Two new infinite families of APN functions in triviariate form

Kangquan Li[1], Nikolay Kaleyski[2]
[1] National University of Defense Technology, China;
likangquan11@nudt.edu.cn
[2] University of Bergen, Norway;
nikolay.kaleyski@uib.no

Abstract

We present two infinite families of APN functions in triviariate form over finite fields of the form $\mathbb{F}_{2^{3m}}$. We show that the functions from both families are permutations when m is odd, and are 3-to-1 functions when m is even. In particular, our functions are AB permutations for m odd. Furthermore, we observe that for $m = 3$, i.e. for $\mathbb{F}_{2^9}$, the functions from our families are CCZ-equivalent to the two bijective sporadic APN instances discovered by Beierle and Leander.

1. Introduction

We consider (n, n)-functions, that is, mappings over the finite field $\mathbb{F}_{2^n}$ or, equivalently, over the vector space $\mathbb{F}_2^n$. Such functions play an important role in i.a. symmetric cryptography where they are used as substitution boxes, or S-boxes, in practically all modern block ciphers. Since the S-boxes are typically the only nonlinear components of the cipher, its resistance to various kinds of cryptanalytic attacks directly depends on the properties of its S-boxes. For this reason, it is necessary for the design of secure ciphers to find (n, n)-functions with good cryptographic properties.

One of the most important such properties is the differential uniformity which measures the resistance of a function to differential cryptanalysis. The differential uniformity should be as low as possible in order to provide good resistance against this type of attack, and its lowest possible value is equal to 2. The (n, n)-functions attaining this optimal bound are called almost perfect nonlinear (APN), and have been the subject of multiple studies since their introduction in the early 90's. APN functions are also of interest due to their correspondence with optimal objects in coding theory, combinatorics, and other areas of mathematics and computer science.

Unfortunately, very few constructions of APN functions are known to date; these include six infinite families of APN monomials, and around 20 (depending on how one counts and classifies them) infinite

Kangquan Li is supported by the Research Fund of National University of Defense Technology under Grant ZK22-14 and the National Natural Science Foundation of China (NSFC) under Grant 62202476 and 62172427.

families of APN polynomials (here “infinite” refers to the fact that these constructions provide APN functions over $\mathbb{F}_{2^n}$ for infinitely many values of n). Furthermore, it is clear that this small number of known constructions covers only a tiny portion of what is possible: we are aware of thousands of distinct APN instances in dimensions n as low as $n = 8$, and only a handful of these are explained by the known infinite families. Constructing APN functions is thus a very difficult problem, especially when APN-ness is combined with other desirable properties such as bijectivity.

In this paper, we introduce two new infinite families of APN functions for dimensions of the form $n = 3m$. We identify the finite field $\mathbb{F}_{2^{3m}}$ with the vector space $\mathbb{F}_{2^m}^3$ which lets us represent the functions in “trivariate form”. This, in turn, allows us to express the families of functions in a simple and tractable way. We also show that the constructed functions are almost bent permutations in the case of odd dimensions, and are 3-to-1 in the case of even dimensions. We note that while APN permutations are of particular interest (since they combine two desirable properties), very few constructions of APN permutations are known at present. To the authors’ knowledge, besides the infinite APN monomial families over $\mathbb{F}_{2^n}$ with n odd, there is only one infinite family of APN permutations, namely the one given in [10, Corollary 1].

Even in the case of sporadic instances (as opposed to infinite families), few APN permutations are known. In [3], Beierle and Leander presented 35 new instances of APN functions over $\mathbb{F}_{2^9}$. Two of these instances are permutations, and are thus of particular interest. A triviariate representation of these two APN permutations as $f(x, y, z) = (x^3 + uy^2z, y^3 + uxz^2, z^3 + ux^2y)$ was given and further studied in [2] in the hope that it could lead to further instances of APN permutations in higher dimensions. However, in [1], Bartoli and Timpanella proved that the above trivariate representation does not contain any other APN permutation for larger dimensions.

Remarkably, the APN permutations arising from the families that we introduce in this paper over $\mathbb{F}_{2^9}$ are CCZ-equivalent to the two APN permutations found by Beierle and Leander in [3]. We have thus not only provided two new infinite constructions of APN permutations, but also classified the aforementioned two instances (up to CCZ-equivalence) into infinite families.

The rest of the paper is organized as follows. In Section 2, we provide the necessary background used in the rest of our work. In Sections 3 and 4 we introduce two new infinite families of APN functions which are bijective in odd dimensions. In Section 5 we present some computational data that demonstrates, among other things, that the our new infinite families give rise to functions CCZ-inequivalent to any of the previously known constructions. Section 6 concludes the paper.

2. Preliminaries

Let n, k be a natural numbers. We denote by $\mathbb{F}_{2^n}$ the finite field of extension degree n over $\mathbb{F}_2$, and by $\mathbb{F}_{2^n}^k$ the k-dimensional vector space over $\mathbb{F}_{2^n}$; in particular, $\mathbb{F}_2^n$ is the vector space of dimension n over the prime field $\mathbb{F}_2$, which can be naturally identified with $\mathbb{F}_{2^n}$. An (n, m)**-function** is any mapping F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. When $m = 1$, we call such functions **Boolean functions**. For values of m greater than 1, we refer to (n, m)-functions as **vectorial Boolean functions**. This name is due to the fact that any (n, m)-function F

can be represented as a vector $F = (f_1, f_2, \dots, f_m)$ of Boolean functions $f_1, f_2, \dots, f_m : \mathbb{F}_2^n \to \mathbb{F}_2$. These Boolean functions are called the **coordinate functions** of F. The **component functions** of F are all non-zero linear combinations of its coordinate functions, i.e. all Boolean functions of the form $F_c = \sum_{i=1}^{m} c_i f_i$ for $c = (c_1, c_2, \dots, c_m) \in \mathbb{F}_2^m$ with $c \neq 0$.

We will mostly concentrate on the case when $m = n$. While by definition (n, n)-functions are mappings from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, they can equivalently be seen as functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Any such function has a unique representation as a univariate polynomial of the form

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i$$

with $a_i \in \mathbb{F}_{2^n}$. The **algebraic degree** $\deg(F)$ of F is defined as the largest binary weight of any exponent i with $a_i \neq 0$, i.e.

$$\deg(F) = \max\{\mathrm{wt}_2(i) : 0 \leq i \leq 2^n - 1 \mid a_i \neq 0\}.$$

A function of algebraic degree at most 1 is called **affine**, and an affine function mapping 0 to 0 is called **linear**. Functions of algebraic degree exactly 2 are called **quadratic**.

In the case when $n = 3m$ for some natural number m, we can also represent an (n, n)-function F as a triple $F = (f, g, h)$ of $(3m, m)$-functions f, g, h so that

$$F(x, y, z) = (f(x, y, z), g(x, y, z), h(x, y, z))$$

for any $x, y, z \in \mathbb{F}_{2^m}$. We will refer to this representation as the **trivariate representation** of F. We note that bivariate representations (when the dimension n is divisible by 2) have been used in some constructions of infinite families before (see Table III) since some functions having a complex univariate representation can be expressed more simply in bivariate form. In the sequel, we follow a similar rationale and consider APN functions with a succinct representation in trivariate form. To the best of our knowledge, no infinite families of APN functions in triviariate form are given in the literature at the time of writing.

The **differential uniformity** $\Delta(F)$ of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is the maximum number of solutions x to any equation of the form $F(a + x) + F(x) = b$, i.e.

$$\Delta(F) = \max\{\#\{x \in \mathbb{F}_{2^n} \mid F(a + x) + F(x) = b\} : a, b \in \mathbb{F}_{2^n} \mid a \neq 0\}.$$

The function $D_a F(x) = F(a + x) + F(x)$ is called the **derivative** of F in direction $a \in \mathbb{F}_{2^n}$. Intuitively, it expresses the difference between two outputs $F(x)$ and $F(a + x)$ of the function when we know that the difference between their corresponding inputs is $a \in \mathbb{F}_{2^n}$. Roughly speaking, differential cryptanalysis exploits dependencies between the input and output of a function [6], which is why the differential uniformity should be kept as low as possible in order to prevent this. Clearly, $\Delta(F) \geq 2$ for any $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, and if $\Delta(F) = 2$, then we say that F is **almost perfect nonlinear (APN)**.

The multiset of all values $\delta_F(a, b)$ for all $0 \neq a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}$ is called the **differential spectrum** of F. In particular, the differential uniformity of F is the largest element in its differential spectrum.

Another important property of vectorial Boolean functions is the nonlinearity which measures their resistance to linear cryptanalysis [31]. Intuitively speaking, the nonlinearity F is the distance between any component function of F and any affine Boolean function. Recall that the Hamming distance $d_H(f, g)$ between two Boolean functions $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ is defined as the number of inputs on which f and g disagree, i.e. $d_H(f, g) = \#\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}$. The **nonlinearity** of an (n, n)-function F is then defined as

$$\mathcal{NL}(F) = \min_{c \in \mathbb{F}_{2^n}^*, a \text{ affine}} d_H(F_c, a),$$

where a goes through all affine $(n, 1)$-functions.

The nonlinearity is desired to be high, and its value for any (n, n)-function can be upper bounded by $2^{n-1} - 2^{(n-1)/2}$ [20]. The functions that attain this upper bound with equality are called **almost bent (AB)**. Any AB function is APN, but the converse is not true; however, we know that any quadratic APN function over $\mathbb{F}_{2^n}$ with n odd is AB [18].

Due to the large number of (n, n)-functions, they are usually considered up to some notion of equivalence. At present, the most general notion of equivalence used in practice is that of CCZ-equivalence. We say that $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are **CCZ-equivalent** if there exists an affine permutation $A : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$ mapping the graph $\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_2^n\}$ of F to the graph Γ_G of G.

While the definition of CCZ-equivalence is straightforward, deciding whether two given (n, n)-functions are CCZ-equivalent is a hard computational problem. However, since APN functions are classified up to CCZ-equivalence, being able to demonstrate that the functions arising from some new construction are inequivalent to the previously known ones is a crucial part of showing that a given construction is new.

Fortunately, justifying the CCZ-inequivalence of two quadratic APN functions can almost always be done very easily by means of their so-called orthoderivatives. An **orthoderivative** of an (n, n)-function F is an (n, n)-function π_F such that $\pi_F(0) = 0$ and for any $0 \neq a \in \mathbb{F}_{2^n}$, we have $\pi_F(a) \cdot (F(x) + F(a + x) + F(a) + F(0)) = 0$ for all $x \in \mathbb{F}_{2^n}$, where "$\cdot$" denotes some scalar product over $\mathbb{F}_2^n$. It is known that any quadratic APN function has a uniquely defined orthoderivative [17].

Refuting CCZ-equivalence through the orthoderivatives involves going through some notions of equivalence less general than CCZ-equivalence, which we define now. Let F, G be (n, n)-functions and suppose that $A_1 \circ F + A_2 + A = G$ for some affine functions A_1, A_2, A, where A_1, A_2 are permutations. Then we say that F and G are **extended affine (EA) equivalent**. If $A = 0$, then we say that F and G are **affine equivalent**. If, in addition, $A_1(0) = A_2(0) = 0$, we say that F and G are **linear equivalent**.

We know that two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent [34]; and that if F and G are EA-equivalent, then π_F and π_G are affine equivalent. This means that any property that is invariant under affine equivalence, when applied to π_F and π_G, can be used to distinguish between CCZ-inequivalent quadratic APN functions. In particular, it is known that the differential spectrum is invariant under affine equivalence (and, more generally, under CCZ-equivalence), and it is observed in

TABLE I
KNOWN INFINITE FAMILIES OF APN POWER FUNCTIONS OVER $\mathbb{F}_{2^n}$

Family	Exponent	Conditions	Algebraic degree	Source
Gold	$2^i + 1$	$\gcd(i, n) = 1$	2	[25, 32]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	$i + 1$	[28, 29]
Welch	$2^t + 3$	$n = 2t + 1$	3	[22]
Niho	$2^t + 2^{t/2} - 1$, t even $2^t + 2^{(3t+1)/2} - 1$, t odd	$n = 2t + 1$	$(t + 2)/2$ $t + 1$	[21]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$	[5, 32]
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	$i + 3$	[23]

[17] that computing the differential spectra of the orthoderivatives is almost always sufficient to distinguish between CCZ-inequivalent APN functions. There are some rare cases in which CCZ-inequivalent functions have orthoderivatives with the same differential spectrum, in which case other invariants such as the Walsh spectrum can be applied to the orthoderivatives. In our case, the differential spectra of the orthoderivatives of the functions that we construct are already distinct from those of all known quadratic APN functions, and so we do not need to take any further steps like this.

Despite the large number of known APN instances over $\mathbb{F}_{2^n}$ for e.g. $n = 8$, see e.g. [3, 35], very few of them have been generalized into infinite families. Table I lists the known infinite families of APN monomials, while Tables II and III list the known non-monomial families. The former lists the families given in univariate form, while the latter lists those given in bivariate form.

TABLE II

KNOWN INFINITE FAMILIES OF QUADRATIC APN POLYNOMIALS OVER $\mathbb{F}_{2^n}$ IN UNIVARIATE FORM

ID	Functions	Conditions	Source
F1-F2	$x^{2^s+1} + u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n = pk, \gcd(k,3) = \gcd(s,3k) = 1, p \in \{3,4\}, i = sk \bmod p, m = p - i, n \geq 12, u$ primitive in $\mathbb{F}^*_{2^n}$	[10]
F3	$sx^{q+1} + x^{2^i+1} + x^{q(2^i+1)} + cx^{2^iq+1} + c^qx^{2^i+q}$	$q = 2^m, n = 2m$, $\gcd(i,m) = 1$, $c \in \mathbb{F}_{2^n}, s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q, X^{2^i+1} + cX^{2^i} + c^qX + 1$ has no solution x s.t. $x^{q+1} = 1$	[9]
F4	$x^3 + a^{-1}\mathrm{Tr}_n(a^3x^9)$	$a \neq 0$	[11]
F5	$x^3 + a^{-1}\mathrm{Tr}^3_n(a^3x^9 + a^6x^{18})$	$3 \mid n$, $a \neq 0$	[12]
F6	$x^3 + a^{-1}\mathrm{Tr}^3_n(a^6x^{18} + a^{12}x^{36})$	$3 \mid n, a \neq 0$	[12]
F7-F9	$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} + vx^{2^{-k}+1} + wu^{2^k+1}x^{2^s+2^{k+s}}$	$n = 3k, \gcd(k,3) = \gcd(s,3k) = 1, v, w \in \mathbb{F}_{2^k}, vw \neq 1, 3 \mid (k+s), u$ primitive in $\mathbb{F}^*_{2^n}$	[7]
F10	$a^2x^{2^{2m+1}+1} + b^2x^{2^{m+1}+1} + ax^{2^{2m}+2} + bx^{2^m+2} + (c^2+c)x^3$	$n = 3m, m$ odd, $L(x) = ax^{2^{2m}} + bx^{2^m} + cx$ satisfies the conditions of Lemma 8 of [8]	[8]
F11	$x^3 + a(x^{2^i+1})^{2^k} + bx^{3\cdot 2^m} + c(x^{2^{i+m}+2^m})^{2^k}$	$n = 2m = 10$, $(a,b,c) = (\beta,1,0,0)$, $i = 3$, $k = 2$, β primitive in $\mathbb{F}_{2^2}$ $n = 2m$, m odd, $3 \nmid m$, $(a,b,c) = (\beta,\beta^2,1)$, β primitive in $\mathbb{F}_{2^2}$, $i \in \{m-2, m, 2m-1, (m-2)^{-1} \mod n\}$	[13]
F12	$a\mathrm{Tr}^n_m(bx^{2^i+1}) + a^q\mathrm{Tr}^n_m(cx^{2^s+1})$	$n = 2m, m$ odd, $q = 2^m$, $a \notin \mathbb{F}_q$, $\gcd(i,n) = 1$, i, s, b, c satisfy the conditions of Theorem 2	[36]
F13	$L(z)^{2^m+1} + vz^{2^m+1}$	$\gcd(s,m) = 1, v \in \mathbb{F}^*_{2^m}, \mu \in \mathbb{F}^*_{2^{3m}}, L(z) = z^{2^{m+s}} + \mu z^{2^s} + z$ permutes $\mathbb{F}_{2^{3m}}$	[30]

3. AN INFINITE FAMILY OF APN FUNCTIONS OVER $\mathbb{F}^3_{2^m}$

Theorem 1. *Let* $\gcd(i,m) = 1$, $q = 2^i$ *and*

$$F(x,y,z) = \left(x^{q+1} + x^qz + yz^q, x^qz + y^{q+1}, xy^q + y^qz + z^{q+1}\right).$$

Assume that the polynomials $X^{q^2+q+1} + X + 1$, $X^{q^2+q+1} + X^{q^2} + 1$ *and* $X^{q^2+q+1} + X^{q^2+1} + X^{q+1} + X + 1$ *have no roots in* $\mathbb{F}_{2^m}$*, and the polynomial*

$$X^{q^2+q+1} + XY^{q^2+q} + XY^q + X^{q^2+q} + X^qY^{q^2} + X^{q^2}Y + Y^{q^2+q+1} + Y^{q^2+q} + Y^{q^2} + Y^q + 1$$

has no roots in $\mathbb{F}^2_{2^m}$*. Then* F *is APN over* $\mathbb{F}^3_{2^m}$*.*

Proof. Since F is quadratic and $F(0,0,0) = (0,0,0)$, it suffices to show that the equation

$$F(x+a, y+b, z+c) + F(x,y,z) + F(a,b,c) = (0,0,0) \tag{1}$$

TABLE III
KNOWN INFINITE FAMILIES OF QUADRATIC APN POLYNOMIALS OVER $\mathbb{F}_{2^{2m}}$ IN BIVARIATE FORM

ID	Functions	Conditions	Source
F14	$(xy, x^{2^k+1} + \alpha y^{(2^k+1)2^i})$	$\gcd(k, m) = 1$, m even, α not a cube	[37]
F15	$(xy, x^{2^{2m}+2^{3m}} + ax^{2^{2m}}y^{2^m} + by^{2^m+1})$	$x^{2^m+1} + ax + b$ has no root in $\mathbb{F}_{2^m}$	[33]
F16	$(xy, x^{2^i+1} + x^{2^{i+m/2}}y^{2^{m/2}} + bxy^{2^i} + cy^{2^i+1})$	$(cx^{2^i+1} + bx^{2^i} + 1)^{2^{m/2}+1} + x^{2^{m/2}+1}$ has no roots in $\mathbb{F}_{2^m}$	[15]
F17	$(x^{2^i+1} + xy^{2i} + y^{2^i+1}, x^{2^{2i}+1} + x^{2^{2i}}y + y^{2^{2i}+1})$	$\gcd(3i, m) = 1$	[26]
F18	$(x^{2^i+1} + xy^{2^i} + y^{2^i+1}, x^{2^{3i}}y + xy^{2^{3i}})$	$\gcd(3i, m) = 1$, m odd	[26]
F19	$(x^3 + xy^2 + y^3 + xy, x^5 + x^4y + y^5 + xy + x^2y^2)$	$\gcd(3, m) = 1$	[30]
F20	$(x^{q+1} + By^{q+1}, x^ry + \frac{a}{B}xy^r)$	$0 < k < m$, $q = 2^k$, $r = 2^{k+m/2}$, $m \equiv 2 \pmod 4$, $\gcd(k, m) = 1$, $a \in \mathbb{F}^*_{2^{m/2}}$, $B \in \mathbb{F}_{2^m}$, B not a cube, $B^{q+r} \neq a^{q+1}$	[27]
F21	$(x^{q+1} + xy^q + \alpha y^{q+1}, x^{q^2+1} + \alpha x^{q^2}y + (1+\alpha)^q xy^{q^2} + \alpha y^{q^2+1})$	$k, m > 0$, $\gcd(k, m) = 1$, $q = 2^k$, $\alpha \in \mathbb{F}_{2^m}$, $x^{q+1} + x + \alpha$ has no roots in $\mathbb{F}_{2^m}$	[16]
F22	$(x^3+xy+xy^2+\alpha y^3, x^5+xy+\alpha x^2y^2+\alpha x^4y+(1+\alpha)^2xy^4 + \alpha y^5)$	$\alpha \in \mathbb{F}_{2^m}$, $x^3 + x + \alpha$ has no roots in $\mathbb{F}_{2^m}$	[16]

has exactly two solutions in $\mathbb{F}_{2^m}^3$ for any $(a, b, c) \in \mathbb{F}_{2^m}^3 \backslash \{(0, 0, 0)\}$. By simplifying, Eq. (1) is equivalent to the following equation system:

$$\begin{cases} (a+c)x^q + a^q x + c^q y + bz^q + a^q z = 0, & (2.1)\\ cx^q + by^q + b^q y + a^q z = 0, & (2.2)\\ b^q x + (a+c)y^q + cz^q + (b^q + c^q)z = 0. & (2.3) \end{cases}$$

Next we divide the proof into several cases and sub-cases depending on whether the elements a, b, c are zero or non-zero.

Case (I): $a = 0$**.** In this case, Eqs. (2) become

$$\begin{cases} cx^q + c^q y + bz^q = 0, & (3.1)\\ cx^q + by^q + b^q y = 0, & (3.2)\\ b^q x + cy^q + cz^q + (b^q + c^q)z = 0. & (3.3) \end{cases}$$

Subcase (I.1): $b=0, c\neq 0$. In this subcase, by Eq. (3.2), we have $x=0$ and then $y=0$ from Eq. (3.1). Together with $x=y=0$ and Eq. (3.3), we know that $cz^q+c^qz=0$, implying that $z\in\{0,c\}$ since $\gcd(i,m)=1$. Thus Eqs. (2) have exactly two solutions $(x,y,z)\in\{(0,0,0),(0,0,c)\}$ in this subcase.

Subcase (I.2): $b\neq 0, c=0$. In this subcase, from Eq. (3.1) and Eq. (3.2), we can get $z=0$ and $by^q+b^qy=0$, i.e., $y\in\{0,b\}$, respectively. Moreover, by Eq. (3.3), we have $x=0$. Therefore Eqs. (2) have exactly two solutions $(x,y,z)\in\{(0,0,0),(0,b,0)\}$ in this subcase.

Subcase (I.3): $bc\neq 0$. In this subcase, we replace x,y,z by cx,by,cz, respectively in Eqs. (3) and get

$$\begin{cases} c^{q+1}x^q+bc^qy+bc^qz^q=0, & (4.1)\\ c^{q+1}x^q+b^{q+1}y^q+b^{q+1}y=0, & (4.2)\\ b^qcx+b^qcy^q+c^{q+1}z^q+(b^qc+c^{q+1})z=0. & (4.3)\end{cases}$$

It is clear that the numbers of solutions of Eqs. (3) and Eqs. (4) are the same. After multiplying $\frac{1}{bc^q}$ (resp. $\frac{1}{b^{q+1}}$, $\frac{1}{b^qc}$) into the two parts of Eq. (4.1) (resp. Eq. (4.2), Eq. (4.3)), we obtain

$$\begin{cases} \Delta x^q+y+z^q=0, & (5.1)\\ \Delta^{q+1}x^q+y^q+y=0, & (5.2)\\ x+y^q+\Delta^qz^q+(\Delta^q+1)z=0, & (5.3)\end{cases}$$

where $\Delta=\frac{c}{b}$. By Eq. (5.1), we have $y=\Delta x^q+z^q$ and then plugging it into Eq. (5.2) and (5.3), we obtain

$$\Delta^qx^{q^2}+\Delta(\Delta^q+1)x^q+z^{q^2}+z^q=0 \tag{6}$$

and

$$\Delta^qx^{q^2}+x+z^{q^2}+\Delta^qz^q+(\Delta^q+1)z=0, \tag{7}$$

respectively. After summing Eqs. (6) and (7), we get

$$\Delta(\Delta^q+1)x^q+x+(\Delta^q+1)(z^q+z)=0. \tag{8}$$

Raising Eq. (8) into its q-th power and plugging $z^{q^2}+z^q=\Delta^qx^{q^2}+\Delta(\Delta^q+1)x^q$ from Eq. (6) into it, we acquire

$$\Delta^q(\Delta^{q^2}+1)x^{q^2}+x^q+(\Delta^{q^2}+1)(\Delta^qx^{q^2}+\Delta(\Delta^q+1)x^q)=0,$$

i.e.,

$$(\Delta^{q^2+q+1}+\Delta^{q^2+1}+\Delta^{q+1}+\Delta+1)x^q=0. \tag{9}$$

According to the condition that polynomial $X^{q^2+q+1}+X^{q^2+1}+X^{q+1}+X+1$ has no roots in $\mathbb{F}_{2^m}$, we have $x^q=0$, i.e., $x=0$. Plugging it into Eq. (6) and $y=\Delta x^q+z^q$ (from (5.1)), we get $z^{q^2}+z^q=0$ and $y=z^q$, respectively. Thus $z\in\{0,1\}$ and $y=z^q$. Namely, Eqs. (2) have exactly two solutions in this subcase.

Case (II): $a \neq 0$.

Subcase (II.1): $b = c = 0$. In this subcase, from Eqs. (2), we obtain $ax^q + a^q x = 0$, $a^q z = 0$ and $ay^q = 0$, respectively. Thus it is trivial that Eqs. (2) have exactly two solutions $(x, y, z) \in \{(0,0,0), (a,0,0)\}$ in this subcase.

Subcase (II.2): $b = 0, c \neq 0$. In this subcase, Eqs. (2) become

$$\begin{cases} (a+c)x^q + a^q x + c^q y + a^q z = 0, & (10.1) \\ cx^q + a^q z = 0, & (10.2) \\ (a+c)y^q + cz^q + c^q z = 0. & (10.3) \end{cases}$$

We replace x, z by ax, cz, respectively in Eqs. (10) and get

$$\begin{cases} (a+c)a^q x^q + a^{q+1} x + c^q y + a^q cz = 0, & (11.1) \\ a^q cx^q + a^q cz = 0, & (11.2) \\ (a+c)y^q + c^{q+1}(z^q + z) = 0. & (11.3) \end{cases}$$

From Eq. (11.2), we have $z = x^q$ and then plugging it into Eq. (11.1) and Eq. (11.3), we obtain

$$a^{q+1}(x^q + x) + c^q y = 0 \tag{12}$$

and

$$(a+c)y^q + c^{q+1}(x^{q^2} + x^q) = 0, \tag{13}$$

respectively. Summing the q-th power of Eq. (12) multiplied by c^{q+1} and Eq. (13) multiplied by a^{q^2+q}, we obtain

$$(a^{q^2+q+1} + a^{q^2+q}c + c^{q^2+q+1})y^q = 0.$$

If $a^{q^2+q+1} + a^{q^2+q}c + c^{q^2+q+1} = 0$, then $(c/a)^{q^2+q+1} + c/a + 1 = 0$, which contradicts the hypothesis. Thus $y = 0$. Plugging $y = 0$ into Eq. (12), we have $a^{q+1}(x^q + x) = 0$, implying $x \in \{0, 1\}$. Therefore, Eqs. (2) have exactly two solutions in this subcase.

Subcase (II.3): $b \neq 0, c = 0$. In this subcase, Eqs. (2) become

$$\begin{cases} ax^q + a^q x + bz^q + a^q z = 0, & (14.1) \\ by^q + b^q y + a^q z = 0, & (14.2) \\ b^q x + ay^q + b^q z = 0. & (14.3) \end{cases}$$

We replace x, y, z by ax, by, az, respectively in Eqs. (14) and get

$$\begin{cases} a^{q+1}x^q + a^{q+1}x + a^q b z^q + a^{q+1}z = 0, & (15.1) \\ b^{q+1}y^q + b^{q+1}y + a^{q+1}z = 0, & (15.2) \\ ab^q x + ab^q y^q + ab^q z = 0. & (15.3) \end{cases}$$

Let $\Delta = \frac{b}{a}$. Then we obtain $x^q + x + \Delta z^q + z = 0$, $z = \Delta^{q+1}(y^q + y)$ and $z = x + y^q$, respectively, from Eqs. (15). From the last two equations, we have $x = (1 + \Delta^{q+1})y^q + \Delta^{q+1}y$. Plugging it and $z = \Delta^{q+1}(y^q + y)$ into $x^q + x + \Delta z^q + z = 0$, we acquire

$$(1 + \Delta^{q^2+q} + \Delta^{q^2+q+1})(y^{q^2} + y^q) = 0.$$

By the condition that the polynomial $X^{q^2+q+1} + X + 1$ has no roots in $\mathbb{F}_{2^m}$, we easily know that $1 + \Delta^{q^2+q} + \Delta^{q^2+q+1} \neq 0$ and thus $y^{q^2} + y^q = 0$, i.e., $y \in \{0, 1\}$. Therefore, Eqs. (2) have exactly two solutions in this subcase.

Subcase (II.4): $bc \neq 0$. In this subcase, we replace x, y, z by ax, by, cz, respectively in Eqs. (2) and get

$$\begin{cases} (a^{q+1} + a^q c)x^q + a^{q+1}x + bc^q y + bc^q z^q + a^q cz = 0, & (16.1) \\ a^q c x^q + b^{q+1}y^q + b^{q+1}y + a^q cz = 0, & (16.2) \\ ab^q x + (ab^q + b^q c)y^q + c^{q+1}z^q + (b^q c + c^{q+1})z = 0. & (16.3) \end{cases}$$

By Eq. (16.2), we have

$$z = x^q + \frac{b^{q+1}}{a^q c}y^q + \frac{b^{q+1}}{a^q c}y. \tag{17}$$

After plugging Eq. (17) into Eq. (16.1) and multiplying it by a^{q^2}, we obtain

$$a^{q^2}bc^q x^{q^2} + a^{q^2+q+1}x^q + a^{q^2+q+1}x + b^{q^2+q+1}y^{q^2} + b^{q+1}(a^{q^2} + b^{q^2})y^q + a^{q^2}b(b^q + c^q)y = 0. \tag{18}$$

After plugging Eq. (17) into Eq. (16.3) and multiplying it by a^{q^2+q}, we acquire

$$\begin{aligned} &a^{q^2+q}c^{q+1}x^{q^2} + a^{q^2+q}c(b^q + c^q)x^q + a^{q^2+q+1}b^q x + a^q b^{q^2+q}cy^{q^2} + \\ &b^q(a^{q^2+q+1} + a^{q^2+q}c + a^q b^{q^2}c + a^{q^2}b^{q+1} + a^{q^2}bc^q)y^q + a^{q^2}b^{q+1}(b^q + c^q)y = 0. \end{aligned} \tag{19}$$

Summing the left-hand side of Eq. (18) multiplied by $a^q c$ and that of Eq. (19) multiplied by b, we get after dividing by aq^2

$$\begin{aligned} &a^q c(a^{q+1} + b^{q+1} + bc^q)x^q + a^{q+1}(a^q c + b^{q+1})x + b^{q+1}(a^{q+1} + b^{q+1} + bc^q)y^q + \\ &(a^q c + b^{q+1})(b^{q+1} + bc^q)y = 0. \end{aligned} \tag{20}$$

Raising Eq. (20) into its q-th power, we have

$$a^{q^2}c^q(a^{q^2+q}+b^{q^2+q}+b^qc^{q^2})x^{q^2}+a^{q^2+q}(a^{q^2}c^q+b^{q^2+q})x^q+b^{q^2+q}(a^{q^2+q}+b^{q^2+q}+b^qc^{q^2})y^{q^2}+ \\ (a^{q^2}c^q+b^{q^2+q})(b^{q^2+q}+b^qc^{q^2})y^q=0. \tag{21}$$

Summing the left-hand side of Eq. (21) multiplied by b with that of Eq. (18) multiplied by $a^{q^2+q}+b^{q^2+q}+b^qc^{q^2}$, we obtain after dividing by a^{q^2}

$$a^q(a^{q^2+q+1}+ab^{q^2+q}+ab^qc^{q^2}+a^{q^2}bc^q+b^{q^2+q+1})x^q+a^{q+1}(a^{q^2+q}+b^{q^2+q}+b^qc^{q^2})x+ \\ b^{q+1}(a^{q^2+q}+a^qb^{q^2}+b^{q^2+q}+b^qc^{q^2}+b^{q^2}c^q+c^{q^2+q})y^q+b(b^q+c^q)(a^{q^2+q}+b^{q^2+q}+b^qc^{q^2})y=0 \tag{22}$$

Summing the left-hand side of Eq. (21) multiplied by a^qc and that of Eq. (19) multiplied by $a^{q^2+q}+b^{q^2+q}+b^qc^{q^2}$, we obtain after dividing by $a^{q^2}b^q$

$$a^qc(a^{q^2+q}+a^qb^{q^2}+b^{q^2+q}+b^qc^{q^2}+b^{q^2}c^q+c^{q^2+q})x^q+a^{q+1}(a^{q^2+q}+b^{q^2+q}+b^qc^{q^2})x+ \\ Sy^q+b(b^q+c^q)(a^{q^2+q}+b^{q^2+q}+b^qc^{q^2})y=0, \tag{23}$$

where

$$\begin{aligned} S &= a^{q^2+2q+1}+a^{q+1}b^{q^2+q}+a^{q+1}b^qc^{q^2}+a^{q^2+2q}c+a^{2q}b^{q^2}c+a^{q^2+q}b^{q+1}+a^{q^2+q}bc^q+a^qb^{q^2+q}c+ \\ &\quad a^qb^qc^{q^2+1}+a^qb^{q^2}c^{q+1}+a^qc^{q^2+q+1}+b^{q^2+2q+1}+b^{2q+1}c^{q^2}+b^{q^2+q+1}c^q+b^{q+1}c^{q^2+q}. \end{aligned}$$

Adding Eq. (22) and Eq. (23), we can find that

$$a^qT(x^q+y^q)=0, \tag{24}$$

where

$$T=a^{q^2+q+1}+ab^{q^2+q}+ab^qc^{q^2}+a^{q^2+q}c+a^qb^{q^2}c+a^{q^2}bc^q+b^{q^2+q+1}+b^{q^2+q}c+b^qc^{q^2+1}+b^{q^2}c^{q+1}+c^{q^2+q+1}.$$

If $T=0$, let $A=\frac{a}{c}$ and $B=\frac{b}{c}$. Then we have

$$\frac{T}{c^{q^2+q+1}}=A^{q^2+q+1}+AB^{q^2+q}+AB^q+A^{q^2+q}+A^qB^{q^2}+A^{q^2}B+B^{q^2+q+1}+B^{q^2+q}+B^{q^2}+B^q+1=0,$$

which contradicts the condition that the polynomial

$$X^{q^2+q+1}+XY^{q^2+q}+XY^q+X^{q^2+q}+X^qY^{q^2}+X^{q^2}Y+Y^{q^2+q+1}+Y^{q^2+q}+Y^{q^2}+Y^q+1$$

has no roots in $\mathbb{F}_{2^m}^2$. Thus we get $x=y$ by Eq. (24). Now we plug $x=y$ into Eq. (20) and get

$$(a^qc+b^{q+1})(a^{q+1}+b^{q+1}+bc^q)(x+x^q)=0. \tag{25}$$

If $a^qc+b^{q+1}=0$, plugging $c=\frac{b^{q+1}}{a^q}$ and $x=y$ into Eq. (18), we obtain

$$a^{q^2+q+1}x^q+a^{q^2+q+1}x+(a^{q^2}b^{q+1}+b^{q^2+q+1})x^q+(a^{q^2}b^{q+1}+b^{q^2+q+1})x=0,$$

i.e.,

$$(a^{q^2+q+1}+a^{q^2}b^{q+1}+b^{q^2+q+1})(x^q+x)=0.$$

Since $a^{q^2+q+1}+a^{q^2}b^{q+1}+b^{q^2+q+1}\neq 0$ thanks to the condition that $X^{q^2+q+1}+X^{q^2}+1$ has no roots in $\mathbb{F}_{2^m}$, we have $x^q+x=0$, i.e, $x\in\{0,1\}$. Thus Eqs. (2) have exactly two solutions when $a^qc+b^{q+1}=0$.

If $a^{q+1}+b^{q+1}+bc^q=0$, plugging $bc^q=a^{q+1}+b^{q+1}$ and $x=y$ into Eq. (18), we can get

$$\begin{aligned}&(a^{q^2+q+1}+a^{q^2}b^{q+1})x^{q^2}+a^{q^2+q+1}x^q+a^{q^2+q+1}x+b^{q^2+q+1}x^{q^2}+\\&b^{q+1}(a^{q^2}+b^{q^2})x^q+(a^{q^2}b^{q+1}+a^{q^2+q+1}+a^{q^2}b^{q+1})x=0,\end{aligned}$$

i.e.,

$$(a^{q^2+q+1}+a^{q^2}b^{q+1}+b^{q^2+q+1})(x^{q^2}+x^q)=0.$$

Clearly, we have $x^{q^2}+x^q=0$, implying $x\in\{0,1\}$. Thus Eqs. (2) have exactly two solutions when $a^qc+b^{q+1}=0$.

If $(a^qc+b^{q+1})(a^{q+1}+b^{q+1}+bc^q)\neq 0$, then by Eq. (25), we have $x^q+x=0$, and then $x\in\{0,1\}$. Thus Eqs. (2) have exactly two solutions when $(a^qc+b^{q+1})(a^{q+1}+b^{q+1}+bc^q)\neq 0$.

In conclusion, Eqs. (2) have exactly two solutions in this subcase.

Together with the above two cases, we can conclude that Eqs. (2) have exactly two solutions in $\mathbb{F}_{2^m}^3$ and thus F is APN. □

We now show that when m is odd, the functions described in Theorem 1 are permutations.

Theorem 2. *Let* $\gcd(i,m)=1$*,* m *be odd,* $q=2^i$ *and*

$$F(x,y,z)=\left(x^{q+1}+x^qz+yz^q,x^qz+y^{q+1},xy^q+y^qz+z^{q+1}\right).$$

Assume that the polynomials $X^{q^2+q+1}+X+1$*,* $X^{q^2+q+1}+X^{q^2}+1$ *and* $X^{q^2+q+1}+X^{q^2+1}+X^{q+1}+X+1$ *have no roots in* $\mathbb{F}_{2^m}$*, and the polynomial*

$$X^{q^2+q+1}+XY^{q^2+q}+XY^q+X^{q^2+q}+X^qY^{q^2}+X^{q^2}Y+Y^{q^2+q+1}+Y^{q^2+q}+Y^{q^2}+Y^q+1$$

has no roots in $\mathbb{F}_{2^m}^2$*. Then* F *is a permutation over* $\mathbb{F}_{2^m}^3$*.*

Proof. It suffices to show that the equation

$$F(x+a,y+b,z+c)+F(x,y,z)=(0,0,0) \tag{26}$$

has no solutions in $\mathbb{F}_{2^m}^3$ for any $(a,b,c)\in\mathbb{F}_{2^m}^3\backslash\{(0,0,0)\}$. By simplifying, Eq. (26) is equivalent to the following equation system:

$$\begin{cases} (a+c)x^q + a^q x + c^q y + bz^q + a^q z = a^{q+1} + a^q c + bc^q, & (27.1) \\ cx^q + by^q + b^q y + a^q z = a^q c + b^{q+1}, & (27.2) \\ b^q x + (a+c)y^q + cz^q + (b^q + c^q)z = ab^q + b^q c + c^{q+1}. & (27.3) \end{cases}$$

Next, we divide the proof into two cases depending on whether $a = 0$ or $a \neq 0$. For each case, we consider several sub-cases depending on whether the elements a, b, c are zero or not.

Case (I): $a = 0$**.** In this case, Eqs. (27) become

$$\begin{cases} cx^q + c^q y + bz^q = bc^q, & (28.1) \\ cx^q + by^q + b^q y = b^{q+1}, & (28.2) \\ b^q x + cy^q + cz^q + (b^q + c^q)z = b^q c + c^{q+1}. & (28.3) \end{cases}$$

Subcase (II.1): $b = 0, c \neq 0$. In this subcase, by Eqs. (28), we get $cx^q + c^q y = 0, cx^q = 0$ and $cy^q + cz^q + c^q z = c^{q+1}$, respectively. Thus it is clear that $x = y = 0$ and $cz^q + c^q z = c^{q+1}$, which implies $\left(\frac{z}{c}\right)^q + \frac{z}{c} = 1$. Applying the absolute trace function Tr_m to both parts of the above equation, we have

$$0 = \mathrm{Tr}_m\left(\left(\frac{z}{c}\right)^q + \frac{z}{c}\right) = \mathrm{Tr}_m(1) = 1,$$

where the last equality holds due to m being odd by assumption. We thus obtain a contradiction, and therefore Eqs. (27) do not have a solution.

Subcase (II.2): $b \neq 0, c = 0$. In this subcase, from Eqs. (28), we obtain $bz^q = 0$, $by^q + b^q y = b^{q+1}$ and $b^q x + b^q z = 0$, respectively. Similarly to the proof of Subcase (II.1), we can conclude that Eqs. (27) have no solutions in this subcase.

Subcase (II.3): $bc \neq 0$. After replacing x, y, z by cx, by, cz in Eqs. (28) and simplifying, we get

$$\begin{cases} \Delta x^q + y + z^q + 1 = 0, & (29.1) \\ \Delta^{q+1} x^q + y^q + y + 1 = 0, & (29.2) \\ x + y^q + \Delta^q z^q + (1 + \Delta^q)z + 1 + \Delta^q = 0, & (29.3) \end{cases}$$

where $\Delta = \frac{c}{b}$. From Eq. (29.1), we have $y = \Delta x^q + z^q + 1$. Plugging it into Eq. (29.2) and Eq. (29.3), we get

$$\Delta^q x^{q^2} + (\Delta^{q+1} + \Delta)x^q + z^{q^2} + z^q + 1 = 0, \tag{30}$$

and

$$\Delta^q x^{q^2} + x + z^{q^2} + \Delta^q z^q + (1 + \Delta^q)z + \Delta^q = 0, \tag{31}$$

respectively. Summing Eqs. (30) and (31), we obtain

$$(\Delta^{q+1} + \Delta)x^q + x + (\Delta^q + 1)(z^q + z + 1) = 0. \tag{32}$$

Raising Eq. (32) into its q-th power, we get

$$(\Delta^{q^2+q}+\Delta^q)x^{q^2}+x^q+(\Delta^{q^2}+1)(z^{q^2}+z^q+1)=0. \tag{33}$$

Adding the left-hand side of Eq. (30) multiplied by $\Delta^{q^2}+1$ and that of Eq. (33), we acquire

$$(\Delta^{q^2+q+1}+\Delta^{q^2+1}+\Delta^{q+1}+\Delta+1)x^q=0. \tag{34}$$

From the fact that the polynomial $X^{q^2+q+1}+X^{q^2+1}+X^{q+1}+X+1$ has no roots in $\mathbb{F}_{2^m}$ and Eq. (34), we know that $x=0$. Plugging it into Eq. (30), we get $z^{q^2}+z+1=0$. Applying the absolutely trace function $\mathrm{Tr}_m(\cdot)$ to the above equation, we have $0=\mathrm{Tr}_m(0)=\mathrm{Tr}_m(z^{q^2}+z+1)=\mathrm{Tr}_m(1)=1$, which is a contradiction. Therefore, Eqs. (27) do not have a solution.

Case (II): $a\neq 0$**.**

Subcase (II.1): $b=0, c=0$. In this subcase, from Eqs. (27), we have $ax^q+a^qx+a^qz=a^{q+1}, a^qz=0$ and $ay^q=0$, respectively. Similar to the proof of Subcase (II.1), we can conclude that Eqs. (27) do not have a solution.

Subcase (II.2): $b=0, c\neq 0$. In this subcase, Eqs. (27) become

$$\begin{cases} (a+c)x^q+a^qx+c^qy+a^qz=a^{q+1}+a^qc, & (35.1)\\ cx^q+a^qz=a^qc, & (35.2)\\ (a+c)y^q+cz^q+c^qz=c^{q+1}. & (35.3)\end{cases}$$

By replacing x,y,z by ax,cy,cz, respectively, and simplifying, we get

$$\begin{cases} (\Delta^{q+1}+\Delta^q)x^q+\Delta^{q+1}x+y+\Delta^qz+\Delta^{q+1}+\Delta^q=0, & (36.1)\\ x^q+z+1=0, & (36.2)\\ (\Delta+1)y^q+z^q+z+1=0, & (36.3)\end{cases}$$

where $\Delta=\frac{a}{c}$. From Eq. (36.2), we get $z=x^q+1$. Plugging it into Eq. (36.1), we have

$$y=\Delta^{q+1}(x^q+x+1). \tag{37}$$

After plugging $z=x^q+1$ and Eq. (37) into Eq. (36.3) and simplifying, we can obtain

$$(\Delta^{q^2+q+1}+\Delta^{q^2+q}+1)(x^{q^2}+x^q+1)=0.$$

According to the condition that $X^{q^2+q+1}+X+1$ has no roots in $\mathbb{F}_{2^m}$, we know that $\Delta^{q^2+q+1}+\Delta^{q^2+q}+1\neq 0$ and thus $x^{q^2}+x^q+1=0$, which implies a contradiction since $\mathrm{Tr}_m(x^{q^2}+x^q)=0$ but $\mathrm{Tr}_m(1)=1$. Therefore Eqs. (27) have no solutions in this subcase either.

Subcase (II.3): $b \neq 0, c = 0$. In this subcase, Eqs. (27) become

$$\begin{cases} ax^q + a^q x + bz^q + a^q z = a^{q+1}, & (38.1) \\ by^q + b^q y + a^q z = b^{q+1}, & (38.2) \\ b^q x + ay^q + b^q z = ab^q. & (38.3) \end{cases}$$

After replacing x, y, z by ax, by, az, respectively, we get

$$\begin{cases} x^q + x + \Delta z^q + z + 1 = 0, & (39.1) \\ \Delta^{q+1} y^q + \Delta^{q+1} y + z + \Delta^{q+1} = 0, & (39.2) \\ x + y^q + z + 1 = 0, & (39.3) \end{cases}$$

where $\Delta = \frac{b}{a}$. From Eq. (39.2), we have $z = \Delta^{q+1}(y^q + y + 1)$. Summing Eqs. (39.2) and (39.3), we get

$$x = (1 + \Delta^{q+1})y^q + \Delta^{q+1} y + \Delta^{q+1} + 1. \tag{40}$$

Plugging Eq. (40) and $z = \Delta^{q+1}(y^q + y + 1)$ into Eq. (39.1), we can obtain

$$(\Delta^{q^2+q+1} + \Delta^{q^2+q} + 1)(y^{q^2} + y^q + 1) = 0.$$

Similarly to the proof of Subcase (II.2), we can conclude that Eqs. (27) have no solutions in this subcase.

Subcase (II.4): $bc \neq 0$. After replacing x, y, z by ax, by, cz, respectively in Eqs. (27) and simplifying, we have

$$\begin{cases} (a^{q+1} + a^q c)x^q + a^{q+1} x + bc^q y + bc^q z^q + a^q cz = a^{q+1} + a^q c + bc^q, & (41.1) \\ a^q cx^q + b^{q+1} y^q + b^{q+1} y + a^q cz = a^q c + b^{q+1}, & (41.2) \\ ab^q x + (ab^q + b^q c)y^q + c^{q+1} z^q + (b^q c + c^{q+1})z = ab^q + b^q c + c^{q+1}. & (41.3) \end{cases}$$

By Eq. (41.2), we have

$$z = x^q + \frac{b^{q+1}}{a^q c} y^q + \frac{b^{q+1}}{a^q c} y + \frac{b^{q+1}}{a^q c} + 1. \tag{42}$$

After plugging Eq. (42) into Eq. (41.1) and multiplying it by a^{q^2}, we obtain

$$\begin{aligned} &a^{q^2} bc^q x^{q^2} + a^{q^2+q+1} x^q + a^{q^2+q+1} x + b^{q^2+q+1} y^{q^2} + b^{q+1}(a^{q^2} + b^{q^2})y^q + \\ &a^{q^2} b(b^q + c^q)y + a^{q^2+q+1} + a^{q^2} b^{q+1} + b^{q^2+q+1} = 0. \end{aligned} \tag{43}$$

Next, we plug Eq. (42) into Eq. (41.3), multiply it by a^{q^2+q}, and get

$$\begin{aligned} &a^{q^2+q} c^{q+1} x^{q^2} + a^{q^2+q} c(b^q + c^q)x^q + a^{q^2+q+1} b^q x + a^q b^{q^2+q} c y^{q^2} + b^q(a^{q^2+q+1} + a^{q^2+q} c + a^q b^{q^2} c + a^{q^2} b^{q+1} + \\ &a^{q^2} bc^q)y^q + a^{q^2} b^{q+1}(b^q + c^q)y + a^{q^2+q+1} b^q + a^{q^2+q} c^{q+1} + a^{q^2} b^{2q+1} + a^{q^2} b^{q+1} c^q + a^q b^{q^2+q} c = 0. \end{aligned} \tag{44}$$

Summing the left-hand side of Eq. (43) multiplied by $a^q c$ and that of Eq. (44) multiplied by b, and dividing by a^{q^2}, we get

$$a^qc(a^{q+1}+b^{q+1}+bc^q)x^q+a^{q+1}(a^qc+b^{q+1})x+b^{q+1}(a^{q+1}+b^{q+1}+bc^q)y^q+ \\ (a^qc+b^{q+1})(b^{q+1}+bc^q)y+(a^qc+b^{q+1})(a^{q+1}+b^{q+1}+bc^q)=0. \quad (45)$$

Raising Eq. (45) into its q-th power, we have

$$a^{q^2}c^q(a^{q^2+q}+b^{q^2+q}+b^qc^{q^2})x^{q^2}+a^{q^2+q}(a^{q^2}c^q+b^{q^2+q})x^q+b^{q^2+q}(a^{q^2+q}+b^{q^2+q}+b^qc^{q^2})y^{q^2}+ \\ (a^{q^2}c^q+b^{q^2+q})(b^{q^2+q}+b^qc^{q^2})y^q+(a^{q^2}c^q+b^{q^2+q})(a^{q^2+q}+b^{q^2+q}+b^qc^{q^2})=0. \quad (46)$$

Summing the left-hand side of Eq. (46) multiplied by b and that of Eq. (43) multiplied by $a^{q^2+q}+b^{q^2+q}+b^qc^{q^2}$, and dividing by a^{q^2}, we obtain

$$a^q(a^{q^2+q+1}+ab^{q^2+q}+ab^qc^{q^2}+a^{q^2}bc^q+b^{q^2+q+1})x^q+a^{q+1}(a^{q^2+q}+b^{q^2+q}+b^qc^{q^2})x+ \\ b^{q+1}(a^{q^2+q}+a^qb^{q^2}+b^{q^2+q}+b^qc^{q^2}+b^{q^2}c^q+c^{q^2+q})y^q+b(b^q+c^q)(a^{q^2+q}+b^{q^2+q}+b^qc^{q^2})y+ \\ (a^{q^2+q}+b^{q^2+q}+b^qc^{q^2})(a^{q+1}+b^{q+1}+bc^q)=0. \quad (47)$$

Summing the left-hand side of Eq. (46) multiplied by a^qc and that of Eq. (44) multiplied by $a^{q^2+q}+b^{q^2+q}+b^qc^{q^2}$, and dividing by $a^{q^2}b^q$, we obtain

$$a^qc(a^{q^2+q}+a^qb^{q^2}+b^{q^2+q}+b^qc^{q^2}+b^{q^2}c^q+c^{q^2+q})x^q+a^{q+1}(a^{q^2+q}+b^{q^2+q}+b^qc^{q^2})x+ \\ Sy^q+b(b^q+c^q)(a^{q^2+q}+b^{q^2+q}+b^qc^{q^2})y+(a^{q^2+q}+b^{q^2+q}+b^qc^{q^2})(a^{q+1}+b^{q+1}+bc^q)=0, (48)$$

where

$$\begin{aligned} S &= a^{q^2+2q+1}+a^{q+1}b^{q^2+q}+a^{q+1}b^qc^{q^2}+a^{q^2+2q}c+a^{2q}b^{q^2}c+a^{q^2+q}b^{q+1}+a^{q^2+q}bc^q+a^qb^{q^2+q}c+ \\ &\quad a^qb^qc^{q^2+1}+a^qb^{q^2}c^{q+1}+a^qc^{q^2+q+1}+b^{q^2+2q+1}+b^{2q+1}c^{q^2}+b^{q^2+q+1}c^q+b^{q+1}c^{q^2+q}. \end{aligned}$$

Summing Eqs. (47) and (48), we get

$$a^qT(x^q+y^q)=0, \quad (49)$$

where

$$T=a^{q^2+q+1}+ab^{q^2+q}+ab^qc^{q^2}+a^{q^2+q}c+a^qb^{q^2}c+a^{q^2}bc^q+b^{q^2+q+1}+b^{q^2+q}c+b^qc^{q^2+1}+b^{q^2}c^{q+1}+c^{q^2+q+1}.$$

Similarly to the proof of Theorem 1, we have $T\neq 0$ due to the condition that the polynomial

$$X^{q^2+q+1}+XY^{q^2+q}+XY^q+X^{q^2+q}+X^qY^{q^2}+X^{q^2}Y+Y^{q^2+q+1}+Y^{q^2+q}+Y^{q^2}+Y^q+1$$

has no roots in $\mathbb{F}_{2^m}^2$. Therefore by Eq. (49), we see that we must have $x=y$. Now we plug $x=y$ into Eq. (45) and get

$$(a^qc+b^{q+1})(a^{q+1}+b^{q+1}+bc^q)(x^q+x+1)=0. \quad (50)$$

If $a^qc + b^{q+1} = 0$, plugging $c = \frac{b^{q+1}}{a^q}$ and $x = y$ into Eq. (43), we obtain

$$a^{q^2+q+1}x^q + a^{q^2+q+1}x + (a^{q^2}b^{q+1} + b^{q^2+q+1})x^q + (a^{q^2}b^{q+1} + b^{q^2+q+1})x + a^{q^2+q+1} + a^{q^2}b^{q+1} + b^{q^2+q+1} = 0,$$

i.e.,

$$(a^{q^2+q+1} + a^{q^2}b^{q+1} + b^{q^2+q+1})(x^q + x + 1) = 0.$$

Since $a^{q^2+q+1} + a^{q^2}b^{q+1} + b^{q^2+q+1} \neq 0$ thanks to the condition that $X^{q^2+q+1} + X^{q^2} + 1$ has no roots in $\mathbb{F}_{2^m}$, we have $x^q + x + 1 = 0$, which has no solutions in $\mathbb{F}_{2^m}$ since m is odd. Thus $a^qc + b^{q+1} \neq 0$.

If $a^{q+1} + b^{q+1} + bc^q = 0$, plugging $bc^q = a^{q+1} + b^{q+1}$ and $x = y$ into Eq. (43), we can get

$$(a^{q^2+q+1} + a^{q^2}b^{q+1} + b^{q^2+q+1})(x^{q^2} + x^q + 1) = 0.$$

It is clear that we have $x^{q^2} + x^q + 1 = 0$, which has no solutions in $\mathbb{F}_{2^m}$, either. Thus $a^{q+1} + b^{q+1} + bc^q \neq 0$.

Therefore, Eq. (50) implies $x^q + x + 1 = 0$ which once again leads to contradiction.

We have thus shown that Eqs. (27) have no solutions in $\mathbb{F}_{2^m}^3$, and thus F is a permutation as claimed. □

The APN-ness and bijectivity of the functions described above depends on several polynomials not having roots. In the following proposition, we use Theorems 1 and 2 to give a direct construction of APN functions over $\mathbb{F}_{2^{3m}}$ which are bijective for odd values of m.

Proposition 3. *Let* $\gcd(m, 7) = 1$,

$$F(x, y, z) = \left(x^3 + x^2z + yz^2, x^2z + y^3, xy^2 + y^2z + z^3\right).$$

Then F is APN over $\mathbb{F}_{2^m}^3$. In particular, when m is odd, F is AB and is also a permutation over $\mathbb{F}_{2^m}^3$.

Proof. In Theorem 1, let $q = 2$. Then it can be easily verified that $X^{q^2+q+1} + X + 1 = X^7 + X + 1$, $X^{q^2+q+1} + X^{q^2} + 1 = X^7 + X^4 + 1$ and $X^{q^2+q+1} + X^{q^2+1} + X^{q+1} + X + 1 = X^7 + X^5 + X^3 + X + 1$ are irreducible over $\mathbb{F}_2$. Since $\gcd(m, 7) = 1$, the polynomials $X^7 + X + 1$, $X^7 + X^4 + 1$, $X^7 + X^5 + X^3 + X + 1$ are also irreducible over $\mathbb{F}_{2^m}$ and then clearly have no roots in $\mathbb{F}_{2^m}$.

Now it suffices to show that the polynomial

$$\begin{aligned} f(X,Y) &= X^{q^2+q+1} + XY^{q^2+q} + XY^q + X^{q^2+q} + X^qY^{q^2} + X^{q^2}Y + Y^{q^2+q+1} + Y^{q^2+q} + Y^{q^2} + Y^q + 1 \\ &= X^7 + XY^6 + XY^2 + X^6 + X^2Y^4 + X^4Y + Y^7 + Y^6 + Y^4 + Y^2 + 1 \end{aligned}$$

has no roots in $\mathbb{F}_{2^m}^2$ when $\gcd(m, 7) = 1$. Let ω be a primitive element of $\mathbb{F}_{2^7}$. Then it is easy to check that

$$f(X, Y) = \prod_{i=0}^{6}(X + \omega^{2^i}Y + \omega^{63\cdot 2^i}).$$

Thus, if $f(X, Y)$ has a root (x_0, y_0) in $\mathbb{F}_{2^m}^2$, then there must exist some $0 \le i \le 6$ such that $x_0 + \omega^{2^i}y_0 + \omega^{63\cdot 2^i} = 0$. Hence x_0 or y_0 is in $\mathbb{F}_{2^7}$ and then $\mathbb{F}_{2^7} \subseteq \mathbb{F}_{2^m}$, which contradicts $\gcd(m, 7) = 1$.

The permutation property of F is directly from Theorem 2. □

Remark 4. *In the case of even dimensions, it is easy to see that the functions from Theorem 1 are 3-to-1. Indeed, if $n = 3m$ is even, then m bust be even as well, and the condition $\gcd(i, m) = 1$ implies that i must be odd. Then $q + 1 = 2^m + 1$ is divisible by 3. We can readily verify that the (multivariate) degree of all terms in the trivariate expression of $F(x, y, z)$ from Theorem 1 is precisely $q + 1$. Therefore, denoting by ω a primitive element of $\mathbb{F}_4$, we have $F(\omega^i x, \omega^i y, \omega^i z) = F(x, y, z)$ for any $i \in \{0, 1, 2\}$. Consequently, the exponents of the univariate representation of F must be multiples of 3, and by [19], F is 3-to-1.*

This has two immediate but important consequences. As shown in [19], we can see that in the case of even dimensions, F has a Gold-like Walsh spectrum. On the other hand, as proven in [14], in the case of doubly even n, we know that F cannot be CCZ-equivalent to a permutation.

We computationally verify that the Walsh spectrum is also Gold-like for $n = 9$. We observe that F is CCZ-equivalent to the Gold function x^3 for $n = 6$, and so it cannot be CCZ-equivalent to a permutation. We leave the computation of the Walsh spectrum of the family from Theorem 1 and the question of whether it can be CCZ-equivalent to a permutation over singly-even dimensions as problems for future work.

4. Another infinite family of APN functions over $\mathbb{F}_{2^m}^3$

In this section, we introduce a second family of APN functions over $\mathbb{F}_{2^{3m}}$. Once again, we express this family using the trivariate representation. In Theorem 5 we show that the family consists of APN functions, while in Theorem 6 we show that the functions are permutations over odd dimensions.

Theorem 5. *Let $\gcd(i, m) = 1$, $q = 2^i$ and*

$$F(x, y, z) = \left(x^{q+1} + xy^q + yz^q, xy^q + z^{q+1}, x^q z + y^{q+1} + y^q z\right).$$

Assume that the polynomials $X^{q^2+q+1} + X^{q+1} + X^q + X + 1$, $X^{q^2+q+1} + X^{q^2} + 1$, $X^{q^2+q+1} + X + 1$ have no roots in $\mathbb{F}_{2^m}$, and the polynomial

$$X^{q^2+q+1} + X^{q+1}Y^{q^2} + XY^q + X^q Y^{q^2} + X^{q^2} Y + X^{q^2} + Y^{q^2+q+1} + Y^{q^2+1} + Y^{q^2+q} + Y^{q^2} + 1$$

has no roots in $\mathbb{F}_{2^m}^2$. Then F is APN over $\mathbb{F}_{2^m}^3$.

Proof. Since F is quadratic and $F(0, 0, 0) = (0, 0, 0)$, it suffices to show that the equation

$$F(x + a, y + b, z + c) + F(x, y, z) + F(a, b, c) = (0, 0, 0) \tag{51}$$

has exactly two solutions in $\mathbb{F}_{2^m}^3$ for any $(a, b, c) \in \mathbb{F}_{2^m}^3 \backslash \{(0, 0, 0)\}$. By simplifying, Eq. (51) is equivalent to the following equation system:

$$\begin{cases} ax^q + (a^q + b^q)x + ay^q + c^q y + bz^q = 0, & (52.1) \\ b^q x + ay^q + cz^q + c^q z = 0, & (52.2) \\ cx^q + (b + c)y^q + b^q y + (a^q + b^q)z = 0. & (52.3) \end{cases}$$

Now we divide the proof into several cases and subcases depending on whether the elements a, b, c are zero or non-zero.

Case (I): $a = 0$**.** In this case, Eqs. (52) become

$$\begin{cases} b^q x + c^q y + b z^q = 0, & (53.1) \\ b^q x + c z^q + c^q z = 0, & (53.2) \\ c x^q + (b+c) y^q + b^q y + b^q z = 0. & (53.3) \end{cases}$$

Subcase (I.1): $b = 0, c \neq 0$. In this subcase, by Eqs. (53), we get $c^q y = 0$, $cz^q + c^q z = 0$ and $cx^q + cy^q = 0$, respectively. Thus $x = y = 0$ and $z \in \{0, c\}$. In other words, Eqs. (52) have exactly two solutions $(x, y, z) \in \{(0,0,0), (0,0,c)\}$ in this subcase.

Subcase (I.2): $b \neq 0, c = 0$. In this subcase, by Eqs. (53), we have $b^q x + bz^q = 0$, $b^q x = 0$ and $by^q + b^q y + b^q z = 0$, respectively. It is easy to get $x = z = 0$ and $y \in \{0, b\}$. Thus Eqs. (52) have exactly two solutions $(x, y, z) \in \{(0,0,0), (0,b,0)\}$ in this subcase.

Subcase (I.3): $bc \neq 0$. In this subcase, we replace x, y, z by bx, by, cz, respectively in Eqs. (53), simplify, and obtain

$$\begin{cases} x + \Delta^q y + \Delta^q z^q = 0, & (54.1) \\ x + \Delta^{q+1} z^q + \Delta^{q+1} z = 0, & (54.2) \\ \Delta x^q + (1+\Delta) y^q + y + \Delta z = 0, & (54.3) \end{cases}$$

where $\Delta = \frac{c}{b}$. Adding Eq. (54.1) and Eq. (54.2) and dividing by Δ^q, we get

$$y = (1+\Delta) z^q + \Delta z. \tag{55}$$

Summing the q-th power of Eq. (54.1) multiplied by Δ with Eq. (54.3), we obtain

$$(\Delta^{q^2+1} + \Delta + 1) y^q + y + \Delta^{q^2+1} z^{q^2} + \Delta z = 0. \tag{56}$$

We now compute the summation of the q-th power of Eq. (55) multiplied by $\Delta^{q^2+1} + \Delta + 1$, Eq. (55) and Eq. (56), and obtain

$$(\Delta^{q^2+q+1} + \Delta^{q+1} + \Delta^q + \Delta + 1)(z^{q^2} + z^q) = 0.$$

Since $\Delta^{q^2+q+1} + \Delta^{q+1} + \Delta^q + \Delta + 1 \neq 0$ according to the condition, we have $z^{q^2} + z^q = 0$, i.e., $z \in \{0, 1\}$. Then we can see that Eqs. (52) have exactly two solutions in this subcase.

Case (II): $a \neq 0$**.**

Subcase (II.1): $b = c = 0$. From Eqs. (52), we get $ax^q + a^q x + ay^q = 0, ay^q = 0, a^q z = 0$, respectively. Then it is trivial that $x \in \{0, a\}, y = z = 0$. Consequently, Eqs. (52) have exactly two solutions $(x, y, z) \in \{(0,0,0), (a,0,0)\}$ in this subcase.

Subcase (II.2): $b = 0, c \neq 0$. In this subcase, Eqs. (52) become

$$\begin{cases} ax^q + a^q x + ay^q + c^q y = 0, & (57.1) \\ ay^q + cz^q + c^q z = 0, & (57.2) \\ cx^q + cy^q + a^q z = 0. & (57.3) \end{cases}$$

We replace x, y, z by ax, ay, cz, respectively in Eqs. (57), simplify, and get

$$\begin{cases} x^q + x + y^q + \Delta^q y = 0, & (58.1) \\ y^q + \Delta^{q+1}(z^q + z) = 0, & (58.2) \\ x^q + y^q + z = 0, & (58.3) \end{cases}$$

where $\Delta = c/a$. From Eq. (58.3), we get $z = x^q + y^q$ and thus

$$z^q + z = x^{q^2} + x^q + y^{q^2} + y^q = (\Delta^{q^2} + 1)y^q, \tag{59}$$

where the second equality is due to Eq. (58.1). Plugging Eq. (59) into Eq. (58.2), we obtain

$$(\Delta^{q^2+q+1} + \Delta^{q+1} + 1)y^q = 0.$$

According to the condition that the polynomial $X^{q^2+q+1} + X^{q^2} + 1$ has no roots in $\mathbb{F}_{2^m}$, we know that $\Delta^{q^2+q+1} + \Delta^{q+1} + 1 \neq 0$ and then $y = 0$. Moreover, from Eq. (58.1) and Eq. (58.3), we have $x^q + x = 0$ and $z = x^q$, respectively. Thus $x \in \{0, 1\}$ and then Eqs. (52) have exactly two solutions in this subcase.

Subcase (II.3): $b \neq 0, c = 0$. In this subcase, Eqs. (52) become

$$\begin{cases} ax^q + (a^q + b^q)x + ay^q + bz^q = 0, & (60.1) \\ b^q x + ay^q = 0, & (60.2) \\ by^q + b^q y + (a^q + b^q)z = 0. & (60.3) \end{cases}$$

Replacing x, y, z by ax, by, bz in Eqs. (60) and simplifying, we get

$$\begin{cases} \Delta^{q+1}x^q + (\Delta^{q+1} + \Delta)x + \Delta y^q + z^q = 0, & (61.1) \\ x + y^q = 0, & (61.2) \\ y^q + y + (\Delta^q + 1)z = 0, & (61.3) \end{cases}$$

where $\Delta = \frac{a}{b}$. From Eq. (61.2), we have $x = y^q$. Plugging it into Eq. (61.1) and simplifying, we obtain $z^q = \Delta^{q+1}y^{q^2} + \Delta^{q+1}y^q$. Raising Eq. (61.3) into its q-th power and plugging $z^q = \Delta^{q+1}y^{q^2} + \Delta^{q+1}y^q$ into it, we acquire

$$(\Delta^{q^2+q+1} + \Delta^{q+1} + 1)(y^{q^2} + y^q) = 0.$$

Again, $\Delta^{q^2+q+1} + \Delta^{q+1} + 1 \neq 0$ according to the hypothesis. Thus $y^{q^2} + y^q = 0$, i.e., $y \in \{0, 1\}$ and then

$z=0$. In particular, Eqs. (52) have exactly two solutions in this subcase.

Subcase (II.4): $bc \neq 0$. In this subcase, we replace x, y, z by ax, by, cz, respectively in Eqs. (52) and get

$$\begin{cases} a^{q+1}x^q + (a^{q+1}+ab^q)x + ab^q y^q + bc^q y + bc^q z^q = 0, & (62.1) \\ ab^q x + ab^q y^q + c^{q+1}z^q + c^{q+1}z = 0, & (62.2) \\ a^q c x^q + (b^{q+1}+b^q c)y^q + b^{q+1}y + (a^q c + b^q c)z = 0. & (62.3) \end{cases}$$

By Eq. (62.2), we have

$$x = y^q + \frac{c^{q+1}}{ab^q}z^q + \frac{c^{q+1}}{ab^q}z. \tag{63}$$

After plugging Eq. (63) into Eq. (62.1) and multiplying it by b^{q^2+q}, we obtain

$$\begin{aligned} &a^{q+1}b^{q^2+q}y^{q^2} + a^{q+1}b^{q^2+q}y^q + b^{q^2+q+1}c^q y + ab^q c^{q^2+q}z^{q^2} + (ab^q c^{q^2+q} + b^{q^2+q}c^{q+1} + \\ &a^q b^{q^2}c^{q+1} + b^{q^2+q+1}c^q)z^q + (a^q b^{q^2}c^{q+1} + b^{q^2+q}c^{q+1})z = 0. \end{aligned} \tag{64}$$

Further, we plug Eq. (63) into Eq. (62.3) and multiply it by b^{q^2}, obtaining

$$a^q b^{q^2} c y^{q^2} + (b^{q^2+q+1} + b^{q^2+q}c)y^q + b^{q^2+q+1}y + c^{q^2+q+1}z^{q^2} + c^{q^2+q+1}z^q + (a^q b^{q^2}c + b^{q^2+q}c)z = 0. \tag{65}$$

After summing the left-hand part of Eq. (64) multiplied by c with that of Eq. (65) multiplied by ab^q, and dividing by b^{q^2}, we get

$$\begin{aligned} &ab^q(a^q c + b^{q+1} + b^q c)y^q + b^{q+1}(ab^q + c^{q+1})y + c^{q+1}(a^q c + b^{q+1} + b^q c)z^q + \\ &c(a^q + b^q)(ab^q + c^{q+1})z = 0. \end{aligned} \tag{66}$$

Raising Eq. (66) into its q-th power, we get

$$\begin{aligned} &a^q b^{q^2}(a^{q^2}c^q + b^{q^2+q} + b^{q^2}c^q)y^{q^2} + b^{q^2+q}(a^q b^{q^2} + c^{q^2+q})y^q + c^{q^2+q}(a^{q^2}c^q + b^{q^2+q} + b^{q^2}c^q)z^{q^2} + \\ &c^q(a^{q^2} + b^{q^2})(a^q b^{q^2} + c^{q^2+q})z^q = 0. \end{aligned} \tag{67}$$

After summing the left-hand side of Eq. (64) multiplied by $a^{q^2}c^q + b^{q^2+q} + b^{q^2}c^q$ with that of Eq. (67) multiplied by ab^q and dividing by $b^{q^2}c^q$, we obtain

$$\begin{aligned} &ab^q(a^{q^2+q} + a^q b^{q^2} + b^q c^{q^2})y^q + b^{q+1}(a^{q^2}c^q + b^{q^2+q} + b^{q^2}c^q)y + \\ &Sz^q + c(a^q + b^q)(a^{q^2}c^q + b^{q^2+q} + b^{q^2}c^q)z = 0, \end{aligned} \tag{68}$$

where

$$\begin{aligned} S \;=\; &a^{q^2+q+1}b^q + a^{q+1}b^{q^2+q} + ab^{2q}c^{q^2} + a^{q^2+q}c^{q+1} + a^q b^{q^2+q}c + a^q b^{q^2}c^{q+1} + a^{q^2}b^{q+1}c^q + \\ &a^{q^2}b^q c^{q+1} + b^{q^2+2q+1} + b^{q^2+q+1}c^q + b^{q^2+2q}c + b^{q^2+q}c^{q+1}. \end{aligned}$$

Further, summing the left-hand side of Eq. (65) multiplied by $a^{q^2}c^q + b^{q^2+q} + b^{q^2}c^q$ with that of Eq. (67) multiplied by c and dividing by b^{q^2}, we obtain

$$b^q(a^qb^{q^2}c + a^{q^2}bc^q + a^{q^2}c^{q+1} + b^{q^2+q+1} + b^{q^2+1}c^q + b^{q^2+q}c + b^{q^2}c^{q+1} + c^{q^2+q+1})y^q + b^{q+1}(a^{q^2}c^q + b^{q^2+q} + b^{q^2}c^q)y + c^{q+1}(a^{q^2+q} + a^qb^{q^2} + b^qc^{q^2})z^q + c(a^q + b^q)(a^{q^2}c^q + b^{q^2+q} + b^{q^2}c^q)z = 0. \qquad (69)$$

Now we sum Eqs. (68) and (69), and get

$$b^qT(y^q + z^q) = 0, \qquad (70)$$

where

$$T = a^{q^2+q+1} + a^{q+1}b^{q^2} + ab^qc^{q^2} + a^qb^{q^2}c + a^{q^2}bc^q + a^{q^2}c^{q+1} + b^{q^2+q+1} + b^{q^2+1}c^q + b^{q^2+q}c + b^{q^2}c^{q+1} + c^{q^2+q+1}.$$

If $T = 0$, let $A = \frac{a}{c}$ and $B = \frac{b}{c}$. Then we have

$$\frac{T}{c^{q^2+q+1}} = A^{q^2+q+1} + A^{q+1}B^{q^2} + AB^q + A^qB^{q^2} + A^{q^2}B + A^{q^2} + B^{q^2+q+1} + B^{q^2+1} + B^{q^2+q} + B^{q^2} + 1 = 0,$$

which contradicts the condition that the polynomial

$$X^{q^2+q+1} + X^{q+1}Y^{q^2} + XY^q + X^qY^{q^2} + X^{q^2}Y + X^{q^2} + Y^{q^2+q+1} + Y^{q^2+1} + Y^{q^2+q} + Y^{q^2} + 1$$

has no roots in $\mathbb{F}_{2^m}^2$. Thus $T \neq 0$ and then $y = z$ by Eq. (70). Furthermore, plugging $y = z$ into Eq. (66) yields

$$(ab^q + c^{q+1})(a^qc + b^{q+1} + b^qc)(y^q + y) = 0. \qquad (71)$$

If $ab^q + c^{q+1} = 0$, after plugging $ab^q = c^{q+1}$ and $y = z$ into Eq. (65), we have

$$(b^{q^2+q+1} + b^{q^2+q}c + c^{q^2+q+1})(y^q + y) = 0.$$

Since $b^{q^2+q+1} + b^{q^2+q}c + c^{q^2+q+1} \neq 0$ due to the condition that $X^{q^2+q+1} + X + 1$ has no roots in $\mathbb{F}_{2^m}$, we can see that $y^q + y = 0$, i.e., $y \in \{0, 1\}$. Together with $z = y$ and Eq. (63), we know that Eqs. (52) have exactly two solutions when $ab^q + c^{q+1} = 0$.

If $a^qc + b^{q+1} + b^qc = 0$, after plugging $a^qc = b^{q+1} + b^qc$ and $y = z$ into Eq. (65), we get

$$(b^{q^2+q+1} + b^{q^2+q}c + c^{q^2+q+1})(y^{q^2} + y^q) = 0.$$

We thus have $y^{q^2} + y^q = 0$, i.e., $y \in \{0, 1\}$, and Eqs. (52) have exactly two solutions when $a^qc + b^{q+1} + b^qc = 0$.

If $(ab^q + c^{q+1})(a^qc + b^{q+1} + b^qc) \neq 0$, then by Eq. (71), we can see that $y^q + y = 0$, i.e., $y \in \{0, 1\}$. Thus Eqs. (52) have exactly two solutions in this case as well.

We thus see that $F(x + a, y + b, z + c) + F(x, y, z) + F(a, b, c) = (0, 0, 0)$ has at most two solutions in all cases, and therefore F is APN as claimed. □

As mentioned previously, the functions from Theorem 5 are permutations over fields of odd degree. We formalize this in the following theorem.

Theorem 6. *Let* $\gcd(i, m) = 1$*,* m *be odd,* $q = 2^i$ *and*

$$F(x, y, z) = \left(x^{q+1} + xy^q + yz^q, xy^q + z^{q+1}, x^q z + y^{q+1} + y^q z\right).$$

Assume that the polynomials $X^{q^2+q+1} + X^{q+1} + X^q + X + 1$*,* $X^{q^2+q+1} + X^{q^2} + 1$*,* $X^{q^2+q+1} + X + 1$ *have no roots in* $\mathbb{F}_{2^m}$*, and the polynomial*

$$X^{q^2+q+1} + X^{q+1}Y^{q^2} + XY^q + X^qY^{q^2} + X^{q^2}Y + X^{q^2} + Y^{q^2+q+1} + Y^{q^2+1} + Y^{q^2+q} + Y^{q^2} + 1$$

has no roots in $\mathbb{F}_{2^m}^2$*, then* F *is a permutation over* $\mathbb{F}_{2^m}^3$*.*

Proof. It suffices to show that the equation

$$F(x + a, y + b, z + c) + F(x, y, z) = (0, 0, 0) \tag{72}$$

has no solutions in $\mathbb{F}_{2^m}^3$ for any $(a, b, c) \in \mathbb{F}_{2^m}^3 \backslash \{(0, 0, 0)\}$. By simplifying, Eq. (72) is equivalent to the following equation system:

$$\begin{cases} ax^q + (a^q + b^q)x + ay^q + c^q y + bz^q = a^{q+1} + ab^q + bc^q, & (73.1) \\ b^q x + ay^q + cz^q + c^q z = ab^q + c^{q+1}, & (73.2) \\ cx^q + (b + c)y^q + b^q y + (a^q + b^q)z = a^q c + b^{q+1} + b^q c. & (73.3) \end{cases}$$

The proof is similar to that of Theorem 5 and we omit it here. □

As in the previous section, we now use Theorems 5 and 6 to give a direct construction of APN functions over $\mathbb{F}_{2^{3m}}$.

Proposition 7. *Let* $\gcd(m, 7) = 1$*,*

$$F(x, y, z) = \left(x^3 + xy^2 + yz^2, xy^2 + z^3, x^2 z + y^3 + y^2 z\right).$$

Then F *is APN over* $\mathbb{F}_{2^m}^3$*. In particular,* F *is AB and is also a permutation over* $\mathbb{F}_{2^m}^3$ *when* m *is odd.*

Proof. In Theorem 5, let $q = 2$. Then it is clear that $X^{q^2+q+1} + X + 1 = X^7 + X + 1$, $X^{q^2+q+1} + X^{q^2} + 1 = X^7 + X^4 + 1$ and $X^{q^2+q+1} + X^{q^2+1} + X^{q+1} + X + 1 = X^7 + X^5 + X^3 + X + 1$ are irreducible over $\mathbb{F}_2$. Since $\gcd(m, 7) = 1$, the polynomials $X^7 + X + 1$, $X^7 + X^4 + 1$, $X^7 + X^5 + X^3 + X + 1$ are also irreducible over $\mathbb{F}_{2^m}$ and then clearly have no roots in $\mathbb{F}_{2^m}$.

Let ω be a primitive element of $\mathbb{F}_{2^7}$. Then it is easy to check that

$$\begin{aligned} & X^{q^2+q+1} + X^{q+1}Y^{q^2} + XY^q + X^qY^{q^2} + X^{q^2}Y + X^{q^2} + Y^{q^2+q+1} + Y^{q^2+1} + Y^{q^2+q} + Y^{q^2} + 1 \\ = \ & X^7 + X^3Y^4 + XY^2 + X^2Y^4 + X^4Y + X^4 + Y^7 + Y^5 + Y^6 + Y^4 + 1 \\ = \ & \prod_{i=0}^{6}(X + \omega^{11\cdot 2^i}Y + \omega^{58\cdot 2^i}). \end{aligned}$$

Thus, if $f(X,Y)$ has a root (x_0, y_0) in $\mathbb{F}_{2^m}^2$, then there must exist some $0 \leq i \leq 6$ such that $x_0 + \omega^{11\cdot 2^i} y_0 + \omega^{58\cdot 2^i} = 0$. Hence x_0 or y_0 is in $\mathbb{F}_{2^7}$ and then $\mathbb{F}_{2^7} \subseteq \mathbb{F}_{2^m}$, which contradicts $\gcd(m,7) = 1$.

The permutation property of F then follows immediately from Theorem 6. □

Remark 8. *We can make similar observations to those in Remark 4. More precisely, it is easy to observe that the functions from Theorem 5 are 3-to-1, and so have a Gold-like Walsh spectrum for even dimensions, and cannot be CCZ-equivalence to permutations for doubly-even dimensions. We also computationally verify that these functions have a Gold-like Walsh spectrum for odd dimensions, and that for* $n = 6$ *they are equivalent to* x^3 *and thus cannot be CCZ-equivalent to a permutation. We leave the computation of the Walsh spectrum for odd dimensions and that of their potential CCZ-equivalent to permutations as problems for future work.*

5. CCZ-Inequivalence to the known families

It remains to show that the functions arising from Theorems 1 and 5 are CCZ-inequivalent to representatives from the known infinite families. We recall that two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent [34], and so it suffices to consider EA-equivalence. In the case of quadratic APN functions, the most efficient and convenient way to show inequivalence is via the differential spectrum and the Walsh spectrum of their associated orthoderivatives [17].

In Table IV, we list the differential spectra of the orthoderivatives of all functions from the known infinite families in Tables I and II. We note that since 9 is odd, none of the functions from Table III are defined over this dimension. Similarly, families F1-F2, F7-F9, F11, and F12 are not defined for dimension 9. Out of the monomial functions in Table I, only the Gold functions are relevant, since the remaining families consist of functions of algebraic degree greater than 2.

We now proceed to compute the differential spectra of the orthoderivatives of the functions from Theorems 1 and 5. The function from Theorem 1 for $n = 9$ is

$$F_1(x,y,z) = (x^3 + x^2z + yz^2, x^2z + y^3, xy^2 + y^2z + z^3),$$

or

$$F_1(x) = \alpha^{373}x^{192} + \alpha^{492}x^{136} + \alpha^{414}x^{129} + \alpha^{98}x^{80} + \alpha^{503}x^{66} + \alpha^{488}x^{24} + \alpha^{464}x^{17} + \alpha^{405}x^{10} + \alpha^{428}x^3$$

in univariate form (where α is a primitive element of $\mathbb{F}_{2^9}$), and its orthoderivative has the differential spectrum

$$0 \times 164199, 2 \times 76734, 4 \times 13524, 6 \times 4312, 8 \times 2205, 12 \times 147, 16 \times 294, 18 \times 147, 20 \times 49, 22 \times 21.$$

TABLE IV

Orthoderivative differential spectra of all previously known quadratic APN functions over $\mathbb{F}_{2^9}$

Family	Orthoderivative differential spectra
Gold	0 × 153811, 2 × 96579, 6 × 10731, 8 × 511 0 × 159943, 2 × 78183, 4 × 18396, 6 × 4599, 8 × 511
F4	0 × 159016, 2 × 79389, 4 × 19089, 6 × 3483, 8 × 493, 10 × 144, 12 × 18
F5	0 × 159226, 2 × 78813, 4 × 19683, 6 × 3201, 8 × 529, 10 × 162, 12 × 18
F6	0 × 160525, 2 × 77058, 4 × 19467, 6 × 3792, 8 × 598, 10 × 126, 12 × 45, 14 × 12, 16 × 9
F10	0 × 160097, 2 × 79128, 4 × 17808, 6 × 3269, 8 × 700, 10 × 357, 12 × 231, 14 × 42
F13	0 × 168994, 2 × 68712, 4 × 15141, 6 × 6279, 8 × 1659, 10 × 336, 12 × 21, 14 × 21, 16 × 105, 18 × 147, 20 × 189, 24 × 21, 26 × 7 0 × 169022, 2 × 68341, 4 × 16093, 6 × 5621, 8 × 1561, 10 × 364, 12 × 91, 14 × 63, 16 × 140, 18 × 196, 20 × 84, 22 × 35, 24 × 7, 26 × 14 0 × 169428, 2 × 68040, 4 × 15561, 6 × 6034, 8 × 1533, 10 × 420, 12 × 126, 14 × 21, 16 × 84, 18 × 189, 20 × 126, 22 × 63, 26 × 7 0 × 169484, 2 × 68159, 4 × 15463, 6 × 5719, 8 × 1736, 10 × 420, 12 × 105, 14 × 63, 16 × 133, 18 × 175, 20 × 126, 22 × 28, 24 × 21 0 × 170079, 2 × 66297, 4 × 16737, 6 × 6160, 8 × 1407, 10 × 420, 12 × 21, 14 × 42, 16 × 63, 18 × 210, 20 × 133, 22 × 63, 0 × 170100, 2 × 67592, 4 × 15232, 6 × 5628, 8 × 1848, 10 × 553, 12 × 98, 14 × 98, 16 × 126, 18 × 189, 20 × 126, 22 × 28, 24 × 14 0 × 170667, 2 × 66297, 4 × 15911, 6 × 5705, 8 × 1974, 10 × 385, 12 × 140, 14 × 84, 16 × 168, 18 × 147, 20 × 63, 22 × 63, 24 × 21, 26 × 7 0 × 171430, 2 × 64617, 4 × 16842, 6 × 5733, 8 × 1932, 10 × 483, 12 × 105, 14 × 21, 16 × 147, 18 × 105, 20 × 154, 22 × 21, 24 × 42

The function from Theorem 5 for $n = 9$ is

$$F_2(x, y, z) = (x^3 + xy^2 + yz^2, xy^2 + z^3, x^2z + y^3 + y^2z),$$

or

$$F_2(x) = \alpha^{32}x^{192} + \alpha^{222}x^{136} + \alpha^{147}x^{129} + \alpha^{426}x^{80} + \alpha^{469}x^{66} + \alpha^{435}x^{24} + \alpha^{352}x^{17} + \alpha^{499}x^{10} + \alpha^{349}x^{3}$$

in univariate form (where α is a primitive element of $\mathbb{F}_{2^9}$), and its orthoderivative has the differential spectrum

$$0 \times 172557, 2 \times 68355, 4 \times 12201, 6 \times 3871, 8 \times 1638, 10 \times 735, 12 \times 1470, 14 \times 49,$$
$$16 \times 147, 18 \times 441, 20 \times 147, 42 \times 21.$$

One can easily verify that the above differential spectra do not appear among the ones given in Table IV, and therefore our construction produces APN functions inequivalent to the known ones in dimension 9.

While the functions do not intersect any of the known families, they are equivalent to sporadic instances documented in [3]. More precisely, the differential spectra of the orthoderivatives match those of representatives nos. 34, and 35 from the representatives listed in the dataset [4]. Using the linear code equivalence test [24], we can verify that our functions are, in fact, CCZ-equivalent to the representatives from [3]. We note that these are precisely the two instances that were observed to be bijective in [3].

6. Conclusion

We have described two new infinite families of APN functions over $\mathbb{F}_{2^{3m}}$ in trivariate form. We have shown that these functions are AB permutations whenever m is odd, and that they are 3-to-1 functions whenever m is even. We have computed the differential spectra of the orthoderivatives of these functions over $\mathbb{F}_{2^9}$, and have computationally verified that they are equivalent to the sporadic APN permutations of Beierle and Leander discovered in [3]; we have thus generalized these sporadic instances into infinite families.

References

[1] Daniele Bartoli and Marco Timpanella. On a conjecture on APN permutations. *Cryptography and Communications*, 14(4):925–931, 2022.

[2] Christof Beierle, Claude Carlet, Gregor Leander, and Léo Perrin. A further study of quadratic APN permutations in dimension nine. *Finite Fields and Their Applications*, 81:102049, 2022.

[3] Christof Beierle and Gregor Leander. New instances of quadratic APN functions. *IEEE Transactions on Information Theory*, 68(1):670–678, 2021.

[4] Christof Beierle and Gregor Leander. New instances of quadratic APN functions in small dimension, May 2021.

[5] Thomas Beth and Cunsheng Ding. On almost perfect nonlinear permutations. In *Workshop on the Theory and Application of Cryptographic Techniques*, pages 65–76. Springer, 1993.

[6] Eli Biham and Adi Shamir. *Differential cryptanalysis of the data encryption standard*. Springer Science & Business Media, 2012.

[7] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. A few more quadratic APN functions. *Cryptography and Communications*, 3(1):43–53, 2011.

[8] Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert S Coulter, and Irene Villa. Constructing APN functions through isotopic shifts. *IEEE Transactions on Information Theory*, 66(8):5299–5309, 2020.

[9] Lilya Budaghyan and Claude Carlet. Classes of quadratic APN trinomials and hexanomials and related structures. *IEEE Transactions on Information Theory*, 54(5):2354–2357, 2008.

[10] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Transactions on Information Theory*, 54(9):4218–4229, 2008.

[11] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Constructing new APN functions from known ones. *Finite Fields and Their Applications*, 15(2):150–159, 2009.

[12] Lilya Budaghyan, Claude Carlet, and Gregor Leander. On a construction of quadratic apn functions. In *2009 IEEE Information Theory Workshop*, pages 374–378. IEEE, 2009.

[13] Lilya Budaghyan, Tor Helleseth, and Nikolay Kaleyski. A new family of APN quadrinomials. *IEEE Transactions on Information Theory*, 66(11):7081–7087, 2020.

[14] Lilya Budaghyan, Ivana Ivkovic, and Nikolay Kaleyski. Triplicate functions. *Cryptography and Communications*, pages 1–49, 2022.

[15] Marco Calderini, Lilya Budaghyan, and Claude Carlet. On known constructions of APN and AB functions and their relation to each other. *Rad Hrvatske akademije znanosti i umjetnosti: Matematičke znanosti*, (546= 25):79–105, 2021.

[16] Marco Calderini, Kangquan Li, and Irene Villa. Two new families of bivariate APN functions. *arXiv preprint arXiv:2204.07462*, 2022.

[17] Anne Canteaut, Alain Couvreur, and Léo Perrin. Recovering or testing extended-affine equivalence. *IEEE Transactions on Information Theory*, 2022.

[18] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for des-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

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

[20] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 356–365. Springer, 1994.

[21] Hans Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case. *Information & Computation*, 151(1):57–72, 1999.

[22] Hans Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, 1999.

[23] Hans Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: A new case for n divisible by 5. *International Conference on Finite Fields and Applications*, pages 113–121, 2001.

[24] Yves Edel and Alexander Pott. On the equivalence of nonlinear functions. In *Enhancing cryptographic primitives with techniques from error correcting codes*, pages 87–103. IOS Press, 2009.

[25] Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). *IEEE Transactions on Information Theory*, 14(1):154–156, 1968.

[26] Faruk Göloğlu. Biprojective almost perfect nonlinear functions. *IEEE Transactions on Information Theory*, 2022.

[27] Faruk Göloğlu and Lukas Kölsch. Equivalences of biprojective almost perfect nonlinear functions. *arXiv preprint arXiv:2111.04197*, 2021.

[28] Heeralal Janwa and Richard M Wilson. Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 180–194. Springer, 1993.

[29] Tadao Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary reed-

muller codes. *Information & Computation*, 18(4):369–394, 1971.

[30] Kangquan Li, Yue Zhou, Chunlei Li, and Longjiang Qu. Two new families of quadratic APN functions. *IEEE Transactions on Information Theory*, 2022.

[31] Mitsuru Matsui. Linear cryptanalysis method for des cipher. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 386–397. Springer, 1993.

[32] Kaisa Nyberg. Differentially uniform mappings for cryptography. *Lecture Notes in Computer Science*, 765:55–64, 1994.

[33] Hiroaki Taniguchi. On some quadratic APN functions. *Designs, Codes and Cryptography*, 87(9):1973–1983, 2019.

[34] Satoshi Yoshiara. Equivalences of quadratic APN functions. *Journal of Algebraic Combinatorics*, 35(3):461–475, 2012.

[35] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A matrix approach for constructing quadratic APN functions. *Designs, codes and cryptography*, 73(2):587–600, 2014.

[36] Lijing Zheng, Haibin Kan, Yanjun Li, Jie Peng, and Deng Tang. Constructing new APN functions through relative trace functions. *IEEE Transactions on Information Theory*, 2022.

[37] Yue Zhou and Alexander Pott. A new family of semifields with 2 parameters. *Advances in Mathematics*, 234:43–60, 2013.