PAPER

New Infinite Classes of 0-APN Power Functions over $\mathbb{F}_{2^n}$*

Huijuan ZHOU[†], *Student Member*, Zepeng ZHUO[†a)], *and* Guolong CHEN[††], *Nonmembers*

SUMMARY Constructing new families of APN functions is an important and challenging topic. Up to now, only six infinite families of APN monomials have been found on finite fields of even characteristic. To study APN functions, partially APN functions have attracted plenty of researchers' particular interests recently. In this paper, we propose several new infinite classes of 0-APN power functions over $\mathbb{F}_{2^n}$ by using the multivariate method and resultant elimination. Furthermore, we use Magma soft to show that these 0-APN power functions are CCZ-inequivalent to the known 0-APN power functions.

key words: *APN function, 0-APN power function, multivariate method, resultant*

1. Introduction

Differential uniformity is an important concept that quantifies the security of highly nonlinear functions used in many block ciphers. The definitions of differential uniformity and APN (Almost Perfect Nonlinear) functions were introduced by Nyberg [14]. Cryptographic functions over $\mathbb{F}_{2^n}$ with low differential uniformity and high nonlinearity are widely used in symmetric cipher design, allowing to resist known attacks (such as resisting differential cryptanalysis in block ciphers [8]). Throughout this paper, let $\mathbb{F}_{2^n}$ be the finite field consisting with 2^n elements and $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n}\backslash\{0\}$. For a function $f\colon \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$, the derivative of $f(x)$ is defined by $D_a f(x) = f(x+a) + f(x)$, where $x \in \mathbb{F}_{2^n}$ and $a \in \mathbb{F}_{2^n}^*$. For any $b \in \mathbb{F}_{2^n}$, we define

$$\delta_f(a,b) = |\{x \in \mathbb{F}_{2^n} \mid f(x+a) + f(x) = b\}|,$$

where $\mid S \mid$ denotes the cardinality of a set S, and define $\triangle_f = \max\{\delta_f(a,b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\}$, which is called the differential uniformity of f. A function f over $\mathbb{F}_{2^n}$ is called APN function if its differential uniformity $\triangle_f = 2$. APN functions (differentially 2-uniform functions) have optimal differential uniformity over $\mathbb{F}_{2^n}$, and they are often used in block ciphers and coding theory [1], [12], [19]. In the last three decades, one of the most important topics in the study of APN functions is constructing new families of APN functions. For instance, Yu et al. constructed more quadratic APN functions with the QAM method in [21], Beierle et al. presented new instances of quadratic APN functions in [3], and Zheng et al. constructed new APN functions by relative trace functions in [22]. However, it has been difficult to summarize these known constructions in a general form. The reader may refer to [4], [7], [18] for more results of APN functions.

Since it is difficult to construct APN functions directly, some researchers propose to modify the definition of APN functions, that is, to construct APN-like functions with some properties of APN functions by changing the determined points. Blondeau et al. proposed the concept of locally-APN to study the differential properties of the functions $x \longrightarrow x^{2^t-1}$ and obtained an infinite class of locally-APN but not APN functions in [2]. Budaghyan et al. in [6] proposed the concept of the partially APN as follows.

Definition 1: ([6]) Let $x_0 \in \mathbb{F}_{2^n}$. We call an (n,n)-function F a (partial) x_0-*APN* function, or simply x_0-APN function, if all the points u, v satisfying $F(x_0) + F(u) + F(v) + F(x_0 + u + v) = 0$, belong to the curve $(x_0 + u)(x_0 + v)(u + v) = 0$.

We usually refer to the partial APN function simply as x_0-APN or pAPN. If F is an APN function, then F is a x_0-APN function for any $x_0 \in \mathbb{F}_{2^n}$. This is a sufficient and unnecessary condition since there are many examples that they are x_0-APN functions for some $x_0 \in \mathbb{F}_{2^n}$ but not APN functions. Hence, the x_0-APN function is an interesting research object, and one of its important directions is to construct more infinite classes of x_0-APN functions. Furthermore, F is a 0-APN function if and only if the equation $F(x+1)+F(x)+1 = 0$ has no solution in $\mathbb{F}_{2^n}\backslash\mathbb{F}_2$. In [5], [6] Budaghyan et al. explicitly constructed some 0-APN power functions $f(x) = x^d$ over $\mathbb{F}_{2^n}$, and they further gave the exponents of all power functions over $\mathbb{F}_{2^n}$ for $1 \leq n \leq 11$ that are 0-APN but not APN functions. Moreover, Pott proved that for any $n \geq 3$, there are partial 0-APN permutations on $\mathbb{F}_{2^n}$ in [16]. In [17], Qu and Li got seven classes of 0-APN power functions over $\mathbb{F}_{2^n}$ and gave that two of them are locally-APN. In [20], Wang and Zha proposed several new infinite classes of 0-APN power functions using the multivariate method and resultant elimination. Very recently, some infinite classes of 0-APN power functions over $\mathbb{F}_{2^n}$ were constructed in [10], [13]. To further investigate the new 0-APN functions, we list some pairs of (d,n) that are not yet "explained" in [5], seeing Table 1. In this paper, we give new infinite classes of 0-APN functions using the multivariate method and resultant elim-

Manuscript received December 7, 2023.
Manuscript revised April 11, 2024.
Manuscript publicized May 23, 2024.

[†] School of Mathematics and Statistics, Huaibei Normal University, Huaibei, Anhui 235000, China.

[††] School of Computer Engineering, Bengbu University, Bengbu, Anhui 233030, China.

[*] This paper was supported by the National Natural Science Foundation of China under Grants 61902140.

a) E-mail: zzp781021@163.com

DOI: 10.1587/transfun.2023EAP1158

Table 1 Power functions $F(x) = x^i$ over $\mathbb{F}_{2^n}$ for $1 \leq n \leq 11$ which are not yet "explained".

n	d
9	61, 91, 175, 187
10	111, 117, 147, 87, 237, 375
11	79, 109, 183, 251, 367, 695, 29, 51, 53, 55, 75, 83, 101 111, 113, 125, 139, 149, 155, 157, 167, 173, 179, 181 185, 187, 201, 203, 213, 215, 217, 219, 223, 229, 247 295, 309, 311, 317, 331, 333, 335, 339, 347, 351, 359 371, 373, 375,379, 427, 469, 471, 475, 477, 491, 493 727, 735, 751, 763, 61, 77, 87, 91, 105, 119, 123, 141 147, 165, 175, 211, 233, 237, 239, 349, 363, 415, 431 439, 501, 503, 699, 509, 115, 207, 253, 299, 437, 759 103

ination. Moreover, the 0-APN power functions obtained in this paper are CCZ-inequivalent to the known ones.

The rest of this paper is organized as follows. Section 2 gives some necessary definitions and results. Section 3 presents some infinite classes of 0-APN power functions over $\mathbb{F}_{2^n}$. Section 4 verifies the inequality of our constructed functions with the existing 0-APN functions. Section 5 summarizes the work of this paper.

2. Preliminaries

In this section, we provide some known results which will be used in this paper. We first recall the conditions for the CCZ equivalence of power functions on $\mathbb{F}_{p^n}$.

Lemma 1: ([9]) The power functions $p_k(x) = x^k$ and $p_l(x) = x^l$ on $GF(p^n)$ are CCZ equivalent, if and only if there exists a number $0 \leq a < n$, such that $l \equiv p^a k \pmod{p^n - 1}$ or $kl \equiv p^a \pmod{p^n - 1}$.

Remark 1: To demonstrate the inequality between two power functions, it suffices to verify whether their exponents satisfy the aforementioned equation. However, confirming the equivalence among multiple power functions poses a difficult work. Therefore, we adopt a novel approach to confirm the inequality between the 0-APN functions. In [5], Budaghyan et al. proposed the size of the pAPN spectrum is preserved under CCZ-equivalence. So if two pAPN functions are equivalent, then their corresponding spectrums are also equal. Conversely, if two pAPN functions have different spectrums, then they must be not equivalent. If the two functions belong to different finite fields, then their spectrums must be different.

Lemma 2: ([11]) Let q be a prime power and let f be an irreducible polynomial over $\mathbb{F}_{q^n}$ of degree n. Then $f(x) = 0$ has n distinct roots x in $\mathbb{F}_{q^n}$.

Next, we give the resultant of two polynomials to solve the solutions of a system of polynomial equations.

Definition 2: ([11]) Let q be a prime power, and $\mathbb{F}_q[x]$ be the polynomial ring over $\mathbb{F}_q$. Let $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{F}_q[x]$ and $g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m \in \mathbb{F}_q[x]$ be two polynomials of degree n and m respectively, where n, $m \in \mathbb{N}$. Then the resultant $R(f, g)$ of f and g is defined by the determinant

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & \cdots & a_n & 0 & & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & 0 & a_0 & a_1 & & \cdots & a_n \\ b_0 & b_1 & \cdots & & b_m & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & & b_m & \cdots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \cdots & 0 & b_0 & b_1 & & \cdots & b_m \end{vmatrix}$$

of order $m + n$.

If the degree of f is $\deg(f) = n$ $(i.e., a_0 \neq 0)$ and $f(x) = a_0(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ in splitting field of f over $\mathbb{F}_q$, then $R(f, g)$ is also given by the formula

$$R(f,g) = a_0^m \prod_{i=1}^{n} g(\alpha_i).$$

In this paper, we have $R(f, g) = 0$ if and only if f and g have a common root, which means that f and g have a common divisor in $\mathbb{F}_q[x]$ of positive degree. For two polynomials $F(x, y), G(x, y) \in \mathbb{F}_q[x, y]$ of positive degree in y, the resultant $R(F, G, y)$ of F and G with respect to y is the resultant of F and G when considered as polynomials in the single variable y. In this case, $R(F, G, y) \in \mathbb{F}_q[x] \cap \langle F, G \rangle$, where $\langle F, G \rangle$ is the ideal generated by F and G. Thus any pair (a, b) with $F(a, b) = G(a, b) = 0$ is such that $R(F, G, y)(a) = 0$.

3. Some New Classes of 0-APN Power Functions over $\mathbb{F}_{2^n}$

In this section, we show several new classes of 0-APN power functions over $\mathbb{F}_{2^n}$ using the multivariate method and resultant elimination.

Theorem 1: Let n and k be positive integers with $n = 2k + 1$. Then $f(x) = x^{5 \cdot 2^{k+1} + 2^k - 1}$ is a 0-APN function over $\mathbb{F}_{2^n}$.

Proof 1: To show f is 0-APN, it suffices to prove that the equation

$$(x+1)^{5 \cdot 2^{k+1} + 2^k - 1} + x^{5 \cdot 2^{k+1} + 2^k - 1} + 1 = 0 \tag{1}$$

has no solution in $\mathbb{F}_{2^n} \backslash \mathbb{F}_2$. Assume that $x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2$ is a solution of Eq. (1). Multiplying $x(x + 1)$ on both sides of Eq. (1). We have

$$\begin{aligned} &x^{4 \cdot 2^{k+1} + 2^k + 1} + x^{2 \cdot 2^{k+1} + 2^k + 1} + x^{2^k + 1} + x^{5 \cdot 2^{k+1} + 1} \\ &+ x^{4 \cdot 2^{k+1} + 1} + x^{2^{k+1} + 1} + x^{5 \cdot 2^{k+1} + 2^k} + x^2 = 0. \end{aligned} \tag{2}$$

Let $y = x^{2^k}$, then $y^{2^{k+1}} = x$. Eq. (2) can be written as

$$y^9x + y^3x + yx + y^{10}x + y^8x + y^2x + y^{11} + x^2 = 0. \tag{3}$$

Raising the 2^{k+1}-th power on both sides of Eq. (3), we get

$$x^9y^2 + x^3y^2 + xy^2 + x^{10}y^2 + x^8y^2 + x^2y^2 + x^{11} + y^4 = 0. \tag{4}$$

Computing the resultant of Eq. (3) and Eq. (4) with respect to y, and then decomposing it into the product of irreducible factors as

$$\begin{aligned}&x^7(x+1)^7(x^{18}+x^{15}+x^{14}+x^{10}+x^9+x^8\\&+x^4+x^3+1)(x^{18}+x^{16}+x^{15}+x^{13}+x^{11}\\&+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1)(x^{18}\\&+x^{17}+x^{16}+x^{13}+x^{11}+x^{10}+x^9+x^7+x^5\\&+x^4+x^2+x+1)(x^{18}+x^{17}+x^{16}+x^{13}+x^{12}\\&+x^{11}+x^9+x^7+x^6+x^5+x^2+x+1)(x^{18}\\&+x^{17}+x^{16}+x^{14}+x^{13}+x^{11}+x^9+x^8+x^7\\&+x^5+x^2+x+1)(x^{18}+x^{17}+x^{16}+x^{14}+x^{13}\\&+x^{11}+x^{10}+x^8+x^7+x^5+x^3+x^2+1).\end{aligned}\tag{5}$$

Note that $x \notin \mathbb{F}_2$, we assert that $x \in \mathbb{F}_{2^{18}} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^{\gcd(18,n)}}$, i.e., $x \in \mathbb{F}_{2^3}$ or $\mathbb{F}_{2^9}$.

(1) Assume $x \in \mathbb{F}_{2^3}$. If $k \not\equiv 1 \pmod 3$, then $x \in \mathbb{F}_{2^3} \cap \mathbb{F}_{2^n} = \mathbb{F}_2$, which is a contradiction. If $k \equiv 1 \pmod 3$, then $x \in \mathbb{F}_{2^3} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^3}$. This means that the solutions of Eq. (5) belong into $\mathbb{F}_{2^3}$ and $k+2 \equiv 0 \pmod 3$. We raising the 2^2-th power to Eq. (2) gives

$$x^{13}+x^7+x^5+x^{14}+x^{12}+x^6+x^{11}+x^8=0. \tag{6}$$

Which can be simplified as

$$x^5(x+1)^5(x^2+x+1)^2=0. \tag{7}$$

The solutions of Eq. (7) are in $\mathbb{F}_{2^2}$. Notice that $\mathbb{F}_{2^3} \cap \mathbb{F}_{2^2} = \mathbb{F}_2$, which contradicts with $x \in \mathbb{F}_2$.

(2) Assume $x \in \mathbb{F}_{2^9}$. If $k \not\equiv 4 \pmod 9$ and $k \not\equiv 1$ (mod 3), then $x \in \mathbb{F}_{2^9} \cap \mathbb{F}_{2^n} = \mathbb{F}_2$, which is a contradiction. If $k \not\equiv 4 \pmod 9$ and $k \equiv 1 \pmod 3$, then $\mathbb{F}_{2^9} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^3}$. From the results of the above discussion, it can be seen that it is contradictory. If $k \equiv 4 \pmod 9$, then $\mathbb{F}_{2^9} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^9}$. This means that the solutions of Eq. (5) belong into $\mathbb{F}_{2^9}$. Furthermore, $k+5 \equiv 0 \pmod 9$. We raising the 2^5-th power to Eq. (2) gives, which can be simplified as

$$\begin{aligned}&x^{11}(x+1)^{11}(x^6+x^3+1)(x^6+x^4+x^3+x+1)\\&(x^6+x^5+x^3+x^2+1)(x^8+x^6+x^5+x^4+x^3\\&+x+1)(x^8+x^7+x^5+x^4+x^3+x^2+1)(x^8\\&+x^7+x^6+x^4+x^2+x+1)=0.\end{aligned}$$

Then $x \in \mathbb{F}_{2^6}$ or $\mathbb{F}_{2^8}$. When $x \in \mathbb{F}_{2^6} \cap \mathbb{F}_{2^9} = \mathbb{F}_{2^3}$, which is a contradiction. If $x \in \mathbb{F}_{2^8} \cap \mathbb{F}_{2^9} = \mathbb{F}_2$, it is a contradiction. Hence, Eq. (2) has no solution in $\mathbb{F}_{2^n} \backslash \mathbb{F}_2$. □

Theorem 2: Let n and k be positive integers with $n = 3k$, $2 \nmid k$ and $k \not\equiv 2 \pmod 3$. Then $f(x) = x^{3 \cdot 2^{2k}-5}$ is a 0-APN function over $\mathbb{F}_{2^n}$.

Proof 2: To show f is 0-APN, we need to prove that the equation

$$(x+1)^{3\cdot 2^{2k}-5}+x^{3\cdot 2^{2k}-5}+1=0 \tag{8}$$

has no solution in $\mathbb{F}_{2^n} \backslash \mathbb{F}_2$. Assume $x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2$ is a solution of Eq. (8). Multiplying $x^5(x+1)^5$ on both sides of Eq. (8). And let $y = x^{2^k}$, $z = y^{2^k}$ then $z^{2^k} = x$. Raising the 2^k-th power and 2^{2k}-th power to Eq. (8) respectively obtains

$$\begin{cases} z^3x^4+z^3x+z^3+z^2x^5+zx^5+x^{10}+x^9+x^6=0, & \text{(9a)}\\ x^3y^4+x^3y+x^3+x^2y^5+xy^5+y^{10}+y^9+y^6=0, & \text{(9b)}\\ y^3z^4+y^3z+y^3+y^2z^5+yz^5+z^{10}+z^9+z^6=0. & \text{(9c)}\end{cases}$$

With the help of Magma, computing the resultant of Eq. (9a) and Eq. (9c) with respect to z, and then we get $R(x,y)$ Then we continue to compute the resultant of $R(x,y)$ and Eq. (9b) with respect to y, by Magma computation and then decompose it into the product of irreducible factors as

$$\begin{aligned}&x^{27}(x+1)^{27}(x^2+x+1)^{20}(x^3+x+1)(x^3+x^2\\&+1)(x^8+x^5+x^3+x^2+1)^3(x^8+x^5+x^4+x^3\\&+1)^3(x^8+x^6+x^5+x^3+1)^3(x^8+x^6+x^5+x^4\\&+x^3+x+1)^3(x^8+x^7+x^5+x^4+x^3+x^2+1)^3\\&(x^8+x^7+x^6+x^4+x^2+x+1)^3(x^{12}+x^7+x^5\\&+x^2+1)(x^{12}+x^8+x^7+x^6+x^4+x^3+1)(x^{12}\\&+x^9+x^5+x^4+x^2+x+1)^3(x^{12}+x^9+x^6+x^5\\&+x^2+x+1)(x^{12}+x^9+x^6+x^5+x^4+x+1)\\&(x^{12}+x^9+x^8+x^5+x^4+x+1)^3(x^{12}+x^9+x^8\\&+x^6+x^5+x^2+1)(x^{12}+x^9+x^8+x^6+x^5+x^4\\&+1)(x^{12}+x^{10}+x^7+x^5+1)(x^{12}+x^{10}+x^7+x^6\\&+x^4+x^3+1)(x^{12}+x^{11}+x^8+x^6+x^4+x^3+x^2\\&+x+1)^3(x^{12}+x^{11}+x^8+x^7+x^4+x^3+1)^3(x^{12}\\&+x^{11}+x^8+x^7+x^6+x^3+1)(x^{12}+x^{11}+x^9+x^6\\&+x^5+x^4+x^3+x+1)(x^{12}+x^{11}+x^9+x^7+x^6\\&+x^5+x^3+x+1)^3(x^{12}+x^{11}+x^9+x^8+x^7\\&+x^5+x^2+x+1)(x^{12}+x^{11}+x^9+x^8+x^7\\&+x^5+x^4+x^3+x^2+x+1)(x^{12}+x^{11}+x^9\\&+x^8+x^7+x^6+x^3+x+1)(x^{12}+x^{11}+x^{10}\\&+x^7+x^5+x^4+x^3+x+1)(x^{12}+x^{11}+x^{10}\\&+x^7+x^6+x^3+1)(x^{12}+x^{11}+x^{10}+x^7+x^6\\&+x^4+x^2+x+1)(x^{12}+x^{11}+x^{10}+x^8+x^6\\&+x^5+x^2+x+1)(x^{12}+x^{11}+x^{10}+x^8+x^7\\&+x^3+1)^3(x^{12}+x^{11}+x^{10}+x^9+x^8+x^6+x^4\\&+x+1)^3(x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^5\\&+x^4+x^3+x+1)(x^{12}+x^{11}+x^{10}+x^9+x^8\\&+x^7+x^6+x^5+x^4+x^3+x^2+x+1)^3(x^{18}\\&+x^{13}+x^{10}+x^8+x^6+x^5+x^4+x+1)(x^{18}\\&+x^{16}+x^{13}+x^{12}+x^{10}+x^9+x^8+x^6+x^2\\&+x+1)(x^{18}+x^{17}+x^{14}+x^{13}+x^{12}+x^9+x^8\\&+x^6+x^2+x+1)(x^{18}+x^{17}+x^{14}+x^{13}+x^{12}\end{aligned}$$

$$\begin{aligned}
&+ x^{10} + x^8 + x^5 + 1)(x^{18} + x^{17} + x^{16} + x^{12} + x^{10}\\
&+ x^9 + x^6 + x^5 + x^4 + x + 1)(x^{18} + x^{17} + x^{16}\\
&+ x^{12} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1)(x^{24}\\
&+ x^{21} + x^{19} + x^{17} + x^{12} + x^7 + x^6 + x^5 + x^4\\
&+ x^3 + 1)(x^{24} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17}\\
&+ x^{12} + x^7 + x^5 + x^3 + 1)(x^{24} + x^{23} + x^{17} + x^8\\
&+ x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(x^{24} + x^{23}\\
&+ x^{20} + x^{18} + x^{17} + x^8 + x^5 + x^3 + x^2 + x + 1)\\
&(x^{24} + x^{23} + x^{22} + x^{21} + x^{19} + x^{16} + x^7 + x^6 + x^4\\
&+ x + 1)(x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18}\\
&+ x^{16} + x^7 + x + 1).
\end{aligned}$$

Observe that $x \notin \mathbb{F}_2$, thus the solutions of Eq. (9) are in $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^{12}}$, $\mathbb{F}_{2^{18}}$ or $\mathbb{F}_{2^{24}}$.

(1) Assume $x \in \mathbb{F}_{2^2}$. Since $2 \nmid k$ and $n = 3k$, then n is an odd number, we have $\mathbb{F}_{2^2} \cap \mathbb{F}_{2^n} = \mathbb{F}_2$, which contradicts with $x \neq 0, 1$.

(2) Assume $x \in \mathbb{F}_{2^3}$. When $k \equiv 0 \pmod 3$, we obtain $x^{2^k} = x$, $x^{2^{2k}} = x$. Hence, it follows from Eq. (9) that

$$x^{10} + x^9 + x^4 + x^3 = x^3(x+1)^3(x^2+x+1)^2 = 0,$$

it is impossible since $x \notin \mathbb{F}_2$ and $\mathbb{F}_{2^2}$. When $k \equiv 1 \pmod 3$, at this point, we have $x^{2^{2k}} = x^4$, $x^{2^k} = x^2$. We conclude from Eq. (9) that

$$x^{16} + x^{12} + x^{10} + x^6 = x^6(x+1)^6(x^2+x+1)^2 = 0.$$

Notice that $x^2 + x + 1$ is an irreducible polynomial in $\mathbb{F}_2$. It leads to $x \in \mathbb{F}_{2^2} \cap \mathbb{F}_{2^3} = \mathbb{F}_2$, which contradicts with $x \notin 0, 1$.

(3) $x \in \mathbb{F}_{2^{12}}$. When $k \equiv 1 \pmod 4$ or $k \equiv 3 \pmod 4$, we get $\mathbb{F}_{2^{12}} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^3}$, which contradicts with the above discussion. When $k \equiv 2 \pmod 4$ or $k \equiv 0 \pmod 4$, we obtain k is even. Therefore, this situation is not discussed.

(4) $x \in \mathbb{F}_{2^{18}}$. When $k \equiv 1 \pmod 4$ or $k \equiv 3 \pmod 4$, we get $\mathbb{F}_{2^{18}} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^3}$, it means that the solutions of Eq. (9) are in $\mathbb{F}_{2^3}$ which is impossible. When $k \equiv 2 \pmod 4$ or $k \equiv 0 \pmod 4$, we obtain k is even. This is contrary to the conditions of Theorem 2.

(5) Assume $x \in \mathbb{F}_{2^{24}}$. When $k \equiv 1 \pmod 4$ or $k \equiv 3 \pmod 4$, we get $\mathbb{F}_{2^{24}} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^3}$, this is impossible to achieve. When $k \equiv 2 \pmod 4$ or $k \equiv 0 \pmod 4$, we derive k is even contradicting with $2 \nmid k$. Hence, Eq. (9) has no solution in $\mathbb{F}_{2^n} \backslash \mathbb{F}_2$. □

Theorem 3: Let n and k be positive integers with $n = 3k + 1$. Then $f(x) = x^{2^{2k+1} - 2^{k+1} - 1}$ is a 0-APN function over $\mathbb{F}_{2^n}$.

Proof 3: It suffices to show that the equation

$$(x+1)^{2^{2k+1} - 2^{k+1} - 1} + x^{2^{2k+1} - 2^{k+1} - 1} + 1 = 0 \tag{10}$$

has no solution in $\mathbb{F}_{2^n} \backslash \mathbb{F}_2$. Assume that $x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2$ is a solution of Eq. (10). Multiplying $x^{2^{k+1}+1}(x+1)^{2^{k+1}+1}$ on both sides of Eq. (10). And let $y = x^{2^k}$, $z = y^{2^k}$ then $z^{2^{k+1}} = x$ and we raise the 2^{k+1}-th power and 2^{2k+1}-th power to Eq. (10) respectively obtains

$$\begin{cases}
z^2y^2 + z^2x + z^2 + y^4x^2 + y^4x + y^2x^2 = 0, & \text{(11a)}\\
x^2z^4 + x^2y^2 + x^2 + z^8y^4 + z^8y^2 + z^4y^4 = 0, & \text{(11b)}\\
y^2x^2 + y^2z^2 + y^2 + x^4z^4 + x^4z^2 + x^2z^4 = 0. & \text{(11c)}
\end{cases}$$

Computing the resultant of (11a) and (11b), (11a) and (11c) with respect to z respectively. We have $R_1(x, y)$ and $R_2(x, y)$. Next we compute the resultant of $R_1(x, y)$ and $R_2(x, y)$ with respect to y, with the help of Magma, the resultant can be decomposed into the following product of irreducible factors as

$$\begin{aligned}
&x^{128}(x+1)^{128}(x^2+x+1)^{184}(x^8+x^5+x^3+x^2\\
&+1)^8(x^8+x^5+x^4+x^3+1)^8(x^8+x^6+x^5+x^3\\
&+1)^8 = 0.
\end{aligned}$$

Observe that $x \notin \mathbb{F}_2$, thus the solutions of Eq. (10) are in $\mathbb{F}_{2^2}$ or $\mathbb{F}_{2^8}$.

(1) Assume $x \in \mathbb{F}_{2^2}$. When k is even, we have $\mathbb{F}_{2^2} \cap \mathbb{F}_{2^n} = \mathbb{F}_2$, which is a contradiction. However, when k is odd, in other words, $k \equiv 1 \pmod 2$, then we get $\mathbb{F}_{2^2} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^2}$, the solutions of Eq. (10) belong into $\mathbb{F}_{2^2}$. Notice that $k+1 \equiv 0 \pmod 2$. Raising the square to Eq. (10) derives

$$\begin{aligned}
&x^{2^{2(k+1)}+2^{(k+1)+1}} + x^{2^{2(k+1)}+2} + x^{2^{2(k+1)}}\\
&+ x^{2^{(k+1)+1}+2^{(k+1)+1}+4} + x^{2^{(k+1)+1}+2^{(k+1)+1}+2}\\
&+ x^{2^{(k+1)+1}+4} = 0.
\end{aligned}$$

Since $x \in \mathbb{F}_{2^2}$, the equation can be written as

$$x + x^8 = x(1 + x^7) = 0.$$

The solutions of Eq. (10) are in $\mathbb{F}_{2^7}$. But we know $\mathbb{F}_{2^2} \cap \mathbb{F}_{2^7} = \mathbb{F}_{2^7} \cap \mathbb{F}_{2^n} = \mathbb{F}_2$, which contradicts with $x \notin \mathbb{F}_2$.

(2) Assume $x \in \mathbb{F}_{2^8}$. When k is even, we have $\mathbb{F}_{2^8} \cap \mathbb{F}_{2^n} = \mathbb{F}_2$, we derive a contradiction. When k is odd, as discussed above, we also get a contradiction. Hence, the proof is completed. □

Theorem 4: Let n and k be positive integers with $n = 3k + 1$. Then $f(x) = x^{2^{2k} + 2^{k+1} + 2^k - 1}$ is a 0-APN function over $\mathbb{F}_{2^n}$.

Proof 4: We need to show that the equation

$$(x+1)^{2^{2k} + 2^{k+1} + 2^k - 1} + x^{2^{2k} + 2^{k+1} + 2^k - 1} + 1 = 0 \tag{12}$$

has no solution in $\mathbb{F}_{2^n} \backslash \mathbb{F}_2$. Assume that $x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2$ is a solution of Eq. (12). Multiplying $x(x+1)$ on both sides of Eq. (12). We have

$$\begin{aligned}
&x^{2^{2k}+2^k+1} + x^{2^{k+1}+2^k+1} + x^{2^k+1} + x^{2^{2k}+2^{k+1}+1}\\
&+ x^{2^{2k}+2^{k+1}+2^k} + x^{2^{2k+1}} + x^{2^{k+1}+1} + x^2 = 0.
\end{aligned} \tag{13}$$

And let $y = x^{2^k}$, $z = y^{2^k}$ and $x = z^{2^{k+1}}$, and raising the 2^{k+1}-th power, 2^{2k+2}-th power to Eq. (13) respectively gives

$$\begin{cases} zyx+y^3x+yx+zy^2x+zx+y^2x+zy^3+x^2 \\ =0, & (14a) \\ xz^2y^2+z^6y^2+z^2y^2+xz^4y^2+xy^2+z^4y^2 \\ +xz^6+y^4=0, & (14b) \\ y^2x^2z^4+x^6z^4+x^2z^4+y^2x^4z^4+y^2z^4+x^4z^4 \\ +y^2x^6+z^8=0. & (14c) \end{cases}$$

With the help of Magma, computing the resultant of Eq. (14a) and Eq. (14b), Eq. (14b) and Eq. (14c) with respect to z, we can get $R_1(x,y)$ and $R_2(x,y)$. We continue to compute the resultant of $R_1(x,y)$ and $R_2(x,y)$ with respect to y, and then the resultant can be decomposed into the product of irreducible factors as

$$\begin{aligned} &x^{284}(x+1)^{284}(x^2+x+1)^8(x^3+x+1)^{16}(x^3+x^2 \\ &+1)^{16}(x^5+x^2+1)^4(x^5+x^3+1)^4(x^5+x^3+x^2 \\ &+x+1)^4(x^5+x^4+x^2+x+1)^4(x^5+x^4+x^3 \\ &+x+1)^4(x^5+x^4+x^3+x^2+1)^4(x^8+x^5+x^3 \\ &+x^2+1)^4(x^8+x^5+x^4+x^3+1)^4(x^8+x^6+x^5 \\ &+x^3+1)^4(x^{10}+x^3+1)^4(x^{10}+x^7+1)^4(x^{10}+x^8 \\ &+x^3+x+1)^4(x^{10}+x^8+x^7+x^6+x^5+x^4+x^3 \\ &+x+1)^4(x^{10}+x^9+x^7+x^2+1)^4(x^{10}+x^9+x^7 \\ &+x^6+x^5+x^4+x^3+x^2+1)^4(x^{10}+x^9+x^8+x^3 \\ &+x^2+x+1)^4(x^{10}+x^9+x^8+x^7+x^2+x+1)^4 \\ &(x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x \\ &+1)^4. \end{aligned}$$

Observe that $x \notin \mathbb{F}_2$, thus the solutions of Eq. (12) are in $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^3}$, $\mathbb{F}_{2^5}$, $\mathbb{F}_{2^{10}}$.

(1) Assume $x \in \mathbb{F}_{2^2}$, when k is even, then $n = 3k+1$ is odd, $\mathbb{F}_{2^2} \cap \mathbb{F}_{2^n} = \mathbb{F}_2$, which is a contradiction. When k is odd, then $n = 3k+1$ is even, $\mathbb{F}_{2^2} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^2}$, then we can derive from Eq. (13) that

$$x^4+x^3+x^6+x^5 = x^3(x+1)^3 = 0,$$

since $x^{2^{2k}} = x$ and $x^{2^k} = x^2$. At this moment, $x \in \mathbb{F}_2$, it is inconsistent.

(2) Assume $x \in \mathbb{F}_{2^3}$, $\mathbb{F}_{2^3} \cap \mathbb{F}_{2^n} = \mathbb{F}_2$ since n is not divisible by 3, which is a contradiction.

(3) Assume $x \in \mathbb{F}_{2^5}$, when $k \not\equiv 3 \pmod 5$, we get $\mathbb{F}_{2^5} \cap \mathbb{F}_{2^n} = \mathbb{F}_2$, which contradicts with $x \notin \{0,1\}$. When $k \equiv 3 \pmod 5$, we know $\mathbb{F}_{2^5} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^5}$. Thereby $x^{2^{2k}} = x^2$ and $x^{2^k} = x^8$. It follows from Eq. (13) that

$$\begin{aligned} &x^{11}+x^{25}+x^9+x^{19}+x^{26}+x^4+x^{17}+x^2 \\ =\ &x^2(x+1)(x^{23}+x^{16}+x^{15}+x^8+x^7+x+1). \end{aligned}$$

It can be checked that the polynomial $x^{23}+x^{16}+x^{15}+x^8+x^7+x+1$ is irreducible in $\mathbb{F}_2$. Thus the solutions of the above equation are in $\mathbb{F}_{2^{23}}$, which implies that $x \in \mathbb{F}_{2^{23}} \cap \mathbb{F}_{2^5} = \mathbb{F}_2$, it is unsuitable.

(4) Assume $x \in \mathbb{F}_{2^{10}}$, we can infer that $x \in \mathbb{F}_{2^2}$, $\mathbb{F}_{2^5}$ or $\mathbb{F}_{2^{10}}$. Aiming at the former two cases, we have already discussed it above. When $x \in \mathbb{F}_{2^{10}}$, we can get contradictions. We complete the proof. □

Theorem 5: Let n and k be positive integers with $n = 4k-1$, and $n \not\equiv 0 \pmod 3$, $n \not\equiv 0 \pmod{47}$. Then $f(x) = x^{2^{2k}+2^{k+1}+2^k-1}$ is a 0-APN function over $\mathbb{F}_{2^n}$.

Proof 5: We will certify that the equation

$$(x+1)^{2^{2k}+2^{k+1}+2^k-1} + x^{2^{2k}+2^{k+1}+2^k-1} + 1 = 0 \tag{15}$$

has no solution in $\mathbb{F}_{2^n} \backslash \mathbb{F}_2$. Assume that $x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2$ is a solution of Eq. (15). Multiplying $x(x+1)$ on both sides of Eq. (15). We have

$$\begin{aligned} &x^{2^{2k}+2^k+1} + x^{2^{k+1}+2^k+1} + x^{2^k+1} + x^{2^{2k}+2^{k+1}+1} \\ &+ x^{2^{2k}+1} + x^{2^{k+1}+1} + x^{2^{2k}+2^{k+1}+2^k} + x^2 = 0. \end{aligned} \tag{16}$$

And let $y = x^{2^k}$, $z = y^{2^k}$ and $u = z^{2^k}$, and raising the 2^k-th power, 2^{2k}-th power and 2^{3k}-th power to equation (16) respectively gives

$$\begin{cases} zyx+y^3x+yx+zy^2x+zx+y^2x+zy^3 \\ +x^2=0, & (17a) \\ uzy+z^3y+zy+uz^2y+uy+z^2y+uz^3 \\ +y^2=0, & (17b) \\ x^2uz+u^3z+uz+x^2u^2z+x^2z+u^2z+x^2u^3 \\ +z^2=0, & (17c) \\ y^2x^2u+x^6u+x^2u+y^2x^4u+y^2u+x^4u+y^2x^6 \\ +u^2=0. & (17d) \end{cases}$$

With the help of Magma, computing the resultant of Eq. (17b) and Eq. (17c), Eq. (17b) and Eq. (17d) with respect to u, and we get two formulas $R_1(x,y,z)$ and $R_2(x,y,z)$. And then continue to compute the resultant of $R_1(x,y,z)$ and Eq. (17a), $R_2(x,y,z)$ and Eq. (16a) with respect to z, we obtain two formulas $R_3(x,y)$ and $R_4(x,y)$. Finally, we compute the resultant of $R_3(x,y)$ and $R_4(x,y)$ with respect to y, and decompose it into the product of irreducible factors as

$$\begin{aligned} &x^{329}(x+1)^{329}(x^3+x+1)(x^{47}+x^{43}+x^{42}+x^{41} \\ &+x^{40}+x^{38}+x^{37}+x^{36}+x^{32}+x^{30}+x^{29}+x^{28} \\ &+x^{26}+x^{24}+x^{22}+x^{21}+x^{20}+x^{18}+x^{17}+x^{14} \\ &+x^{11}+x^{10}+x^9+x^6+x^4+x+1)(x^{47}+x^{44} \\ &+x^{43}+x^{40}+x^{36}+x^{35}+x^{33}+x^{32}+x^{30}+x^{23} \\ &+x^{22}+x^{19}+x^{18}+x^{17}+x^{15}+x^8+x^7+x^6 \\ &+x^5+x^3+x^2+x+1)(x^{47}+x^{45}+x^{42}+x^{41} \\ &+x^{39}+x^{38}+x^{36}+x^{33}+x^{30}+x^{29}+x^{27}+x^{26} \\ &+x^{25}+x^{24}+x^{23}+x^{21}+x^{19}+x^{17}+x^{13}+x^{12} \\ &+x^{11}+x^{10}+x^9+x^8+x^2+x+1)(x^{47}+x^{46} \\ &+x^{43}+x^{41}+x^{38}+x^{37}+x^{36}+x^{33}+x^{30}+x^{29} \end{aligned}$$

Table 2 All known CCZ-inequivalent 0-APN power functions $F(x) = x^d$ over $\mathbb{F}_{2^n}$.

number	d	conditions	Reference
1	21	$n \not\equiv 0 \pmod 6$	[5]
2	$2^r + 2^t - 1$	$gcd(r,n) = gcd(t,n) = 1$	[5]
3	$2^{2k} + 2^k + 1$	$n = 4k$, k is even	[5]
4	$2^n - 2^s$	$gcd(n, s+1) = 1$	[5]
5	$2^i - 1$	$gcd(i-1, n) = 1$	[6]
6	$3 \cdot 2^k - 7$	$n = 2k+1$	[10]
7	$2^{2k+1} - 2^{k+1} - 2^k + 1$	$n = 3k+1$	[10]
8	$3(2^k - 1$	$n = 2k$, $3 \nmid k$	[10]
9	$5(2^{k+1} + 2^k + 1)$	$n = 2k+1$, $m \not\equiv 2 \pmod 5$	[10]
10	$3(2^k - 1)$	$n = 2k+1$, $k \not\equiv 13 \pmod{27}$	[10]
11	$3(2^{k+1} + 1)$	$n = 3k+1$, $k \not\equiv 9 \pmod{14}$	[10]
12	-9	$9 \nmid n$	[10]
13	$2^{k+1} + 3$	$n = 2k+1$	[13]
14	$5 \cdot 2^k + 3$	$n = 2k+1$	[13]
15	$3(2^k - 1)$	$n = 3k-1$	[13]
16	$5 \cdot 2^{k-1} + 1$	$n = 3k-1$, $k \not\equiv 5 \pmod{14}$	[13]
17	$2^{2k+1} - 3 \cdot 2^{k-1} + 1$	$n = 3k$, $k \not\equiv 2 \pmod 3$	[13]
18	$2^{2k} + 2^{k-1} + 1$	$n = 3k+1$	[13]
19	$2^{2k} + 3 \cdot 2^{k-1} - 1$	$n = 3k+1$	[13]
20	$2^{2k-1} + 2^k + 1$	$n = 4k-1$	[13]
21	$3 \cdot 2^k + 1$	$n = 4k-1$, $n = 4k-1$	[13]
22	$2^{2k-1} - 2^{k-1} - 1$	$n = 4k-1$	[13]
23	$3(2^{2k+1} - 1)$	$n = 4k-1$	[13]
24	$2^{2k+1} + 2^{k-1} + 1$	$n = 4k+1$,k$\not\equiv 13 \pmod{53}$	[13]
25	$2^{3k} + 2^k + 1)$	$n = 5k$	[13]
26	$2^{2k+1} - 2^k - 1$	$n = 5k$, $k \not\equiv 0 \pmod 3$	[13]
27	$2^{2k-1} - 2^k - 1$	$n = 2k$, k is even, $k \nmid 3$	[17]
28	$2^{2k-1} - 2^{k-1} - 1$	$n = 2k$, k is odd	[17]
29	$2^{3k} - 2^{2k} + 2^k - 1$	$n = 2m$, $m = 2k$, k is even	[17]
30	$2^{2k} - 2^k - 1$	$n = 2k+1$, $k \not\equiv 1 \pmod 3$	[17]
31	$2^{2k-1} - 2^{k-1} - 1$	$n = 2k+1$	[17]
32	$2^{2k-1} - 2^k - 1$	$n = 2k+1$	[17]
33	$2^{2k-1} - 2^{k-1} - 1$	$n = 4k$, k is odd	[20]
34	$2^{2k-1} + 2^k + 1$	$n = 2k+1$	[20]
35	$2^{2k} + 2^{k+1} + 1$	$n = 2k+1$,$k \not\equiv 1 \pmod 3$	[20]
36	$2^{k+1} - 2^{k-1} - 1$	$n = 2k+1$,$k \not\equiv 1 \pmod 3$	[20]
37	$2^{2k} - 2^{k+1} - 1$	$n = 2k+1$,$k \not\equiv 4 \pmod 9$	[20]
38	$2^{2k} + 2^{k+1} + 1$	$n = 3k-1$	[20]
39	$2^{2k+1} + 2^{k+1} + 1$	$n = 3k-1$, k is even	[20]
40	$2^{2k+1} + 2^k + 1$	$n = 3k-1$, k is even	[20]
41	$3{\cdot}2^{2k} + 1$	$n = 3k-1$, k is even	[20]
42	$2^{2k-1} - 2^k - 1$	$n = 3k-1$, $k \not\equiv 4 \pmod 9$	[20]
43	$2^{2k-1} + 2^k + 1$	$n = 3k$, k is odd	[20]
44	$2^{2k} - 2^{k+1} - 1$	$n = 3k$, k is odd	[20]
45	$2^{2k+1} - 2^k - 1$	$n = 3k$	[20]
46	$3 \cdot (2^{k+1} - 1)$	$n = 3k+1$ $k \not\equiv 11 \pmod{34}$	[20]
47	$2^{2k} + 2^k + 1$	$gcd(3k,n) = gcd(2k,n) = 1$	[15]
48	$5 \cdot 2^{k+1} + 2^k - 1$	$n = 2k+1$	Theorem 3.1
49	$3 \cdot 2^{2k} - 5$	$n = 3k$, $2 \nmid k$, $k \not\equiv 2 \pmod 3$	Theorem 3.2
50	$2^{2k+1} - 2^{k+1} - 1$	$n = 3k+1$	Theorem 3.3
51	$2^{2k} + 2^{k+1} + 2^k - 1$	$n = 3k+1$	Theorem 3.4
52	$2^{2k} + 2^{k+1} + 2^k - 1$	$n = 4k-1$, $n \not\equiv 0 \pmod 3$, $k \not\equiv 0 \pmod{47}$	Theorem 3.5
53	$3 \cdot 2^{2k+1} - 5$	$n = 4k+1$	Theorem 3.6

$$+ x^{27} + x^{26} + x^{25} + x^{23} + x^{21} + x^{19} + x^{18} + x^{17}$$
$$+ x^{15} + x^{11} + x^{10} + x^{9} + x^{7} + x^{6} + x^{5} + x^{4} + 1)$$
$$(x^{47} + x^{46} + x^{45} + x^{39} + x^{38} + x^{37} + x^{36} + x^{35}$$
$$+ x^{34} + x^{30} + x^{28} + x^{26} + x^{24} + x^{23} + x^{22} + x^{21}$$
$$+ x^{20} + x^{18} + x^{17} + x^{14} + x^{11} + x^{9} + x^{8} + x^{6}$$
$$+ x^{5} + x^{2} + 1)(x^{47} + x^{46} + x^{45} + x^{44} + x^{42} + x^{41}$$
$$+ x^{40} + x^{39} + x^{32} + x^{30} + x^{29} + x^{28} + x^{25} + x^{24}$$
$$+ x^{17} + x^{15} + x^{14} + x^{12} + x^{11} + x^{7} + x^{4} + x^{3} + 1).$$

Observe that $x \notin \mathbb{F}_2$, thus the solutions of Eq. (15) are in $\mathbb{F}_{2^3}$ or $\mathbb{F}_{2^{47}}$.

(1) Assume $x \in \mathbb{F}_{2^3}$. Since $4k - 1 \not\equiv 0 \pmod 3$, we

Table 3 Differential spectrum of x^d over $\mathbb{F}_{2^n}$ for $n = 9$.

number	d	conditions	Differential spectrum	Reference
48	$5 \cdot 2^{k+1} + 2^k - 1$	$n = 2k + 1$	$2^{127}, 4^{63}, 6$	Theorem 3.1
6	$3 \cdot 2^k - 7$	$n = 2k + 1$	$2^{103}, 4^{45}, 6^9, 8^9$	[10]
13	$2^{k+1} + 3$	$n = 2k + 1$	$2^{154}, 4^{36}, 6^{10}$	[13]
14	$5 \cdot 2^k + 3$	$n = 2k + 1$	$2^{121}, 4^{54}, 6^9$	[13]
31	$2^{2k-1} - 2^{k-1} - 1$	$n = 2k + 1$	$2^{145}, 4^{27}, 6^{19}$	[17]
32	$2^{2k-1} - 2^k - 1$	$n = 2k + 1$	$2^{112}, 4^{45}, 6^{18}$	[17]
34	$2^{2k-1} + 2^k + 1$	$n = 2k + 1$	$2^{103}, 4^{45}, 6^9, 8^9$	[20]

Table 4 Differential spectrum of x^d over $\mathbb{F}_{2^n}$ for $n = 13$.

number	d	conditions	Differential spectrum	Reference
50	$2^{2k+1} - 2^{k+1} - 1$	$n = 3k + 1$	$2^{2484}, 4^{624}, 6^{104}, 8^{13}$	Theorem 3.3
51	$2^{2k} + 2^{k+1} + 2^k - 1$	$n = 3k + 1$	$2^{3082}, 4^{507}$	Theorem 3.4
7	$2^{2k+1} - 2^{k+1} - 2^k + 1$	$n = 3k + 1$	$2^{2575}, 4^{663}, 6^{65}$	[10]
18	$2^{2k} + 2^{k-1} + 1$	$n = 3k + 1$	$2^{2484}, 4^{611}, 6^{91}, 8^{13}, 10^{13}$	[13]
19	$2^{2k} + 3 \cdot 2^{k-1} - 1$	$n = 3k + 1$	$2^{2562}, 4^{624}, 6^{78}, 8^{13}$	[13]

have $\mathbb{F}_{2^3} \cap \mathbb{F}_{2^n} = \mathbb{F}_2$, it's a paradox.

(2) Assume $x \in \mathbb{F}_{2^{47}}$. Since $4k - 1 \not\equiv 0 \pmod{47}$, we have $\mathbb{F}_{2^{47}} \cap \mathbb{F}_{2^n} = \mathbb{F}_2$, we derive a contradiction. Hence, the proof is completed. □

Theorem 6: Let n and k be positive integers with $n = 4k + 1$. Then $f(x) = x^{3 \cdot 2^{2k+1} - 5}$ is a 0-APN function over $\mathbb{F}_{2^n}$.

Proof 6: To illustrate f is 0-APN, it suffices to prove that the equation

$$(x+1)^{3 \cdot 2^{2k+1} - 5} + x^{3 \cdot 2^{2k+1} - 5} + 1 = 0 \tag{18}$$

has no solution in $\mathbb{F}_{2^n} \backslash \mathbb{F}_2$. Assume that $x \in \mathbb{F}_{2^n} \backslash \mathbb{F}_2$ is a solution of Eq. (18). Multiplying $x^5(x+1)^5$ on both sides of Eq. (18). We have

$$\begin{aligned} &x^{2 \cdot 2^{2k+1} + 5} + x^{2^{2k+1} + 5} + x^{3 \cdot 2^{2k+1} + 4} \\ &+ x^{3 \cdot 2^{2k+1} + 1} + x^{3 \cdot 2^{2k+1}} + x^{10} + x^9 + x^6 = 0. \end{aligned} \tag{19}$$

Let $y = x^{2^k}$, and raising the 2^{2k+1}-th power to equation (19) gives

$$\begin{cases} y^4x^5 + y^2x^5 + y^6x^4 + y^6x + y^6 + x^{10} + x^9 \\ +x^6 = 0, & (20a) \\ x^4y^{10} + x^2y^{10} + x^6y^8 + x^6y^2 + x^6 + y^{20} \\ +y^{18} + y^{12} = 0. & (20b) \end{cases}$$

With the help of Magma, computing the resultant of Eq. (20a) and Eq. (20b), and then the resultant can be decomposed into the product of irreducible factors in $\mathbb{F}_2$ as

$$\begin{aligned} &x^{36}(x+1)^{36}(x^2+x+1)^{16}(x^8+x^5+x^3+x^2+1)^2 \\ &(x^8+x^5+x^4+x^3+1)^2(x^8+x^6+x^5+x^3+1)^2 \\ &(x^8+x^6+x^5+x^4+x^3+x+1)^2(x^8+x^7+x^5 \\ &+x^4+x^3+x^2+1)^2(x^8+x^7+x^6+x^4+x^2 \\ &+x+1)^2. \end{aligned}$$

Observe that $x \notin \mathbb{F}_2$, thus the solutions of Eq. (18) are in $\mathbb{F}_{2^2}$ or $\mathbb{F}_{2^8}$. We know that $n = 4k + 1$, this means n is odd, however, multiples of 2 or 8 are even. Hence, $\mathbb{F}_{2^2} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^8} \cap \mathbb{F}_{2^n} = \mathbb{F}_2$, we derive a contradiction. This completes the proof. □

4. An Analysis of the Inequivalence between Constructed Functions and Existing 0-APN Power Functions

We enumerate all existing 0-APN power functions in Table 2. The differential spectrums of power functions in distinct finite fields must be distinct, thus they are not equivalent. Therefore, Theorems 3.2, 3.5, and 3.6 are not equivalent to the enumerated 0-APN functions. By screening, we categorize the functions with the same finite field in the Table 2 into two groups: $n = 2k + 1$ and $n = 3k + 1$. Using the Magma software, we compute that their differential spectrums are different in a same finite field, as presented in Tables 3 and 4. Hence, Theorems 3.1, 3.3, and 3.4 are also not equivalent to other functions.

5. Conclusion

This paper has provided several new infinite classes of 0-APN power functions over $\mathbb{F}_{2^n}$ by using the multivariate method and resultant elimination. Based on Remark 1 and Magma experiments, our results also indicated 0-APN power functions over $\mathbb{F}_{2^n}$ in this paper are not CCZ-equivalent to the known 0-APN power functions.

References

[1] A. Bogdanov and V. RijmenLin, "Linear hulls with correlation zero and linear cryptanalysis of block ciphers," Des. Codes Cryptogr., vol.70, pp.369–383, 2014. DOI: 10.1007/s10623-012-9697-z

[2] C. Blondeau, A. Canteaut, and P. Charpin, "Differential properties of $x \to x^{2^t - 1}$," IEEE Trans. Inf. Theory, vol.57, no.12, pp.8127–8137, 2011. DOI: 10.1109/TIT.2011.2169129

[3] C. Beierle and G. Leander, "New instances of quadratic APN functions," IEEE Trans. Inf. Theory, vol.68, no.1, pp.670–678, 2022.

DOI: 10.1109/TIT.2021.3120698

[4] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, and I. Villa, "Construting APN functions through iostopic shift," IEEE Trans. Inf. Theory, vol.66, no.8, pp.5299–5309, 2020. DOI: 10.1109/TIT.2020.2974471

[5] L. Budaghyan, N. Kaleyski, C. Riera, and P. Stănică, "Partially APN functions with APN-like polynomial representations," Des. Codes Cryptogr., vol.88, no.6, pp.1159–1177, 2020. DOI: 10.1007/s10623-020-00739-6

[6] L. Budaghyan, N. Kaleyski, S. Kwon, C. Riera, and P. Stănică, "Partially APN Boolean functions and classes of functions that are not APN infinitely often," Cryptogr. Commun., vol.12, no.3, pp.527–545, 2020. DOI: 10.1007/s12095-019-00372-8

[7] C. Carlet, Boolean Functions for Cryptography and Coding Theory, Cambridge University, 2021. DOI: 10.1017/9781108606806

[8] M. Calderini, "Differentially low uniform permutations from known 4-uniform functions," Des. Codes Cryptogr., vol.89, no.1, pp.33–52, 2021. DOI: 10.1007/s10623-020-00807-x

[9] U. Dempwolff, "CCZ equivalence of power functions," Des. Codes Cryptogr., vol.86, no.3, pp.665–692, 2018. DOI: 10.1007/s10623-017-0350-8

[10] T. Fu and H.D. Yan, "Several classes of 0-APN power functions over $\mathbb{F}_{2^n}$," arXiv e-print, https://doi.org/10.48550/arXiv.2210.15103, 2022.

[11] L. Lidl and H. Niederreiter, Finite Fields, Cambridge University, 1997.

[12] Z.B. Liu, Y.Q. Li, L. Jiao, and M.S. Wang, "A new method for searching optimal differential and linear trails in ARX ciphers," IEEE Trans. Commun., vol.67, no.2, pp.1054–1068, 2020. DOI: 10.1109/TIT.2020.3040543

[13] Y.Y. Man, S.Z. Tian, N. Li, and X.Y. Zeng, "Several new infinite classes of 0-APN power functions over $\mathbb{F}_{2^n}$," Applicable Algebra Eng Commun Comput., https://doi.org/10.1007/s00200-024-00651-9, accessed April 1. 2024.

[14] K. Nyberg, "Differentially uniform mappings for cryptography," Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science, vol.765, pp.55–64, 1994. DOI: 10.1007/3-540-48285-7_6

[15] K.A. Nesheim, "Computational investigation of 0-APN monomials," The University of Bergen, 2022.

[16] A. Pott, "Partially almost perfect nonlinear permutations," LOOPS, Hungary, 2019.

[17] L.J. Qu and K.Q. Li, "More infinite classes of APN-like power functions," arXiv e-print, https://doi.org/10.48550/arXiv.2209.13456, 2022.

[18] Q.H. Wan, L.J. Qu, and C. Li, "On equivalence between known polynomial APN functions and power APN functions," Finite Fields Appl., vol.14, no.1, pp.161–182, 2021. DOI: 10.1016/j.ffa.2020.101762

[19] Y.N. Wu, N. Li, and X.Y. Zeng, "Linear codes from perfect nonlinear functions over finite fields," IEEE Trans. Commun., vol.68, no.1, pp.3–11, 2019. DOI: 10.1109/TCOMM.2019.2953674

[20] Y.P. Wang and Z.B. Zha, "New results of 0-APN power functions over $\mathbb{F}_{2^n}$," arXiv e-print, https://doi.org/10.48550/arXiv.2210.02207, 2022.

[21] Y. Yu and L. Perrin, "Constructing more quadratic APN functions with the QAM method," Cryptogr. Commun., vol.14, no.6, pp.1359–1369, 2022. DOI: 10.1007/s12095-022-00598-z

[22] L.J. Zheng, H.B. Kan, Y.J. Li, J. Peng, and D. Tang, "Constructing new APN functions through relative trace functions," IEEE Trans. Inf. Theory, vol.68, no.11, pp.7528–7537, 2022. DOI: 10.1109/TIT.2022.3186899

Huijuan Zhou is currently studying for a master's degree and her main research area is cryptographic functions.

Zepeng Zhuo received the M.S. degree from Huaibei Normal University in 2007, and the Ph.D. degree from Xidian University in 2012. Since 2002, he has been with the School of Mathematical Science, Huaibei Normal University, where he is now a professor. His research interests include cryptography and information theory.

Guolong Chen received the M.S. and Ph.D. degree from Beijing Normal University in 1993 and 1998, respectively. During 1998–2000, he was a postdoctoral fellow at the Institute of Software, Chinese Academy of Sciences. His research interests include mathematical logic and computer science.