DOI:10.19789/j.1004-9398.2025.05.004
文献引用:朱思敏,王艳,李顺波,等.低c-差分及回旋镖均匀度置换的构造[J].首都师范大学学报(自然科学版),2025,46(5):20-27. ZHU S M, WANG Y, LI S B, et al. Construction of permutations with low c-differential and boomerang uniformities[J]. Journal of Capital Normal University (Natural Science Edition),2025,46(5):20-27.

低c-差分及回旋镖均匀度置换的构造*

朱思敏, 王 艳**, 李顺波, 付妍希
(西安建筑科技大学理学院, 陕西 西安 710311)

摘要:具有低c-差分均匀度及低回旋镖均匀度的向量布尔函数,尤其是几乎完全c-非线性函数,在密码学中有广泛的应用。本文利用有限域上的迹函数构造了一类新的非单项函数,通过计算Weil和获得了这类函数的c-差分分布表,并推断其在有限域上是几乎完全c-非线性函数。进而证明了已构造的函数具有低回旋镖均匀度。

关键词:向量布尔函数;c-差分均匀度;回旋镖均匀度;完全c-非线性函数;几乎完全c-非线性函数
中图分类号:TN918.1 **文献标志码**:A

Construction of permutations with low c-differential and boomerang uniformities*

ZHU Simin, WANG Yan**, LI Shunbo, FU Yanxi
(School of Science, Xi'an University of Architecture and Technology, Xi'an Shaanxi 710311)

Abstract: Vectorial boolean functions with low c-differential and boomerang uniformities, especially the almost perfect c-nonlinear functions, are widely used in cryptography. This paper constructed a new class of non-monomial functions over finite fields by using trace functions. By calculating Weil sums we obtained the c-difference distribution table of this class of functions, and we concluded that they are almost perfect c-nonlinear functions over finite fields. Furthermore, it is proved that the constructed functions have low boomerang uniformity.

Keywords: Vectorial boolean function; c-differential uniformity; boomerang uniformity; perfect c-nonlinear function; almost perfect c-nonlinear function
CLC: TN918.1 **DC**: A

0 引 言

为抵抗多种针对密码系统的攻击,设计满足相应安全性指标的密码函数受到广泛关注。学者们比较关注的密码函数安全性指标包括非线性度、平衡性、差分均匀度、c-差分均匀度和回旋镖均匀度等。

在分组密码中,差分密码攻击[1-2]是常见的攻击方式之一。为了评估密码函数抵抗差分攻击的能力,1993年,Nyberg[3]首次提出了差分均匀度的概念。低差分均匀度函数通常是指差分均匀度值<4的函数。对于$\mathbb{F}_{2^n}$上的向量布尔函数,当其差分均匀度为1时,称其为完全非线性函数;当其差分均匀度

收稿日期:2023-09-12
*国家自然科学基金项目(61902304);应用数学湖北省重点实验室2022年度开放基金项目(HBAM202202)
**通信作者:wangyan@xauat.edu.cn

为 2 时，称其为几乎完全非线性函数。目前，学者们对于低差分均匀度函数已经做了大量研究，参见文献[4-14，16-20]，以及其中的参考文献。

2002 年，Borisov 等[11]介绍了一种新的乘法差分分析方法，即通过输入明文对 (cx, x) 来分析输出的密文对 $(F(cx), F(x))$。基于这种新的差分分析方法，Ellingsen 等[12]提出了 c-差分均匀度的概念，具体定义如下。

定义 1.1[12]　设 n 为正整数，p 为素数，$\mathbb{F}_{p^n}$ 是有 p^n 个元素的有限域，f 是从 $\mathbb{F}_{p^n}$ 到自身的函数。对于 $a, c \in \mathbb{F}_{p^n}$，$f$ 的 c-差分为

$$_cD_f(x, a) = f(x + a) + cf(x)。$$

设 $_c\Delta_f(a, b) = \#\{x \in \mathbb{F}_{p^n} : {}_cD_a f(x) = b\}$，其中 $b \in \mathbb{F}_{p^n}$。称

$$_c\Delta_f \coloneqq \max_{a, b \in \mathbb{F}_{p^n}} \{{}_c\Delta_f(a, b)：若 c = 1，则 a \neq 0\}$$

为 f 的 c-差分均匀度。若 $_c\Delta_f = 1$，则称 f 为完全 c-非线性函数（perfect c-nonlinear function，PcN）；若 $_c\Delta_f = 2$，则称 f 为几乎完全 c-非线性函数（almost perfect c-nonlinear function，APcN）。特别地，当 $c = 1$ 时，函数的 1-差分均匀度即为差分均匀度。且以方程 $_cD_f(x, a) = b$ 的解 $x \in \mathbb{F}_{p^n}$ 的个数为 (a, b) 处的值，可形成 f 的 c-差分分布表（c-difference distribution table，c-DDT），其中，c-DDT 中除去第 1 行和第 1 列的最大数，即 f 的 c-差分均匀度。

当 $c \notin \{0, 1\}$ 时，Ellingsen 等[12]研究了一些已知的幂函数以及它们逆函数的 c-差分均匀度；Hasan 等[15]给出线性化多项式为完全 c-非线性函数的充要条件，并利用 Dickson 多项式研究了当 $c = -1$ 时，几类幂函数的 c-差分均匀度；Wu 等[20]运用分圆法、AGW 准则等构造了几类 c-差分均匀度 ≤2 的函数。Bartoli 和 Calderini[21]、Stanica[22]通过运用 AGW 准则及其推广与交换的方法构造了几类非单项式 APcN 函数。目前，常见的 PcN 和 APcN 幂函数可见表 1[12-18]和表 2[12,15-16,19]。

回旋镖均匀度是另一个关于密码函数安全性的重要指标，刻画的是函数抵抗回旋镖攻击的能力。回旋镖攻击是由 Wagner[23]提出的差分密码攻击的一种变体。为了简化回旋镖攻击的复杂度分析，Cid 等[24]首次提出了回旋镖连接表（boomerang connectivity table，BCT），并分析了回旋镖连接表与差分分布表之间的关系。为了量化函数抵抗回旋镖攻击的能力，Boura 和 Canteaut[25]介绍了回旋镖均匀度的概念，其是回旋镖连接表中去掉第 1 行与第 1 列的最大值；Li 等[26]给出了回旋镖均匀度的等价定义，并找到了 $\mathbb{F}_{2^n}$ 中一类 4 回旋镖均匀度的置换二项式。随后，Calderini 和 Villa[27]给出了 3 类 4 回旋镖均匀度的置换二项式；Hasan 等[28]、Stanica[29]利用 Weil 和得到几类低回旋镖均匀度函数。本文推广了文献[28]中非单项函数的构造，并进一步研究了此类非单项式函数的 c-差分均匀度与回旋镖均匀度。

表 1　$\mathbb{F}_{p^n}$ 上常见的 $F(x) = x^d$ 型 PcN 幂函数

p	d	条件	参考文献
任意	2	c=0	[12]
2	$(3^k + 1)/2$	c=−1，$\frac{n}{\gcd(k, m)} = 1$	[12]
奇数	$(p^2 + 1)/2$	c=−1，m 是奇数	[13]
奇数	$p^2 - p + 1$	c=−1，m=3	[13]
奇数	$p^4 + (p - 2)p^2 + (p - 1) + 1$	c=−1，m=5	[14]
奇数	$(p^5 + 1)/(p + 1)$	c=−1，m=5	[14]
奇数	$(p - 1)p^6 + p^5 + (p - 2)p^3 + (p - 1)p^2 + p$	c=−1，m=7	[14]
奇数	$(p - 1)p^6 + (p - 2)p^5 + (p - 1)p^4 + p^3 + p^2 + p$	c=−1，m=7	[14]
奇数	$(p^7 + 1)/(p + 1)$	c=−1，m=7	[14]
奇数	$(p^k + 1)/2$	$v_2(m) \leqslant v_2(k) + 1$，$c$=−1	[15]
2	$2^k + 1$	$v_2(m) \leqslant v_2(k) + 1$，$c \in \mathbb{F}_{2^{\gcd(m,k)}}$	[18]
3	$\frac{3^k + 1}{2} d \equiv \frac{3^m + 1}{2} \pmod{3^m - 1}$，$d$ 是奇数	k, m 是奇数，$\gcd(m, k) = 1$	[17]
5	$\frac{5^k + 1}{2} d \equiv \frac{5^m + 1}{2} \pmod{5^m - 1}$，$d$ 是奇数	k, m 是正整数，$\gcd(2m, k) = 1$	[16]

表2 $\mathbb{F}_{p^n}$上常见的$F(x)=x^d$型APcN幂函数

p	d	条件	参考文献
任意	2	$c\neq 1$	[12]
2	2^m-2	$\mathrm{Tr}_1^m(c)=\mathrm{Tr}_1^m(c^{-1})=1$	[12]
奇数	p^m-2	$c=4,4^{-1}$或$\chi(c^2-4c)=\chi(1-4c)=-1$	[12]
3	$\frac{3^n+3}{2}$	$c=-1,m$是偶数	[15]
3	3^n-3	$c=0$	[15]
奇数	p^k+1	$v_2(m)\leqslant v_2(k)+1, c\in\mathbb{F}_{p^{\gcd(m,k)}}$	[15]
3	$\frac{3^k+1}{2}$	k是奇数, $c=-1$ $\gcd(k,m)=1$	[16]
2	$2^{3n}+2^{2n}+2^n-1$	$c\in\mathbb{F}_{2^{4n}}\setminus\{1\}, c^{2^{2n}+1}=1$	[19]

1 预备知识

设p为素数,n为正整数,$\mathbb{F}_{p^n}$是具有p^n个元素的有限域,记$\mathbb{F}_{p^n}$的乘法群为$\mathbb{F}_{p^n}^*$,$\mathbb{F}_{p^n}[x]$是$\mathbb{F}_{p^n}$上的一元多项式环且$\#S$表示集合S中元素的个数。令正整数n, d, m满足$n=md$,定义

$$\mathrm{Tr}_d^n(x)=\sum_{k=0}^{m-1}x^{p^{dk}}=x+x^{p^d}+x^{p^{2d}}+\cdots+x^{p^{(m-1)d}}$$

为$\mathbb{F}_{p^n}$到$\mathbb{F}_{p^d}$的迹函数[30]。特别地,$\mathrm{Tr}_1^n(x)$被称为$\mathbb{F}_{p^n}$到$\mathbb{F}_p$的绝对迹函数,简记为$\mathrm{Tr}(x)$。

定义1.2[24] 设F是从$\mathbb{F}_{p^n}$到自身的可逆函数。对于$(a,b)\in\mathbb{F}_{p^n}\times\mathbb{F}_{p^n}$,称以

$$\mathcal{B}_F(a,b)=\#\{x\in\mathbb{F}_{p^n}: F^{-1}(F(x)+b)+F^{-1}(F(x+a)+b)=a\}$$

为元素的表格为$F(x)$在(a,b)处的BCT;称BCT中除去第1行第1列的最大数值$\mathcal{B}_F:=\max\limits_{a,b\in\mathbb{F}_{p^n}^*}\mathcal{B}_F(a,b)$为$F(x)$的回旋镖均匀度;此时,称$F(x)$是一个$\mathcal{B}_F$-回旋镖均匀度函数。

引理1.1[26] 设F是$\mathbb{F}_{p^n}$到自身的置换。则$F(x)$在(a,b)处的BCT的值等价于满足方程组

$$\begin{cases}F(x)+F(y)=b,\\ F(x+a)+F(y+a)=b\end{cases}\tag{1}$$

的解$(x,y)\in\mathbb{F}_{p^n}\times\mathbb{F}_{p^n}$的个数,其中$a,b\in\mathbb{F}_{p^n}^*$。

定义1.3[31] 设F是从$\mathbb{F}_{p^n}$到自身的函数。称

$$\mathcal{W}_F(u)=\sum_{x\in\mathbb{F}_{p^n}}(-1)^{F(x)+\mathrm{Tr}(ux)},\ u\in\mathbb{F}_{p^n}$$

为F的Walsh-Hadamard变换,其中$\mathrm{Tr}(\cdot)$是$\mathbb{F}_{p^n}$到$\mathbb{F}_p$的绝对迹函数。

定义1.4[30] 设$\chi_1:\mathbb{F}_{2^n}\to\mathbb{C}$,

$$\chi_1(x):=\exp\left(\frac{2\pi i\mathrm{Tr}(x)}{2}\right)=(-1)^{\mathrm{Tr}(x)},$$

称$\chi_1(x)$为$\mathbb{F}_{2^n}$的加法群的正则加法特征。

定义1.5[30] 称$\mathbb{F}_{p^n}$上的多项式

$$l(x)=\sum_{i=0}^{n}a_ix^i\text{和}L(x)=\sum_{i=0}^{n}a_ix^{p^i}$$

为p-相互关联的;称$l(x)$是$L(x)$的常规p-关联,$L(x)$是$l(x)$的线性化p-关联。

定义1.6[30] 设F是$\mathbb{F}_{p^n}$到自身的函数,“$\circ$”为映射的复合。若$F\circ F(x)=x$,则称F是$\mathbb{F}_{p^n}$上的对合。

引理1.2[30] 设F是$\mathbb{F}_{2^n}^n=\mathbb{F}_{2^n}\times\cdots\times\mathbb{F}_{2^n}$到$\mathbb{F}_{2^n}$的任意映射。对于确定的$b\in\mathbb{F}_{2^n}$,记方程$F(x_1,x_2,\cdots,x_n)=b$的解$(x_1,x_2,\cdots,x_n)\in\mathbb{F}_{2^n}^n$的个数为$N(b)$,其中

$$N(b)=\frac{1}{2^n}\sum_{x_1\in\mathbb{F}_{2^n}}\cdots\sum_{x_n\in\mathbb{F}_{2^n}}\sum_{\beta\in\mathbb{F}_{2^n}}\chi_1(\beta(F(x_1,x_2,\cdots,x_n)+b))=$$
$$\frac{1}{2^n}\sum_{x_1\in\mathbb{F}_{2^n}}\cdots\sum_{x_n\in\mathbb{F}_{2^n}}\sum_{\beta\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(F(x_1,x_2,\cdots,x_n)+b))}。\tag{2}$$

引理1.3[30] 设F是$\mathbb{F}_{2^n}^n$到$\mathbb{F}_{2^n}$的任意映射。对于确定的$b=(b_1,b_2)\in\mathbb{F}_{2^n}^2$,记方程组$\begin{cases}F_1(x_1,x_2,\cdots,x_n)=b_1,\\ F_2(x_1,x_2,\cdots,x_n)=b_2\end{cases}$的解$(x_1,x_2,\cdots,x_n)\in\mathbb{F}_{2^n}^n$的个数为$\hat{N}(b)$,其中

$$\hat{N}(b)=$$
$$\frac{1}{2^{2n}}\sum_{x_1\in\mathbb{F}_{2^n}}\cdots\sum_{x_n\in\mathbb{F}_{2^n}}\sum_{\beta\in\mathbb{F}_{2^n}}x_1(\beta(F_1(x_1,x_2,\cdots,x_n)+b_1))\cdot$$
$$\sum_{\gamma\in\mathbb{F}_{2^n}}x_1(\gamma(F_2(x_1,x_2,\cdots,x_n)+b_2))=$$
$$\frac{1}{2^{2n}}\sum_{x_1\in\mathbb{F}_{2^n}}\cdots\sum_{x_n\in\mathbb{F}_{2^n}}\sum_{\beta\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(F_1(x_1,x_2,\cdots,x_n)+b_1))}\cdot$$
$$\sum_{\gamma\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\gamma(F_2(x_1,x_2,\cdots,x_n)+b_2))}。\tag{3}$$

2 一类非单项置换的c-差分均匀度

设n, k, i, m, $d\in\mathbb{N}^+$,且$n=2k+1$,$i=2m+$

$1, m = 2^{d-1}$。构造 $\mathbb{F}_{2^n}$ 上的函数 $H(x)$ 为

$$H(x) = x + \mathrm{Tr}(x^{2^k+i} + (x+1)^{2^k+i}),$$

式中 $\mathrm{Tr}(\cdot)$ 是 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_2$ 的绝对迹函数。等价地,

$$H(x) = x + \mathrm{Tr}(x^{2^k+i} + (x+1)^{2^k+i}) = x + 1 + \mathrm{Tr}(x^{2^k+i-1} + x^{2^k+1} + x^i + x)。 \quad (4)$$

引理 2.1　设 $n, k, i, m, d \in \mathbb{N}^+$, $n=2k+1$, $i=2m+1$ 且 $m=2^{d-1}$。则函数 $H(x)=x+\mathrm{Tr}(x^{2^k+i}+(x+1)^{2^k+i})$ 是 $\mathbb{F}_{2^n}$ 上的对合。

证明　对于所有的 $x \in \mathbb{F}_{2^n}$,

$$H \circ H(x) = x + \mathrm{Tr}(x^{2^k+i} + (x+1)^{2^k+i}) + \mathrm{Tr}((x + \mathrm{Tr}(x^{2^k+i} + (x+1)^{2^k+i}))^{2^k+i} + (x + 1 + \mathrm{Tr}(x^{2^k+i} + (x+1)^{2^k+i}))^{2^k+i}) = x。$$

式中

$$\mathrm{Tr}((x + \mathrm{Tr}(x^{2^k+i} + (x+1)^{2^k+i}))^{2^k+i}) = \mathrm{Tr}((x + \mathrm{Tr}(x^{2^k+i} + (x+1)^{2^k+i}))^{2^k} \cdot (x + \mathrm{Tr}(x^{2^k+i} + (x+1)^{2^k+i}))^i) = \mathrm{Tr}((x + \mathrm{Tr}(x^{2^k+i} + (x+1)^{2^k+i}))^{2^k} \cdot (x^i + (x^{i-1} + x + 1)\mathrm{Tr}(x^{2^k+i} + (x+1)^{2^k+i}))) = \mathrm{Tr}(x^{2^k+i}) + \mathrm{Tr}(x^{2^k+i-1} + x^{2^k+i-1} + x^{2^k+1} + x^i + x + 1) \cdot \mathrm{Tr}(x^{2^k+i} + (x+1)^{2^k+i})。$$

$$\mathrm{Tr}(x + 1 + \mathrm{Tr}(x^{2^k+i} + (x+1)^{2^k+i})^{2^k+i}) = \mathrm{Tr}(((x+1) + \mathrm{Tr}(x^{2^k+i} + (x+1)^{2^k+i}))^{2^k} \cdot ((x+1)^i + ((x+1)^{i-1} + x)\mathrm{Tr}(x^{2^k+i} + (x+1)^{2^k+i}))) = \mathrm{Tr}(x+1)^{2^k+i} + \mathrm{Tr}(x^{2^k+i-1} + x^{2^k+i-1} + x^{2^k+1} + x^i + x + 1)\mathrm{Tr}(x^{2^k+i} + (x+1)^{2^k+i})。$$

引理 2.2　设 $n, k, i, m, d \in \mathbb{N}^+$, 且 $n = 2k+1$, $i = 2m+1$, $m = 2^{d-1}$, $\gcd(n, d) = 1$, $(k-d) | d$。设 $g(x) = x^{2^{k-d}} + x^{2^{d-k}} + x^{2^k} + x^{2^{-k}} + x^{2^d} + x^{2^{-d}}$。则

$$\mathrm{Tr}(x^{i-1}a^{2^k} + x^{2^k}a^{i-1} + x^{2^k}a + xa^{2^k} + x^{i-1}a + xa^{i-1}) = \mathrm{Tr}(g(x)a) = \mathrm{Tr}(xg(a))。$$

证明

$$\mathrm{Tr}(x^{i-1}a^{2^k} + x^{2^k}a^{i-1} + x^{2^k}a + xa^{2^k} + x^{i-1}a + xa^{i-1}) = \mathrm{Tr}(x^{2^d}a^{2^k}) + \mathrm{Tr}(x^{2^k}a^{2^d}) + \mathrm{Tr}(x^{2^k}a) + \mathrm{Tr}(xa^{2^k}) + \mathrm{Tr}(x^{2^d}a) + \mathrm{Tr}(xa^{2^d}) = \mathrm{Tr}((x^{2^{k-d}} + x^{2^{d-k}} + x^{2^k} + x^{2^{-k}} + x^{2^d} + x^{2^{-d}})a) = \mathrm{Tr}(g(x)a)。$$

同理可得

$$\mathrm{Tr}(x^{i-1}a^{2^k} + x^{2^k}a^{i-1} + x^{2^k}a + xa^{2^k} + x^{i-1}a + xa^{i-1}) = \mathrm{Tr}(x(a^{2^{k-d}} + a^{2^{d-k}} + a^{2^k} + a^{2^{-k}} + a^{2^d} + a^{2^{-d}})) = \mathrm{Tr}(xg(a))。$$

引理 2.3　设 $n, k, i, m, d \in \mathbb{N}^+$, 且 $n = 2k+1$, $i = 2m+1$, $m = 2^{d-1}$, $\gcd(n, d) = 1$, $(k-d) | d$。设 $h(x) = x^{2^k+i-1} + x^{2^k+1} + x^i$ 是 $\mathbb{F}_{2^n}$ 上的函数。则

$$W_h(u) = \begin{cases} 0, & \text{若 } \mathrm{Tr}(u) = 0, \\ (-1)^{\mathrm{Tr}(\sigma^{2^{k+1+d}} + \sigma^{2^{k+1}+1} + \sigma^{2^{k+1-d}+1} + \sigma^{2^{k+1}+1} + \delta\sigma)} W_h(\sigma), & \\ \text{若 } \mathrm{Tr}(u) = 1, & \end{cases}$$

式中, $\sigma, \delta \in \mathbb{F}_{2^n}$, $\mathrm{Tr}(\delta) = 1$ 且 $g(\sigma) = u + \delta$。

证明　设 $\sigma \in \mathbb{F}_{2^n}$, 则根据定义 1.3 得

$$\mathcal{W}_h(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}((x+\sigma)^{2^k+i-1} + (x+\sigma)^{2^k+1} + (x+\sigma)^i + u(x+\sigma))} = (-1)^{\mathrm{Tr}(\sigma^{2^k+i-1} + \sigma^{2^k+1} + \sigma^i + u\sigma)} \cdot \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(x^{2^k+i-1} + x^{2^k+1} + x^i + x(g(\sigma)+u))}。 \quad (5)$$

显然, $\mathrm{Tr}(g(\sigma)) = 0$。若 $\mathrm{Tr}(u) = 0$, 可选一个 σ 使得 $g(\sigma) = u$。则式 (5) 中的求和变为 $\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(x^{2^k+i-1} + x^{2^k+1} + x^i)} = 0$, 即 $\mathcal{W}_h(u) = 0$。

若 $\mathrm{Tr}(u) = 1$, 可选一个 σ 使得 $g(\sigma) = u + \delta$, 其中 $\mathrm{Tr}(\delta) = 1$。则式 (5) 中的求和变为 $\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(x^{2^k+i-1} + x^{2^k+1} + x^i + \delta x)} = W_h(\delta)$, 即

$$\mathcal{W}_h(u) = (-1)^{\mathrm{Tr}(\sigma^{2^k+i-1} + \sigma^{2^k+1} + \sigma^i + u\sigma)} W_h(\sigma) = (-1)^{\mathrm{Tr}(\sigma^{2^{k+1+d}} + \sigma^{2^{k+1}+1} + \sigma^{2^{k+1-d}+1} + \sigma^{2^{k+1}+1} + \delta\sigma)} W_h(\delta)。$$

定理 2.1　设 $n, k, i, m, d \in \mathbb{N}^+$, 且 $n = 2k+1$, $i = 2m+1$, $m = 2^{d-1}$, $\gcd(n, d) = 1$, $(k-d) | d$。则对于任意的 $a, b \in \mathbb{F}_{2^n}$, $c \in \mathbb{F}_{2^n} \setminus \{0, 1\}$, $H(x)$ 在 (a, b) 处的 c-差分分布表的值为

$${}_c\Delta_H(a, b) = \begin{cases} 0, & \text{若 } A = 1 \text{ 且 } B = 1, \\ 1, & \text{若 } B = 0, \\ 2, & \text{若 } A = 0 \text{ 且 } B = 1, \end{cases}$$

即 $H(x)$ 是 $\mathbb{F}_{2^n}$ 上的 APcN 置换, 式中,

$$A = \mathrm{Tr}((a+b)g(a)(1+c)^{-1} + a^{2^k+i-1} + a^{2^k+1} + a^i + a),$$
$$B = \mathrm{Tr}(g(a)(1+c)^{-1})。$$

证明　$H(x)$ 在点 (a, b) 处的值为下列方程的解 $x \in \mathbb{F}_{p^n}$ 的个数, 其中 $a, b \in \mathbb{F}_{2^n}$。

$$b = H(x+a) + cH(x) = x + a + 1 + \mathrm{Tr}((x+a)^{2^k+i-1} + (x+a)^{2^k+1} + (x+a)^i + x + a) + c(x + 1 + \mathrm{Tr}(x^{2^k+i-1} + x^{2^k+1} + x^i + x)) = (c+1)(x + 1 + \mathrm{Tr}(x^{2^k+i-1} + x^{2^k+1} + x^i + x)) + a + 1 + \mathrm{Tr}(a^{2^k+i-1} + a^{2^k+1} + a^i + a) + \mathrm{Tr}(x^{i-1}a^{2^k} + x^{2^k}a^{i-1} + x^{2^k}a + xa^{2^k} + x^{i-1}a + xa^{i-1}) + 1 = (c+1)H(x) + H(a) + \mathrm{Tr}(xg(a)) + 1,$$

上式等价于

$$(c+1)H(x)+H(a)+\mathrm{Tr}(xg(a))+1+b=0。\tag{6}$$

根据引理1.2,方程(6)的解$x\in\mathbb{F}_{2^n}$的个数为

$$_c\Delta_H(a,b)=$$

$$\frac{1}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta((c+1)H(x)+H(a)+\mathrm{Tr}(xg(a))+1+b))}=$$

$$\frac{1}{2^n}\sum_{\beta\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(H(a)+1+b))}\cdot$$

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(c+1)H(x))+\mathrm{Tr}(\beta)\mathrm{Tr}(xg(a))}=$$

$$\frac{1}{2^n}(C_0+C_1),$$

式中C_0与C_1分别是$\mathrm{Tr}(\beta)=0$与$\mathrm{Tr}(\beta)=1$时的和。下面将分别计算C_0和C_1。

$$C_0=\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=0}(-1)^{\mathrm{Tr}(\beta(H(a)+1+b))}\cdot$$

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(1+c)H(x))}=$$

$$2^n+\sum_{\beta\in\mathbb{F}_{2^n}^*,\,\mathrm{Tr}(\beta)=0}(-1)^{\mathrm{Tr}(\beta(H(a)+1+b))}\cdot$$

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(1+c)H(x))}=2^n,$$

因为$\beta(1+c)\neq0$且$H(x)$是$\mathbb{F}_{2^n}$上的对合,所以

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(1+c)H(x))}=0。$$

$$C_1=\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta(H(a)+1+b))}\cdot$$

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(c+1)H(x))+\mathrm{Tr}(xg(a))}=$$

$$\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta(H(a)+1+b))}\cdot$$

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(c+1)(x+1+\mathrm{Tr}(x^{2^k+i-1}+x^{2^k+1}+x^i+x)))+\mathrm{Tr}(xg(a))}=$$

$$\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta(H(a)+b+c))}\cdot$$

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(c+1))\mathrm{Tr}(x^{2^k+i-1}+x^{2^k+1}+x^i+x)+\mathrm{Tr}(x(\beta(c+1)+g(a)))}=$$

$$C_{1,0}+C_{1,1},$$

式中$C_{1,0}$与$C_{1,1}$分别是$\mathrm{Tr}(\beta(c+1))=0$(即$\mathrm{Tr}(\beta c)=1$)与$\mathrm{Tr}(\beta(c+1))=1$(即$\mathrm{Tr}(\beta c)=0$)时的和。下面将分别计算$C_{1,0}$和$C_{1,1}$。

$$C_{1,0}=\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=1=\mathrm{Tr}(\beta c)}(-1)^{\mathrm{Tr}(\beta(H(a)+b+c))}\cdot$$

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(x(\beta(c+1)+g(a)))}=$$

$$\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=1=\mathrm{Tr}(\beta c)}(-1)^{\mathrm{Tr}(\beta(a+1+\mathrm{Tr}(a^{2^k+i-1}+a^{2^k+1}+a^i+a)+b+c))}\cdot$$

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(x(\beta(c+1)+g(a)))}=$$

$$\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=1=\mathrm{Tr}(\beta c)}(-1)^{\mathrm{Tr}(\beta(a+b)+a^{2^k+i-1}+a^{2^k+1}+a^i+a)}\cdot$$

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(x(\beta(c+1)+g(a)))}=$$

$$\begin{cases}0, & \text{若 } B=0,\\ 2^n\cdot(-1)^A, & \text{若 } B=1,\end{cases}$$

式中:$A=\mathrm{Tr}((a+b)g(a)(1+c)^{-1}+a^{2^k+i-1}+a^{2^k+1}+a^i+a)$;$B=\mathrm{Tr}(g(a)(1+c)^{-1})$,最后1个等号成立当且仅当$\beta(c+1)=g_1(a)$。

$$C_{1,1}=\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=1,\,\mathrm{Tr}(\beta c)=0}(-1)^{\mathrm{Tr}(\beta(H(a)+b))}\cdot$$

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(x^{2^k+i-1}+x^{2^k+1}+x^i+x(\beta(c+1)+g(a)))}=$$

$$\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=1,\,\mathrm{Tr}(\beta c)=0}(-1)^{\mathrm{Tr}(\beta(H(a)+b))}\mathcal{W}_h(u),$$

式中$\mathcal{W}_h(u)$见定义1.3,$u=1+\beta(c+1)+g(a)$,且$h(x)=\mathrm{Tr}(x^{2^k+i-1}+x^{2^k+1}+x^i)$是$\mathrm{F}_{2^n}$上的函数。显然,$\mathrm{Tr}(u)=\mathrm{Tr}(1+\beta(c+1)+g(a))=0$,由引理2.3可得$C_{1,1}=0$。

综上所述,对于$c\in\mathbb{F}_{2^n}\backslash\{0,1\}$,方程(6)的解$x\in\mathbb{F}_{2^n}$的个数为

$$_c\Delta_H(a,b)=\begin{cases}0, & \text{若}A=1\text{ 且 }B=1,\\ 1, & \text{若}B=0,\\ 2, & \text{若}A=0\text{ 且 }B=1,\end{cases}$$

即$H(x)$是$\mathbb{F}_{2^n}$上的APcN置换,式中:$A=\mathrm{Tr}((a+b)g(a)(1+c)^{-1}+a^{2^k+i-1}+a^{2^k+1}+a^i+a)$,$B=\mathrm{Tr}(g(a)(1+c)^{-1})$。

3 一类非单项置换的回旋镖均匀度

本节进一步研究了$H(x)$的回旋镖均匀度。下面先给出一个有用的引理。

引理3.1 设$n,k,i,m,d\in\mathbb{N}^+$,且$n=2k+1$,$i=2m+1$,$m=2^{d-1}$,$\gcd(n,d)=1$,$(k-d)|d$。设$g(x)$是引理2.2中的多项式,则$g(x)=0$在$\mathbb{F}_{2^n}$中仅有2个解$x=0,1$。

证明 由于$n=2k+1$,则$\gcd(n,k)=\gcd(2k+1,k)=1$。又因为$\gcd(n,d)=1$,且$(k-d)|d$,则$\gcd(n,d)=\gcd(n,k-d)=1$。

对等式$g(x)=0$两边同时取2^k次幂可得

$$x^{2^{2k-d}}+x^{2^d}+x^{2^{2k}}+x+x^{2^{k+d}}+x^{2^{k-d}}=0。$$

设$g'(x)=x^{2^{2k-d}}+x^{2^d}+x^{2^{2k}}+x+x^{2^{k+d}}+x^{2^{k-d}}$,由

定义 1.5 可知,$g'(x)$ 的常规 2-关联多项式为

$$G(x)=x^{2k}+x^{2k-d}+x^{k+d}+x^{k-d}+x^{d}+1,$$

且 $\gcd(g'(x),x^{2^n}+x)$ 是 $\gcd(G(x),x^n+1)$ 的线性化关联。又因为 $G(x)=(x^k+1)(x^{k-d}+1)(x^d+1)$ 且 $\gcd(n,k)=\gcd(n,k-d)=\gcd(n,d)=1$,容易得到 $\gcd(G(x),x^n+1)=x+1$。因此,$g(x)=0$ 在 F_{2^n} 中仅有 2 个解为 $x=0,1$。

定理 3.1　设 $n,\ k,\ i,\ m,\ d\in\mathbb{Z}^*$,且 $n=2k+1$,$i=2m+1$,$m=2^{d-1}$,$\gcd(n,d)=1$,$(k-d)|d$。则 $H(x)$ 在点 $(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}^*$ 处 BCT 的值为

$$\mathcal{B}_H(a,b)=\begin{cases}2^n, & \text{若 } \mathrm{Tr}(g(a)b)=0,\\ 0, & \text{若 } \mathrm{Tr}(g(a)b)=1,\end{cases}$$

式中 $g(a)=a^{2^{k-d}}+a^{2^{d-k}}+a^{2^k}+a^{2^{-k}}+a^{2^d}+a^{2^{-d}}$。

证明　由于 $H(x)$ 在 (a,b) 处的 BCT 的值等价于满足方程组(1)的解 $(x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ 的数量,将 $H(x)=x+\mathrm{Tr}(x^{2^k+i}+(x+1)^{2^k+i})$ 带入方程组(1)得

$$\begin{cases}x+y+\mathrm{Tr}(x^{2^{k+i-1}}+y^{2^{k+i-1}})+\mathrm{Tr}(x^{2^{k+1}}+y^{2^{k+1}})+\\ \quad\mathrm{Tr}(x^i+y^i)+\mathrm{Tr}(x+y)=b,\\ x+y+\mathrm{Tr}((x+a)^{2^{k+i-1}}+(y+a)^{2^{k+i-1}})+\\ \quad\mathrm{Tr}((x+a)^{2^{k+1}}+(y+a)^{2^{k+1}})+\mathrm{Tr}(x+y)+\\ \quad\mathrm{Tr}((x+a)^i+(y+a)^i)=b。\end{cases}\tag{7}$$

简化方程组(7)中第 1 个等式可得

$$\begin{aligned}b=&x+y+\mathrm{Tr}(x^{2^{k+i-1}}+y^{2^{k+i-1}})+\\ &\mathrm{Tr}(x^{2^{k+1}}+y^{2^{k+1}})+\mathrm{Tr}(x^i+y^i)+\mathrm{Tr}(x+y)=\\ &x+y+\mathrm{Tr}(x+y)^{2^{k+i-1}}+\mathrm{Tr}(x+y)^{2^{k+1}}+\\ &\mathrm{Tr}(x+y)^i+\mathrm{Tr}(x+y)+\\ &\mathrm{Tr}(x^{2^k}y^{i-1}+x^{i-1}y^{2^k}+x^{2^k}y+xy^{2^k}+x^{i-1}y+xy^{i-1})=\\ &H(x+y)+\mathrm{Tr}(x^{2^k}y^{i-1}+x^{i-1}y^{2^k}+x^{2^k}y+xy^{2^k}+\\ &x^{i-1}y+xy^{i-1})+1。\end{aligned}$$

将方程组(7)中的 2 式相加可得

$$\begin{cases}\mathrm{Tr}(x^{2^k}y^{i-1}+x^{i-1}y^{2^k}+x^{2^k}y+xy^{2^k}+x^{i-1}y+xy^{i-1})+\\ \quad H(x+y)+1=b,\\ \mathrm{Tr}((x+y)^{2^k}a^{i-1}+(x+y)^{i-1}a^{2^k}+(x+y)^{2^k}a+\\ \quad(x+y)a^{2^k}+(x+y)^{i-1}a+(x+y)a^{i-1})=0。\end{cases}$$

令 $x+y=z\in\mathbb{F}_{2^n}$,上述方程组变为

$$\begin{cases}H(z)+\mathrm{Tr}(x^{2^k}z^{i-1}+x^{i-1}z^{2^k}+x^{2^k}z+xz^{2^k}+\\ \quad x^{i-1}z+xz^{i-1})+1=b,\\ \mathrm{Tr}(z^{2^k}a^{i-1}+z^{i-1}a^{2^k}+z^{2^k}a+za^{2^k}+z^{i-1}a+za^{i-1})=0。\end{cases}$$

即

$$\begin{cases}H(z)+\mathrm{Tr}(xg(z))+1=b,\\ \mathrm{Tr}(g(z)a)=0。\end{cases}\tag{8}$$

根据引理 1.3,方程组(8)的解 $(x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ 的个数为

$$\begin{aligned}&\mathcal{B}_H(a,b)=\\ &\frac{1}{2^{2n}}\sum_{x,z\in\mathbb{F}_{2^n}}\sum_{\beta\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(1+H(z)+\mathrm{Tr}(xg(z))+b))}\cdot\\ &\qquad\sum_{\gamma\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\gamma\mathrm{Tr}(ag(z)))}=\\ &\frac{1}{2^{2n}}\sum_{x,z\in\mathbb{F}_{2^n}}\sum_{\beta\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta)+\mathrm{Tr}(\beta H(z))+\mathrm{Tr}(\beta)\mathrm{Tr}(xg(z))+\mathrm{Tr}(\beta b)}\cdot\\ &\qquad\sum_{\gamma\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\gamma)\mathrm{Tr}(g(z)a)}=\\ &\frac{1}{2^{2n}}\sum_{\gamma,\beta\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(1+b))}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta H(z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(g(z)a)}\cdot\\ &\qquad\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta)\mathrm{Tr}(xg(z))}=\\ &\qquad\frac{1}{2^{2n}}(D_0+D_1),\end{aligned}\tag{9}$$

式中 D_0 与 D_1 分别是 $\mathrm{Tr}(\beta)=0$ 与 $\mathrm{Tr}(\beta)=1$ 时的和。下面将分别计算 D_0 和 D_1。

$$\begin{aligned}D_0=&\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=0}(-1)^{\mathrm{Tr}(\beta b)}\sum_{\gamma\in\mathbb{F}_{2^n}}\cdot\\ &\sum_{x,z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta H(z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(g(z)a)}=\\ &2^n\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=0}(-1)^{\mathrm{Tr}(\beta b)}\sum_{\gamma\in\mathbb{F}_{2^n}}\cdot\\ &\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta H(z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(g(z)a)}=\\ &2^n\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=0}(-1)^{\mathrm{Tr}(\beta b)}(D_{0,0}+D_{0,1}),\end{aligned}\tag{10}$$

式中 $D_{0,0}$ 与 $D_{0,1}$ 分别是 $\mathrm{Tr}(\gamma)=0$ 与 $\mathrm{Tr}(\gamma)=1$ 时的和。下面将分别计算 $D_{0,0}$ 和 $D_{0,1}$。

$$\begin{aligned}D_{0,0}=&\sum_{\gamma\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\gamma)=0}(-1)^{\mathrm{Tr}(\beta b)}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta H(z))}=\\ &2^{n-1}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta H(z))}。\end{aligned}$$

同理可得

$$\begin{aligned}D_{0,1}=&\sum_{\gamma\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\gamma)=1}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta H(z))+\mathrm{Tr}(g(z)a)}=\\ &2^{n-1}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(z+1+\mathrm{Tr}(z^{2^{k+i-1}}+z^{2^{k+1}}+z^i+z)))+\mathrm{Tr}(g(z)a)}=\\ &2^{n-1}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(z(\beta+g(a)))}。\end{aligned}$$

将 $D_{0,0}$ 和 $D_{0,1}$ 的值代入式(10)得

$$D_0=2^n\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=0}(-1)^{\mathrm{Tr}(\beta b)}(2^{n-1}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta H(z))}+$$

$$2^{n-1}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(z(\beta+g(a)))}=$$

$$2^{2n-1}(2^n+\sum_{\beta\in\mathbb{F}_{2^n}^*,\,\mathrm{Tr}(\beta)=0}(-1)^{\mathrm{Tr}(\beta b)}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta H(z))}+$$

$$\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=0}(-1)^{\mathrm{Tr}(\beta b)}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(z(\beta+g(a)))})=$$

$$2^{3n-1}+2^{2n-1}\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=0}(-1)^{\mathrm{Tr}(\beta b)}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(z(\beta+g(a)))}=$$

$$2^{3n-1}+2^{2n-1}(-1)^{\mathrm{Tr}(g(a)b)},$$

其中,由于$\beta\neq 0$且$H(z)$是$\mathbb{F}_{2^n}$上的对合,则$\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta H(z))}=0$。最后一个等号成立当且仅当$\beta=g(a)$。

$$D_1=\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta b)}\sum_{\gamma\in\mathbb{F}_{2^n}}\cdot$$

$$\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta H(z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(g(z)a)}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xg(z))}=$$

$$\sum_{\beta\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta b)}(D_{1,0}+D_{1,1}),\qquad(11)$$

式中$D_{1,0}$和$D_{1,1}$分别是$\mathrm{Tr}(\gamma)=0$和$\mathrm{Tr}(\gamma)=1$时的和。下面将分别计算$D_{1,0}$和$D_{1,1}$。

$$D_{1,0}=\sum_{\gamma\in\mathbb{F}_{2^n},\,\mathrm{Tr}(\gamma)=0}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta H(z))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xg(z))}=$$

$$2^{n-1}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta H(z))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xg(z))}=$$

$$2^{n-1}(2^n(-1)^{\mathrm{Tr}(\beta H(0))}+2^n(-1)^{\mathrm{Tr}(\beta H(1))}+$$

$$\sum_{z\in\mathbb{F}_{2^n}\setminus\{0,1\}}(-1)^{\mathrm{Tr}(\beta H(z))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xg(z))})=$$

$$2^{2n-1}((-1)^{\mathrm{Tr}(\beta)}+1)=0,$$

式中:$H(0)=1$,$H(1)=0$,且由引理3.1得$g(z)\neq 0$对于$z\in\mathbb{F}_{2^n}\setminus\{0,1\}$。

$$D_{1,1}=\sum_{\gamma\in\mathbb{F}_{2^n},\,\mathrm{Tr}(r)=1}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta H(z))+\mathrm{Tr}(g(z)a)}\cdot$$

$$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xg(z))}=$$

$$2^{n-1}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta H(z))+\mathrm{Tr}(g(z)a)}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xg(z))}=$$

$$2^{n-1}(2^n(-1)^{\mathrm{Tr}(\beta H(0))}+2^n(-1)^{\mathrm{Tr}(\beta H(1))}+$$

$$\sum_{z\in\mathbb{F}_{2^n}\setminus\{0,1\}}(-1)^{\mathrm{Tr}(\beta H(z))+\mathrm{Tr}(g(z)a)}\cdot\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xg(z))})=$$

$$2^{2n-1}((-1)^{\mathrm{Tr}(\beta)}+1)=0。$$

显然,将$D_{1,0}$和$D_{1,1}$的值代入式(11)得$D_1=0$。再将D_0和D_1的值代入式(9)得

$$\mathcal{B}_H(a,b)=2^{n-1}+2^{n-1}(-1)^{\mathrm{Tr}(g(a)b)}$$

$$=\begin{cases}2^n, & \text{若 } \mathrm{Tr}(g(a)b)=0,\\ 0, & \text{若 } \mathrm{Tr}(g(a)b)=1。\end{cases}$$

4 结 论

本文首先利用迹函数构造了一类$\mathbb{F}_{2^n}$上的非单项函数$H(x)=x+\mathrm{Tr}(x^{2^k+i}+(x+1)^{2^k+i})$。接着,研究了$H(x)$的$c$-差分均匀度及回旋镖均匀度,并确定$H(x)$是$\mathbb{F}_{2^n}$上的APcN置换且该函数具有低回旋镖均匀度,能够较好的抵抗差分攻击以及回旋镖攻击。需要指出的是,到目前为止,寻找多种密码学指标良好的向量布尔函数仍是学者们关注的热点。

参 考 文 献

[1] SHELDON B, AKERS J. On a theory of Boolean functions[J]. Journal of the Society for Industrial and Applied Mathematics, 1959, 7(4): 487-498.

[2] BIHAM E, SHAMIR A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991, 4(1): 3-72.

[3] NYBERG K. Differentially uniform mappings for cryptography[J]. Proc of Eurocrypt, 1993, 4357(3): 150-164.

[4] BETH T, DING C S. On almost perfect nonlinear permutations[C]//STINSON D R. Workshop on the theory and application of cryptographic techniques. Berlin: Springer, 1993: 65-76.

[5] CARLET C, KIM K, MESNAGER S. A direct proof of APN-ness of the Kasami functions[J]. Designs, Codes and Cryptography, 2021, 89: 441-446.

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

[7] 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.

[8] 王彦平.低差分置换函数的研究[D].西安:西安电子科技大学,2022.

[9] CALDERINI M, BUDAGHYAN L, CARLET C. On known constructions of APN and AB functions and their relation to each other[J]. Rad Hrvatske akademije znanosti i umjetnosti: Matematičke znanosti, 2021, 546(25): 79-105.

[10] PANARIO D, SAKZAD A, STEVENS B. et al. Ambiguity and deficiency of ermutations from finite fields[C]//POOR H V, ULUKUS S. 2011 IEEE Information Theory Workshop. New York: IEEE, 2011: 165-169.

[11] BORISOV N, CHEW M, JOHNSON R, et al. Multiplicative differentials [C]//DAEMEN J, RIJMEN V. Fast software encryption-FSE 2002. Berlin: Springer, 2002:17-33.

[12] ELLINGSEN P, FELKE P, RIERA C. et al. *C*-differentials, multiplicative uniformity, and (almost) perfect c-nonlinearity [J]. IEEE Transactions on Information Theory, 2020, 66(9):5781-5789.

[13] BARTOLI D, TIMPANELLA M. On a generalization of planar functions [J]. Journal of Algebraic Combinatorics, 2020(52):187-213.

[14] MESNAGER S, RIERA C, STĂNICĂ P. et al. Investigations on c-(almost) perfect nonlinear functions [J]. IEEE Transactions on Information Theory, 2021, 67(10):6916-6925.

[15] HASAN S U, PAL M, RIERA C. et al. On the c-differential uniformity of certain maps over finite fields [J]. Designs, Codes and Cryptography, 2021, 89(2): 221-239.

[16] YAN H D, MESNAGER S, ZHOU Z C. Power functions over finite fields with low c-differential uniformity [EB/OL]. [2023-09-01]. https://arxiv. org/abs/2003.13019.

[17] ZHA Z, HU L. Some classes of power functions with low c-differential uniformity over finite fields [J]. Designs, Codes and Cryptography, 2021, 89:1193-1210.

[18] WANG X Q, ZHENG D B, LEI H B. Several classes of PcN power functions over finite fields [J]. Discrete Applied Mathematics, 2022(322):171-182.

[19] TU Z R, LI N, WU Y N, et al. On the differential spectrum and the APcN property of a class of power functions over finite fields [J]. IEEE Transactions on Information Theory, 2022, 69(1):582-597.

[20] WU Y N, LI N, ZENG X Y. New PcN and APcN functions over finite fields [J]. Designs, Codes and Cryptography, 2021(89):2637-2651.

[21] BARTOLI D, CALDERINI M. On construction and (non) existence of c-(almost) perfect nonlinear functions [J]. Finite Fields and Their Applications, 2021, 72(1): 1-16.

[22] STĂNICĂ P. Low c-differential and c-boomerang uniformity of the swapped inverse function [J]. Discrete Mathematics, 2021, 344(10):1-13.

[23] WAGNER D. The boomerang attack [C]//KNUDSEN L R, CANNIERE C D. International workshop on fast software encryption. Berlin: Springer, 1999:156-170.

[24] CID C, HUANG T, PEYRIN T, et al. Boomerang connectivity table: a new ryptanalysis tool [C]// NIELSEN J B, RIJMEN V. Advances in Cryptology-EUROCRYPT 2018: 37th Annual international conference on the theory and applications of cryptographic techniques. Cham: Springer, 2018: 683-714.

[25] BOURA C, CANTEAUT A. On the boomerang uniformity of cryptographic Sboxes [J]. IACR Transactions on Symmetric Cryptology, 2018, 2018(3): 290-310.

[26] LI K Q, QU L J, SUN B. et al. New results about the boomerang uniformity of permutation polynomials [J]. IEEE Transactions on Information Theory, 2019, 65(11):7542-7553.

[27] CALDERINI M, VILLA I. On the boomerang uniformity of some permutation polynomials [J]. Cryptography and Communications, 2020, 12(6): 1161-1178.

[28] HASAN S U, PAL M, STĂNICĂ P. The c-differential uniformity and boomerang uniformity of two classes of permutation polynomials [J]. IEEE Transactions on Information Theory, 2021, 68(1):679-691.

[29] STĂNICĂ P. Using double Weil sums in finding the c-boomerang connectivity table for monomial functions on finite fields [J]. Applicable Algebra in Engineering, Communication and Computing, 2023, 34(4):581-602.

[30] LIDL R, NIEDERREITER H. Finite fields [M]. Cambridge: Cambridge University Press, 1997.

[31] CARLET C. Boolean functions for cryptography and error correcting codes [M]. Cambridge: Cambridge University Press, 2010.

（责任编辑：马田田）