberg 和 Knudsen 设计的 64 b 类似 DES 的 KN 密码中,使用了域 $F_{2^{33}}$ 上二次单项式 $x \mapsto x^3$[104]. 但随后 Jakobsen 和 Knudsen 利用 x^3 函数代数次数太低的弱点提出了高阶差分攻击[105],攻破了 KN 密码. KASUMI 算法[106]使用了 64 b 的 8 轮 DES-类置换,FO 和 FL 是其中的 2 轮置换. FO 函数是一个 32 b 置换,它由含有 FI 轮置换的 3 轮 MISTY 型变换所组成. FI 函数是一个 4 轮非平衡 MISTY-type 变换所组成的 16 b 置换,它由一个 7 b APN 置换与一个 9 b APN 置换组成.

1998 年 NIST 发起了一场为了建立新分组密码标准的比赛,由比利时密码学家 Daemen 和 Rijmen 设计的 Rijndael 算法最终胜出,被遴选为 AES 算法[107]. AES 算法使用的 S-盒是有限域 F_{2^8} 上逆函数的仿射变换,这个 4 差分置换[108]达到了 8 维空间上已知最优的差分均匀度和已知最优的非线性度. 除了 AES 算法以外,Camellia 算法[109]、PRESENT 算法[110]、PRINCE 算法[111]、LED 算法[112]等近期设计算法中均使用了逆函数作为 S 盒.

FIDES 是 Bilgin 等设计的认证加密算法[113],其置换由 32 个 Dillon 等发现的 APN 置换组成. 该 APN 置换的代数次数是 4,非线性度与逆函数的非线性度相同均为 16,同样达到已知最大非线性度. 这表明对该函数的差分攻击和线性攻击与逆函数的情况类似. 但 FIDES 算法的构造设计存在缺陷. Dinur 和 Jean[114]使用猜测-决定攻击破译了 FIDES 算法,该攻击基于线性层中扩散上的弱点,S-盒的差分性质对这种攻击完全不起作用. 该结果表明,密码算法设计即使使用密码学性质良好的低差分置换,也还需要精心设计密码结构,避免存在安全缺陷.

6 总 结

综上所述,近年来国内外学者在有限域上低差分函数研究方面已经取得了许多重要的结果,但仍有许多问题亟需进一步的研究. 例如已有 PN 函数和 APN 函数构造都集中在幂函数和二次函数,如何构造一个(CCZ 等价意义下)非二次的多项式 PN 函数和 APN 函数是低差分函数研究中的一个非常重要的问题. 还有,已知的 PN 幂函数和 APN 幂函数列表是否完全? 二次 PN 函数和 APN 函数的 CCZ 等价类个数是否随变元个数增长而呈指数增长?"大 APN 问题",即一般偶扩张上是否存在 APN 置换的问题,还远没有解决. 另外,能否构造与 Gold 函数具有不同 Walsh 谱的二次 APN 函数类也是一个非常有趣的问题. 最后,尽管人们在偶扩张已经构造了大量的 4 差分置换,但像逆函数那样多种密码学指标折衷最优的密码函数的构造还很匮乏. 另外,已知偶扩张上 4 差分置换无限类要么是从逆函数出发构造的,要么与 Gold 函数联系紧密,能否通过其他的方法进行构造是非常有趣的问题. 所有这些问题都值得我们继续深入研究.

参 考 文 献

[1] Carlet C. Boolean Functions for Cryptography and Error-Correcting Codes [G] //Crama Y, Hammer P L, eds. Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge: Cambridge University Press, 2010: 257-397

[2] Carlet C. Vecotrial Boolean Functions for Cryptography [G] //Crama Y, Hammer P L, eds. Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge: Cambridge University Press, 2010: 398-469

[3] Cusick T W, Stanica P. Cryptographic Boolean Functions and Applications [M]. Amsterdam: Elsevier Press, 2009

[4] Li Chao, Qu Longjiang, Zhou Yue. Analysis of Properties of Cryptographic Functions [M]. Beijing: Science Press, 2011 (in Chinese)
(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)

[5] Wen Qiaoyan, Niu Xinxin, Yang Yixian. Boolean Functions in Modern Cryptography [M]. Beijing: Science Press, 2000 (in Chinese)
(温巧燕,钮心忻,杨义先. 现代密码学中的布尔函数[M]. 北京:科学出版社, 2000)

[6] Feng Dengguo. Spectrum Theory and Its Application in Cryptography [M]. Beijing: Science Press, 2010 (in Chinese)
(冯登国. 频谱理论及其在密码学中的应用[M]. 北京:科学出版社, 2000)

[7] Wang Shichang. S-box randomization and randomized DES chain structure [J]. Journal of Computer Research and Development, 1997, 34(7): 551-556 (in Chinese)
(王世昌. S-盒随机化与随机化 DES 链式结构[J]. 计算机研究与发展, 1997, 34(7): 551-556)

[8] Yi Jun, Ma Chuyan, Song Jian, et al. Security analysis of lightweight block cipher algorithm ESF [J]. Journal of Computer Research and Development, 2017, 54(10): 2224-2231 (in Chinese)

(尹军, 马楚焱, 宋健, 等. 轻量级分组密码算法 ESF 的安全性分析[J]. 计算机研究与发展, 2017, 54(10): 2224-2231)

[9] Xie Gaoqi, Wei Hongru. Impossible differential attack of block cipher ARIA [J]. Journal of Computer Research and Development, 2018, 55(6): 1201-1210 (in Chinese)
(谢高淇, 卫宏儒. ARIA 分组密码算法的不可能差分攻击[J]. 计算机研究与发展, 2018, 55(6): 1201-1210)

[10] 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

[11] Qu Longjiang, Li Chao, Dai Qingpin, et al. On the differential uniformities of functions over finite fields [J]. Science China Mathematics, 2013, 56(7): 1477-1484

[12] Carlet C, Ding C. Highly nonlinear mappings [J]. Journal of Complexity, 2004, 20(2/3): 205-244

[13] Ding Cunsheng, Yin Jianxing. Signal sets from functions with optimum nonlinearity [J]. IEEE Trans on Communications, 2007, 55(5): 936-940

[14] Abdukhalikov K. Symplectic spreads, planar functions, and mutually unbiased bases [J]. Journal of Algebraic Combinatorics, 2015, 41(4): 1055-1077

[15] Li Shuxing, Ge Gennian. Deterministic sensing matrices arising from near orthogonal systems [J]. IEEE Trans on Information Theory, 2014, 60(4): 2291-2302

[16] Kyureghyan G M, Pott A. Some theorems on planar mappings [C] //Proc of Int Workshop on the Arithmetic of Finite Fields (WAIFI 2008). Berlin: Springer, 2008: 117-122

[17] Weng Guobiao, Zeng Xiangyong. Further results on planar DO functions and commutative semifields [J]. Designs, Codes and Cryptography, 2012, 63(3): 413-423

[18] Dembowski P, Ostrom T G. Planes of order n with collineation groups of order n^2 [J]. Mathematische Zeitschrift, 1968, 103(3): 239-258

[19] Coulter R S, Matthews R W. Planar functions and planes of Lenz-Barlotti class Ⅱ [J]. Designs, Codes and Cryptography, 1997, 10(2): 167-184

[20] Ding Cunsheng, Yuan Jin. A family of skew Hadamard difference sets [J]. Journal of Combinatorial Theory, Series A, 2006, 113(7): 1526-1535

[21] Zha Zhengbang, Kyureghyan G M, Wang Xueli. Perfect nonlinear binomials and their semifields [J]. Finite Fields and Their Applications, 2009, 15(2): 125-133

[22] Budaghyan L, Helleseth T. New perfect nonlinear multinomials over $F_{p^{2k}}$ for any odd prime p [C] //Proc of Int Conf on Sequences and Their Applications. Berlin: Springer, 2008: 403-414

[23] Bierbrauer J. New semifields, PN and APN functions [J]. Designs, Codes and Cryptography, 2010, 54(3): 189-200

[24] Dickson L E. Linear algebras with associativity not assumed [J]. Duke Mathematical Journal, 1935, 1(2): 113-125

[25] Ganley M J. Central weak nucleus semifields [J]. European Journal of Combinatorics, 1981, 2(4): 339-347

[26] Cohen S D, Ganley M J. Commutative semifields, two dimensional over their middle nuclei [J]. Journal of Algebra, 1982, 75(2): 373-385

[27] Zhou Yue, Pott A. A new family of semifields with 2 parameters [J]. Advances in Mathematics, 2013, 234: 43-60

[28] Coulter R S, Kosick P. Commutative semifields of order 243 and 3125 [C] //Proc of the 9th Int Conf on Finite Fields and Applications. Dublin: American Mathematical Society, 2010: 129-136

[29] Weng Guobiao, Zeng Xiangyong. Further results on planar DO functions and commutative semifields [J]. Designs, Codes and Cryptography, 2012, 63(3): 413-423

[30] Coulter R S, Henderson M, Kosick P. Planar polynomials for commutative semifields with specified nuclei [J]. Designs, Codes and Cryptography, 2007, 44(1/3): 275-286

[31] Pott A. Almost perfect and planar functions [J]. Designs, Codes and Cryptography, 2016, 78(1): 141-195

[32] Zieve M E. Planar functions and perfect nonlinear monomials over finite fields [J]. Designs, Codes and Cryptography, 2015, 75(1): 71-80

[33] Zhou Yue. $(2^n, 2^n, 2^n, 1)$-relative difference sets and their representations [J]. Journal of Combinatorial Designs, 2013, 21(12): 563-584

[34] Schmidt K U, Zhou Yue. Planar functions over fields of characteristic two [J]. Journal of Algebraic Combinatorics, 2014, 40(2): 503-526

[35] Scherr Z, Zieve M E. Some planar monomials in characteristic 2 [J]. Annals of Combinatorics, 2014, 18(4): 723-729

[36] Hu Sihuang, Li Shuxing, Zhang Tao, et al. New pseudo-planar binomials in characteristic two and related schemes [J]. Designs, Codes and Cryptography, 2015, 76(2): 345-360

[37] Qu Longjiang. A new approach to constructing quadratic pseudo-planar functions over F_{2^n} [J]. IEEE Trans on Information Theory, 2016, 62(11): 6644-6658

[38] Dobbertin H, Mills D, Müller E N, et al. APN functions in odd characteristic [J]. Discrete Mathematics, 2003, 267(1/3): 95-112

[39] Helleseth T, Rong C, Sandberg D. New families of almost perfect nonlinear power mappings [J]. IEEE Trans on Information Theory, 1999, 45(2): 475-485

[40] Zha Zhengbang, Wang Xueli. Power functions with low uniformity on odd characteristic finite fields [J]. Science China Mathematics, 2010, 53(8): 1931-1940

[41] Berger T, Canteaut A, Charpin P, et al. On Almost Perfect Nonlinear Functions Over F_{2^n} [J]. IEEE Trans on Information Theory, 2006, 52(9): 4160-4170

[42] Carlet C. Characterizations of the differential uniformity of vectorial functions by the Walsh transform [J]. IEEE Trans on Information Theory, 2018, 64(9): 6443-6453

[43] Chabaud F, Vaudenay S. Links between differential and linear cryptanalysis [C] //Proc of Workshop on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1994: 356-365

[44] Leander G, Rodier F. Bounds on the degree of APN polynomials: The case of $x^{-1}+g(x)$ [J]. Designs, Codes and Cryptography, 2011, 59(1/3): 207-222

[45] Budaghyan L, Carlet C, Helleseth T, et al. On upper bounds for algebraic degrees of APN functions [J]. IEEE Trans on Information Theory, 2018, 64(6): 4399-4441

[46] Gorodilova A. Characterization of almost perfect nonlinear functions in terms of subfunctions [J]. Discrete Mathematics and Applications, 2016, 26(4): 193-202

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

[48] Nyberg K. Differentially uniform mappings for cryptography [G] //LNCS 765: Advances in Cryptology-EUROCRYPT'93. Berlin: Springer, 1994: 55-64

[49] 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

[50] Dobbertin H. Almost perfect nonlinear power functions on F_{2^n}: The Welch case [J]. IEEE Trans on Information Theory, 1999, 45(4): 1271-1275

[51] Dobbertin H. Almost perfect nonlinear power functions on F_{2^n}: The Niho case [J]. Information and Computation, 1999, 151(1/2): 57-72

[52] Beth T, Ding C. On almost perfect nonlinear permutations [G] //Proc of Workshop on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1993: 65-76

[53] Dobbertin H. Almost perfect nonlinear power functions on F_{2^n}: A new case for n divisible by 5 [C] //Proc of Finite Fields and Applications. Berlin: Springer, 2001: 113-121

[54] Dillon J. APN polynomials and related codes [OL]. [2018-03-01]. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.422.6913&rep=rep1&type=pdf

[55] Budaghyan L, Carlet C, Leander G. Two classes of quadratic APN binomials inequivalent to power functions [J]. IEEE Trans on Information Theory, 2008, 54(9): 4218-4229

[56] 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

[57] Bracken C, Byrne E, Markin N, et al. A few more quadratic APN functions [J]. Cryptography and Communications, 2011, 3(1): 43-53

[58] Budaghyan L, Carlet C, Leander G. Constructing new APN functions from known ones [J]. Finite Fields and Their Applications, 2009, 15(2): 150-159

[59] Budaghyan L, Helleseth T, Li Nian, et al. Some results on the known classes of quadratic APN functions [C]. Codes, Cryptology and Information Security. Berlin: Springer, 2017: 3-16

[60] 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

[61] Carlet C. Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions [J]. Designs, Codes and Cryptography, 2011, 59(1/3): 89-109

[62] Yu Yuyin, Wang Mingsheng, Li Yongqiang. A matrix approach for constructing quadratic APN functions [J]. Designs, Codes and Cryptography, 2014, 73(2): 587-600

[63] Weng Guobiao, Tan Yin, Gong Guang. On quadratic almost perfect nonlinear functions and their related algebraic object [C] //Proc of Workshop on Coding and Cryptography (WCC 2013). Berlin: Springer, 2013

[64] Carlet C, Gong Guang, Tan Yin. Quadratic zero-difference balanced functions, APN functions and strongly regular graphs [J]. Designs, Codes and Cryptography, 2016, 78(3): 629-654

[65] Hernando F, McGuire G. Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions [J]. Journal of Algebra, 2011, 343(1): 78-92

[66] Dempwolff U. CCZ equivalence of power functions [J]. Designs, Codes and Cryptography, 2018, 86(3): 665-692

[67] Budaghyan L. On inequivalence between known power APN functions [C] //Proc of the 4th Workshop on Boolean Functions: Cryptography and Applications (BFCA 08). Mont-Saint-Aignan: Universités de Rouen et du Havre, 2008

[68] Lachaud G, Wolfmann J. The weights of the orthogonals of the extended quadratic binary Goppa codes [J]. IEEE Trans on Information Theory, 1990, 36(3): 686-692

[69] Canteaut A, Charpin P, Dobbertin H. Weight divisibility of cyclic codes, highly nonlinear functions on Berlin F_{2^m} Berlin, and crosscorrelation of maximumlength sequences [J]. Society for Industrial and Applied Mathematics, 2000, 13(1): 105-138

[70] Yoshiara S. Equivalences of quadratic APN functions [J]. Journal of Algebraic Combinatorics, 2012, 35(3): 461-475

[71] Yoshiara S. Equivalences among plateaued APN functions [J]. Designs, Codes and Cryptography, 2017, 85(2): 205-217

[72] Bracken C, Zha Zhengbang. On the Fourier spectra of the infinite families of quadratic APN functions [J]. Advances in Mathematics of Communications, 2017, 3(3): 219-226

[73] Tan Yin, Qu Longjiang, Ling San, et al. On the Fourier spectra of new APN functions [J]. SIAM Journal on Discrete Mathematics, 2013, 27(2): 791-801

[74] Dillon J F. APN polynomials: An update [C] //Proc of the 10th Int Conf on Finite Fields and Their Applications. Dublin: University College Dublin, 2009

[75] Perrin L, Udovenko A, Biryukov A. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem [G] //Proc of Annual Cryptology Conf. Berlin: Springer, 2016: 93-122

[76] Langevin P, Saygi Z, Saygi E. Classification of APN cubics in dimension 6 over GF(2) [OL]. [2018-03-01]. http://langevin.univ-tln.fr/project/apn-6/apn-6.html

[77] Pasalic E, Charpin P. Some results concerning cryptographically significant mappings over F_{2^n} [J]. Designs, Codes and Cryptography, 2010, 57(3): 257-269

[78] Li Yongqiang, Wang Mingsheng. On EA-equivalence of certain permutations to power mappings [J]. Designs, Codes and Cryptography, 2011, 58(3): 259-269

[79] Li Yongqiang, Wang Mingsheng. Permutation polynomials EA-equivalent to the inverse function over F_{2^n} [J]. Cryptography and Communications, 2011, 3(3): 175-186

[80] Calderini M, Sala M, Villa I. A note on APN permutations in even dimension [J]. Finite Fields and Their Applications, 2017, 46(7): 1-16

[81] 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

[82] Hertel D. A note on the Kasami power function [OL]. [2018-03-01]. https://eprint.iacr.org/2005/436.pdf

[83] Bracken C, Leander G. A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree [J]. Finite Fields and Their Applications, 2010, 16(4): 231-242

[84] Bracken C, Tan C H, Tan Yin. Binomial differentially 4-uniform permutations with high nonlinearity [J]. Finite Fields and Their Applications, 2012, 18(3): 537-546

[85] Carlet C. On known and new differentially uniform functions [C] //Proc of Australasian Conf on Information Security and Privacy. Berlin: Springer, 2011: 1-15

[86] Li Yongqiang, Wang Mingsheng. Constructing differentially 4-uniform permutations over $F_{2^{2m}}$ from quadratic APN permutations over GF($2^{(2m+1)}$) [J]. Designs, Codes and Cryptography, 2014, 72(2): 249-264

[87] 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 Trans on Information Theory, 2017, 63(11): 7575-7591

[88] Fu Shihui, Feng Xiutao. Further results of the cryptographic properties on the butterfly structures [OL]. [2018-03-01]. http://arxiv.1607.08455

[89] Fu Shihui, Feng Xiutao, Wu Baofeng. Differentially 4-uniform permutations with the best known nonlinearity from butterflies [J]. IACR Trans on Symmetric Cryptology, 2017, 2017(2): 228-249

[90] Qu Longjiang, Tan Yin, Tan Chik How, et al. Constructing differentially 4-uniform permutations Over $F_{2^{2k}}$, via the switching method [J]. IEEE Trans on Information Theory, 2013, 59(7): 4675-4686

[91] Qu Longjiang, Tan Yin, Li Chao, et al. More constructions of differentially 4-uniform permutations on $F_{2^{2k}}$ [J]. Designs, Codes and Cryptography, 2016, 78(2): 391-408

[92] Chen Xi, Deng Yazhi, Zhu Min, et al. An equivalent condition on the switching construction of differentially 4-uniform permutations on from the inverse function [J]. International Journal of Computer Mathematics, 2017, 94(6): 1252-1267

[93] Zha Zhengbang, Hu Lei, Sun Siwei. Constructing new differentially 4-uniform permutations from the inverse function [J]. Finite Fields and Their Applications, 2014, 25(4): 64-78

[94] Zha Zhenbang, Hu Lei, Sun Siwei, et al. Further results on differentially 4-uniform permutations over $F_{2^{2m}}$ [J]. Science China Mathematics, 2015, 58(7): 1577-1588

[95] Peng Jie, Tan C H. New explicit constructions of differentially 4-uniform permutations via special partitions of $F_{2^{2m}}$ [J]. Finite Fields and Their Applications, 2016, 40(7): 73-89

[96] Fu Shihui, Feng Xiutao. Involutory differentially 4-uniform permutations from known constructions [OL]. [2018-03-01]. http://eprint.iacr.org/2017/292

[97] Li Yongqiang, Wang Mingsheng, Yu Yuyin. Constructing differentially 4-uniform permutations over GF(2^{2k}) from the inverse function revisited, 2013/731 [OL]. [2018-03-01]. https://eprint.iacr.org/2013/731

[98] Peng Jie, Tan C H. New differentially 4-uniform permutations by modifying the inverse function on subfields [J]. Cryptography and Communications, 2017, 9(3): 363-378

[99] Peng Jie, Tan C H, Wang Qichun. A new family of differentially 4-uniform permutations over $F_{2^{2k}}$ for odd k [J]. Science China Mathematics, 2016, 59(6): 1221-1234

[100] Peng Jie, Tan C H, Wang Qichun. New secondary construction of differentially 4-uniform permutations over $F_{2^{2k}}$ [J]. International Journal of Computer Mathematics, 2017, 94(8): 1670-1693

[101] Tang Deng, Carlet C, Tang Xiaohu. Differentially 4-uniform bijections by permuting the inverse function [J]. Designs, Codes and Cryptography, 2015, 77(1): 117-141

[102] Carlet C, Tang Deng, Tang Xiaohu, et al. New construction of differentially 4-uniform bijections [C] //Proc of Int Conf on Information Security and Cryptology. Berlin: Springer, 2013: 22-38

[103] Chen Xi, Qu Longjiang, Li Chao, et al. A new method to investigate the CCZ-equivalence between functions with low differential uniformity [J]. Finite Fields and Their Applications, 2016, 42(11): 165-186

[104] Nyberg K, Knudsen L R. Provable security against a differential attack[J]. Journal of Cryptology, 1995, 8(1): 27-37

[105] Jakobsen T, Knudsen L R. The interpolation attack on block ciphers[C]//Proc of Int Workshop on Fast Software Encryption (FSE 1997). Berlin: Springer, 1997: 28-40

[106] Matsui M. New block encryption algorithm MISTY[C]// Proc of Int Workshop on Fast Software Encryption (FSE 1997). Berlin: Springer, 1997: 54-68

[107] Daemen J, Rijmen V. AES proposal: Rijndael[OL]. 1999 [2018-03-01]. http://www.cs.miami.edu/home/burt/learning/Csc688.012/rijndael/rijndael_doc_V2.pdf

[108] Nyberg K. Differentially uniform mappings for cryptography[C]//Proc of Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT 1993). Berlin: Springer, 1993: 55-64

[109] Aoki K, Ichikawa T, Kanda M, et al. Camellia: A 128-bit block cipher suitable for multiple platforms—design and analysis[C]//Proc of Int Workshop on Selected Areas in Cryptography (SAC 2000). Berlin: Springer, 2000: 39-56

[110] Bogdanov A, Knudsen L R, Leander G, et al. PRESENT: An ultralightweight block cipher [C]//Proc of Int Workshop on Crypto-graphic Hardware and Embedded Systems (CHES 2007). Berlin: Springer, 2007: 450-466

[111] Borghoff J, Canteaut A, Güneysu T, et al. Prince-a low-latency block cipher for pervasive computing applications [C]//Proc of Int Conf on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2012). Berlin: Springer, 2012: 208-225

[112] Guo Jian, Peyrin T, Poschmann A, et al. The LED block cipher[C]//Proc of Cryptographic Hardware and Embedded Systems (CHES 2011). Berlin: Springer, 2011: 326-341

[113] Bilgin B, Bogdanov A, Knežević M, et al. Fides: Lightweight authenticated cipher with side-channel resistance for constrained hardware[C]//Proc of Cryptographic Hardware and Embedded Systems (CHES 2013). Berlin: Springer, 2013: 142-158

[114] Dinur I, Jean J. Cryptanalysis of FIDES[C]//Proc of Int Workshop on Fast Software Encryption (FSE 2014). Berlin: Springer, 2014: 224-240

Qu Longjiang, born in 1980. PhD, professor, PhD supervisor. His main research interests includes cryptography and coding theory.

Chen Xi, born in 1990. PhD candidate. His main research interests includes cryptography and Boolean functions (1138470214@qq.com).

Niu Tailin, born in 1995. Master candidate. His main research interests include cryptography and Boolean functions (runingniu@live.cn).

Li Chao, born in 1966. PhD, professor, PhD supervisor. His main research interests include cryptography and coding theory (lichao_nudt@sina.com).