两类面向算术化幂函数的差分性质

胡志泽,夏永波*
(中南民族大学 数学与统计学学院,武汉 430074)

摘 要 设p为素数,n为正整数.主要研究有限域$\mathbb{F}_{p^n}$上低阶非线性幂函数x^5以及x^7的差分性质.通过研究函数x^5和x^7的差分方程,刻画了差分方程有特定解数的条件,利用二次特征和确定了这两类幂函数差分谱.在面向算术的密码原语中,这两类低阶非线性幂函数可用于构造S盒或轮函数,其差分性质可为评估他们抗差分攻击的性能提供参考.

关键词 有限域;幂函数;差分方程;差分谱;特征和
中图分类号 O157 **文献标志码** A **文章编号** 1672-4321(2025)03-0426-07
doi:10.20056/j.cnki.ZNMDZK.20250317

Differential properties of two classes of arithmetization-oriented power mappings

HU Zhize, XIA Yongbo*
(College of Mathematics and Statistics, South-Central Minzu University, Wuhan 430074, China)

Abstract Let p be a prime number and n be a positive integer. The differential properties of two classes of low-degree nonlinear power mappings x^5 and x^7 over finite field $\mathbb{F}_{p^n}$ are investigated. By investigating the derivative equations of the functions x^5 and x^7, the conditions under which the differential equations have a specific number of solutions are characterized. Utilizing quadratic character sums, the differential spectrum of these two classes of power mappings are determined. These two classes of low-degree nonlinear power mappings can be used to design S-boxes or round functions in arithmetization-oriented cryptographic primitives, and their differential properties can provide a reference for evaluating their performance against differential attack.

Keywords finite field; power mapping; derivative equation; differential spectrum; character sums

密码Hash函数对于实际的零知识证明应用至关重要,有时直接作为零知识证明(Zero-Knowledge, ZK)协议的一部分使用.现代密码Hash函数,如SHA-2、SHA-3和p是一个较大的素数.为了在$\mathbb{F}_p$上实现高效的Hash运算,需要开发新的Hash函数,这类函数称为面向算术的(Arithmetization-Oriented, AO)Hash函数.研究人员和工程师们已经提出了多种AO Hash函数的设计,如MiMCHash[1],Rescue-Prime[2-3],Reinforced Concrete[4]BLAKE,通常设计在偶特征的有限域上[5].然而,ZK协议往往在大素数域$\mathbb{F}_p$上操作,其中Anemoi[6],Poseidon[7]和Grende[8]等这些新的Hash函数旨在提供$\mathbb{F}_p$上高效的算术运算,同时保持必要的安全性和实用性,以支持大规模的加密货币和其他需要高效ZK证明的应用.

由于面向算术Hash函数的概念相对较新,对这些函数的严格密码分析尚未完成.除了Anemoi[6]和Grende[8]之外,这些面向算术的Hash函数都使用低阶非线性函数作为轮函数,例如幂映射.MiMCHash[2]和Poseidon[7]两类AO Hash函数使用幂映射$x^d, d \in \{3,5\}$作为轮函数.当x^d的次数较低时,其抵抗代数攻击的能力较弱,因此必须使用大量的轮数.为了克服这一问题,对于满足$\gcd(d, p-1)=1$的低阶幂

收稿日期 2024-04-09
* **通信作者** 夏永波(1979-),男,教授,博士,研究方向:无线通讯中的序列设计、编码和密码学,E-mail:xia@mail.scuec.edu.cn
基金项目 国家自然科学基金资助项目(62171479);中央高校基本科研业务费专项资金资助项目(CZZ23004)

映射x^d,人们常选择x^d的复合逆$x^{d^{-1}}$来构造轮函数,$x^{d^{-1}}$具有较高的阶,其抵抗代数攻击的能力较强,同时保持了与x^d相同的差分均匀度和非线性度.本文主要分析两类低阶幂函数x^5和x^7的差分性质[9],为抗差分攻击的轮函数设计和选择提供理论依据.

1　基础知识

设p为素数,n为正整数,$\mathbb{F}_{p^n}$是含有p^n个元素的有限域,$\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n}\backslash\{0\}$.下面给出差分均匀度和差分谱的概念.

定义 1[10]　设f为有限域$\mathbb{F}_{p^n}$上的函数,对任意的$a \in \mathbb{F}_{p^n}^*, b \in \mathbb{F}_{p^n}$,令$\delta_f(a,b)$表示差分方程$f(x+a)-f(x)=b$在有限域$\mathbb{F}_{p^n}$中解的个数.定义:

$$\delta(f) = \max_{a \in \mathbb{F}_{p^n}^*,\ b \in \mathbb{F}_{p^n}} \delta_f(a,b)$$

为函数$f(x)$的差分均匀度,特别当$\delta(f)=\delta$时,$f(x)$也被称作δ-差分一致性函数.

若函数$f(x)$是有限域$\mathbb{F}_{p^n}$上的幂函数,即$f(x)=x^d$,当$a \in \mathbb{F}_{p^n}^*$时,根据:

$$f(x+a)-f(x)=(x+a)^d-x^d=a^d\left(\left(\frac{x}{a}+1\right)^d-\left(\frac{x}{a}\right)^d\right),$$

故$\delta_f(a,b)=\delta_f(1,\ b/a^d)$,从而幂函数$f(x)=x^d$的差分性质由$\delta_f(1,b)$的取值完全确定,其中$b$遍历$\mathbb{F}_{p^n}$.幂函数$f(x)=x^d$的差分谱即为$b$遍历$\mathbb{F}_{p^n}$时$\delta_f(1,b)$的取值分布.下面给出其精确描述.

定义 2[11]　设$f(x)=x^d$为定义在有限域$\mathbb{F}_{p^n}$上的幂函数,其差分均匀度为δ,则其差分谱定义为序列$[\omega_0,\omega_1,\cdots,\omega_\delta]$,其中:

$$\omega_i = \left|\left\{b \in \mathbb{F}_{p^n} | \delta_f(1,b)=i\right\}\right|,\ 0 \leqslant i \leqslant \delta.$$

根据ω_i的定义,可以得到幂函数差分谱的两个基本性质:

$$\sum_{i=0}^{\delta}\omega_i = p^n \text{和} \sum_{i=0}^{k} i\omega_i = p^n.$$

定义 3　定义$\chi(\cdot)$为有限域$\mathbb{F}_{p^n}$上二次特征,即对任意的$x \in \mathbb{F}_{p^n}$,有:

$$\chi(x) = x^{\frac{p^n-1}{2}} = \begin{cases} 1, & \text{如果 } x \text{ 是}\mathbb{F}_{p^n}\text{中的平方元,} \\ -1, & \text{如果 } x \text{ 是}\mathbb{F}_{p^n}\text{中的非平方元,} \\ 0, & x=0. \end{cases}$$

对于$f(x) \in \mathbb{F}_{p^n}[x]$,$\sum_{x \in \mathbb{F}_{p^n}} \chi(f(x))$表示$f(x)$的二次特征和.

引理 1[12]　设$f(x)=a_2x^2+a_1x+a_0 \in \mathbb{F}_{p^n}[x]$,且$a_2 \neq 0$.令$d={a_1}^2-4a_0a_2$,$\chi(\cdot)$是有限域$\mathbb{F}_{p^n}$上的二次特征,那么有:

$$\sum_{x \in F_{p^n}} \chi(f(x)) = \begin{cases} -\chi(a_2), & \text{若} d \neq 0, \\ (p^n-1)\chi(a_2), & \text{若} d=0. \end{cases}$$

引理 2[13]　设$\mathbb{F}_{3^n}$上的方程

$$x^3+ax^2+bx+c=0 \tag{1}$$

在$\mathbb{F}_{3^n}$中有一根x_0,则有:

(1)当方程

$$y^2+ay+(2ad+b)=0 \tag{2}$$

在$\mathbb{F}_{3^n}$中有根y_0时,方程(1)在$\mathbb{F}_{3^n}$中有根y_0+x_0;

(2)对于方程(1)的根$r, r \neq x_0$,则$r-x_0$为方程(2)的根.

2　主要结果及证明

为方便表示,令$\delta(1,b)$表示差分方程$(x+a)^d-x^d=b$的解数.本节主要研究幂函数x^5,x^7在有限域$\mathbb{F}_{p^n}$上的差分性质,对$d=5,7$,在一定条件下将给出$\delta(1,b)$的取值及其分布,即确定幂函数x^5,x^7的差分谱.

首先考虑$\mathbb{F}_{p^n}$上的幂函数x^5(p为奇素数且$p \neq 5$)的差分均匀度和差分谱.当$p=2$时,$f(x)=x^5$是$\mathbb{F}_{2^n}$上的Gold函数,其差分谱BLONDEAU等人在文献[9]已给出结果.

命题 1　$f(x)=x^{2^t+1}$是定义在$\mathbb{F}_{2^n}$上的幂函数,其中$\gcd(t,n)=s, s \geqslant 1$,对任意$(a,b) \in (\mathbb{F}_{2^n})^2$,函数差分谱为:

$$[\omega_0,\omega_{2^s},\omega_{2^n}]=\left[(2^n-1)(2^n-2^{n-s}+1),\ 2^{n-s}(2^n-1),\ 1\right];$$

当k为奇数时,$\omega_k=0$.

特别$t=2$时,可由命题1得到$\mathbb{F}_{2^n}$上幂函数$f(x)=x^5$的差分谱:

$$\begin{cases} [\omega_0,\omega_2,\omega_{2^n}]=[(2^n-1)(2^n-2^{n-1}+1),\ 2^{n-1}(2^n-1),\ 1] & n\text{为奇数,} \\ [\omega_0,\omega_4,\omega_{2^n}]=[(2^n-1)(2^n-2^{n-2}+1),\ 2^{n-2}(2^n-1),\ 1] & n\text{为偶数,} \end{cases}$$

且k为奇数时,$\omega_k = 0$.

下面定理1考虑$p > 2, p \neq 5$时的情况(当$p = 5$时差分方程为线性方程,结论是平凡的).

定理1 设$f(x) = x^5$是定义在有限域$\mathbb{F}_{p^n}$上的幂函数,其中p为奇素数且$p \neq 5$,此时函数$f(x)$为4-差分一致性函数,差分谱情况如下:

(1)当$\chi(-2) = 1$时,函数$f(x)$的差分谱为:

$$[\omega_0, \omega_1, \omega_2, \omega_3, \omega_4] = \left[\frac{5p^n - 3\chi(-1) - 2}{8}, 0, \frac{p^n + \chi(-1) + (1 + \chi(-1))^2 - 2}{4}, 1, \frac{p^n - \chi(-1) - (1 + \chi(-1))^2 - 4}{8}\right],$$

(2)当$\chi(-2) = -1$时,函数$f(x)$的差分谱为:

$$[\omega_0, \omega_1, \omega_2, \omega_3, \omega_4] = \left[\frac{5p^n - \chi(-1) - (1 + \chi(-1))^2 - 4}{8}, 1, \frac{p^n + \chi(-1) + (1 + \chi(-1))^2 - 2}{4}, 0, \frac{p^n - \chi(-1) - (1 + \chi(-1))^2}{8}\right].$$

证明 对任意$b \in \mathbb{F}_{p^n}$,考虑差分方程

$$(x + 1)^5 - x^5 = b \tag{3}$$

在$\mathbb{F}_{p^n}$中解的个数.将(3)展开,得到如下方程

$$5x^4 + 10x^3 + 10x^2 + 5x + 1 = b. \tag{4}$$

令$x = y - \frac{1}{2}$,则方程(4)等价于

$$y^4 + \frac{1}{2}y^2 + \frac{1 - 16b}{80} = 0. \tag{5}$$

当$b = \frac{1}{16}$时,方程(5)为$y^2\left(y^2 + \frac{1}{2}\right) = 0$,此时若$\chi\left(-\frac{1}{2}\right) = \chi(-2) = 1$,方程的解为$y = 0, \pm\sqrt{-\frac{1}{2}}$,即差分方程(3)有三个解;若$\chi\left(-\frac{1}{2}\right) = \chi(-2) = -1$,差分方程(3)仅有一个零解.

接下来考虑$b \neq \frac{1}{16}$时方程(5)解的情况.当$b \neq \frac{1}{16}$时,显然方程(5)的解都是成对出现的(y和$-y$都是方程(5)的解).设$y^2 = u, \frac{1 - 16b}{80} = c$,此时方程(5)化简为:

$$u^2 + \frac{1}{2}u + c = 0. \tag{6}$$

方程(6)的判别式$\Delta = \frac{1}{4} - 4c$,解的情况如下:

(1)当$\chi(\Delta) = -1$时,(6)无解;

(2)当$\chi(\Delta) = 0$时,(6)的解为$u = -\frac{1}{4}$,此时若$\chi(-1) = 1$,方程(5)有两个解;若$\chi(-1) = -1$,方程(5)无解;

(3)当$\chi(\Delta) = 1$时,(6)有两解,不妨设为u_1, u_2,则$u_1 = -\frac{1}{4} + \frac{\sqrt{1 - 16c}}{4}, u_2 = -\frac{1}{4} - \frac{\sqrt{1 - 16c}}{4}$此时方程(5)最多有4解,有四解时当且仅当$\chi(u_1) = \chi(u_2) = 1$.

设$u_1 = -\frac{1}{4} + \frac{\sqrt{1 - 16c}}{4} = t$,则$u_2 = -\frac{1}{2} - t$.当$c$遍历$\mathbb{F}_{p^n}^*$时,$1 - 16c$遍历$\mathbb{F}_{p^n} \setminus \left\{1, \frac{1}{16}\right\}$,此时$t$遍历$\mathbb{F}_{p^n} \setminus \left\{0, -\frac{1}{4}, -\frac{1}{2}\right\}$.令$T = \left\{t \mid \chi(t) = 1, \chi\left(-\frac{1}{2} - t\right) = 1, t \in \mathbb{F}_{3^n} \setminus \left\{0, -\frac{1}{4}, -\frac{1}{2}\right\}\right\}, N = |T|$.利用二次特征和可得:

$$\begin{aligned}
4N &= \sum_{t \in \mathbb{F}_{p^n} \setminus \{0, -\frac{1}{2}, -\frac{1}{4}\}} (1 + \chi(t))\left(1 + \chi\left(-\frac{1}{2} - t\right)\right) \\
&= \sum_{t \in \mathbb{F}_{p^n}} (1 + \chi(t))\left(1 + \chi\left(-\frac{1}{2} - t\right)\right) - \left(1 + \chi\left(-\frac{1}{2}\right)\right) - \left(1 + \chi\left(-\frac{1}{2}\right)\right) - \left(1 + \chi\left(-\frac{1}{4}\right)\right)^2 \\
&= \sum_{t \in \mathbb{F}_{p^n}} 1 + \sum_{t \in \mathbb{F}_{p^n}} \chi(t) + \sum_{t \in \mathbb{F}_{p^n}} \chi\left(-t - \frac{1}{2}\right) + \sum_{t \in \mathbb{F}_{p^n}} \chi\left(-t^2 - \frac{1}{2}t\right) - 2\left(1 + \chi\left(-\frac{1}{2}\right)\right) - \left(1 + \chi(-1)\right)^2 \\
&= p^n - \chi(-1) - 2\left(1 + \chi\left(-\frac{1}{2}\right)\right) - \left(1 + \chi(-1)\right)^2.
\end{aligned}$$

由等式$-\frac{1}{4} + \frac{\sqrt{1 - 16c}}{4} = t$可知$1 - 16c = (4t + 1)^2$,易验证$t$与$-\frac{1}{2} - t$对应同一个$c$,即当$t \neq -\frac{1}{2} - t$时$1 - 16c = (4t + 1)^2$是$t$是与$c$之间的二对一映射.当

$t \in T$ 时 $\chi(u_1) = \chi(u_2) = 1$，方程(5)有 4 解；此外当 $t \in T$ 时，有 $-\frac{1}{2} - t \in T$ 且 $t \neq -\frac{1}{2} - t$. 所以使得方程(5)有4解的 c 的个数是 $|T|$ 的二分之一，又因为 c 与 b 是一一对应，所以使得差分方程(3)有四个解的 b 的个数等于 $\frac{N}{2}$，当 p^n 足够大时 $\frac{N}{2} > 0$.

综上，幂函数 x^5 在 $\mathbb{F}_{p^n}(p > 2$，且 $p \neq 5)$ 上是 4-差分一致性函数，设其差分谱为 $[\omega_0, \omega_1, \omega_2, \omega_3, \omega_4]$，前述讨论知：$\omega_4 = \frac{N}{2}$；当 $\chi(-2) = 1$ 时，$\omega_3 = 1, \omega_1 = 0$；当 $\chi(-2) = -1$ 时，$\omega_3 = 0,\ \omega_1 = 1$. 再由定义 2 的性质计算出差分谱.

定理 1 证毕.

接下来分析 $\mathbb{F}_{p^n}$ 上的幂函数 x^7 的差分均匀度和差分谱. 当 $p = 2$ 时，$f(x) = x^7$ 在 $\mathbb{F}_{2^n}$ 上的差分谱 BLONDEAU 等人在文献[14]已给出.

命题 2　$f(x) = x^7$ 是有限域 $\mathbb{F}_{2^n}$ 上的幂函数，$f(x)$ 的差分均匀度等于 6. 令 $i = \sqrt{-1}$，$f(x)$ 的差分谱可表示如下：

(1) n 是奇数时：

$$[\omega_0, \omega_2, \omega_4, \omega_6] = \left[2^{n-1} + 2\omega_6,\ 2^{n-1} - 3\omega_6,\ 0,\ \frac{2^n + 1}{24} - \frac{1}{8}\left(\frac{1 - i\sqrt{7}}{2}\right)^n - \frac{1}{8}\left(\frac{1 + i\sqrt{7}}{2}\right)^n\right];$$

当 $k \notin \{0, 2, 4, 6\}, \omega_k = 0$.

(2) n 是偶数时：

$$[\omega_0, \omega_2, \omega_4, \omega_6] = \left[2^{n-1} + 2\omega_6 + 1,\ 2^{n-1} - 3\omega_6 - 2,\ 1,\ \frac{2^n - 13}{24} - \frac{1}{8}\left(\frac{1 - i\sqrt{7}}{2}\right)^n - \frac{1}{8}\left(\frac{1 + i\sqrt{7}}{2}\right)^n\right];$$

当 $k \notin \{0, 2, 4, 6\}, \omega_k = 0$.

定理 2　设 $f(x) = x^7$ 是定义在 $\mathbb{F}_{p^n}$ 上的幂函数，其中 $p > 2, p \neq 7$，其差分均匀度小于等于 6，且：

(1) 当 $p = 3$ 时，

1) 若 $n > 1$ 为奇数时，$f(x)$ 为 4-差分一致性函数且差分谱为

$$[\omega_0, \omega_1, \omega_2, \omega_3, \omega_4] = \left[\frac{5 \cdot 3^n + 1}{8},\ 0,\ \frac{3^n - 3}{4},\ 1,\ \frac{3^n - 3}{8}\right];$$

2) 若 $n > 2$ 为偶数时，函数 $f(x)$ 为 6-差分一致性函数且差分谱为：

$$[\omega_0, \omega_1, \omega_2, \omega_3, \omega_4, \omega_5, \omega_6] = \left[\frac{7 \cdot 3^{n-1} - 1}{4},\ 0,\ \frac{3^{n+1} - 3}{8},\ 1,\ 0,\ 0,\ \frac{3^{n-1} - 3}{8}\right].$$

(2) 当 $p = 5, n > 2$ 时，设函数 $f(x) = x^7$ 的差分谱分布为 $[\omega_0, \omega_1, \omega_2, \omega_3, \omega_4, \omega_5, \omega_6]$，若 n 是 4 的倍数，则有 $\omega_1 = 0,\ \omega_3 = 0,\ \omega_5 = 1$；若 n 不是 4 的倍数，则有 $\omega_1 = 1,\ \omega_3 = 0,\ \omega_5 = 0$.

证明　对任意 $b \in \mathbb{F}_{p^n}$，下面讨论差分方程

$$(x + 1)^7 - x^7 = b \tag{7}$$

在域中解的个数.

方程(7)展开为：

$$x^6 + 3x^5 + 5x^4 + 3x^2 + x + \frac{1 - b}{7} = 0, \tag{8}$$

令 $x = y + 1$，(8)等价于：

$$y^6 + \frac{5}{4}y^4 + \frac{3}{16}y^2 + \frac{1 - 64b}{448} = 0, \tag{9}$$

设 $y^2 = z, \frac{1 - 64b}{448} = c$ 此时(9)化简为：

$$z^3 + \frac{5}{4}z^2 + \frac{3}{16}z + c = 0. \tag{10}$$

当 $p > 7$ 时，考虑方程(9). 首先当 $b = \frac{1}{64}$，即 $c = 0$ 时，此时方程(10)的解就转化为考虑方程 $z^2 + \frac{5}{4}z + \frac{3}{16} = 0$ 的解，方程 $z^2 + \frac{5}{4}z + \frac{3}{16} = 0$ 的判别式 $\Delta = \frac{13}{16}$.

(1) 当 $\chi(13) = 1$ 时，方程(10)的解为 $z = 0, \frac{\pm\sqrt{13} - 5}{8}$. 当 $\chi(\frac{\pm\sqrt{13} - 5}{8})$ 只有一个等于 1 时，方程(9)有三个解；当都等于 1 时方程(9)有五个解；当都不等于 1 时，方程(9)只有零解.

(2) 当 $\chi(13) = -1$ 时，方程(9)只有零解.

(3) 当 $\chi(13) = 0$ 时，方程(10)的解为 $z = 0, 1$，此时方程(9)有三个解.

当 $b \neq \frac{1}{64}$ 时，方程(9)的解成对出现. 又因为方程(9)最高次数为 6，因此差分方程(7)在 $\mathbb{F}_{p^n}(p > 7)$ 上最多有 6 个解. 由此我们可知幂函数 x^7 在 $\mathbb{F}_{p^n}(p > 3, p \neq 7)$ 上的差分均匀度小于等于 6.

下面考虑两种特殊情况：$p = 3$ 和 $p = 5$.

情况 1　当 $p = 3$ 时方程(9)等价为：

$$y^6 - y^4 + 1 - b = 0, \tag{11}$$

方程(10)等价为：

$$z^3 - z^2 + c = 0. \tag{12}$$

当 $b = 1$ 时即 $c = 0$ 时，方程(11)变为 $y^4(y^2 -$

1) = 0,则方程的解为$y = 0, \pm 1$.

当$b \neq 1 (c \neq 0)$时,方程(11)的解是成对出现的.假设方程(12)在$\mathbb{F}_{3^n}$中有一根为z_0,由引理2可知:当方程

$$u^2 - u - 2z_0 = 0 \tag{13}$$

在$\mathbb{F}_{3^n}$中有一根u_0时,方程(12)在$\mathbb{F}_{3^n}$中有根$r = u_0 + z_0$.方程(13)的判别式$\Delta = 1 + 2z_0$,根据$\chi(\Delta)$的取值情况也即z_0的取值情况,可以得到方程(12)在$\mathbb{F}_{3^n}$中根的情况:

(1)当$\Delta = 0$时$z_0 = 1$,则$c = 0$,矛盾;

(2)当$\chi(\Delta) = -1$时方程(12)只有一根z_0,当$\chi(z_0) = 1$时方程(11)有两个解,当$\chi(z_0) = -1$时,方程(11)无解;

(3)当$\chi(\Delta) = 1$时,设u_1, u_2是方程(13)的两个互异根,此时方程(12)有三个根$z_0, z_0 + u_1, z_0 + u_2$.假设有二重根,不妨设$u_1 + z_0 = z_0$,那么$u_1 = 0$,则$z_0 = 0$,从而$c = 0$,矛盾.所以,当$\chi(\Delta) = 1$时,方程(12)有三个互异的根$z_0, z_0 + u_1, z_0 + u_2$.

下面讨论方程(12)有三个互异根时的情况.此时$\chi(\Delta) = \chi(1 + 2z_0) = 1$,且方程(12)的三个互异的根为$z_0, z_1 = z_0 + u_1, z_2 = z_0 + u_2$.由方程(13)可知$u_1 = \dfrac{1 + \sqrt{1 + 2z_0}}{2}$, $u_2 = \dfrac{1 - \sqrt{1 + 2z_0}}{2}$, 则 $z_1 = \dfrac{1 + 2z_0 + \sqrt{1 + 2z_0}}{2}$, $z_2 = \dfrac{1 + 2z_0 - \sqrt{1 + 2z_0}}{2}$. 令

$$\begin{aligned}
8N = & \sum_{t \in \mathbb{F}_{3^n} \setminus \{0, \pm 1\}} (1 + \chi(t))(1 - \chi(t + 1))(1 + \chi(t - 1)) + \sum_{t \in \mathbb{F}_{3^n} \setminus \{0, \pm 1\}} (1 - \chi(t))(1 + \chi(t + 1))(1 - \chi(t - 1)) \\
& + \sum_{t \in \mathbb{F}_{3^n} \setminus \{0, \pm 1\}} (1 + \chi(t))(1 + \chi(t + 1))(1 - \chi(t - 1)) + \sum_{t \in \mathbb{F}_{3^n} \setminus \{0, \pm 1\}} (1 - \chi(t))(1 - \chi(t + 1))(1 + \chi(t - 1)) \\
& + \sum_{t \in \mathbb{F}_{3^n} \setminus \{0, \pm 1\}} (1 + \chi(t))(1 - \chi(t + 1))(1 - \chi(t - 1)) + \sum_{t \in \mathbb{F}_{3^n} \setminus \{0, \pm 1\}} (1 - \chi(t))(1 + \chi(t + 1))(1 + \chi(t - 1)) \\
= & 2 \sum_{t \in \mathbb{F}_{3^n}} 1 - 2 \sum_{t \in \mathbb{F}_{3^n}} \chi(t^2 + t) - 2 \sum_{t \in \mathbb{F}_{3^n}} \chi(t^2 - 1) + 2 \sum_{t \in \mathbb{F}_{3^n}} \chi(t^2 - t) - 8 \\
& + 2 \sum_{t \in \mathbb{F}_{3^n}} 1 + 2 \sum_{t \in \mathbb{F}_{3^n}} \chi(t^2 + t) - 2 \sum_{t \in \mathbb{F}_{3^n}} \chi(t^2 - 1) - 2 \sum_{t \in \mathbb{F}_{3^n}} \chi(t^2 - t) - 8 \\
& + 2 \sum_{t \in \mathbb{F}_{3^n}} 1 - 2 \sum_{t \in \mathbb{F}_{3^n}} \chi(t^2 + t) + 2 \sum_{t \in \mathbb{F}_{3^n}} \chi(t^2 - 1) - 2 \sum_{t \in \mathbb{F}_{3^n}} \chi(t^2 - t) - 8,
\end{aligned}$$

由引理1可得$8N = 6 \times 3^n - 18$,即$N = \dfrac{3 \times 3^n - 9}{4}$.

因为$\sqrt{1 + 2z_0} = t$即$1 + 2z_0 = t^2$,可知$\pm t$对应同一个z_0,且$t \in T$时有$-t \in T$及$t \neq 0$.所以使得$\chi(1 + 2z_0) = 1$且情况(i)出现的z_0个数是N的二分之一.根据z_0的任意性及关系式(12)知:(12)的三个互异的根$z_0, z_0 + u_1, z_0 + u_2$对应同一个$c$,所以使得方程(11)有4个解的$c$的个数是前述$z_0$数目的三分之一,即使得方程(11)有四个解的$b$的个数为$\dfrac{N}{6} = \dfrac{3^n - 3}{8}$.当$n$为大于1的奇数时,$\dfrac{N}{6} > 0$.

故当n为大于1的奇数时幂函数x^7在$\mathbb{F}_{3^n}$上是4-差分一致性函数函数,设其差分谱为$[\omega_0, \omega_1, \omega_2, \omega_3, \omega_4]$,前述讨论知:$\omega_4 = \dfrac{3^n - 3}{8}$,$\omega_3 = 1 (b = 1$时$)$;当$\sqrt{1 + 2z_0} = t$,那么$z_0 = \dfrac{(t + 1)(t - 1)}{2}$,$z_1 = \dfrac{t(t + 1)}{2}$,$z_2 = \dfrac{t(t - 1)}{2}$.

(1)当n为大于1的奇数时,有$\chi(2) = -1$.此时当z_0遍历$\mathbb{F}_{p^n} \setminus \{0, 1\}$时,$t$遍历$\mathbb{F}_{p^n} \setminus \{0, \pm 1\}$. z_0, z_1, z_2这三个根是否为平方元由$\chi(t), \chi(t + 1), \chi(t - 1)$的取值决定,当$t \in \mathbb{F}_{p^n} \setminus \{0, \pm 1\}$时,它们所有的情况由表1给出:

表1 平方元分布表

Tab. 1 Square element distribution table

$\chi(t)$	$\chi(t + 1)$	$\chi(t - 1)$	$\chi(z_0)$	$\chi(z_1)$	$\chi(z_2)$
1	−1	1	1	1	−1
−1	1	−1	1	1	−1
1	1	−1	1	−1	1
−1	−1	1	1	−1	1
1	−1	−1	−1	1	1
−1	1	1	−1	1	1
1	1	1	−1	−1	−1
−1	−1	−1	−1	−1	−1

如表所示,z_0, z_1, z_2分为两种情况:(i)z_0, z_1, z_2仅有两个为平方元;(ii)z_0, z_1, z_2全为非平方元.情况(i)出现时方程(11)有4个解,情况(ii)出现时方程(11)无解.

令T为表1中满足前6行条件的t构成的集合,N表示该集合包含的元素数目.当$t \in T$时前述情况(i)出现,方程(11)有四个解.利用二次特征和有:

$b\neq1$，此时方程(11)的解成对出现，所以$\omega_1=0$. 再由定义2的性质可计算出差分谱.

(2)当n为大于2的偶数时，有$\chi(2)=1$，同理，根据$\chi(t)$，$\chi(t+1)$，$\chi(t-1)$的取值，z_0,z_1,z_2的平方元分布情况如表2所示.

所以此时z_0,z_1,z_2也只存在两种情况：(i)z_0,z_1,z_2全为平方元；(ii)z_0,z_1,z_2中仅有一个为平方元. 当出现情况(i)时方程(11)有六个解，当出现情况(ii)时方程(11)有两个解. 由此可知，当$b\neq1$($c\neq0$)时，方程(11)可能的解数为2，6.

类似地，令T为表2中满足前2行条件的t构成的集合，N表示该集合包含的元素数目. 当$t\in T$时

表2　平方元分布表

Tab. 2　Square element distribution table

$\chi(t)$	$\chi(t+1)$	$\chi(t-1)$	$\chi(z_1)$	$\chi(z_2)$	$\chi(z_3)$
1	1	1	1	1	1
−1	−1	−1	1	1	1
1	−1	1	−1	−1	1
1	−1	−1	1	−1	−1
1	1	−1	−1	1	−1
−1	1	1	1	−1	−1
−1	−1	1	−1	1	−1
−1	1	−1	−1	−1	1

$$\begin{aligned}8N&=\sum_{t\in\mathbb{F}_{3^n}\setminus\{0,\pm1\}}(1+\chi(t))(1+\chi(t+1))(1+\chi(t-1))+\sum_{t\in\mathbb{F}_{3^n}\setminus\{0,\pm1\}}(1-\chi(t))(1-\chi(t+1))(1-\chi(t-1))\\&=2\sum_{t\in\mathbb{F}_{3^n}}1+2\sum_{t\in\mathbb{F}_{3^n}}\chi(t^2+t)+2\sum_{t\in\mathbb{F}_{3^n}}\chi(t^2-1)+2\sum_{t\in\mathbb{F}_{3^n}}\chi(t^2-t)-12,\end{aligned}$$

由引理1可得$8N=2\times3^n-18$，即$N=\dfrac{3^n-9}{4}$.

同情况(1)的讨论类似，可知使得方程(12)有6个解的b的个数为$\dfrac{N}{6}=\dfrac{3^{n-1}-3}{8}$. 当$n$为大于2的偶数时，$\dfrac{N}{6}>0$.

故当n为大于2的偶数时，函数$f(x)$为6-差分一致性函数且$\omega_6=\dfrac{3^{n-1}-3}{8}$. 设其差分谱为$[\omega_0,\omega_1,\omega_2,\omega_3,\omega_4,\omega_5,\omega_6]$，前述讨论知：$\omega_6=\dfrac{3^{n-1}-3}{8}$，$\omega_4=0$，$\omega_3=1$($b=1$时)，$\omega_1=0$，$\omega_5=0$. 再由定义2的性质即可计算出差分谱.

情况2　当$p=5$时，方程(9)可化简为：

$$y^6+3y^2+\frac{1+b}{3}=0. \tag{14}$$

显然$n>2$时，方程(14)的解至多为6，且当$b\neq-1$时方程(14)的解成对出现. 当$b=-1$时，方程(14)转化为$y^2(y^4-2)=0$，下面讨论$y^4=2$的解.

设$\mathbb{F}_{5^n}$的本原元为α，则$\mathbb{F}_5$的本原元可表示为$\alpha^{\frac{5^n-1}{5-1}}$，注意到2为$\mathbb{F}_5$的本原元，不妨设$\alpha^{\frac{5^n-1}{5-1}}=2$. 设$y=\alpha^i$($i$为任意整数)，则方程$y^4=2$变形为$(\alpha^i)^4=\alpha^{\frac{5^n-1}{5-1}}$，该方程等价于$4i\equiv\dfrac{5^n-1}{4}\pmod{5^n-1}$. 所以当$n$为4的倍数时同余方程有四个解，进而方程(14)有5个解；当n不为4的倍数时同余方程无解. 因此，方程(14)有5个解时当且仅当4整除n，方程(14)有1个解时当且仅当4不整除n. 综上所述，当$n>2$时，方程(14)在$\mathbb{F}_{5^n}$上可能的解数为$\{0,1,2,4,5,6\}$，前述情况(i)出现，方程(11)有6个解. 令$N=|T|$，利用二次特征和有：

其中解数1和5不同时出现，且仅在$b=-1$时出现1次. 基于前述讨论可得：当n为4的倍数时，$\omega_1=0$，$\omega_5=1$；当n不为4的倍数时，$\omega_1=1$，$\omega_5=0$. 当$b\neq-1$时方程(14)的解成对出现，恒有$\omega_3=0$.

定理2证毕.

注[14]：设$F(x)=x^d$和$G(x)=x^e$是$\mathbb{F}_{p^n}$上的幂函数，如果$\gcd(d,p^n-1)=1$且$e\equiv d^{-1}\pmod{p^n-1}$，即$G(x)$是$F(x)$的复合逆，则$F(x)$与$G(x)$有相同的差分谱. 原因如下所述：由$F(x)$的差分方程$(x+a)^d-x^d=b$可得$x+a=(x^d+b)^{1/d}$. 令$y=x^d$，代入得$a=(y+b)^{1/d}-y^{1/d}$，该方程即为$G(x)$的差分方程(输入差分为$b$，输出差分为$a$)，故$F(x)$与$G(x)$差分方程解数的分布相同，从而具有相同的差分谱.

下面提供一些数值实验的结果来说明定理1和定理2的正确性.

例1　取$p=7,n=4$，利用Magma计算，$\mathbb{F}_{7^4}$上幂函数$f(x)=x^5$的差分谱为：

$[\omega_0,\omega_1,\omega_2,\omega_3,\omega_4]=[1500,\ 0,\ 601,\ 1,\ 299]$.

再取$p=7,n=3$，利用Magma计算$\mathbb{F}_{7^3}$上幂函数$f(x)=x^5$差分谱为：

$[\omega_0,\omega_1,\omega_2,\omega_3,\omega_4]=[214,\ 1,\ 85,\ 0,\ 43]$.

以上结果与利用定理1中的公式进行计算所得的结果是一致的.

例2　令$p=3,n=5$，利用Magma计算，$\mathbb{F}_{3^5}$上幂函数$f(x)=x^7$的差分谱为：

$[\omega_0,\omega_1,\omega_2,\omega_3,\omega_4]=[152,\ 0,\ 60,\ 1,\ 30]$.

再令$p=3,n=6$，利用Magma计算$\mathbb{F}_{3^6}$上幂函数$f(x)=x^7$的差分谱为：

$[\omega_0,\omega_1,\omega_2,\omega_3,\omega_4,\omega_5,\omega_6]=[425, 0, 273, 1, 0, 0, 30]$. 上述数值结果与定理2是相符的.

3 结论

对于有限域$\mathbb{F}_{p^n}$上两类低阶非线性幂函数x^5和x^7,本文通过研究差分方程$(x+1)^d-x^d=b$,在一定条件下刻画了差分方程具有特定解数时元素b满足的条件,再利用二次特征和求出满足条件的b的个数,从而确定了$\mathbb{F}_{p^n}$上幂函数x^5(其中$p>2, p\neq 5$)和$\mathbb{F}_{3^n}$上幂函数x^7的差分谱. 当$\gcd(d,p^n-1)=1$,幂函数x^d和其复合逆$x^{1/d}$具有相同的差分均匀度和差分谱,所以本文所得结果也相应地给出了幂函数$x^{1/5}$和$x^{1/7}$的差分性质. 以上两类低阶非线性幂函数作为轮函数或S盒用于构造面向算术的Hash函数时,本文所得结果可以很好地评估他们抵抗差分攻击的性能. 本文的方法未能解决$p>3$时$\mathbb{F}_{p^n}$上幂函数x^7的差分谱,欢迎感兴趣的读者解决这一遗留问题.

参 考 文 献

[1] ALBRECHT M, GRASSI L, RECHBERGER C, et al. MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity[M]Berlin: Springer , 2016.

[2] ALY A, ASHUR T, BEN-SASSON E, et al. Design of symmetric-key primitives for advanced cryptographic protocols[J]. IACR Transactions on Symmetric Cryptology, 2020:1-45.

[3] SZEPIENIEC A, ASHUR T, DHOOGHE S. Rescue-prime: A standard specification (SoK)[J]. IACR Cryptol EPrint Arch, 2020:1143.

[4] BARBARA M, GRASSI L, KHOVRATOVICH D, et al. Reinforced concrete: Fast hash function for zero knowledge proofs and verifiable computation[J]. IACR Cryptol EPrint Arch, 2021:1038.

[5] AUMASSON J P, NEVES S, WILCOX-O'HEARN Z, et al. BLAKE2: simpler, smaller, fast as MD5[M]Berlin: Springer, 2013.

[6] BOUVIER C, BRIAUD P, CHAIDOS P, et al. New design techniques for efficient arithmetization-oriented hash functions[C]//Annual International Cryptology Conference. Cham: Springer, 2023: 507-539.

[7] GRASSI L, KHOVRATOVICH D, RECHBERGER C, et al. Poseidon: A new hash function for Zero-Knowledge proof systems [C]//30th USENIX Security Symposium. Vancouver:ACM: 2021: 519-535.

[8] GOLDWASSER S, MIT, MICALI S, et al. The knowledge complexity of interactive proof-systems [M] Micali: Association for Computing Machinery, 2019.

[9] BLONDEAU C, CANTEAUT A, CHARPIN P. Differential properties of power functions[C]//2010 IEEE International Symposium on Information Theory. Austin:IEEE, 2010: 2478-2482.

[10] NYBERG K. Differentially uniform mappings for cryptography[C]//Workshop on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1993: 55-64.

[11] XIA Y, ZHANG X, LI C, et al. The differential spectrum of a ternary power mapping[J]. Finite Fields and Their Applications, 2020, 64:101660.

[12] LIDL R, NIEDERREITER H. Finite fields[M]. Cambridge: Cambridge university press, 1997.

[13] 孙宗明, 牟兴祥, 李振国. 3^k元域上的三次方程根的简况[J]. 广西师院学报(自然科学版), 1995(2): 32-34.

[14] BLONDEAU C, CANTEAUT A, CHARPIN P. Differential properties of power functions[C]//2010 IEEE International Symposium on Information Theory. Austin: IEEE, 2010: 2478-2482.

(责编&校对 雷建云)