Two new families of quadratic APN functions

Kangquan Li, Yue Zhou, Chunlei Li and Longjiang Qu

Abstract

In this paper, we present two new families of APN functions. The first family is in bivariate form $\left(x^3+xy^2+y^3+xy, x^5+x^4y+y^5+xy+x^2y^2\right)$ over $\mathbb{F}_{2^m}^2$. It is obtained by adding certain terms of the form $\sum(a_ix^{2^i}y^{2^i}, b_ix^{2^i}y^{2^i})$ to a family of APN functions recently proposed by Göloğlu. The second family has the form $L(z)^{2^m+1}+vz^{2^m+1}$ over $\mathbb{F}_{2^{3m}}$, which generalizes a family of APN functions by Bracken et al. in 2011. By calculating the Γ-rank of the constructed APN functions over $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^9}$, we demonstrate that the two families are CCZ-inequivalent to all known families. In addition, the two families cover two known sporadic APN instances over $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^9}$, which were found by Edel and Pott in 2009 and by Beierle and Leander in 2021, respectively.

Index Terms

APN function, CCZ-equivalence, Adding term, Bivariate form

1. Introduction

S-boxes are crucial nonlinear components in block ciphers. They should satisfy a variety of cryptographic criteria [16], such as having low differential uniformity to resist differential attacks [4]. An $n\times n$ S-box can be seen as a function from the finite field $\mathbb{F}_{2^n}$ to itself, which is commonly termed an (n,n)-function. The differential uniformity of an (n,n)-function is defined as follows.

Definition 1. *[28] Given an (n,n)-function $f:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$, its differential uniformity is given by*

$$\delta_f=\max_{a\in\mathbb{F}_{2^n}^*,b\in\mathbb{F}_{2^n}}\#\left\{z: z\in\mathbb{F}_{2^n}\mid f(z+a)+f(z)=b\right\}.$$

Furthermore, when $\delta_f=2$, the function f is called almost perfect nonlinear (APN for short).

APN functions provide the best resistance against differential attacks [28] and also find applications in sequence design and coding theory [15]. In the last three decades, one of the most important topics in the

Kangquan Li, Yue Zhou and Longjiang Qu are with the College of Liberal Arts and Sciences, National University of Defense Technology, Changsha, 410073, China and Hunan Engineering Research Center of Commercial Cryptography Theory and Technology Innovation, Changsha, 410073, China. Chunlei Li is with the Department of Informatics, University of Bergen, Bergen N-5020, Norway. The work of Longjiang Qu was supported by the National Natural Science Foundation of China under Grant (No. 62032009). The work of Yue Zhou was supported by the Natural Science Foundation of Hunan Province under Grant (No. 2019JJ30030) and the National Natural Science Foundation of China under Grant (No. 62172427). The work of Chunlei Li was supported by the Research Council of Norway (No. 247742/O70 and No. 311646/O70) and the National Natural Science Foundation of China under Grant (No. 61771021). **Emails**: likangquan11@nudt.edu.cn, gabelozhou@gmail.com, chunlei.li@uib.no and ljqu_happy@hotmail.com.

TABLE I
All known APN monomials over $\mathbb{F}_{2^n}$

Family	Function	Conditions	Ref.
Gold	z^{2^i+1}	$\gcd(i,n)=1$	[23]
Kasami	$z^{2^{2i}-2^i+1}$	$\gcd(i,n)=1$	[25]
Welch	z^{2^t+3}	$n=2t+1$	[19]
Niho-1	$z^{2^t+2^{t/2}-1}$	$n=2t+1, t$ even	[18]
Niho-2	$z^{2^t+2^{(3t+1)/2}-1}$	$n=2t+1, t$ odd	[18]
Inverse	$z^{2^{2t}-1}$	$n=2t+1$	[28]
Dobbertin	$z^{2^{4i}+2^{3i}+2^{2i}+2^i-1}$	$n=5i$	[20]

TABLE II
All known polynomial APN families in univariate form over $\mathbb{F}_{2^n}$

No.	Function	Conditions	Ref.
F1- F2	$z^{2^s+1}+u^{2^k-1}z^{2^{ik}+2^{mk+s}}$	$n=pk, \gcd(k,3)=\gcd(s,3k)=1,$ $p\in\{3,4\}, i=sk \pmod{p}, m=p-i,$ $n\geq 12,$ u primitive in $\mathbb{F}_{2^n}^*$	[11]
F3	$sz^{2^i(q+1)}+z^{2^i+1}+z^{q(2^i+1)}$ $+cz^{2^iq+1}+c^qz^{2^i+q}+z^{q+1}$	$q=2^m$, $n=2m$, $\gcd(i,m)=1$, $c\in\mathbb{F}_{2^n}, s\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}, z^{2^i+1}+cz^{2^i}+$ c^qz+1 has no solution x with $x^{q+1}=1$	[10]
F4	$z^3+a^{-1}\mathrm{Tr}_1^n(a^3z^9)$	$a\neq 0$	[12]
F5	$z^3+a^{-1}\mathrm{Tr}_3^n(a^3z^9+a^6z^{18})$	$3\mid n, a\neq 0$	[13]
F6	$z^3+a^{-1}\mathrm{Tr}_3^n(a^6z^{18}+a^{12}z^{36})$	$3\mid n, a\neq 0$	[13]
F7-F9	$uz^{2^s+1}+u^{2^m}z^{2^{-m}+2^{m+s}}+$ $vz^{2^{-m}+1}+wu^{2^m+1}z^{2^s+2^{m+s}}$	$n=3m, \gcd(m,3)=\gcd(s,3m)=1, v,w\in\mathbb{F}_{2^m}$ $vw\neq 1, 3\mid m+s, u$ primitive in $\mathbb{F}_{2^n}^*$	[6]
F10	$a^2z^{2^{2m+1}+1}+b^2z^{2^{m+1}+1}+$ $az^{2^{2m}+2}+bz^{2^m+2}+(c^2+c)z^3$	$n=3m, m$ odd, $L(z)=az^{2^{2m}}+bz^{2^m}+cz$ satisfies the conditions of Lemma 8 of [8]	[8]
F11	$z^3+wz^{2^{i+1}}+w^2z^{3\cdot 2^m}$ $+z^{2^{i+m}+2^m}$	$n=2m, m$ odd, $3\nmid m,$ w primitive in $\mathbb{F}_{2^2}, s=m-2, (m-2)^{-1} \pmod{n}$	[14]
F12	$a\mathrm{Tr}_m^n(bz^3)+a^q\mathrm{Tr}_m^n(b^3z^9)$	$n=2m, m$ odd, $q=2^m$, $a\notin\mathbb{F}_q$, b not a cube	[31]

study of APN functions is to construct new families of APN functions. Several infinite families of APN functions are described in the literature. We summarize all known families of APN functions in Tables I-III according to [9, Table 3], where in Tables I and II functions are given in univariate form in $z\in\mathbb{F}_{2^n}$ and in Table III functions are given in bivariate form in $(x,y)\in\mathbb{F}_{2^m}^2$. More specifically, Table I lists all known APN monomials, which is conjectured to be complete [18]; Table II lists all known families of polynomial APN functions, where Tr_m^n denotes the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ for any $m\mid n$, i.e., $\mathrm{Tr}_m^n(z)=z+z^{2^m}+\cdots+z^{2^{(\frac{n}{m}-1)m}}$; and Table III lists all known families of APN functions proposed originally in bivariate form, where $P_1(z)=z^{2^k+1}+az+b$ and $P_2(z)=(cz^{2^i+1}+bz^{2^i}+1)^{2^{m/2}+1}+z^{2^{m/2}+1}$.

TABLE III

ALL KNOWN APN FAMILIES IN BIVARIATE FORMS OVER $\mathbb{F}_{2^m}^2$

No.	Function	Conditions	Ref.
F13	$(xy, x^{2^k+1}+\alpha x^{(2^k+1)2^i})$	$\gcd(k,m)=1$, m even, α non-cubic	[32]
F14	$(xy, x^{2^{3k}+2^{2k}}+ax^{2^{2k}}y^{2^k}+by^{2^k+1})$	$\gcd(k,m)=1$, P_1 has no root in $\mathbb{F}_{2^m}$	[29]
F15	$(xy, x^{2^i+1}+x^{2^{i+m/2}}y^{2^{m/2}}+bxy^{2^i}+cy^{2^i+1})$	m even, $\gcd(i,m)=1$, P_2 has no root in $\mathbb{F}_{2^m}$	[15]
F16	$(x^{2^i+1}+xy^{2^i}+y^{2^i+1}, x^{2^{2i}+1}+x^{2^{2i}}y+y^{2^{2i}+1})$	$\gcd(3i,m)=1$	[24]
F17	$(x^{2^i+1}+xy^{2^i}+y^{2^i+1}, x^{2^{3i}}y+xy^{2^{3i}})$	$\gcd(3i,m)=1$, m odd	[24]

In this paper, we propose two new families of quadratic APN functions. The construction of the first family is inspired by Dillon's method [7] and its generalization by Budaghyan and Carlet [10]. Dillon in [7] presented a way to construct APN functions of the form

$$f(z)=z(Az^2+B^q+Cz^{2q})+z^2(Dz^q+Ez^{2q})+Gz^{3q} \tag{1}$$

over $\mathbb{F}_{q^2}$ with $q=2^m$. In particular, Budaghyan and Carlet in [10] obtained a family of APN hexanomials of this form, namely, the family F3 in Table II. Let $f_1(z)=Az^3+Cz^{2q+1}+Dz^{q+2}+Gz^{3q}$. Recently Li, Li, Helleseth and Qu completely characterized the coefficients for which f_1 is APN [26]. Later, Chase and Lisoněk [17] proved that when $m\geq 4$, f_1 is APN if and only if f_1 is CCZ-equivalent to one of two instances of Gold functions. This indicates that the APN hexanomials of the form (1) can be seen as the summation of a known APN function $f_1(z)$ and $Bz^{q+1}+Ez^{2(q+1)}$. Such an observation inspired us to seek new APN functions over $\mathbb{F}_{q^2}$ by adding special terms of the form $\sum_i c_i z^{2^i(q+1)}$, $c_i\in\mathbb{F}_{q^2}^*$ to known APN families. Note that for the bivariate form over $\mathbb{F}_q^2$, $\sum_i c_i z^{2^i(q+1)}$ is actually of the form $\sum_i(a_i x^{2^i}y^{2^i}, b_i x^{2^i}y^{2^i})$, $a_i, b_i\in\mathbb{F}_q^*$. It turns out that this approach can give rise to a new family of APN functions over $\mathbb{F}_{2^m}^2$ by adding the terms $(xy, xy+x^2y^2)$ to F16 in Table III.

Theorem 2. *Let m be a positive integer with $\gcd(3,m)=1$. Then the function*

$$f(x,y)=\big(x^3+xy^2+y^3+xy, x^5+x^4y+y^5+xy+x^2y^2\big)$$

is APN over $\mathbb{F}_{2^m}^2$.

The construction of our second family arises from the following APN quadrinomial over $\mathbb{F}_{2^{3m}}$ [6]:

$$f(z)=uz^{2^s+1}+u^{2^m}z^{2^{-m}+2^{m+s}}+vz^{2^{-m}+1}+wu^{2^m+1}z^{2^s+2^{m+s}}.$$

Assume $w\neq 0$ and take $\gamma=w^{\frac{1}{1-2^s}}$, which always exists since $\gcd(2^m-1,2^s-1)=2^{\gcd(m,s)}-1=1$. Then $f(\gamma z)^{2^m}=\gamma^{2^s+1}(L(z)^{2^m+1}+(vw+1)z^{2^m+1})$, where $L(z)=u^{2^m}z^{2^{m+s}}+z$. Note that the equation $L(z)=0$ only has $z=0$ as a solution in $\mathbb{F}_{2^{3m}}$ since $\gcd(2^{3m}-1,2^{m+s}-1)=2^{\gcd(3m,m+s)}-1=7$ and u is primitive in $\mathbb{F}_{2^{3m}}$. Thus L is a linearized permutation of $\mathbb{F}_{2^{3m}}$. Therefore, f is linear equivalent to an

APN family of the form $L(z)^{2^m+1} + vz^{2^m+1}$ with L a permutation binomial and $v \neq 0$. By choosing a linearized permutation trinomial L, we propose another new family of APN functions over $\mathbb{F}_{2^{3m}}$ as follows.

Theorem 3. *Let* $\gcd(s, m) = 1$ *and* $v \in \mathbb{F}_{2^m}^*$. *Choose* $\mu \in \mathbb{F}_{2^{3m}}^*$ *such that* $\mu^{2^{2m}+2^m+1} \neq 1$ *and* $L(z) = z^{2^{m+s}} + \mu z^{2^s} + z$ *permutes* $\mathbb{F}_{2^{3m}}$. *Then* $f(z) = L(z)^{2^m+1} + vz^{2^m+1}$ *is APN over* $\mathbb{F}_{2^{3m}}$.

Interestingly, the two families in Theorems 2 and 3 both contain previously known sporadic APN instances. According to the code isomorphism test, the family in Theorem 2 includes a sporadic APN function over $\mathbb{F}_{2^8}$ (No. 1.9 in Table 9) originally discovered by Edel and Pott in 2009 with the switching method [21]; and the family in Theorem 3 covers a sporadic APN function over $\mathbb{F}_{2^9}$, which was recently found by Beierle and Leander in 2021 using a recursive tree search [3]. Here we emphasize that the APN instances in [21] and [3] were not covered by any family before our constructions.

The remainder of this paper is organized as follows. First, in Section 2 we demonstrate that the proposed two families contain APN functions that are CCZ-inequivalent to those from the known families. Sections 3 and 4 prove the APNness of the families in Theorems 2 and 3, respectively. Section 5 summarizes the work of this paper and presents some related problems.

2. CCZ-EQUIVALENCE

Two functions f and g over $\mathbb{F}_{2^n}$ are said to be *Carlet-Charpin-Zinoviev (CCZ) equivalent* if there is an affine permutation of $\mathbb{F}_{2^n}^2$ that maps the graph $G_f = \{(z, f(z)) : z \in \mathbb{F}_{2^n}\}$ to the graph $G_g = \{(z, g(z)) : z \in \mathbb{F}_{2^n}\}$. CCZ-equivalence is the most general form of equivalence used in the classification of APN functions. To justify that a family of APN functions is indeed new, it is necessary to show that its instances are CCZ-inequivalent to those of the currently known APN families. As a theoretical proof of such a task is rather challenging, in practice one typically chooses to demonstrate that the constructed family contains an APN function that is CCZ-inequivalent to those from another family for small dimensions n. Two common approaches are used for this purpose. The first one, known as the *code isomorphism test*, is to check whether two linear codes associated with the functions are isomorphic. More precisely, for an (n, n)-function f, its associated code $\mathcal{C}_f$ is the linear code defined by the following generating matrix:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & u & \cdots & u^{2^n-1} \\ f(0) & f(u) & \cdots & f\left(u^{2^n-1}\right) \end{pmatrix},$$

where u is a primitive element of $\mathbb{F}_{2^n}$. It is shown [7, 22] that two functions f and g are CCZ-equivalent if and only if $\mathcal{C}_f$ and $\mathcal{C}_g$ are isomorphic. The test of code isomorphism is implemented in MAGMA [5], and it can be used to test CCZ-equivalence between two (n, n)-functions for small integers n. Another common approach is to compare certain CCZ-invariants, i.e., properties that are preserved under CCZ-equivalence, of two (n, n)-functions for small integers n. If two functions exhibit different values of a given CCZ-invariant, then they must be CCZ-inequivalent. One CCZ-invariant is the Γ-rank [21]. The Γ-rank of an (n, n)-function

TABLE IV

CCZ-inequivalent representatives from the known APN families and that in Theorem 2 over $\mathbb{F}_{2^8}$ and their Γ-ranks

No.	Function	Γ-rank	Ref.
1	z^3	11818	Gold
2	z^9	12370	Gold
3	z^{57}	15358	Kasami
4	$z^3+z^{17}+u^{48}z^{18}+u^3z^{33}+uz^{34}+z^{48}$	13200	F3
5	$z^3+\mathrm{Tr}_8(z^9)$	13800	F4
6	$z^3+u^{-1}\mathrm{Tr}_8(u^3z^9)$	13842	F4
7	(xy, x^3+vy^{12})	13642	F13
8	$(xy, x^{12}+x^4y^2+y^3)$	13700	F14
9	$(xy, x^{12}+x^4y^2+v^7y^3)$	13798	F14
10	$(x^3+xy^2+y^3, x^5+x^4y+y^5)$	13642	F16
11	$(xy, x^3+x^2y+vx^4y^8+v^5y^3)$	13960	F15
12	$(x^3+xy^2+y^3+xy, x^5+x^4y+y^5+xy+x^2y^2)$	14034	Theorem 2

TABLE V

CCZ-inequivalent representatives from the known APN families and that in Theorem 3 over $\mathbb{F}_{2^9}$ and their Γ-ranks

No.	Function	Γ-rank	Ref.
1	z^3	38470	Gold
2	z^5	41494	Gold
3	z^{17}	38470	Gold
4	z^{13}	58676	Kasami
5	z^{241}	61726	Kasami
6	z^{19}	60894	Welch
7	z^{255}	130816	Inverse
8	$z^3+\mathrm{Tr}_9(z^9)$	47890	F4
9	$z^3+\mathrm{Tr}_3^9(z^9+z^{18})$	48428	F5
10	$z^3+\mathrm{Tr}_3^9(z^{18}+z^{36})$	48460	F5
11	$z^3+u^{246}z^{10}+u^{47}z^{17}+u^{181}z^{66}+u^{428}z^{129}$	48596	F10
12	$(z^{16}+u^5z^2+z)^9+u^{73}z^9$	48558	Theorem 3

f is defined as the rank of the incidence matrix of a design $\mathrm{dev}(G_f)$, whose set of points is $\mathbb{F}_{2^n}^2$ and whose set of blocks is $\{(z+a, f(z)+b) : z \in \mathbb{F}_{2^n}\}$ for $a, b \in \mathbb{F}_{2^n}$.

In this section, we demonstrate that our newly constructed APN families are CCZ-inequivalent to all known APN families by comparing the Γ-ranks of the representatives from all known APN families and ours over $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^9}$, see Tables IV and V.[1] In Table IV, u and v are elements in $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^4}$ with minimal

[1] In Tables IV and V, the Γ-ranks of the representatives from all known APN families are retrieved from the website https://boolean.h.uib.no/mediawiki/index.php/Tables

polynomials $z^8+z^4+z^3+z^2+1$ and z^4+z+1 over $\mathbb{F}_2$, respectively. In Table V, u denotes an element of $\mathbb{F}_{2^9}$ with minimal polynomial z^9+z^4+1 over $\mathbb{F}_2$. The last column, denoted by "Ref." for short, refers to the known APN families listed in Tables I, II and III. As shown in Tables IV and V, the two families proposed in this paper contain instances that are not covered by any known family, which indicates that the two families in this paper are new up to CCZ-equivalence. Moreover, according to the code isomorphism test, we observe that the two families also cover known sporadic APN instance that does not belong to any other known families. As a matter of fact, our first family in Theorem 2 covers one sporadic APN function over $\mathbb{F}_{2^8}$ (No. 1.9) in [21, Table 9], which was found by the switching method. The covered APN instance is

$$z^3+u\mathrm{Tr}_8\left(u^{63}z^3+u^{252}z^9\right)+u^{154}\mathrm{Tr}_8\left(u^{68}z^3+u^{235}z^9\right)+u^{35}\mathrm{Tr}_8\left(u^{216}z^3+u^{116}z^9\right),$$

where u is defined as in Table IV. In addition, our second APN family in Theorem 3 covers one (No. 9) of the APN functions over $\mathbb{F}_{2^9}$ in the dataset [2], which were obtained by a recursive tree search due to Beierle and Leander [3]. The covered APN instance is CCZ-equivalent to

$$\begin{aligned}
&u^{149}z^{384}+u^{339}z^{320}+u^{498}z^{288}+u^{404}z^{272}+u^{125}z^{264}+u^{274}z^{260}+u^{125}z^{258}+u^{432}z^{257}+\\
&u^{241}z^{192}+u^{14}z^{160}+u^{500}z^{144}+u^{376}z^{136}+u^{258}z^{132}+u^{470}z^{130}+u^{430}z^{129}+u^{407}z^{96}+\\
&u^{317}z^{80}+u^{209}z^{72}+u^{371}z^{68}+u^{77}z^{66}+u^{502}z^{65}+u^{464}z^{48}+u^{6}z^{40}+u^{188}z^{36}+\\
&u^{498}z^{34}+u^{508}z^{33}+u^{199}z^{24}+u^{41}z^{20}+u^{158}z^{18}+u^{218}z^{17}+u^{16}z^{12}+u^{7}z^{10}+\\
&u^{116}z^{9}+u^{437}z^{6}+u^{502}z^{5}+z^{3},
\end{aligned}$$

where u is defined as in Table V.

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

This section is dedicated to the proof of Theorem 2. We first give several useful lemmas. The following lemma allows us to determine the number of solutions of cubic equations over $\mathbb{F}_{2^m}$.

Lemma 4. *[30] Let $a,b\in\mathbb{F}_{2^m}$, $b\neq 0$ and define*

$$f(z)=z^3+az+b, h(t)=t^2+bt+a^3.$$

Let t_1,t_2 be two solutions of $h(t)$ in $\mathbb{F}_{2^{2m}}$. Then:

- *f has three zeros in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_m\left(\frac{a^3}{b^2}\right)=\mathrm{Tr}_m(1)$, t_1 and t_2 are cubes in $\mathbb{F}_{2^m}$ (resp. $\mathbb{F}_{2^{2m}}$) when m is even (resp. odd).*
- *f has exactly one zero in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_m\left(\frac{a^3}{b^2}\right)\neq\mathrm{Tr}_m(1)$.*
- *f has no zeros in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_m\left(\frac{a^3}{b^2}\right)=\mathrm{Tr}_m(1)$, t_1 and t_2 are not cubes in $\mathbb{F}_{2^m}$ (resp. $\mathbb{F}_{2^{2m}}$) when m is even (resp. odd).*

The following simple results will be frequently used in the proof of Theorem 2 later.

Lemma 5. *Let* $\gcd(m,3)=1$. *Then,*

(1) the equation $z^3+z+1=0$ *has no solution in* $\mathbb{F}_{2^m}$*;*

(2) any element $\omega\in\mathbb{F}_{2^2}\backslash\mathbb{F}_2$ *is not cubic in* $\mathbb{F}_{2^m}$ *and* $\mathbb{F}_{2^{2m}}$*;*

(3) the equation $a^3+a^2b+a+b^3+b^2+1=0$ *holds for* $a,b\in\mathbb{F}_{2^m}$ *if and only if* $(a,b)=(1,1)$.

Proof. It is clear that any solution of $z^3+z+1=0$ is in $\mathbb{F}_{2^3}$. Furthermore, any solution in $\mathbb{F}_{2^m}$ actually belongs to $\mathbb{F}_2$ since $\gcd(m,3)=1$. Since $0,1$ are not solutions of the equation, the first statement follows.

For the second statement, the element ω is cubic in a finite field $\mathbb{F}_{2^n}$ if and only if $\omega^{\frac{2^n-1}{3}}=1$, which implies $3|\frac{2^n-1}{3}$ since $\omega\in\mathbb{F}_{2^2}\backslash\mathbb{F}_2$. This is equivalent to saying that $\omega\in\mathbb{F}_{2^2}\backslash\mathbb{F}_2$ is cubic in $\mathbb{F}_{2^n}$ if and only if $9|2^n-1$, which holds only if n is a multiple of 6. Since $\gcd(3,m)=1$, ω cannot be a cubic in $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^{2m}}$.

Let $B=a^3+a^2b+a+b^3+b^2+1$. In the following, we prove that $B=0$ if and only if $(a,b)=(1,1)$. Plugging $a=a_1+b$ into $B=0$ and simplifying it, we get

$$a_1^3+(b^2+1)a_1+(b+1)^3=0. \tag{2}$$

If $b=1$, then $a_1=0$ and thus $a=a_1+b=1$. If $b\neq 1$, plugging $a_1=(b+1)a_2$ into Eq. (2) and simplifying it, we have $a_2^3+a_2+1=0$, which has no solution in $\mathbb{F}_{2^m}$ from the first statement of this lemma. Thus $B=0$ if and only if $(a,b)=(1,1)$. □

Since the resultant of polynomials will be used in our proof, we now recall some basic facts about it. Given two polynomials $u(x)=a_mx^m+a_{m-1}x^{m-1}+\cdots+a_0$ and $v(x)=b_nx^n+b_{n-1}x^{n-1}+\cdots+b_0$ over a field K with degrees m and n, respectively, their resultant $\mathrm{Res}(u,v)\in K$ is the determinant of the following square matrix of order $n+m$:

$$\begin{pmatrix}
a_m & a_{m-1} & \cdots & a_0 & 0 & & \cdots & 0\\
0 & a_m & a_{m-1} & \cdots & a_0 & 0 & \cdots & 0\\
\vdots & & \ddots & & & & & \vdots\\
0 & \cdots & 0 & a_m & a_{m-1} & & \cdots & a_0\\
b_n & b_{n-1} & \cdots & & b_0 & 0 & \cdots & 0\\
0 & b_n & b_{n-1} & \cdots & & b_0 & \cdots & 0\\
\vdots & & \ddots & & & & \ddots & \vdots\\
0 & \cdots & 0 & b_n & b_{n-1} & & \cdots & b_0
\end{pmatrix}.$$

For a field K and two polynomials $F(x,y),G(x,y)\in K[x,y]$, we use $\mathrm{Res}_y(F,G)$ to denote the resultant of F and G with respect to y, which is the resultant of F and G when considered as polynomials in the single variable x. In this case, $\mathrm{Res}_y(F,G)\in K[x]$ belongs to the ideal generated by F and G. It is known that $F(x,y)=0$ and $G(x,y)=0$ has a common solution (x,y) if and only if x is a solution of $\mathrm{Res}_y(F,G)(x)=0$ (see [27, P. 36]).

In the final part of this section, we give the proof of Theorem 2.

Proof of Theorem 2. Since f is a quadratic function with $f(0,0)=(0,0)$, it suffices to show that for any $(a,b)\neq(0,0)\in\mathbb{F}_{2^m}^2$, the equation

$$f(x+a,y+b)+f(x,y)+f(a,b)=0 \tag{3}$$

has exactly two solutions $(x,y)=(0,0),(a,b)$ in $\mathbb{F}_{2^m}^2$. By a simple calculation, Eq. (3) is equivalent to the following equation system:

$$\begin{cases} F(x,y)=ax^2+\left(a^2+b^2+b\right)x+(a+b)y^2+\left(a+b^2\right)y=0 & (4.1)\\ G(x,y)=(a+b)x^4+b^2x^2+\left(a^4+b\right)x+by^4+a^2y^2+\left(a^4+a+b^4\right)y=0. & (4.2)\end{cases}$$

Firstly, we consider the case $(a,b)=(1,1)$. In this case, Eqs. (4) become

$$\begin{cases} x^2+x=0 & (5.1)\\ x^2+y^4+y^2+y=0. & (5.2)\end{cases}$$

From Eq. (5.1), we know $x\in\{0,1\}$. If $x=0$, plugging it into Eq. (5.2), we have $y^4+y^2+y=0$ and then $y=0$ by Lemma 5 (1). If $x=1$, together with Eq. (5.2), we get $y^4+y^2+y+1=0$, which means $y=1$. Thus in this case, Eqs. (4) have only $(x,y)\in\{(0,0),(1,1)\}$ as solutions in $\mathbb{F}_{2^m}^2$.

In the following, we always assume that $(a,b)\neq(1,1)$. With the help of MAGMA (see Appendix-A for more details), we obtain the resultant of F and G with respect to y as follows

$$\mathrm{Res}_y(F,G)(x)=\left(a^3+ab^2+b^3\right)^2x(x+a)H(x,a,b)H(x+a,a,b), \tag{6}$$

where

$$H(x,a,b)=x^3+(a^2+ab+a+b^2+b+1)x+a^3+a^2b+a+b^3+b^2+1.$$

In the sequel we shall show that $\mathrm{Res}_y(F,G)(x)=0$ is equivalent to $x(x+a)=0$.

First of all, we have $a^3+ab^2+b^3\neq0$ for any $(a,b)\neq(0,0)\in\mathbb{F}_{2^m}^2$. Otherwise, for some element $(a,b)\neq(0,0)\in\mathbb{F}_{2^m}^2$, $a^3+ab^2+b^3=0$. If $b=0$, then the above equation becomes $a^3=0$, which contradicts the assumption $(a,b)\neq(0,0)$. If $b\neq0$, then we have $c^3+c+1=0$, where $c=\frac{a}{b}\in\mathbb{F}_{2^m}$, which contradicts Lemma 5 (1).

In addition, we need to show $H(x,a,b)H(x+a,a,b)\neq0$. Note that $H(x,a,b)=0$ has the same number of solutions in $\mathbb{F}_{2^m}$ as $H(x+a,a,b)=0$. It suffices to show that the equation $H(x,a,b)=0$ has no solution in $\mathbb{F}_{2^m}$. Now we consider the equation $H(x,a,b)=0$, i.e.,

$$x^3+Ax+B=0, \tag{7}$$

where $A=a^2+ab+a+b^2+b+1$ and $B=a^3+a^2b+a+b^3+b^2+1$. By Lemma 5 (3), $B\neq0$ holds under the case $(a,b)\neq(1,1)$. Let $h(t)=t^2+Bt+A^3$. By computation, we have

$$\frac{A^3}{B^2}=\frac{C}{B}+\frac{C^2}{B^2}+1,$$

where

$$C=a^2b+a^2+ab^2+a+b^2+b.$$

Thus $\mathrm{Tr}_m\left(\frac{A^3}{B^2}+1\right)=0$ and the equation $h(t)=0$ has two solutions $t_1=C+\omega B$ and $t_2=C+\omega^2 B$ in $\mathbb{F}_{2^m}$ (resp. $\mathbb{F}_{2^{2m}}$) if m is even (resp. odd), where $\omega\in\mathbb{F}_{2^2}\backslash\mathbb{F}_2$. Moreover,

$$\begin{aligned} t_1 &= \omega(\omega^2C+B)\\ &= \omega\left(\omega^2(a^2b+a^2+ab^2+a+b^2+b)+a^3+a^2b+a+b^3+b^2+1\right)\\ &= \omega\left(a+\omega b+\omega^2\right)^3, \end{aligned}$$

which is not cubic by Lemma 5 (2). Similarly, t_2 is not cubic, either. Thus from Lemma 4, the equation $x^3+Ax+B=0$ has no solution in $\mathbb{F}_{2^m}$.

Hence from Eq. (6), we have $x=0$ or $x=a$. Next, we will show that from Eqs. (4), $y=0$ or $y=b$, respectively. Namely, Eqs. (4) have only $(x,y)\in\{(0,0),(a,b)\}$ as solutions.

If $a=0$, then $x=0$. Moreover, Eq. (4.1) and Eq. (4.2) become $by^2+b^2y=0$ and $by^4+b^4y=0$, respectively. Thus $y=0$ or $y=b$. In the following, we assume that $a\neq 0$.

Case 1: $x=0$. In this case Eqs. (4) become

$$\begin{cases} (a+b)y^2+\left(a+b^2\right)y=0 & (8.1)\\ by^4+a^2y^2+\left(a^4+a+b^4\right)y=0. & (8.2)\end{cases}$$

We now show that Eqs. (8) have only one solution $y=0$ for any $(a,b)\in\mathbb{F}_{2^m}^2\backslash\{(0,0),(1,1)\}$. If $a=b\neq 1$, then by Eq. (8.1), we get $y=0$. Suppose now that $a\neq b$. If $b=0$, then $a\neq 0$ and Eq. (8.1) becomes $a(y^2+y)=0$, i.e., $y\in\{0,1\}$. In addition, Eq. (8.2) is equivalent to $a^2y^2+(a^4+a)y=0$. Since $a^4+a^2+a\neq 0$ for any $a\in\mathbb{F}_{2^m}^*$, which holds by Lemma 5 (1), $y=1$ is not a solution of Eq. (8.2). Namely, $y=0$ is the unique solution to Eqs. (8). If $a\neq b$ and $b\neq 0$, then from Eq. (8.1), we get $y\in\{0,\frac{a+b^2}{a+b}\}$. Plugging $y=\frac{a+b^2}{a+b}$ into Eq. (8.2) and simplifying, we get

$$a(a+b^2)(a^3+ab^2+b^3)(a^3+a^2b+a+b^3+b^2+1)=0. \quad (9)$$

Let $c=\frac{a}{b}$. Then $a^3+ab^2+b^3=b^3\left(c^3+c+1\right)\neq 0$ for any $b\neq 0$ due to Lemma 5 (1). In addition, by Lemma 5 (3), we know that $a^3+a^2b+a+b^3+b^2+1\neq 0$ for any $(a,b)\neq(1,1)$. Thus by Eq. (9), we get $a=b^2$, which means that $y=0$ is the unique solution of Eqs. (8).

Case 2: $x = a$. In this case Eqs. (4) become

$$\begin{cases} (a+b)(y+b)^2 + \left(a+b^2\right)(y+b) = 0 & (10.1) \\ b(y+b)^4 + a^2(y+b)^2 + \left(a^4+a+b^4\right)(y+b) = 0. & (10.2) \end{cases}$$

It is clear that $y = b$ is the unique solution of Eqs. (10) by the discussions of the case if $x = 0$.

On the whole, Eqs. (4) have only $(x, y) \in \{(0,0),(a,b)\}$ as solutions in $\mathbb{F}_{2^m}^2$ for any $(a,b) \in \mathbb{F}_{2^m}^2 \backslash \{(0,0)\}$. Therefore, f is APN over $\mathbb{F}_{2^m}^2$. □

4. A NEW FAMILY OF APN FUNCTIONS OVER $\mathbb{F}_{2^{3m}}$

In this section, we will show that the univariate function in Theorem 3 is APN. Before that, we give some important lemmas.

Lemma 6. *Let* $\gcd(m,s) = 1$, $\mu \in \mathbb{F}_{2^{3m}}^*$ *satisfy* $\mu^{2^{2m}+2^m+1} \neq 1$ *and* $L_\beta(z) = z^{2^{m+s}} + \mu z^{2^s} + \beta z$ *with* $\beta \in \mathbb{F}_{2^m}$. *Then* $L_0(z)$ *permutes* $\mathbb{F}_{2^{3m}}$. *Moreover,* L_1 *permutes* $\mathbb{F}_{2^{3m}}$ *if and only if* L_β *does for any* $\beta \in \mathbb{F}_{2^m}^*$.

Proof. Since $L_\beta(x)$ is a linearized polynomial, it suffices to show $L_\beta(x) = 0$ only has $x = 0$ as a solution in $\mathbb{F}_{2^{3m}}$. Suppose $L_\beta(a) = 0$ for some $a \in \mathbb{F}_{2^{3m}}^*$. If $\beta = 0$, we have $a^{2^{m+s}} + \mu a^{2^s} = 0$, which contradicts the condition $\mu^{2^{2m}+2^m+1} \neq 1$. If $\beta \neq 0$, let $\epsilon \in \mathbb{F}_{2^m}^*$ satisfy $\epsilon^{2^s-1} = \beta$, which always exists since $\gcd\left(2^m-1, 2^s-1\right) = 2^{\gcd(m,s)} - 1 = 1$. Then we have

$$L_\beta(\epsilon x) = (\epsilon x)^{2^{m+s}} + \mu(\epsilon x)^{2^s} + \beta(\epsilon x) = \epsilon^{2^s}\left(x^{2^{m+s}} + \mu x^{2^s} + x\right) = \epsilon^{2^s} L_1(x).$$

The desired statement thus follows. □

Lemma 7. *Let* $\mu \in \mathbb{F}_{2^{3m}}^*$, $L(z) = z^{2^{m+s}} + \mu z^{2^s} + z$ *and* $L^{'}(z) = z^{2^{m+s}} + \mu^{2^m} z^{2^m} + z$. *Then* L *permutes* $\mathbb{F}_{2^{3m}}$ *if and only if* $L^{'}$ *does.*

Proof. For the linear polynomial L, it is known that its adjoint polynomial denoted by L^* is $L^*(z) = z^{2^{2m-s}} + \mu^{2^{3m-s}} z^{2^{3m-s}} + z$ and L permutes $\mathbb{F}_{2^{3m}}$ if and only if L^* does. Moreover, it is easy to check that $L^{'}(z) = \left(L^*(z)\right)^{2^{m+s}}$. Thus L permutes $\mathbb{F}_{2^{3m}}$ if and only if $L^{'}$ does. □

Let $\gcd(s,m) = 1$, $a \in \mathbb{F}_{2^{3m}}$ and $v \in \mathbb{F}_{2^m}^*$. Choose $\mu \in \mathbb{F}_{2^{3m}}^*$ such that $\mu^{2^{2m}+2^m+1} \neq 1$ and $L(z) = z^{2^{m+s}} + \mu z^{2^s} + z$ permutes $\mathbb{F}_{2^{3m}}$. Define

$$\begin{cases} A = L(a) a^{2^{2m+s}} \\ B = \left(L(a)^{2^m} + \mu^{2^m} L(a)\right) a^{2^{m+s}} \\ C = (L(a) + va) a^{2^m} \\ D = \mu L(a)^{2^m} a^{2^s} \\ E = (L(a) + va)^{2^m} a \end{cases} \tag{11}$$

and denote

$$\begin{cases} U_1 = D^{2^{2m}} E^{2^m+1} + AC^{2^{2m}} E^{2^m} + B^{2^m} C^{2^{2m}+1} \\ U_2 = A^{2^{2m}} E^{2^m+1} + BC^{2^{2m}} E^{2^m} + C^{2^{2m}+1} D^{2^m} \\ U_3 = B^{2^{2m}} E^{2^m+1} + C^{2^{2m}} DE^{2^m} + A^{2^m} C^{2^{2m}+1} \\ U_4 = C^{2^{2m}+2^m+1} + E^{2^{2m}+2^m+1} \\ V_1 = A^{2^{2m}+2} C^{2^m} + ABC^{2^m} D^{2^{2m}} + AB^{2^m+1} E^{2^{2m}} + A^2 D^{2^m} E^{2^{2m}} \\ V_2 = A^{2^{2m}+2} E^{2^m} + ABD^{2^{2m}} E^{2^m} + A^{2^{2m}+1} B^{2^m} C + ACD^{2^{2m}+2^m} \\ V_3 = A^{2^{2m}+1} B^{2^m} E + AB^{2^m+1} C^{2^{2m}} + A^2 C^{2^{2m}} D^{2^m} + AD^{2^{2m}+2^m} E \\ V_4 = (B^{2^m+1} + AD^{2^m})(AB^{2^{2m}} + D^{2^{2m}+1}) + (A^{2^{2m}+1} + BD^{2^{2m}})(A^{2^m+1} + B^{2^m} D). \end{cases} \tag{12}$$

The following lemma is crucial to the main proof in this section.

Lemma 8. *Let* A, B, C, D, E *be defined as in* (11), U_i, V_i *with* $i = 1, 2, 3, 4$ *be defined as in* (12). *Then for any* $a \in \mathbb{F}_{2^{3m}}^*$,

(i) $A + B + C + D + E = 0$, $ABCDE \neq 0$ *and* $C + E \neq 0$*;*

(ii) $U_i V_i \neq 0$ *with* $i = 1, 2, 3$*;*

(iii) $U_4 = V_4 = 0$*;*

(iv) $U_2 V_1^{2^s} + U_1 V_2^{2^s} + U_3 V_1^{2^s} + U_1 V_3^{2^s} = 0$;

(v) $U_2 V_1^{2^s} + U_1 V_2^{2^s} \neq 0$.

Proof. (i) Recall that $L(a) = a^{2^{m+s}} + \mu a^{2^s} + a$ and $v \in \mathbb{F}_{2^m}$. It is readily seen that

$$A + B + C + D + E = L(a)\left(a^{2^{m+s}} + \mu a^{2^s} + a\right)^{2^m} + L^{2^m}(a)\left(a^{2^{m+s}} + \mu a^{2^s} + a\right) + a^{2^m+1}(v + v^{2^m}) = 0.$$

Next we show $ABCDE \neq 0$. First, the fact $AD \neq 0$ is clear since $A = L(a)a^{2^{2m+s}}$, $D = \mu L(a)^{2^m} a^{2^s}$ and L permutes $\mathbb{F}_{2^{3m}}$. Second, let $H(x) = x^{2^{2m}} + \mu^{2^{2m}} x$. Then H permutes $\mathbb{F}_{2^{3m}}$ since $\mu^{2^{2m}+2^m+1} \neq 1$. In addition, it is easy to check that $B = H(L(a))a^{2^{m+s}}$ and thus $B \neq 0$ for any $a \in \mathbb{F}_{2^{3m}}^*$. Third, $CE \neq 0$ is equivalent to $L(a) + va = a^{2^{m+s}} + \mu a^{2^s} + (v+1)a \neq 0$, which follows easily from Lemma 6.

Finally, assume that there exists some $a \in \mathbb{F}_{2^{3m}}^*$ such that $C + E = (L(a) + va)a^{2^m} + (L(a) + va)^{2^m} a = 0$. Then $L(a) + va = \eta a$ for some $\eta \in \mathbb{F}_{2^m}^*$. Let $\beta = 1 + v + \eta \in \mathbb{F}_{2^m}$. Then $L_\beta(a) = 0$ for some $a \in \mathbb{F}_{2^{3m}}^*$, which is also impossible by Lemma 6. Thus $C + E \neq 0$ for any $a \in \mathbb{F}_{2^{3m}}^*$.

(ii) Let

$$U = \mu^{2^m} a^{2^{m+s}+1} + a^{2^{2m+s}+1} + a^{2^{m+s}+2^m} + \mu^{2^m+1} a^{2^{2m}+2^{m+s}} + \mu^{2^{2m}+1} a^{2^{2m+s}+2^m} + \mu a^{2^{2m+s}+2^{2m}}.$$

Plugging the expressions of A, B, C, D, E into those of U_1, U_2, U_3 and investigating their factorizations with the help of MAGMA (see Appendix-B), we get

$$\begin{cases} U_1 = va^{2^{2m+s}+2^m} C^{2^{2m}} U^{2^{2m}} = va^{2^m} C^{2^{2m}} (a^{2^s} U)^{2^{2m}} \\ U_2 = va^{2^{m+s}+2^m} C^{2^{2m}} U^{2^m} = va^{2^m} C^{2^{2m}} (a^{2^s} U)^{2^m} \\ U_3 = va^{2^m+2^s} C^{2^{2m}} U = va^{2^m} C^{2^{2m}} (a^{2^s} U). \end{cases} \tag{13}$$

Moreover, let

$$V = a^{2^m+2^s} + \mu^{2^m} a^{2^{2m}+2^{m+s}} + \mu^{2^{2m}} a^{2^{2m+s}+2^m} + a^{2^{2m+s}+2^{2m}}$$

and

$$T = (\mu^{2^{2m}+2^m+1} + 1)a^{2^s} + \mu^{2^{2m}+2^m} a + \mu^{2^{2m}} a^{2^m} + a^{2^{2m}}.$$

Similarly, plugging the expressions of A, B, C, D, E into those of V_1, V_2, V_3 and investigating their factorizations (see Appendix-B), we obtain

$$\begin{cases} V_1 = va^{2^{2m+s+1}+2^{m+s}+2^{2m}} L(a)TV^{2^{2m}} = va^{2^{2m+s+1}+2^{m+s}} L(a)T(aV)^{2^{2m}} \\ V_2 = va^{2^{2m+s+1}+2^{m+s}+2^m} L(a)TV^{2^m} = va^{2^{2m+s+1}+2^{m+s}} L(a)T(aV)^{2^m} \\ V_3 = va^{2^{2m+s+1}+2^{m+s}+1} L(a)TV = va^{2^{2m+s+1}+2^{m+s}} L(a)T(aV). \end{cases} \tag{14}$$

Thus in order to show that $U_iV_i \neq 0$ with $i = 1, 2, 3$, it suffices to prove that $UVT \neq 0$. Let $P = a^{2^{2m+s}} + \mu^{2^m} a^{2^{m+s}}$. Then $P \neq 0$ for any $a \in \mathbb{F}_{2^{3m}}^*$ since the binomial $z^{2^{2m+s}} + \mu^{2^m} z^{2^{m+s}}$ clearly permutes $\mathbb{F}_{2^{3m}}$ when $\mu^{2^{2m}+2^m+1} \neq 1$. In addition, we have

$$V = a^{2^{2m}} P + a^{2^m} P^{2^m}.$$

If there exists some $a \in \mathbb{F}_{2^{3m}}^*$ such that $V = 0$, then $P = \tau a^{2^m}$ for some $\tau \in \mathbb{F}_{2^m}^*$. Furthermore, we have $a^{2^{2m+s}} + \mu^{2^m} a^{2^{m+s}} + \tau a^{2^m} = 0$, i.e., $a^{2^{m+s}} + \mu a^{2^s} + \tau a = 0$, which is impossible by Lemma 6. Thus $V \neq 0$. Moreover, $U \neq 0$ due to the crucial observation that

$$U = V^{2^{2m}} + \mu V,$$

which is a permutation in V over $\mathbb{F}_{2^{3m}}$. Finally, if there exists some $a \in \mathbb{F}_{2^{3m}}^*$ such that $T = 0$, then

$$(\mu^{2^{2m}+2^m+1} + 1)a^{2^s} + \mu^{2^{2m}+2^m} a + \mu^{2^{2m}} a^{2^m} + a^{2^{2m}} = 0. \tag{15}$$

Raising (15) to the 2^m-th power, one gets

$$(\mu^{2^{2m}+2^m+1} + 1)a^{2^{m+s}} + \mu^{2^{2m}+1} a^{2^m} + \mu a^{2^{2m}} + a = 0. \tag{16}$$

Comparing (15) and (16), one can eliminate $\mu^{2^{2m}+1} a^{2^m} + \mu a^{2^{2m}}$ in (16) and obtain

$$(\mu^{2^{2m}+2^m+1} + 1)L(a) = 0,$$

which is impossible since $\mu^{2^{2m}+2^m+1} \neq 1$ and $L(a) \neq 0$ for any $a \in \mathbb{F}_{2^{3m}}^*$.

(iii) It is trivial that $U_4 = C^{2^{2m}+2^m+1} + E^{2^{2m}+2^m+1} = 0$ due to the fact $E = C^{2^m} a^{1-2^{2m}}$. The statement $V_4 = 0$ holds due to the following four equations, which can be checked directly.

$$\begin{aligned} B^{2^m+1} + AD^{2^m} &= (L(a)^{2^m} + \mu^{2^m} L(a))^{2^m+1} a^{2^{2m+s}+2^{m+s}} + \mu^{2^m} L(a)^{2^{2m}+1} a^{2^{2m+s}+2^{m+s}} \\ &= a^{2^{2m+s}+2^{m+s}} L(a)^{2^m} \left(L(a)^{2^{2m}} + \mu^{2^{2m}} L(a)^{2^m} + \mu^{2^{2m}+2^m} L(a) \right), \end{aligned}$$

$$\begin{aligned} AB^{2^{2m}} + D^{2^{2m}+1} &= L(a)a^{2^{2m+s}}(L(a)^{2^m} + \mu^{2^m}L(a))^{2^{2m}}a^{2^s} + \mu^{2^{2m}+1}L(a)^{2^m+1}a^{2^{2m+s}+2^s} \\ &= a^{2^{2m+s}+2^s}L(a)\left(\mu L(a)^{2^{2m}} + \mu^{2^{2m}+1}L(a)^{2^m} + L(a)\right), \\ A^{2^{2m}+1} + BD^{2^{2m}} &= L(a)^{2^{2m}+1}a^{2^{2m+s}+2^{m+s}} + (L(a)\mu^{2^m} + L(a)^{2^m})a^{2^{m+s}}\mu^{2^{2m}}L(a)a^{2^{2m+s}} \\ &= a^{2^{2m+s}+2^{m+s}}L(a)\left(L(a)^{2^{2m}} + \mu^{2^{2m}}L(a)^{2^m} + \mu^{2^{2m}+2^m}L(a)\right) \end{aligned}$$

and

$$\begin{aligned} A^{2^m+1} + B^{2^m}D &= L(a)^{2^m+1}a^{2^{2m+s}+2^s} + (L(a)\mu^{2^m} + L(a)^{2^m})^{2^m}a^{2^{2m+s}}\mu L(a)^{2^m}a^{2^s} \\ &= a^{2^{2m+s}+2^s}L(a)^{2^m}\left(\mu L(a)^{2^{2m}} + \mu^{2^{2m}+1}L(a)^{2^m} + L(a)\right). \end{aligned}$$

(iv) Plugging (13) and (14) into $U_2V_1^{2^s} + U_1V_2^{2^s} + U_3V_1^{2^s} + U_1V_3^{2^s}$, we get

$$\begin{aligned} &U_2V_1^{2^s} + U_1V_2^{2^s} + U_3V_1^{2^s} + U_1V_3^{2^s} \\ =&\Delta\left(a^{2^{m+s}}U^{2^m}(a^{2^{2m}}V^{2^{2m}})^{2^s} + a^{2^{2m+s}}U^{2^{2m}}(a^{2^m}V^{2^m})^{2^s} + a^{2^s}U(a^{2^{2m}}V^{2^{2m}})^{2^s} + a^{2^{2m+s}}U^{2^{2m}}(aV)^{2^s}\right) \\ =&a^{2^{2m+s}}\Delta\left(a^{2^{m+s}}U^{2^m}V^{2^{2m+s}} + a^{2^{m+s}}U^{2^{2m}}V^{2^{m+s}} + a^{2^s}UV^{2^{2m+s}} + a^{2^s}U^{2^{2m}}V^{2^s}\right), \end{aligned}$$

where $\Delta = v^{2^s+1}a^{2^{2m+2s+1}+2^{m+2s}+2^m}C^{2^{2m}}L(a)^{2^s}T^{2^s}$. Moreover, it is easy to check

$$a^{2^{2m+s}}U^{2^{2m}} + a^{2^{m+s}}U^{2^m} + a^{2^s}U = 0 \tag{17}$$

and

$$a^{2^{2m}}V^{2^{2m}} + a^{2^m}V^{2^m} + aV = 0. \tag{18}$$

By multiplying both sides of (17) with $V^{2^{2m+s}}$, we get

$$a^{2^{m+s}}U^{2^m}V^{2^{2m+s}} + a^{2^s}UV^{2^{2m+s}} = a^{2^{2m+s}}U^{2^{2m}}V^{2^{2m+s}}.$$

In addition, by raising (18) to its 2^s-th power and multiplying both sides with $U^{2^{2m}}$, we obtain

$$a^{2^{m+s}}U^{2^{2m}}V^{2^{m+s}} + a^{2^s}U^{2^{2m}}V^{2^s} = a^{2^{2m+s}}U^{2^{2m}}V^{2^{2m+s}}.$$

Together with the above two equations, we have

$$a^{2^{m+s}}U^{2^m}V^{2^{2m+s}} + a^{2^{m+s}}U^{2^{2m}}V^{2^{m+s}} + a^{2^s}UV^{2^{2m+s}} + a^{2^s}U^{2^{2m}}V^{2^s} = 0$$

and therefore

$$U_2V_1^{2^s} + U_1V_2^{2^s} + U_3V_1^{2^s} + U_1V_3^{2^s} = 0.$$

(v) By direct computations, we have

$$\begin{aligned} &U_2V_1^{2^s} + U_1V_2^{2^s} \\ =&\Delta\left(a^{2^{m+s}}U^{2^m}(a^{2^{2m}}V^{2^{2m}})^{2^s} + a^{2^{2m+s}}U^{2^{2m}}(a^{2^m}V^{2^m})^{2^s}\right) \\ =&\Delta a^{2^{2m+s}+2^{m+s}}\left(UV^{2^{m+s}} + U^{2^m}V^{2^s}\right)^{2^m}, \end{aligned}$$

where $\Delta = v^{2^s+1}a^{2^{2m+2s+1}+2^{m+2s}+2^m}C^{2^{2m}}L(a)^{2^s}T^{2^s}$. Thus in order to prove $U_2V_1^{2^s}+U_1V_2^{2^s} \neq 0$, it suffices to show $UV^{2^{m+s}} + U^{2^m}V^{2^s} \neq 0$. If there exists some $a \in \mathbb{F}_{2^{3m}}^*$ such that $UV^{2^{m+s}} + U^{2^m}V^{2^s} = 0$, then $U = \gamma V^{2^s}$ for some $\gamma \in \mathbb{F}_{2^m}^*$. In addition, since $U = V^{2^{2m}} + \mu V$, we obtain

$$V^{2^{2m}} + \mu V + \gamma V^{2^s} = 0.$$

Let $\epsilon \in \mathbb{F}_{2^m}^*$ satisfy $\epsilon^{1-2^s} = \gamma$. Replacing V with ϵV in the above equation and multiplying both sides of the equation with ϵ^{-1}, we have $V^{2^{2m}} + \mu V + V^{2^s} = 0$. By raising the above equation to its 2^m-th power, we get

$$V^{2^{m+s}} + \mu^{2^m}V^{2^m} + V = 0,$$

which is impossible by Lemma 7 and the fact that L permutes $\mathbb{F}_{2^{3m}}$. □

Now we give the proof of Theorem 3.

Proof of Theorem 3. Since f is a quadratic function, it suffices to show that for any $a \in \mathbb{F}_{2^{3m}}^*$, the equation $f(az+a)+f(az)+f(a)=0$ has exactly two solutions $z \in \{0,1\}$ in $\mathbb{F}_{2^{3m}}$. More specifically, we need to show that the equation

$$\begin{aligned}&(L(az)+L(a))^{2^m+1} + L(az)^{2^m+1} + L(a)^{2^m+1} + v(az+a)^{2^m+1} + v(az)^{2^m+1} + va^{2^m+1}\\ =&Az^{2^{2m+s}} + Bz^{2^{m+s}} + Cz^{2^m} + Dz^{2^s} + Ez = 0\end{aligned} \tag{19}$$

where A, B, C, D, E are defined as in (11), has exactly two solutions $z \in \{0,1\}$. By Lemma 8 (i), we know $ABCDE \neq 0$ for any $a \in \mathbb{F}_{2^{3m}}^*$. Raising (19) to its 2^m-th power and its 2^{2m}-th power, we have

$$A^{2^m}z^{2^s} + B^{2^m}z^{2^{2m+s}} + C^{2^m}z^{2^{2m}} + D^{2^m}z^{2^{m+s}} + E^{2^m}z^{2^m} = 0 \tag{20}$$

and

$$A^{2^{2m}}z^{2^{m+s}} + B^{2^{2m}}z^{2^s} + C^{2^{2m}}z + D^{2^{2m}}z^{2^{2m+s}} + E^{2^{2m}}z^{2^{2m}} = 0, \tag{21}$$

respectively. In the following, we will use the method of elimination twice and finally acquire two equations (23) and (26).

After computing the summation of (19) multiplied by E^{2^m} and (20) multiplied by C and simplifying it, we get

$$(AE^{2^m} + B^{2^m}C)z^{2^{2m+s}} + C^{2^m+1}z^{2^{2m}} + (BE^{2^m} + CD^{2^m})z^{2^{m+s}} + (DE^{2^m} + A^{2^m}C)z^{2^s} + E^{2^m+1}z = 0. \tag{22}$$

By computing the summation of (21) multiplied by E^{2^m+1} and (22) multiplied by $C^{2^{2m}}$, we have

$$U_1z^{2^{2m+s}} + U_2z^{2^{m+s}} + U_3z^{2^s} + U_4z^{2^{2m}} = 0,$$

i.e.,

$$U_1z^{2^{2m+s}} + U_2z^{2^{m+s}} + U_3z^{2^s} = 0, \tag{23}$$

where U_i with $i = 1, 2, 3, 4$ are defined as in (12) and $U_4 = 0$ by Lemma 8 (iii).

After computing the summation of (19) multiplied by B^{2^m} and (20) multiplied by A and simplifying it, we get

$$AC^{2^m}z^{2^{2m}} + (B^{2^m+1} + AD^{2^m})z^{2^{m+s}} + (B^{2^m}C + AE^{2^m})z^{2^m} + (B^{2^m}D + A^{2^m+1})z^{2^s} + B^{2^m}Ez = 0. \tag{24}$$

By calculating the summation of (20) multiplied by $D^{2^{2m}}$ and (21) multiplied by B^{2^m}, we obtain

$$\begin{aligned}&(C^{2^m}D^{2^{2m}} + B^{2^m}E^{2^{2m}})z^{2^{2m}} + (D^{2^{2m}+2^m} + A^{2^{2m}}B^{2^m})z^{2^{m+s}} + D^{2^{2m}}E^{2^m}z^{2^m} + \\ &(A^{2^m}D^{2^{2m}} + B^{2^{2m}+2^m})z^{2^s} + B^{2^m}C^{2^{2m}}z = 0.\end{aligned} \tag{25}$$

Now computing the summation of (24) multiplied by $(D^{2^{2m}+2^m}+A^{2^{2m}}B^{2^m})$ and (25) multiplied by $(B^{2^m+1}+AD^{2^m})$, we have

$$V_1z^{2^{2m}} + V_2z^{2^m} + V_3z + V_4z^{2^s} = 0,$$

i.e.,

$$V_1^{2^s}z^{2^{2m+s}} + V_2^{2^s}z^{2^{m+s}} + V_3^{2^s}z^{2^s} = 0, \tag{26}$$

where V_i with $i = 1, 2, 3, 4$ are defined as in (12) and $V_4 = 0$ by Lemma 8 (iii).

Now the summation of (23) multiplied by $V_1^{2^s}$ and (26) multiplied by U_1 gives

$$\left(U_2V_1^{2^s} + V_2^{2^s}U_1\right)z^{2^{m+s}} + \left(U_3V_1^{2^s} + V_3^{2^s}U_1\right)z^{2^s} = 0,$$

i.e.,

$$\left(U_2V_1^{2^s} + V_2^{2^s}U_1\right)\left(z^{2^{m+s}} + z^{2^s}\right) = 0$$

since $U_2V_1^{2^s}+V_2^{2^s}U_1+U_3V_1^{2^s}+V_3^{2^s}U_1 = 0$ by Lemma 8 (iv). Moreover, by Lemma 8 (v), $U_2V_1^{2^s}+V_2^{2^s}U_1 \neq 0$ and thus $z^{2^{m+s}} + z^{2^s} = 0$. In other words, $z \in \mathbb{F}_{2^m}$. Plugging it into (19), we get

$$(C + E)(z^{2^s} + z) = 0.$$

By Lemma 8 (i), $C + E \neq 0$ and thus $z^{2^s} + z = 0$. Then $z \in \mathbb{F}_{2^{\gcd(m,s)}} = \mathbb{F}_2$.

In conclusion, Eq. (19) has only two solutions $z \in \{0, 1\}$ in $\mathbb{F}_{2^{3m}}$ for any $a \in \mathbb{F}_{2^{3m}}^*$ and then f is APN over $\mathbb{F}_{2^{3m}}$. □

Remark 9. The existence of the parameter $\mu \in \mathbb{F}_{2^{3m}}^*$ in Theorem 3 for any m is a crucial problem to the significance of the theorem. During the review process, by using techniques from algebraic varieties over finite fields, Bartoli et al. [1] proved that when $m \geq 3$, for the particular case $s = 1$, there always exists $\mu \in \mathbb{F}_{2^{3m}}^*$ satisfying $\mu^{2^{2m}+2^m+1} \neq 1$ such that $L(z) = z^{2^{m+s}} + \mu z^{2^s} + z$ permutes $\mathbb{F}_{2^{3m}}$. That is to say, Theorem 3 indeed always produces APN functions over $\mathbb{F}_{2^{3m}}$ for any positive integer $m \geq 3$.

5. Conclusion and further work

In this paper, we obtained two new infinite families of APN functions over $\mathbb{F}_{2^{2m}}$ and $\mathbb{F}_{2^{3m}}$. It is demonstrated that our APN families are CCZ-inequivalent to all known infinite families of APN functions by comparing their Γ-ranks over $\mathbb{F}_{2^8}$ or $\mathbb{F}_{2^9}$. Furthermore, it is worth mentioning that our two APN families cover two known sporadic APN functions over $\mathbb{F}_{2^8}$ and $\mathbb{F}_{2^9}$, which were found by Edel and Pott [21] in 2009 using the switching method and Beierle and Leander [3] in 2021 using a recursive tree search, respectively.

Note that the newly found APN family over $\mathbb{F}_{2^m}^2$ can be expressed using

$$f(z) = z^3 + Az^{3q} + Bz^{2q+1} + Cz^{q+2} + Dz^5 + Ez^{5q} + Fz^{4q+1} + Gz^{q+4} + Hz^{q+1} + Iz^{2(q+1)}$$

over $\mathbb{F}_{q^2}$ with $q = 2^m$. Thus the next question is whether it is possible to obtain new infinite families of APN functions over $\mathbb{F}_{q^2}$ of the above form, or more generally,

$$\begin{aligned} f(z) &= z(Az^2 + Bz^4 + Cz^q + Dz^{2q} + Ez^{4q}) + z^2(Gz^4 + Hz^q + Iz^{2q} + Jz^{4q}) \\ &\quad + z^4(Kz^q + Lz^{2q} + Mz^{4q}) + z^q(Nz^{2q} + Pz^{4q}) + Qz^{6q}, \end{aligned}$$

which was discussed in [10]. In addition, for the newly found APN family over $\mathbb{F}_{2^{3m}}$, it is important to study the CCZ-equivalence among the APN functions $f(z) = (z^{2^{m+s}} + \mu z^{2^s} + z)^{2^m+1} + vz^{2^m+1}$ with different parameters μ, s, v and to determine a lower bound on the number of CCZ-inequivalent APN functions over $\mathbb{F}_{2^{3m}}$ of this form.

Acknowledgment

The authors would like to thank deeply the Associate Editor Prof. Sihem Mesnager, and the anonymous referees for their valuable comments and suggestions that highly improved both the technical and the editorial qualities of this paper.

References

[1] Daniele Bartoli, Marco Calderini, Olga Polverino, and Ferdinando Zullo. On the infiniteness of a family of APN functions. *arXiv preprint*, https://arxiv.org/abs/2107.09164, 2021.

[2] Christof Beierle and Gregor Leander. New instances of quadratic APN functions in small dimension (version 2.1) [data set]. *Zenodo*, http://doi.org/10.5281/zenodo.4738942, 2021.

[3] Christof Beierle and Gregor Leander. New instances of quadratic APN functions. *IEEE Transactions on Information Theory*, https://doi.org/10.1109/TIT.2021.3120698, 2021.

[4] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.

[5] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system i: The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997.

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

[7] K. A. Browning, J. F. Dillon, R. E. Kibler, and M. T. McQuistan. APN polynomials and related codes. *Journal of Combinatorics, Information and System Science, Special Issue in honor of Prof. D.K Ray-Chaudhuri on the occasion of his 75th birthday*, 34(1-4):135–159, 2009.

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

[9] Lilya Budaghyan, Marco Calderini, and Irene Villa. On equivalence between known families of quadratic APN functions. *Finite Fields and Their Applications*, 66:101704, 2020.

[10] 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.

[11] 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.

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

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

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

[15] Marco Calderini, Lilya Budaghyan, and Claude Carlet. On known constructions of APN and AB functions and their relation to each other. *Matematičke Znanosti*, 25:79–105, 2021.

[16] Claude Carlet. *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2021.

[17] Benjamin Chase and Petr Lisoněk. Kim-type APN functions are affine equivalent to Gold functions. *Cryptography and Communications*, https://doi.org/10.1007/s12095-021-00490-2, 2021.

[18] Hans Dobbertin. Almost perfect nonlinear power functions on $\mathrm{GF}(2^n)$: The Niho case. *Information and Computer*, 151(1-2):57–72, 1999.

[19] Hans Dobbertin. Almost perfect nonlinear power functions on $\mathrm{GF}(2^n)$: The Welch case. *IEEE Transactions and Information Theory*, 45(4):1271–1275, 1999.

[20] Hans Dobbertin. Almost perfect nonlinear power functions on $\mathrm{GF}(2^n)$: a new case for n divisible by 5. In *Finite Fields and Applications*, pages 113–121. Springer, 2001.

[21] Yves Edel and Alexander Pott. A new almost perfect nonlinear function which is not quadratic. *Advance Mathematics Communications*, 3(1):59–81, 2009.

[22] 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.

[23] Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions

(corresp.). *IEEE Transactions on Information Theory*, 14(1):154–156, 1968.

[24] Faruk Göloğlu. Gold-hybrid functions. *Preprint*, 2020.

[25] Tadao Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. *Information and Control*, 18(4):369–394, 1971.

[26] Kangquan Li, Chunlei Li, Tor Helleseth, and Longjiang Qu. A complete characterization of the APN property of a class of quadrinomials. *IEEE Transactions on Information Theory*, 67(11):7535–7549, 2021.

[27] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Cambridge University Press, 1997.

[28] Kaisa Nyberg. Differentially uniform mappings for cryptography. In *Advances in Cryptology—EUROCRYPT*, pages 55–64. Springer, 1993.

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

[30] Kenneth S Williams. Note on cubics over $\mathrm{GF}(2^n)$ and $\mathrm{GF}(3^n)$. *Journal of Number Theory*, 7(4):361–365, 1975.

[31] Lijing Zheng, Haibin Kan, Yanjun Li, Jie Peng, and Deng Tang. Constructing new APN functions through relative trace functions. *arXiv preprint*, https://arxiv.org/abs/2101.11535, 2021.

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

Appendix

A. The MAGMA code in the proof of Theorem 2: In order to calculate the resultant of $F(x,y)$ and $G(x,y)$ for any $(a,b) \neq (1,1)$, we treat them as polynomials in indeterminates x, y, a, b. In this way, we have polynomials

$$\begin{cases} F(x,y,a,b) = ax^2 + \left(a^2+b^2+b\right)x + (a+b)y^2 + \left(a+b^2\right)y \\ G(x,y,a,b) = (a+b)x^4 + b^2x^2 + \left(a^4+b\right)x + by^4 + a^2y^2 + \left(a^4+a+b^4\right)y \end{cases}$$

Observe that the resultant of $F(x,y)$ and $G(x,y)$ with respect to y is the same as the resultant of $F(x,y,a,b)$ and $G(x,y,a,b)$ with respect to y over $\mathbb{F}_2$, where the indeterminates a, b take values from $\mathbb{F}_{2^m}$. In this way, we obtain the resultant of $F(x,y)$ and $G(x,y)$ with respect to y and further factorize it over $\mathbb{F}_2$ with the following Magma code:

```
P<x,y,a,b> := PolynomialRing(GF(2),4);
F := a*x^2+(a^2+b^2+b)*x+(a+b)*y^2+(a+b^2)*y;
G := (a+b)*x^4+b^2*x^2+(a^4+b)*x+b*y^4+a^2*y^2+(a^4+a+b^4)*y;
Res := Resultant(F,G,y);
Factorization(Res);
```

B. The MAGMA code in the proof of Lemma 8.

In the equation system (11), we assume that $a1 := a^{2^m}$, $a2 := a^{2^{2m}}$, $as := a^{2^s}$, $as1 := a^{2^{m+s}}$,

$as2 := a^{2^{2m+s}}$, $u := \mu$, $u1 := \mu^{2^m}$ and $u2 := \mu^{2^{2m}}$. Then A, B, C, D, E can be seen as polynomials in $\mathbb{F}_2[a, a1, a2, as, as1, as2, u, u1, u2, v]$. We also suppose $X1 := X^{2^m}$ and $X2 := X^{2^{2m}}$ for $X \in \{A, B, C, D, E\}$. Then we can use the following MAGMA code to compute the factorizations of the polynomials $U1, U2, U3, V1, V2, V3$.

```
P<a,a1,a2,as,as1,as2,u,u1,u2,v> := PolynomialRing(GF(2),10);
A   := (as1+u*as+a)*as2;
A1  := (as2+u1*as1+a1)*as;
A2  := (as+u2*as2+a2)*as1;
B   := (as2+u1*as1+a1+u1*(as1+u*as+a))*as1;
B1  := (as+u2*as2+a2+u2*(as2+u1*as1+a1))*as2;
B2  := (as1+u*as+a+u*(as+u2*as2+a2))*as;
C   := (as1+u*as+a+v*a)*a1;
C1  := (as2+u1*as1+a1+v*a1)*a2;
C2  := (as+u2*as2+a2+v*a2)*a;
D   := u*(as2+u1*as1+a1)*as;
D1  := u1*(as+u2*as2+a2)*as1;
D2  := u2*(as1+u*as+a)*as2;
E   := (as2+u1*as1+a1+v*a1)*a;
E1  := (as+u2*as2+a2+v*a2)*a1;
E2  := (as1+u*as+a+v*a)*a2;

U1  := D2*E1*E+A*C2*E1+B1*C2*C;
U2  := A2*E1*E+B*C2*E1+C2*C*D1;
U3  := B2*E1*E+C2*D*E1+A1*C2*C;
V1  := A2*A^2*C1+A*B*C1*D2+A*B1*B*E2+A^2*D1*E2;
V2  := A2*A^2*E1+A*B*D2*E1+A2*A*B1*C+A*C*D2*D1;
V3  := A2*A*B1*E+A*B1*B*C2+A^2*C2*D1+A*D2*D1*E;

Factorization(U1);
Factorization(U2);
Factorization(U3);
Factorization(V1);
Factorization(V2);
Factorization(V3);
```