Advances in Applied Mathematics 应用数学进展, **2024, 13(8), 3925-3935**
Published Online August 2024 in Hans. https://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2024.138374

Hans汉斯

一类置换多项式的c-差分均匀度与回旋镖均匀度

陈艺文

西北师范大学数学与统计学院，甘肃 兰州

收稿日期：2024年7月19日；录用日期：2024年8月11日；发布日期：2024年8月20日

摘 要

S盒是分组密码算法中的一个重要组成部分。为抵抗已有的差分攻击、回旋镖攻击等各种攻击，一个理想的S盒通常应该具有低差分均匀度、低回旋镖均匀度等良好的密码学性质。本文利用Weil和技巧证明了一类已知置换多项式具有较低的 c- 差分均匀度，并计算出了这类置换多项式的回旋镖均匀度。

关键词

置换多项式，c-差分均匀度，回旋镖均匀度，Weil和

The c-Differential Uniformity and Boomerang Uniformity of a Class of Permutation Polynomials

Yiwen Chen

College of Mathematics and Statistics, Northwest Normal University, Lanzhou Gansu

Received: Jul. 19^{th}, 2024; accepted: Aug. 11^{th}, 2024; published: Aug. 20^{th}, 2024

文章引用: 陈艺文. 一类置换多项式的c-差分均匀度与回旋镖均匀度[J]. 应用数学进展, 2024, 13(8): 3925-3935.
DOI: 10.12677/aam.2024.138374

Abstract

S-box is an important component of block cipher algorithms. In order to resist various attacks such as differential attacks and boomerang attacks, an ideal S-box is required to have low differential uniformity and low boomerang uniformity. In this paper, we propose a class of known permutation polynomials with low c-differential uniformity by employing Weil sums. Furthermore, we calculate the boomerang uniformity of this function.

Keywords

Permutation Polynomial, c-Differential Uniformity, Boomerang Uniformity, Weil Sums

Copyright © 2024 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

1991 年, 针对DES-算法, Biham和Shamir [1]提出了差分攻击. 1994 年在欧洲密码年会上, Nyberg [2]提出了差分均匀度的概念, 差分均匀度是衡量密码函数抵抗差分攻击能力的指标, 其中差分均匀度越小则函数可抵抗差分攻击的能力就越强. 2002 年，Borisov 等人 [3] 介绍了一种乘法差分分析方法. 2020 年, Ellingsen等人 [4] 在乘法差分分析方法的基础上提出 c-差分均匀度的定义, 并精确描述了逆函数的 c- 差分性质. 其中, c-差分均匀度的具体定义如下:

定义1. 设 p 是一个素数, n 是一个正整数, $\mathbb{F}_{p^n}$ 是具有 p^n 个元素的有限域, 函数 $f:\mathbb{F}_{p^n}\mapsto\mathbb{F}_{p^n}$. 对 $a,c\in\mathbb{F}_{p^n}$, 函数 f 的 c-差分定义为

$$_cD_af(x):=f(x+a)-cf(x).$$

对任意的 $a,b\in\mathbb{F}_{p^n}$, 其中 $a\neq 0$, 定义 $_c\Delta_f(a,b):=\#\{x\in\mathbb{F}_{p^n}:f(x+a)-cf(x)=b\}$. 称 $\delta_{f,c}:=\max\{_c\Delta_f(a,b):a,b\in\mathbb{F}_{p^n}$, 当 $c=1$ 时 $a\neq 0\}$ 为 $f(x)$ 的 c- 差分均匀度. 如果 $\delta_{f,c}=\delta$, 那么我们称 f 是差分 (c,δ)-均匀度.

其中若 $\delta_{f,c}=1$, 即函数 f 的 c-差分均匀度为 1, 我们称 f 是一个完全 c-非线性函数*(perfect c-nonlinear function)*, 简称为*PcN*函数; 若 $\delta_{f,c}=2$, 即函数 f 的 c-差分均匀度为 2, 我们称 f 是一个几乎完全 c-非线性函数*(almost perfect c-nonlinear function)*, 简称为*APcN*函数.

2021 年, Wu, Li和Zeng [5]利用割圆术和Dillon转换法得到了两类PcN 函数和三类APcN函数, 利用广义AGW准则获得了几类 c- 差分均匀度不超过 2 的多项式. 同年, Hasan, Pal和Stănică [6]得到两类偶特征域上置换多项式的 c-差分均匀度与回旋镖均匀度. 2023 年, Jeong, Koo 和Kwon [7] 在二元域上提出几类新的非单项式APcN置换. 同年, Liu 等人 [8]利用Weil 和技巧给出两类APcN 对合函数, 并计算出相关的回旋镖均匀度. 关于 c-差分均匀度和回旋镖均匀度近期的相关研究可见文献 [9]及其中的参考文献.

回旋镖攻击是传统差分攻击的扩展, 由Wagner [10]在 1999 年提出. 2018 年Cid 等人 [11]在欧洲密码年会上首次提出回旋镖连接表的概念, 同年, Boura和Canteaut [12]在回旋镖连接表的基础上提出了回旋镖均匀度的概念, 它可以刻画密码函数抵抗回旋镖攻击的能力. 其定义如下:

定义2. 设函数 $f:\mathbb{F}_{2^n}\mapsto\mathbb{F}_{2^n}$ 是一可逆函数, 对于 $(a,b)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$, $f(x)$ 的回旋镖连接表为一个 $2^n\times\ 2^n$ 的表, 其在 (a,b) 处的值为

$$\mathcal{B}_f(a,b)=\#\{x\in\mathbb{F}_{2^n}\ :\ f^{-1}(f(x)+a)+f^{-1}(f(x+b)+a)=b\}.$$

记 $\mathcal{B}_f=\max\{\mathcal{B}_f(a,b)\mid a,b\in\mathbb{F}_{2^n}^*\}$, 那么, 称 $\mathcal{B}_f$ 为$f(x)$的回旋镖均匀度.

在上述计算回旋镖均匀度的定义中需要求出函数 $f(x)$ 的逆函数, 但是有些函数的逆函数不便于求解, 所以在 2019 年, Li 等人 [13]提出一种计算回旋镖均匀度的简化方式,

定义3. 设函数 $f:\mathbb{F}_{2^n}\mapsto\mathbb{F}_{2^n}$ 是一置换函数, 对任意的 $a,b\in\mathbb{F}_{2^n}^*$, 那么 $f(x)$ 的回旋镖均匀度 $\mathcal{B}_f$ 是下列方程组

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

在 $(x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ 中解的最大个数.

全文组织结构如下, 第二部分介绍有限域上相关知识点以及后续证明中需要用到的引理; 第三部分利用Weil和技巧计算了已知置换多项式的 c-差分均匀度与回旋镖均匀度; 第四部分总结全文.

2. 基础知识

定义4. [14] 设 $\mathrm{Tr}_m^n(x)$ 是从有限域 $\mathbb{F}_{p^n}$ 到子域 $\mathbb{F}_{p^m}$的迹函数, 记为

$$\mathrm{Tr}_m^n(x)=\sum_{i=0}^{n/m-1}x^{p^{i\cdot m}}=x+x^{p^m}+x^{p^{2m}}+\cdots+x^{p^{i\cdot m}},$$

其中 n, m是正整数且 $m\mid n$. 若 $m=1$, 那么 $\mathrm{Tr}_1^n(x)$ 称为绝对迹函数, 简记为 $\mathrm{Tr}(x)$.

定义5. [15] 设 F 是从 $\mathbb{F}_{2^n}$ 到 $\mathbb{F}_2$ 的函数, 则 F 在 v 处的Walsh变换可定义为

$$W_F(v)=\sum_{x\in\mathbb{F}_{2^n}}\omega^{F(x)+\mathrm{Tr}(vx)},\quad v\in\mathbb{F}_{2^n}.$$

引理1. [16] 对任意的 $\beta,\gamma\in\mathbb{F}_{2^n}$ 且 $h(x)\in\mathbb{F}_{2^n}[x]$, 则多项式 $f(x)=x+\gamma\mathrm{Tr}(h(x^2+\gamma x)+\beta x)$ 是 $\mathbb{F}_{2^n}$ 上的置换多项式当且仅当 $\mathrm{Tr}(\beta\gamma)=0$.

从上述引理中易看出, 若 $\beta=0,\gamma=1$ 且 $h(x)=x^{2^i+1}\in\mathbb{F}_{2^n}[x]$, 则函数 $R(x)=x+\mathrm{Tr}((x^2+x)^{2^i+1})=x+\mathrm{Tr}(x^{2^{i+1}+1}+x^{2^{i-1}+1})$ 是 $\mathbb{F}_{2^n}$ 上的置换多项式.

引理2. [14] 设 $\chi_1:\mathbb{F}_{2^n}\to\mathbb{C}$ 为 $\mathbb{F}_{2^n}$ 加法群的标准加法特征, 定义为

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

对于固定的 $b\in\mathbb{F}_{2^n}$, 方程 $f(x_1,x_2,\cdots,x_n)=b$ 的解 $(x_1,x_2,\cdots,x_n)\in\mathbb{F}_{2^n}^n$ 的个数记为

$$N(b)=\frac{1}{2^n}\cdot\sum_{x_1,x_2,\cdots,x_n\in\mathbb{F}_{2^n}}\sum_{\beta\in\mathbb{F}_{2^n}}\chi_1(\beta(f(x_1,x_2,\cdots,x_n)-b)).$$

同样的, 对于固定的 $b=(b_1,b_2)\in\mathbb{F}_{2^n}^2$, 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 $(x_1,x_2,\cdots,x_n)\in\mathbb{F}_{2^n}^n$ 的个数记为

$$\hat{N}(b)=\frac{1}{2^{2n}}\cdot\sum_{x_1,x_2,\cdots,x_n\in\mathbb{F}_{2^n}}\sum_{\beta\in\mathbb{F}_{2^n}}\chi_1(\beta(f_1(x_1,x_2,\cdots,x_n)-b_1))\cdot\sum_{\gamma\in\mathbb{F}_{2^n}}\chi_1(\beta(f_2(x_1,x_2,\cdots,x_n)-b_2)).$$

引理3. [17] 令 $K=\mathbb{F}_{2^k}$, 其中 k 为奇数. $g(x)=\mathrm{Tr}(x^{2^a+1}+x^{2^b+1})$, $0\le a<b$ 且 $(b-a,k)=(b+a,k)=1$. 那么

$$W_g(\alpha)=\begin{cases}(-1)^{\mathrm{Tr}(\beta^{2^a+1}+\beta^{2^b+1}+\alpha\beta)}W_g(0), & \text{如果 } \mathrm{Tr}(\alpha)=0;\\ 0, & \text{如果 } \mathrm{Tr}(\alpha)=1,\end{cases}$$

其中 β 是域 K 中迹为0的一个元素且满足 $\alpha=\beta^{2^a}+\beta^{2^{-a}}+\beta^{2^b}+\beta^{2^{-b}}$.

定义6. [14] 令 $\alpha\in\mathbb{F}_{q^n}$. 则 $\mathbb{F}_{q^n}$ 上的多项式 $l(x)=\sum_{i=0}^{n}\alpha_ix^i$ 和$L(x)=\sum_{i=0}^{n}\alpha_ix^{q^i}$ 称为 q-互相关联的. 特别地, 称 $l(x)$ 是 $L(x)$ 的常规 q-关联, $L(x)$ 是 $l(x)$ 的线性化 q-关联.

引理4. 设 n,k,i 是正整数且满足 $n=2k+1$. 令 $L(x)=x^{2^{-1-i}}+x^{2^{i+1}}+x^{2^{1-i}}+x^{2^{i-1}}$ 是 $\mathbb{F}_{2^n}$ 上的一个线性化多项式. 则 $L(x)$ 在 $\mathbb{F}_{2^n}$ 上仅有两个解 $x=0,1$.

证明 对等式 $L(x)=0$ 两边同时提升 2^{i+1} 次幂可得

$$L_1(x)=x+x^{2^{2i+2}}+x^{2^2}+x^{2^{2i}}=0.$$

由定义6, 可知上式的常规 2-关联多项式为

$$L_2(x) = 1 + x^{2i+2} + x^2 + x^{2i} = (x^2+1)(x^{2i}+1).$$

因为 $\gcd(L_1(x), x^{2^n}+x)$ 是 $\gcd(L_2(x), x^n+1)$ 的线性化 2-关联且 $\gcd(n,2) = \gcd(n,2i) = 1$. 所以可得 $\gcd(L_2(x), x^n+1) = x+1$. 因此, $L(x) = 0$ 在 $\mathbb{F}_{2^n}$ 中仅有两个解为 $x = 0, 1$.

3. 主要结论及证明

定理1. 令 n, k, i 是正整数, 且 $n = 2k+1$, $R(x) = x + \mathrm{Tr}(x^{2^{i+1}+1} + x^{2^{i-1}+1})$. 则对任意 $c \in \mathbb{F}_{2^n} \setminus \{0,1\}$, 置换多项式 $R(x)$ 是 $\mathbb{F}_{2^n}$ 上的$APcN$ 函数.

证明 对任意的 $a \in \mathbb{F}_{2^n}$, 得

$$\begin{aligned} R(x+a) &= x + a + \mathrm{Tr}((x+a)^{2^{i+1}+1} + (x+a)^{2^{i-1}+1}) \\ &= x + a + \mathrm{Tr}(x^{2^{i+1}+1} + a^{2^{i+1}+1} + x^{2^{i+1}}a + xa^{2^{i+1}} + x^{2^{i-1}+1} + a^{2^{i-1}+1} + x^{2^{i-1}}a + xa^{2^{i-1}}) \\ &= R(x) + R(a) + \mathrm{Tr}(x^{2^{i+1}}a + xa^{2^{i+1}} + x^{2^{i-1}}a + xa^{2^{i-1}}). \end{aligned}$$

根据定义 1, 列出方程

$$\begin{aligned} R(x+a) + cR(x) &= (1+c)R(x) + R(a) + \mathrm{Tr}(x^{2^{i+1}}a + xa^{2^{i+1}} + x^{2^{i-1}}a + xa^{2^{i-1}}) \\ &= (1+c)R(x) + R(a) + \mathrm{Tr}(xh(a)) = b. \end{aligned} \tag{1}$$

其中$h(a) = a^{2^{-i-1}} + a^{2^{i+1}} + a^{2^{1-i}} + a^{2^{i-1}}$.

由引理 2, 可得等式(1) 解的个数为

$$\begin{aligned} {}_c\Delta_R(a,b) &= \frac{1}{2^n} \sum_{\beta \in \mathbb{F}_{2^n}} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(R(a)+b)) + \mathrm{Tr}(\beta(1+c)R(x)) + \mathrm{Tr}(\beta)\mathrm{Tr}(xh(a))} \\ &= \frac{1}{2^n}(Q_0 + Q_1), \end{aligned} \tag{2}$$

其中 Q_0 和 Q_1 分别对应于 $\mathrm{Tr}(\beta) = 0$ 和 $\mathrm{Tr}(\beta) = 1$ 时的和.

$$\begin{aligned} Q_0 &= \sum_{\beta \in \mathbb{F}_{2^n}, \mathrm{Tr}(\beta)=0} (-1)^{\mathrm{Tr}(\beta(R(a)+b))} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)R(x))} \\ &= (-1)^{\mathrm{Tr}(0)} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(0)} + \sum_{\beta \in \mathbb{F}_{2^n}^*, \mathrm{Tr}(\beta)=0} (-1)^{\mathrm{Tr}(\beta(R(a)+b))} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(\beta(1+c)R(x))} \\ &= 2^n. \end{aligned}$$

最后一个等号成立, 是因为 $\beta \in \mathbb{F}_{2^n}^*$, $c \in \mathbb{F}_{2^n} \setminus \{0,1\}$, 得 $\beta(1+c) \neq 0$ 且 $R(x)$ 为置换, 所以

$\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(1+c)R(x))}=0$. 同样, 我们可以求得 Q_1.

$$\begin{aligned}Q_1 &= \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta(R(a)+b))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(1+c)R(x))+\mathrm{Tr}(xh(a))}\\ &= \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta(R(a)+b))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(1+c)(x+\mathrm{Tr}(x^{2^{i+1}+1}+x^{2^{i-1}+1})))+\mathrm{Tr}(xh(a))}\\ &= \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta(R(a)+b))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(1+c))\mathrm{Tr}(x^{2^{i+1}+1}+x^{2^{i-1}+1})+\mathrm{Tr}(x(h(a)+\beta(1+c)))}\\ &= Q_{1,0}+Q_{1,1},\end{aligned}$$

其中 $Q_{1,0}$ 和$Q_{1,1}$ 分别对应于 $\mathrm{Tr}(\beta(1+c))=0$ 和$\mathrm{Tr}(\beta(1+c))=1$ 时的和.

当 $\mathrm{Tr}(\beta(1+c))=0$ 且 $\mathrm{Tr}(\beta)=1$ 时, 可得$\mathrm{Tr}(\beta(1+c))=\mathrm{Tr}(\beta)+\mathrm{Tr}(\beta c)=1+\mathrm{Tr}(\beta c)=0$. 从而得出$\mathrm{Tr}(\beta c)=1$.

$$Q_{1,0}=\sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=1=\mathrm{Tr}(\beta c)}(-1)^{\mathrm{Tr}(\beta(R(a)+b))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(x(h(a)+\beta(1+c)))}.$$

注意到, 当 $\beta(1+c)=h(a)$ 时, 内和等于 2^n. 当 $\beta(1+c)\neq h(a)$ 时, 内和等于 0. 因此, 可得

$$Q_{1,0}=\begin{cases}2^n\cdot(-1)^{\mu}, & \text{若 } \beta(1+c)=h(a);\\ 0, & \text{若 } \beta(1+c)\neq h(a),\end{cases}$$

此处 $\mu=\mathrm{Tr}((1+c)^{-1}h(a)(R(a)+b))$.

同样的, 我们可以计算出 $Q_{1,1}$, 当 $\mathrm{Tr}(\beta(1+c))=1$ 且 $\mathrm{Tr}(\beta)=1$ 时, 可得$\mathrm{Tr}(\beta(1+c))=\mathrm{Tr}(\beta)+\mathrm{Tr}(\beta c)=1+\mathrm{Tr}(\beta c)=1$. 从而得出$\mathrm{Tr}(\beta c)=0$.

$$\begin{aligned}Q_{1,1} &= \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=1,\mathrm{Tr}(\beta c)=0}(-1)^{\mathrm{Tr}(\beta(R(a)+b))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(x^{2^{i+1}+1}+x^{2^{i-1}+1})+\mathrm{Tr}(x(h(a)+\beta(1+c)))}\\ &= \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=1,\mathrm{Tr}(\beta c)=0}(-1)^{\mathrm{Tr}(\beta(R(a)+b))}W_g(\alpha),\end{aligned}$$

其中 $W_g(\alpha)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(x^{2^{i+1}+1}+x^{2^{i-1}+1})+\mathrm{Tr}(x\cdot\alpha)}$ 且 $\alpha=h(a)+\beta(1+c)$. 而且, $\mathrm{Tr}(\alpha)=\mathrm{Tr}(h(a)+\beta(1+c))=1$. 因为 $0\leq i-1<i+1$ 且 $\gcd(2,n)=\gcd(2i,n)=1$, 那么通过引理 3, 可得 $W_g(\alpha)=0$. 因此, $Q_{1,1}=0$. 将 Q_0 和 Q_1 的值代入等式(2)得

$${}_c\Delta_R(a,b)=\begin{cases}0, & \text{若 } \mu=1 \text{ 且 } \beta(1+c)=h(a);\\ 1, & \text{若 } \beta(1+c)\neq h(a);\\ 2, & \text{若 } \mu=0 \text{ 且 } \beta(1+c)=h(a).\end{cases}$$

因此, $\delta_{R,c}=\max\{{}_c\Delta_R(a,b):a,b\in\mathbb{F}_{2^n},a\neq 0$ 当 $c=1$时$\}=2$. 即证得 $R(x)$ 是 $\mathbb{F}_{2^n}$ 上的APcN 函数.

定理2. 设 n,k,i 是正整数且 $n=2k+1$. 则 $R(x)=x+\mathrm{Tr}(x^{2^{i+1}+1}+x^{2^{i-1}+1})$ 在点 $(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}^*$ 处的BCT值为

$$\mathcal{B}_R(a,b)=\begin{cases}2^n, & \text{如果 } \mathrm{Tr}(L(a)b)=0;\\ 0, & \text{如果 } \mathrm{Tr}(L(a)b)=1,\end{cases}$$

其中 $L(a)=a^{2^{-1-i}}+a^{2^{i+1}}+a^{2^{1-i}}+a^{2^{i-1}}$. 回旋镖均匀度 $\mathcal{B}_R$ 为 2^n.

证明 根据定义3, $R(x)$ 在 $(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}^*$ 处的BCT值等价于方程组

$$\begin{cases}R(x)+R(y)=b\\ R(x+a)+R(y+a)=b\end{cases}$$

的解 $(x,y)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ 的个数. 即

$$\begin{cases}x+y+\mathrm{Tr}(x^{2^{i+1}+1}+y^{2^{i+1}+1})+\mathrm{Tr}(x^{2^{i-1}+1}+y^{2^{i-1}+1})=b\\ x+y+\mathrm{Tr}((x+a)^{2^{i+1}+1}+(y+a)^{2^{i+1}+1})+\mathrm{Tr}((x+a)^{2^{i-1}+1}+(y+a)^{2^{i-1}+1})=b.\end{cases}\tag{3}$$

将上述两式相加得

$$\mathrm{Tr}(x^{2^{i+1}}a+xa^{2^{i+1}}+y^{2^{i+1}}a+ya^{2^{i+1}}+x^{2^{i-1}}a+xa^{2^{i-1}}+y^{2^{i-1}}a+ya^{2^{i-1}})=0.$$

即

$$\mathrm{Tr}((x+y)^{2^{i+1}}a+(x+y)a^{2^{i+1}})+\mathrm{Tr}((x+y)^{2^{i-1}}a+(x+y)a^{2^{i-1}})=0.$$

方程组(3)等价于

$$\begin{cases}x+y+\mathrm{Tr}((x+y)^{2^{i+1}+1}+x^{2^{i+1}}y+xy^{2^{i+1}})+\mathrm{Tr}((x+y)^{2^{i-1}+1}+x^{2^{i-1}}y+xy^{2^{i-1}})=b\\ \mathrm{Tr}((x+y)^{2^{i+1}}a+(x+y)a^{2^{i+1}})+\mathrm{Tr}((x+y)^{2^{i-1}}a+(x+y)a^{2^{i-1}})=0.\end{cases}\tag{4}$$

令 $x+y=z$, 代入方程组(4)得

$$\begin{cases}z+\mathrm{Tr}(z^{2^{i+1}+1}+x^{2^{i+1}}(x+z)+x(x+z)^{2^{i+1}})+\mathrm{Tr}(z^{2^{i-1}+1}+x^{2^{i-1}}(x+z)+x(x+z)^{2^{i-1}})=b\\ \mathrm{Tr}(z^{2^{i+1}}a+za^{2^{i+1}}+z^{2^{i-1}}a+za^{2^{i-1}})=0.\end{cases}$$

即

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

上式可写为

$$\begin{cases} R(z)+\mathrm{Tr}(xL(z))=b \\ \mathrm{Tr}(aL(z))=0, \end{cases}$$

其中 $L(z)=z^{2^{-1-i}}+z^{2^{i+1}}+z^{2^{1-i}}+z^{2^{i-1}}$.

结合引理2, 得方程组中 $(x,z)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}$ 的个数为

$$\begin{aligned} \mathcal{B}_R(a,b)&=\frac{1}{2^{2n}}\sum_{\beta\in\mathbb{F}_{2^n}}\sum_{x,z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta(R(z)+b))+\mathrm{Tr}(\beta)\mathrm{Tr}(xL(z))}\sum_{\gamma\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\gamma)\mathrm{Tr}(aL(z))} \\ &=\frac{1}{2^{2n}}\sum_{\beta,\gamma\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta b)}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta)\mathrm{Tr}(xL(z))}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta R(z))+\mathrm{Tr}(\gamma)\mathrm{Tr}(aL(z))} \\ &=\frac{1}{2^{2n}}(M_{0,0}+M_{0,1}+M_{1,0}+M_{1,1}). \end{aligned} \tag{5}$$

其中 $M_{0,0}$ 对应于 $\mathrm{Tr}(\beta)=\mathrm{Tr}(\gamma)=0$ 时的和; $M_{0,1}$ 对应于 $\mathrm{Tr}(\beta)=0$ 且 $\mathrm{Tr}(\gamma)=1$ 时的和; $M_{1,0}$ 对应于 $\mathrm{Tr}(\beta)=1$ 且 $\mathrm{Tr}(\gamma)=0$ 时的和; $M_{1,1}$ 对应于 $\mathrm{Tr}(\beta)=\mathrm{Tr}(\gamma)=1$ 时的和. 下面分别对 $M_{0,0}$, $M_{0,1}$, $M_{1,0}$, $M_{1,1}$ 进行计算.

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

同理可得,

$$\begin{aligned} M_{0,1}&=2^n\cdot\sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=0}(-1)^{\mathrm{Tr}(\beta b)}\sum_{\gamma\in\mathbb{F}_{2^n},\mathrm{Tr}(\gamma)=1}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta R(z))+\mathrm{Tr}(aL(z))} \\ &=2^{2n-1}\cdot\sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=0}(-1)^{\mathrm{Tr}(\beta b)}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta\cdot(z+\mathrm{Tr}(z^{2^{i+1}+1}+z^{2^{i-1}+1})))+\mathrm{Tr}(aL(z))} \\ &=2^{2n-1}\cdot\sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=0}(-1)^{\mathrm{Tr}(\beta b)}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(z(L(a)+\beta))}. \end{aligned}$$

$$\begin{aligned} M_{1,0}&=\sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta b)}\sum_{\gamma\in\mathbb{F}_{2^n},\mathrm{Tr}(\gamma)=0}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xL(z))}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta R(z))} \\ &=2^{n-1}\cdot\sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta b)}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xL(z))}\sum_{z\in\mathbb{F}_{2^n}\setminus\{0,1\}}(-1)^{\mathrm{Tr}(\beta R(z))}+2^{n-1}\cdot \\ &\quad\sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta b)}\Big(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xL(0))}\cdot(-1)^{\mathrm{Tr}(\beta R(0))}+\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xL(1))}\cdot(-1)^{\mathrm{Tr}(\beta R(1))}\Big) \\ &=2^{n-1}\cdot\sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta b)}(2^n\cdot(-1)^0+2^n\cdot(-1)^1) \\ &=0. \end{aligned}$$

第三个等号成立是因为 $R(0)=0, R(1)=1$ 且根据引理4, 对于 $z\in\mathbb{F}_{2^n}\setminus\{0,1\}$ 有 $L(z)\neq 0$. 所以可得 $\sum\limits_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xL(z))}=0$. 同样的, 下述计算 $M_{1,1}$,

$$\begin{aligned}
M_{1,1} &= \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta b)}\sum_{\gamma\in\mathbb{F}_{2^n},\mathrm{Tr}(\gamma)=1}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xL(z))}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta R(z))+\mathrm{Tr}(aL(z))}\\
&= 2^{n-1}\cdot\sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta b)}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xL(z))}\sum_{z\in\mathbb{F}_{2^n}\setminus\{0,1\}}(-1)^{\mathrm{Tr}(\beta R(z))+\mathrm{Tr}(aL(z))}\\
&+ 2^{n-1}\cdot\sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta b)}\Big(\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xL(0))}\cdot(-1)^{\mathrm{Tr}(\beta R(0))+\mathrm{Tr}(aL(0))}\\
&+ \sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xL(1))}\cdot(-1)^{\mathrm{Tr}(\beta R(1))+\mathrm{Tr}(aL(1))}\Big)\\
&= 2^{n-1}\cdot\sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=1}(-1)^{\mathrm{Tr}(\beta b)}(2^n\cdot(-1)^0+2^n\cdot(-1)^{\mathrm{Tr}(\beta)})\\
&= 0.
\end{aligned}$$

综上, 将 $M_{0,0}, M_{0,1}, M_{1,0}, M_{1,1}$ 的值代入等式(5) 得,

$$\begin{aligned}
\mathcal{B}_R(a,b) &= \frac{1}{2^{2n}}(M_{0,0}+M_{0,1}+M_{1,0}+M_{1,1})\\
&= \frac{1}{2^{2n}}\Big(2^{2n-1}\cdot\sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=0}(-1)^{\mathrm{Tr}(\beta b)}\cdot\Big(\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta R(z))}+\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(z(L(a)+\beta))}\Big)\Big)\\
&= \frac{1}{2}\Big(2^n+\sum_{\beta\in\mathbb{F}_{2^n}^*,\mathrm{Tr}(\beta)=0}(-1)^{\mathrm{Tr}(\beta b)}\cdot\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(\beta R(z))}\\
&+ \sum_{\beta\in\mathbb{F}_{2^n},\mathrm{Tr}(\beta)=0}(-1)^{\mathrm{Tr}(\beta b)}\sum_{z\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(z(L(a)+\beta))}\Big)\\
&= 2^{n-1}+2^{n-1}(-1)^{\mathrm{Tr}(L(a)b)}\\
&= \begin{cases}2^n, & \text{若 } \mathrm{Tr}(L(a)b)=0;\\ 0, & \text{若 } \mathrm{Tr}(L(a)b)=1.\end{cases}
\end{aligned}$$

根据定义3, 可得

$$\mathcal{B}_R=\max\{\mathcal{B}_R(a,b):a,b\in\mathbb{F}_{2^n}^*\}=2^n.$$

4. 总结

本文利用Weil和技巧计算出置换多项式 $R(x)$ 的 c-差分均匀度, 证得其是几乎完全 c-非线性函数(即APcN函数), 并计算出相应的回旋镖均匀度, 说明此类函数可以较好的抵抗差分攻击.

参考文献

[1] Biham, E. and Shamir, A. (1991) Differential Cryptanalysis of DES-Like Cryptosystems. *Journal of Cryptology*, **4**, 3-72. https://doi.org/10.1007/bf00630563

[2] Nyberg, K. (1994) Differentially Uniform Mappings for Cryptography. In: Helleseth, T., Ed., *Lecture Notes in Computer Science*, Springer, 55-64. https://doi.org/10.1007/3-540-48285-7_6

[3] Borisov, N., Chew, M., Johnson, R. and Wagner, D. (2002) Multiplicative Differentials. In: Daemen, J. and Rijmen, V., Eds., *Lecture Notes in Computer Science*, Springer, 17-33. https://doi.org/10.1007/3-540-45661-9_2

[4] Ellingsen, P., Felke, P., Riera, C., Stănică, P. and Tkachenko, A. (2020) C-Differentials, Multiplicative Uniformity, and (Almost) Perfect c-Nonlinearity. *IEEE Transactions on Information Theory*, **66**, 5781-5789. https://doi.org/10.1109/tit.2020.2971988

[5] Wu, Y., Li, N. and Zeng, X. (2021) New PcN and APcN Functions over Finite Fields. *Designs, Codes and Cryptography*, **89**, 2637-2651. https://doi.org/10.1007/s10623-021-00946-9

[6] Hasan, S.U., Pal, M. and Stănică, P. (2022) The c-Differential Uniformity and Boomerang Uniformity of Two Classes of Permutation Polynomials. *IEEE Transactions on Information Theory*, **68**, 679-691. https://doi.org/10.1109/tit.2021.3123104

[7] Jeong, J., Koo, N. and Kwon, S. (2023) On Non-Monomial APcN Permutations over Finite Fields of Even Characteristic. *Finite Fields and Their Applications*, **89**, Article 102196. https://doi.org/10.1016/j.ffa.2023.102196

[8] Liu, Q., Huang, Z., Xie, J., Liu, X. and Zou, J. (2023) The c-Differential Uniformity and Boomerang Uniformity of Three Classes of Permutation Polynomials over $\mathbb{F}_{2^n}$. *Finite Fields and Their Applications*, **89**, Article 102212. https://doi.org/10.1016/j.ffa.2023.102212

[9] Mesnager, S., Mandal, B. and Msahli, M. (2021) Survey on Recent Trends Towards Generalized Differential and Boomerang Uniformities. *Cryptography and Communications*, **14**, 691-735. https://doi.org/10.1007/s12095-021-00551-6

[10] Wagner, D. (1999) The Boomerang Attack. In: Knudsen, L., Ed., *Lecture Notes in Computer Science*, Springer, 156-170. https://doi.org/10.1007/3-540-48519-8_12

[11] Cid, C., Huang, T., Peyrin, T., Sasaki, Y. and Song, L. (2018) Boomerang Connectivity Table: A New Cryptanalysis Tool. In: Nielsen, J. and Rijmen, V., Eds., *Lecture Notes in Computer Science*, Springer International Publishing, 683-714. https://doi.org/10.1007/978-3-319-78375-8_22

[12] Boura, C. and Canteaut, A. (2018) On the Boomerang Uniformity of Cryptographic Sboxes. *IACR Transactions on Symmetric Cryptology*, No. 3, 290-310. https://doi.org/10.46586/tosc.v2018.i3.290-310

[13] Li, K., Qu, L., Sun, B. and Li, C. (2019) New Results about the Boomerang Uniformity of Permutation Polynomials. *IEEE Transactions on Information Theory*, **65**, 7542-7553. https://doi.org/10.1109/tit.2019.2918531

[14] Lidl, R. and Niederreiter, H. (1997) Finite Fields, Encyclopedia of Mathematics and Its Applications. Vol. 20, Cambridge University Press.

[15] Helleseth, T. and Kholosha, A. (2006) Monomial and Quadratic Bent Functions over the Finite Fields of Odd Characteristic. *IEEE Transactions on Information Theory*, **52**, 2018-2032. https://doi.org/10.1109/tit.2006.872854

[16] Charpin, P. and Kyureghyan, G.M. (2008) On a Class of Permutation Polynomials over $\mathbb{F}_{2^n}$. In: Golomb, S.W., Parker, M.G., Pott, A. and Winterhof, A., Eds., *Lecture Notes in Computer Science*, Springer, 368-376. https://doi.org/10.1007/978-3-540-85912-3_32

[17] Roy, S. (2012) Generalization of Some Results on Gold and Kasami-Welch Functions. *Finite Fields and Their Applications*, **18**, 894-903. https://doi.org/10.1016/j.ffa.2012.06.006