

New infinite families of APN functions from the switching construction in even dimension

Tor Helleseeth, Nadiia Ichanska, Nikolay S. Kaleyski

University of Bergen

This work has been submitted to the IEEE for possible publication.

Copyright may be transferred without notice, after which this version may no longer be accessible.

Abstract—We present the first new infinite family of APN functions obtained by applying the switching construction to a known family since the introduction of the Budaghyan-Carlet-Leander family in 2009. Our construction is also the first example of an infinite APN family obtained via the switching construction from an infinite family of non-power functions. More generally, we study families of APN functions that can be obtained from the Budaghyan-Helleseeth-Kaleyski family by the addition of carefully selected perturbation terms. We perturb the known family by combinations of Frobenius conjugates of the relative norm and obtain four constructions, naturally arranged into two switching pairs. One of these families is EA-equivalent to the Li-Zhou-Li-Qu family, for which our construction yields a new univariate representation. Switching it by a norm-derived Boolean term produces a second family that we prove to be APN in every dimension where the base family is defined, and we show that this family is CCZ-inequivalent to all previously known constructions. Furthermore, we investigate two other infinite families that can be switched to one another, conjecture that they are APN for infinitely many dimensions, and obtain conditions that can be used to characterize their APN-ness. The new infinite APN family and the two conjectured APN families generalize previously known sporadic APN instances in dimension 10.

Index Terms—Almost perfect nonlinear (APN) function, vectorial Boolean function, differential uniformity, secondary construction, switching construction, CCZ-equivalence, ortho-derivative, finite field.

I. INTRODUCTION

Substitution boxes (S-boxes), or vectorial Boolean functions, are typically the only nonlinear components of most modern block ciphers. Their cryptographic properties determine the resistance of the entire cipher to various kinds of cryptanalytic attacks. Differential cryptanalysis, introduced by Biham and Shamir [1] and known as one of the most efficient attacks that can be employed against symmetric block ciphers, recovers information about a cipher by tracking how input differences propagate to output differences through the

cipher's S-boxes. The resistance of an S-box F to this attack is measured by its differential uniformity [2], which should be as low as possible. Over a field of characteristic two, this quantity is at least 2, and the functions attaining the bound are the *almost perfect nonlinear (APN)* functions, which offer the best possible resistance against differential attacks.

APN functions were introduced by Nyberg [2] and have been studied intensively ever since. For a long time, the only known examples were power functions x^d , including the Gold [3], Kasami [4], Welch [5] and Niho [6] mappings, and it was natural to ask whether every APN function is equivalent to a power function. Edel, Kyureghyan and Pott [7] answered this in the negative by exhibiting a quadratic APN function inequivalent to any power mapping. This construction was later generalized into the first infinite family of non-power quadratic APN polynomials [8]. It was subsequently followed by numerous other infinite families of quadratic APN polynomials [9], [10], [11], [12], [13], [14], [15], [16], [17]. Despite intense research over the past few decades, the structure and properties of APN functions are still not well understood, and finding new instances and constructions of APN functions remains a hard and active area of research. In particular, finding and investigating mathematical constructions of APN functions, which can shed more light on the subject, is a fundamental open problem in the area.

Methods for constructing APN functions can be divided into *primary* constructions, which produce APN functions directly, and *secondary* constructions, which build new APN functions from existing ones. Almost all of the known infinite families are primary constructions. Most known sporadic APN instances (that is, instances that can not be explained by the known infinite families), by contrast, have been obtained by computer search [18], [19], [20], [21]. Secondary constructions have also produced sporadic instances but rarely infinite families; the most influential secondary construction is the switching construction of Edel and Pott [22]. It

perturbs a given APN function F by adding a suitable Boolean function f multiplied by a constant c . The construction has yielded, among other results, the only known APN function on $\mathbb{F}_{2^6}$ that is inequivalent to both power functions and quadratic functions, as well as many instances of APN functions in dimensions seven and eight. In practice, the switching construction is used by constructing a system of linear equations based on the starting APN function F and the constant c that can be solved using linear algebra to determine the set of all Boolean functions f for which $F + cf$ is APN. In this sense, the switching construction can be used computationally to generate new APN functions starting from a given concrete APN function F .

Extending a secondary construction, such as the switching construction, to an *infinite* family is considerably harder. The perturbation term $cf(x)$ must be parametrized according to the dimension n , and a mathematical proof that the conditions of the switching construction are satisfied by this perturbation term must be given; it is no longer possible to solve a concrete system of linear equations since the construction must be generalized to work across infinitely many dimensions.

The only infinite families obtained in this way are those of Budaghyan, Carlet and Leander from 2009 [23], [24], in which the Gold function x^3 is perturbed by the trace term $\text{tr}_1^n(x^9)$. To the best of our knowledge, no further infinite constructions based on the switching method have been given since then. In this paper, we present the first such construction since [23].

More specifically, we present a secondary construction of infinite APN families in even dimension. Our starting point is the family of quadrinomials of Budaghyan, Helleseht and Kaleski (BHK) [15], which is APN over $\mathbb{F}_{2^n}$ for $n = 2m$ with m odd and $3 \nmid m$. We perturb these functions by adding terms derived from the relative norm $N(x) = x^{2^m+1} = x\bar{x}$ where $\bar{x} = x^{2^m}$. Since $N(x) \in \mathbb{F}_{2^m}$, its Frobenius conjugates $N(x)^{2^j}$ again lie in $\mathbb{F}_{2^m}$ and provide a structured set of perturbation terms whose total sum $\sum_{j=0}^{m-1} N(x)^{2^j} = \text{tr}_1^m(N(x))$ is Boolean-valued. Adding carefully chosen combinations of these terms to the BHK quadrinomials, we obtain the infinite families F_l, F_1, F_2 and F_3 over $\mathbb{F}_{2^n}$. We show that the family F_l is CCZ-equivalent to the one given in [14] by deriving an alternative univariate representation for the latter family. More importantly, we prove that the functions in F_1 are APN over $\mathbb{F}_{2^n}$ for all $n = 2m$ with $m \geq 5$ odd and $3 \nmid m$, and conjecture that the same is true for the functions in F_2 and F_3 . We support this conjecture with computational data for $n = 10, 14, 22, 26$. Furthermore,

we compute invariants for all functions in dimension $n = 10$ and demonstrate that the functions arising from F_1, F_2 and F_3 are CCZ-inequivalent to any previously known infinite family. At the same time, we observe that these functions are equivalent to some of the sporadic APN instances identified in [25], and therefore generalize them into infinite families.

The four families under investigation naturally form two switching pairs: F_l and F_1 differ by the Boolean function $\beta \text{tr}_1^m(N(x))$, while F_2 and F_3 differ by $\beta^2 \text{tr}_1^m(N(x))$, where β is a primitive element of $\mathbb{F}_4$. In particular, F_1 is obtained from F_l by a switching construction. To the best of our knowledge, we have presented the first new infinite APN family obtained by switching an existing infinite APN family since the construction of Budaghyan, Carlet and Leander [24], and the first new infinite APN family obtained by switching a family of non-power functions.

The remainder of the paper is organized as follows. Section II introduces the notation and recalls the necessary background, including the known infinite families of APN functions relevant to this work. In Section III, we present the new families, prove the APN-ness of F_1 , and establish the equivalence of F_l with the construction of [14]. In Section IV, we study the equivalence between the new families and previously known constructions via the differential spectra of their ortho-derivatives [26], and list representatives of the resulting equivalence classes.

II. PRELIMINARIES

Let n and m denote positive integers, $\mathbb{F}_2$ denote the finite field with two elements, and $\overline{\mathbb{F}}_2$ denote its algebraic closure. Let $\mathbb{F}_{2^n}$ be the finite field with 2^n element. We write $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus 0$ for its multiplicative group. Fixing an $\mathbb{F}_2$ -basis $(\alpha_1, \dots, \alpha_n)$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ allows us to identify the vector $v = (v_1, \dots, v_n) \in \mathbb{F}_2^n$ with the field element $v_1\alpha_1 + \dots + v_n\alpha_n$. We freely pass between the vector space representation $\mathbb{F}_2^n$ and the field representation $\mathbb{F}_{2^n}$. A mapping $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ is called an (n, m) -**function**, or a **vectorial Boolean function**. In the case $m = 1$, it is called a **Boolean function**. Due to the general nature of the definition, vectorial Boolean functions find applications in many areas across mathematics and computer science, and in particular are used as building blocks for symmetric block ciphers in cryptography, where they are referred to as S-boxes, or substitution boxes. Every such function admits a unique representation in **algebraic**

normal form (ANF) as

$$F(x_1, \dots, x_n) = \sum_{u \in \mathbb{F}_2^n} a_u \prod_{i=1}^n x_i^{u_i}, \quad a_u \in \mathbb{F}_2^m,$$

where $u = (u_1, \dots, u_n)$ runs through $\mathbb{F}_2^n$. The **algebraic degree** $\deg(F)$ is the maximum Hamming weight $\sum_{i=1}^n u_i$ among all monomials $\prod_{i=1}^n x_i^{u_i}$ with a nonzero coefficient a_u . Functions of algebraic degree at most 1 are called **affine**. Equivalently, they satisfy $F(x) + F(y) + F(z) = F(x+y+z)$ for all $x, y, z \in \mathbb{F}_2^n$. We call F **linear** if, in addition, $F(0) = 0$. Then clearly a function F is linear if and only if $F(x) + F(y) = F(x+y)$ for all $x, y \in \mathbb{F}_2^n$. Functions of degree 2 and degree 3 are called **quadratic** and **cubic**, respectively.

When $m = n$, any (n, n) -function can be seen as a mapping from $\mathbb{F}_2^n$ to itself. Any such mapping can be uniquely represented as a polynomial of degree at most $2^n - 1$ called the **univariate representation** of F :

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i, \quad a_i \in \mathbb{F}_2^n. \quad (1)$$

In terms of (1), the algebraic degree of F equals the largest binary weight $w_2(i)$ of an exponent i with $a_i \neq 0$. Throughout the remainder of the paper, we consider only (n, n) -functions. Consequently, the symbol m is no longer used for the output dimension and instead denotes the half-dimension whenever $n = 2m$.

The univariate form is not the only representation used in the study of APN functions. When $n = 2m$, fixing an $\mathbb{F}_2^m$ -basis of $\mathbb{F}_2^n$ identifies $\mathbb{F}_2^n$ with $\mathbb{F}_2^m \times \mathbb{F}_2^m$, and an (n, n) -function F then corresponds to a pair $\mathcal{F} = (f_1, f_2)$ of maps $f_1, f_2 : \mathbb{F}_2^m \times \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$. This is the **bivariate representation** of F [27]; it is the natural form for many known families in even dimension, and we use it in Section III to relate one of our families to a previously known one. Similarly, when $3 \mid n$, identifying $\mathbb{F}_2^n$ with $\mathbb{F}_{2^{n/3}}^3$ gives a **trivariate representation** [28]. Known APN families are commonly described in univariate, bivariate, or trivariate form. Since we work in dimension $n = 2m$ with $3 \nmid m$, and therefore $3 \nmid n$, we do not need to consider the trivariate families, since they are defined only in dimensions divisible by 3. We therefore list the relevant known families in univariate and bivariate form in Tables II–III. The algebraic degree, the differential uniformity, and the equivalence relations introduced below are preserved under these identifications.

Resistance against differential cryptanalysis [1] is measured by the behaviour of the derivatives of an S-box. For any function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$, its **derivative** in the direction $a \in \mathbb{F}_2^n \setminus \{0\}$ is $D_a F(x) = F(a+x) +$

$F(x)$. The **differential uniformity** δ_F of a function F is

$$\delta_F = \max_{a, b \in \mathbb{F}_2^n, a \neq 0} |\{x \in \mathbb{F}_2^n : D_a F(x) = b\}|.$$

Low differential uniformity corresponds to strong resistance against differential attacks. Since $D_a F(x) = D_a F(x+a)$ for every x , the solutions of $D_a F(x) = b$ occur in pairs $x, x+a$; hence $\delta_F \geq 2$. A vectorial Boolean function F with $\delta_F = 2$ is called **almost perfect nonlinear (APN)** [2] and therefore provides optimal resistance against differential attacks. We refer to [27] as a general reference to APN functions and their cryptographic properties.

In addition to the differential uniformity, one may consider the **differential spectrum**. For $a, b \in \mathbb{F}_2^n$ with $a \neq 0$, let $\delta_F(a, b) = |\{x \in \mathbb{F}_2^n : D_a F(x) = b\}|$. The differential spectrum of F is the multiset

$$\mathcal{D}_F = [\delta_F(a, b) : a, b \in \mathbb{F}_2^n, a \neq 0]. \quad (2)$$

Then $\mathcal{D}_F$ records the distribution of the number of solutions to $D_a F(x) = b$ over all nonzero input differences a and all output differences b . Clearly, the differential uniformity δ_F is simply the largest value in $\mathcal{D}_F$. Thus, the differential spectrum gives a more fine-grained description of the differential properties of F . We use the differential spectrum as an invariant for distinguishing inequivalent functions.

Due to their large number, (n, n) -functions are typically considered up to some suitable equivalence relation that preserves the properties of interest. Differential uniformity is preserved by several equivalence relations, so that a single function gives an entire class of functions sharing the same differential uniformity. For this reason, showing that an APN function is genuinely new requires demonstrating that it lies outside of the equivalence classes of the already known functions.

Let $F, F' : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$, then F and F' are

- **affine equivalent** (respectively **linear equivalent**) if $F' = A_1 \circ F \circ A_2$ for some affine (respectively linear) permutations A_1, A_2 of $\mathbb{F}_2^n$;
- **extended affine equivalent (EA-equivalent)** if $F' = A_1 \circ F \circ A_2 + A$ for some affine permutations A_1, A_2 and some affine mapping A of $\mathbb{F}_2^n$;
- **Carlet–Charpin–Zinoviev equivalent (CCZ-equivalent)** [29] if $\mathcal{A}(G_F) = G_{F'}$ for some affine permutation $\mathcal{A}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^n$, where $G_F = \{(x, F(x)) : x \in \mathbb{F}_2^n\}$ denotes the graph of F .

Currently, CCZ-equivalence is the most general non-trivial relation known to preserve the differential uniformity, and therefore classifications of APN functions are conventionally stated up to CCZ-equivalence.

A further notion that we need is that of a 3-to-1 function. Following [25], we call a mapping $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ satisfying $F(0) = 0$ a **3-to-1 function** if every nonzero value in its image has exactly three preimages. In even dimension, many known quadratic APN families admit a 3-to-1 representative. Expressing a function in this normalized form facilitates comparison with existing classifications and enables faster equivalence testing using the algorithms developed in [30].

All functions constructed in this paper are quadratic. Two features make quadratic functions considerably more tractable than functions of higher algebraic degree. The first is a collapse of the equivalence hierarchy: by a result of Yoshiara [31], two quadratic APN functions are CCZ-equivalent precisely when they are EA-equivalent. The second is the linearity of the symmetric derivative. The **symmetric derivative** of $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ in direction $a \in \mathbb{F}_{2^n}$ is

$$\Delta_a F(x) = F(x+a) + F(x) + F(a) + F(0). \quad (3)$$

For any fixed $a \in \mathbb{F}_{2^n}^*$, we clearly have $\Delta_a F(x) = D_a F(x) + D_a F(0)$, and since $D_a F(0)$ is a constant that does not depend on x , the differential uniformity of F can be equivalently expressed using $\Delta_a F(x)$ instead of $D_a F(x)$. The advantage of using $\Delta_a F(x)$ is that $\Delta_a F(0) = 0$, so that when F is quadratic, $\Delta_a F(x)$ is a linear function (instead of just affine), which significantly simplifies the analysis of the differential uniformity.

Quadratic APN functions can be associated with a distinguished companion function, which is the sharpest invariant currently available in practice [26]. Let $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ be quadratic and APN. The **ortho-derivative** of F is the map $\pi_F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ determined by $\pi_F(0) = 0$ and, for $a \neq 0$, by $\pi_F(a) \neq 0$ together with

$$\pi_F(a) \cdot (F(x) + F(x+a) + F(a) + F(0)) = 0, \quad (4)$$

for all $x \in \mathbb{F}_{2^n}$, where $\cdot$ is the canonical inner product on $\mathbb{F}_2^n$. The mapping π_F is well-defined and unique: the kernel of $\Delta_a F$ has dimension one, so its image is a hyperplane of $\mathbb{F}_2^n$ and admits a unique non-zero orthogonal vector. Canteaut, Couvreur and Perrin [26] showed that EA-equivalent quadratic APN functions have affine equivalent ortho-derivatives; together with [31], this means that every affine invariant of π_F yields a CCZ-invariant of F . We exploit this in Section IV through the **ortho-derivative differential spectrum (ODDS)** $\mathcal{D}_{\pi_F}$, i.e., the differential spectrum of the ortho-derivative of F . This is inexpensive to compute; it separates the known classes of quadratic APN functions in the dimensions of interest, and distinct spectra certify

CCZ-inequivalence. All computational results reported below were obtained with Magma [32].

While sporadic instances of APN functions can be obtained over a concrete finite field $\mathbb{F}_{2^n}$ (for a specific value of n) using computational searches, this is typically only feasible for small values of n in practice. Finding mathematical constructions of APN functions, especially so-called infinite families that can provide the exact form of APN functions for infinitely many dimensions n , has thus become an active area of research and has generated significant interest and engagement in the research community. Multiple infinite families have been identified over the past decades (as shown in Tables I, II and III), but finding new families remains an open problem, and a rather hard one at that.

Mathematical constructions of APN functions (as with other types of functions and mathematical objects) can broadly be divided into two categories. A **primary construction** exhibits a function – typically an explicit polynomial – and establishes its APN property directly, without reference to any previously known function. The vast majority of known infinite APN families fall into this category, as shown in Tables I, II, III.

A **secondary construction**, on the other hand, produces APN functions from one or more functions that are already known to be APN. We emphasize that the term does not refer to a universal APN-preserving transformation: apart from equivalence transformations, no general method is known that produces a new APN function from an arbitrary APN function without imposing additional conditions on the starting function or on the transformation. Known secondary constructions therefore exploit particular structural properties of the functions involved, and the APN property of the resulting function must be established under the corresponding conditions. Examples include the switching construction [22], [23], the isotopic shift [33], and constructions of APN functions from bent functions [34].

Such constructions have been successfully used computationally to obtain sporadic APN instances from given ones in fixed dimensions, but their application to infinite families is much more limited. To the best of our knowledge, the only previously known infinite APN family obtained by switching an existing infinite family is $F(x) = x^3 + a^{-1} \text{Tr}_n(a^3 x^9)$ constructed from the Gold function x^3 by the addition of the Boolean function $\text{Tr}_n(a^3 x^9)$ [23]; this is given as family F4 in Table II. In this paper, we apply the switching approach to an infinite polynomial APN family and obtain, to the best of our knowledge, the first new infinite APN family produced by switching an infinite family other

than a power function.

Tables I, II and III present, respectively, the monomial, univariate and bivariate constructions of APN functions known at the time of writing. We note that as of very recently, trivariate constructions have also been introduced [28]. Since trivariate constructions by definition can only be applied to finite fields $\mathbb{F}_{2^n}$ where n is a multiple of 3, and since the families discussed in this paper are defined only for dimensions n that are not divisible by 3, we omit them in this survey.

We now describe the switching construction. Two functions $F, F' : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ are called **switching neighbours** if their sum takes values in a one-dimensional $\mathbb{F}_2$ -subspace of $\mathbb{F}_{2^n}$, i.e. if $F'(x) = F(x) + uf(x)$ for some $u \in \mathbb{F}_{2^n}^*$ and some Boolean function $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$. Searching for Boolean functions f that keep F' APN has been remarkably successful in small dimensions: it produced the only APN function on $\mathbb{F}_{2^6}$ known to be CCZ-inequivalent both to power functions and to quadratic functions [22], and it accounts for a substantial share of the sporadic instances catalogued in dimensions seven and eight [7], [41], [20], [21]. Extending the method to infinite families is far harder, because the perturbation f must be constructed and characterized simultaneously for all n . Until now, the only infinite family obtained by switching is that of Budaghyan, Carlet and Leander [23]; see family F4 in Table II. Since this result is the direct source of inspiration for the present work, we state the basic form of family F4.

Theorem 1 ([23], [24]). *For every positive integer n , the function*

$$F(x) = x^3 + \text{tr}_1^n(x^9) \quad (5)$$

is APN over $\mathbb{F}_{2^n}$, and for $n \geq 7$ it is CCZ-inequivalent to the Gold function x^3 .

The Gold function x^3 is perturbed by a trace term. Here and throughout, $\text{tr}_1^n(x) = \sum_{j=0}^{n-1} x^{2^j}$ denotes the absolute trace function from $\mathbb{F}_{2^n}$ onto $\mathbb{F}_2$. As $\text{tr}_1^n(x^9)$ is Boolean, (5) is precisely a switching neighbour of x^3 with $u = 1$.

We close this section by recalling the families to which we apply the switching construction.

The Budaghyan, Helleseht and Kaleycki (BHK) [15] family, listed as F11 in Table II, is given in univariate representation and consists of two sub-cases, G_1 and G_2 , depending on the choice of the parameter i . While the two cases produce CCZ-equivalent functions for $n = 10$, applying the construction to higher dimensions results in G_1 and G_2 that are CCZ-inequivalent to one another.

Theorem 2 ([15]). *Let $n = 2m$, where m is an odd positive integer with $3 \nmid m$, let $\bar{x} = x^{2^m}$, and let β be a primitive element of $\mathbb{F}_4$. Then the quadrimonomials*

$$G_1(x) = x^3 + \beta x^{2^i+1} + \beta^2 \bar{x}^3 + \bar{x}^{2^i+1}, \quad i = m - 2, \quad (6)$$

$$G_2(x) = x^3 + \beta x^{2^i+1} + \beta^2 \bar{x}^3 + \bar{x}^{2^i+1}, \quad i = (m - 2)^{-1}, \quad (7)$$

are APN over $\mathbb{F}_{2^n}$.

Another infinite family of APN functions, introduced in [14] and listed as F19 in Table III, is given in bivariate representation. We denote this family by $\mathcal{F}_{l_0}$.

Theorem 3. [14] *Let m be a positive integer with $3 \nmid m$. Then the function $\mathcal{F}_{l_0} : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \rightarrow \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ defined by the bivariate representation*

$$(x^3 + xy^2 + y^3 + xy, x^5 + x^4y + y^5 + xy + x^2y^2) \quad (8)$$

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

One of the families that we construct turns out to be EA-equivalent to (8), which we establish in Theorem 4 by deriving a univariate representation of $\mathcal{F}_{l_0}$; the remaining families are shown in Section IV to be CCZ-inequivalent to all known ones.

III. NEW INFINITE FAMILIES OF APN FUNCTIONS DERIVED VIA PERTURBATIONS OF KNOWN FAMILIES

In this section, we construct new families obtained as perturbations of a Budaghyan–Helleseht–Kaleycki (BHK) APN function by means of carefully selected norm-derived terms x^{2^m+1} . We prove that two of them are APN (one of which is equivalent to a previously known family, while the other one is completely new). For the remaining two families, we derive conditions that can be used to characterize their APN-ness, and we computationally verify that they are APN for all admissible dimensions up to 26.

A. Infinite families built on $G_1(x)$

Let $m \geq 5$ be a positive odd integer, such that $3 \nmid m$. Consider a finite field $\mathbb{F}_{2^n}$ with 2^n elements, where $n = 2m$. Consider the APN function $G_1(x)$ (6), i.e. BHK for $i = m - 2$.

Let $N(x) = x^{2^m+1}$ be the norm map from $\mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^m}$. Since $N(x) \in \mathbb{F}_{2^m}$, its Frobenius conjugates

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	[3], [2]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	$i + 1$	[35], [4]
Welch	$2^t + 3$	$n = 2t + 1$	3	[5]
Niho	$2^t + 2^{t/2} - 1, t \text{ even}$ $2^t + 2^{(3t+1)/2} - 1, t \text{ odd}$	$n = 2t + 1$	$(t+2)/2$ $t + 1$	[6]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$	[36], [2]
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	$i + 3$	[37]

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

ID	Functions	Conditions	Source
F1-F2	$x^{2^s+1} + u^{2^k-1}x^{2^{i^k}+2^{m^k+s}}$	$n = pk, \gcd(k, 3) = \gcd(s, 3k) = 1, p \in \{3, 4\}, i = sk \bmod p, m = p - i, n \geq 12, u \text{ primitive in } \mathbb{F}_{2^n}^*$	[9]
F3	$sx^{q+1} + x^{2^i+1} + x^{q(2^i+1)} + cx^{2^i q+1} + c^q x^{2^i+q}$	$q = 2^m, n = 2m, \gcd(i, m) = 1, c \in \mathbb{F}_{2^n}, s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q, X^{2^i+1} + cX^{2^i} + c^q X + 1 \text{ has no solution } x \text{ s.t. } x^{q+1} = 1$	[10]
F4	$x^3 + a^{-1} \text{Tr}_n(a^3 x^9)$	$a \neq 0$	[23]
F5	$x^3 + a^{-1} \text{Tr}_3^n(a^3 x^9 + a^6 x^{18})$	$3 n, a \neq 0$	[24]
F6	$x^3 + a^{-1} \text{Tr}_3^n(a^6 x^{18} + a^{12} x^{36})$	$3 n, a \neq 0$	[24]
F7-F9	$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} + vx^{2^{-k}+1} + wu^{2^{k+1}}x^{2^s+2^{k+s}}$	$n = 3k, \gcd(k, 3) = \gcd(s, 3k) = 1, v, w \in \mathbb{F}_{2^k}, vw \neq 1, 3 (k+s), u \text{ primitive in } \mathbb{F}_{2^n}^*$	[11]
F10	$a^2 x^{2^{2m+1}+1} + b^2 x^{2^{m+1}+1} + ax^{2^{2m}+2} + bx^{2^m+2} + (c^2 + c)x^3$	$n = 3m, m \text{ odd}, L(x) = ax^{2^{2m}} + bx^{2^m} + cx \text{ satisfies the conditions of Lemma 8 of [33]}$	[33]
F11	$x^3 + a(x^{2^i+1})^{2^k} + bx^{3 \cdot 2^m} + c(x^{2^{i+m}+2^m})^{2^k}$	$n = 2m = 10, (a, b, c) = (\beta, 1, 0, 0), i = 3, k = 2, \beta \text{ primitive in } \mathbb{F}_{2^2}$ $n = 2m, m \text{ odd}, 3 \nmid m, (a, b, c) = (\beta, \beta^2, 1), \beta \text{ primitive in } \mathbb{F}_{2^2}, i \in \{m-2, m, 2m-1, (m-2)^{-1} \bmod n\}$	[15]
F12	$a \text{tr}_m^n(bx^{2^i+1}) + a^q \text{tr}_m^n(cx^{2^s+1})$	$n = 2m, m \text{ odd}, q = 2^m, a \notin \mathbb{F}_q, \gcd(i, n) = 1, i, s, b, c \text{ satisfy the conditions of Theorem 2}$	[17]
F13	$L(z)^{2^{m+1}} + vz^{2^{m+1}}$	$\gcd(s, m) = 1, v \in \mathbb{F}_{2^m}^*, \mu \in \mathbb{F}_{2^{3m}}^*, L(z) = z^{2^{m+s}} + \mu z^{2^s} + z \text{ permutes } \mathbb{F}_{2^{3m}}$	[14]

provide a natural source of structured perturbation terms. Define

$$P_1(x) = \beta \sum_{j=1}^{m-3} N^{2^j}(x) + N^{2^{m-2}}(x) + N^{2^{m-1}}(x),$$

$$P_0(x) = \beta N(x) + \beta^2 N^{2^{m-2}}(x) + \beta^2 N^{2^{m-1}}(x),$$

where β is a primitive element of $\mathbb{F}_4$. Using these auxiliary functions, we construct the following infinite families of APN functions:

$$F_1(x) = G_1(x) + P_1(x), \quad (9)$$

$$F_l(x) = G_l(x) + P_0(x). \quad (10)$$

We prove that $F_1(x)$ is an infinite family of APN functions CCZ-inequivalent to any known ones so far. Meanwhile, $F_l(x)$ is contained in the family from

Theorem 3 introduced in [14]. In order to see this, we first derive a univariate representation of that family.

Lemma 1. *Let m be an odd integer such that $3 \nmid m$. The function $\mathcal{F}_L(x, y) = (x^3 + xy^2 + y^3 + xy, x^5 + x^4y + y^5 + xy + x^2y^2)$ (8) from Theorem 3 admits the following univariate representation over $\mathbb{F}_{2^{2m}}$ with respect to the basis $(1, \beta)$:*

$$F_{l_0}(X) = \beta^2 X^3 + \beta \bar{X}^3 + \beta^2 X \bar{X}^4 + X^4 \bar{X} + \beta^2 X \bar{X} + \beta X^2 \bar{X}^2 + X^2 + X^4 + \beta \bar{X}^2 + \beta^2 \bar{X}^4, \quad (11)$$

where $\bar{x} = x^{2^m}$, and β is a primitive element of $\mathbb{F}_4$.

Proof. Since m is odd, the field $\mathbb{F}_4$ is not contained in $\mathbb{F}_{2^m}$, and therefore $(1, \beta)$ forms a basis of $\mathbb{F}_{2^{2m}}$ over $\mathbb{F}_{2^m}$. Using the standard basis transformation $x = X + \bar{X}$, $y = \beta X + \beta^2 \bar{X}$ together with the identities

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

ID	Functions	Conditions	Source
F14	$(xy, x^{2^k+1} + \alpha y^{(2^k+1)2^i})$	$\gcd(k, m) = 1, m \text{ even}, \alpha \text{ not a cube}$	[38]
F15	$(xy, x^{2^{2m}+2^{3m}} + ax^{2^{2m}}y^{2^m} + by^{2^m+1})$	$x^{2^m+1} + ax + b \text{ has no root in } \mathbb{F}_{2^m}$	[12]
F16	$(xy, x^{2^i+1} + x^{2^{i+m/2}}y^{2^{m/2}} + bxy^{2^i} + cy^{2^i+1})$	$(cx^{2^i+1} + bx^{2^i} + 1)^{2^{m/2}+1} + x^{2^{m/2}+1} \text{ has no roots in } \mathbb{F}_{2^m}$	[39]
F17	$(x^{2^i+1} + xy^{2^i} + y^{2^i+1}, x^{2^{2i}+1} + x^{2^{2i}}y + y^{2^{2i}+1})$	$\gcd(3i, m) = 1$	[13]
F18	$(x^{2^i+1} + xy^{2^i} + y^{2^i+1}, x^{2^{3i}}y + xy^{2^{3i}})$	$\gcd(3i, m) = 1, m \text{ odd}$	[13]
F19	$(x^3 + xy^2 + y^3 + xy, x^5 + x^4y + y^5 + xy + x^2y^2)$	$\gcd(3, m) = 1$	[14]
F20	$(x^{q+1} + By^{q+1}, x^ry + \frac{a}{B}xy^r)$	$0 < k < m, q = 2^k, r = 2^{k+m/2}, m \equiv 2 \pmod{4}, \gcd(k, m) = 1, a \in \mathbb{F}_{2^{m/2}}^*, B \in \mathbb{F}_{2^m}, B \text{ not a cube}, B^{q+r} \neq a^{q+1}$	[40]
F21	$(x^{q+1} + xy^q + \alpha y^{q+1}, x^{q^2+1} + \alpha x^{q^2}y + (1+\alpha)^q xy^{q^2} + \alpha y^{q^2+1})$	$k, m > 0, \gcd(k, m) = 1, q = 2^k, \alpha \in \mathbb{F}_{2^m}, x^{q+1} + x + \alpha \text{ has no roots in } \mathbb{F}_{2^m}$	[16]
F22	$(x^3 + xy + xy^2 + \alpha y^3, x^5 + xy + \alpha x^2y^2 + \alpha x^4y + (1+\alpha)^2 xy^4 + \alpha y^5)$	$\alpha \in \mathbb{F}_{2^m}, x^3 + x + \alpha \text{ has no roots in } \mathbb{F}_{2^m}$	[16]

$\beta + \beta^2 = 1, \beta^3 = 1$, we rewrite $\mathcal{F}_L$ in univariate form over $\mathbb{F}_{2^{2m}}$:

$$\begin{aligned}
F_{l_0}(X) &= (X + \bar{X})^3 + (X + \bar{X})(\beta X + \beta^2 \bar{X})^2 + \\
&\quad + (\beta X + \beta^2 \bar{X})^3 + (X + \bar{X})(\beta X + \beta^2 \bar{X}) + \\
&\quad + \beta((X + \bar{X})^5 + (X + \bar{X})^4(\beta X + \beta^2 \bar{X}) + \\
&\quad + (\beta X + \beta^2 \bar{X})^5 + (X + \bar{X})(\beta X + \beta^2 \bar{X}) + \\
&\quad + (X + \bar{X})^2(\beta X + \beta^2 \bar{X})^2); \\
F_{l_0}(X) &= \beta^2 X^3 + \beta \bar{X}^3 + \beta^2 X \bar{X}^4 + X^4 \bar{X} + \\
&\quad + \beta^2 X \bar{X} + \beta X^2 \bar{X}^2 + X^2 + X^4 + \beta \bar{X}^2 + \beta^2 \bar{X}^4.
\end{aligned}$$

□

Using this univariate representation, we can now establish the following EA-equivalence.

Theorem 4. *Let $m \geq 5$ be an odd integer such that $3 \nmid m$, and let $n = 2m$. Let $F_l, F_{l_0} : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ be defined as in (10) and (11), respectively. Then F_l and F_{l_0} are EA-equivalent, more precisely*

$$\begin{aligned}
L_1(F_l) + L_2 &= F_{l_0}, \text{ where} \\
L_1 &= \beta x + x^4 + \beta^2 \bar{x} + \beta^2 \bar{x}^4, \\
L_2 &= x^2 + x^4 + \beta \bar{x}^2 + \beta^2 \bar{x}^4.
\end{aligned}$$

Proof. The maps L_1 and L_2 are linearized polynomials over $\mathbb{F}_{2^n}$. Thus, they define $\mathbb{F}_2$ -linear maps on $\mathbb{F}_{2^n}$, and it is enough to show that L_1 has a trivial kernel and that the stated identity holds.

Let $q = 2^m$. Since m is odd, $\mathbb{F}_4 \not\subseteq \mathbb{F}_q$ and $(1, \beta)$ is a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$, every $X \in \mathbb{F}_{q^2}$ can be written uniquely as $X = a + \beta b$, where $a, b \in \mathbb{F}_q$. We can therefore write L_1 as

$$\begin{aligned}
L_1(X) &= \beta X + X^4 + \beta^2 \bar{X} + \beta^2 \bar{X}^4 = \beta(a + \beta b) + \\
&\quad + (a + \beta b)^4 + \beta^2(a + \beta^2 b) + \beta^2(a + \beta^2 b)^4.
\end{aligned}$$

Using $\beta^3 = 1$ and $\beta + \beta^2 = 1$, we obtain

$$\begin{aligned}
L_1(X) &= \beta a + \beta^2 b + a^4 + \beta b^4 + \beta^2 a + \beta b + \\
&\quad + \beta^2 a^4 + \beta b^4 = a + b + \beta^2 a^4.
\end{aligned}$$

Suppose now that $X \in \ker(L_1)$. Then $a + b + \beta^2 a^4 = 0$, or equivalently, $a + b + a^4 + \beta a^4 = 0$. Since $a + b + a^4 \in \mathbb{F}_q$ and $a^4 \in \mathbb{F}_q$, with the basis $(1, \beta)$ both coefficients must vanish:

$$a + b + a^4 = 0, a^4 = 0.$$

Thus $a = 0$, and then $b = 0$. Hence $X = 0, \ker(L_1) = \{0\}$, and L_1 is a linear permutation of $\mathbb{F}_{2^n}$.

It remains to verify that $L_1(F_l) + L_2$ equals F_{l_0} .

We use that $F_l = G_1(x) + P_0(x)$, where

$$G_1(x) = x^3 + \beta x^{2^{m-2}+1} + \beta^2 \bar{x}^3 + \overline{\beta^2 \bar{x}^{2^{m-2}+1}}, \text{ and}$$

$$P_0 = \beta N(x) + \beta^2 N(x)^{2^{m-2}} + \beta^2 N(x)^{2^{m-1}}.$$

Denote $N := N(x)$, then

$$\begin{aligned} L_1(P_0(x)) &= \beta^2 N + N^{2^{m-2}} + N^{2^{m-1}} + \beta N^4 + \\ &\quad + \beta^2(N^{2^m} + N^{2^{m+1}}) + \beta N + N^{2^{m-2}} + N^{2^{m-1}} + \\ &\quad + \beta N^4 + N^{2^m} + N^{2^{m+1}} = \beta^2 N + \beta N^2; \\ L_1(G_1(x)) &= \beta x^3 + \beta^2 x^{2^{m-2}+1} + \bar{x}^3 + \beta \bar{x}^{2^{m-2}+1} + \\ &\quad + x^{12} + \beta \bar{x} x^4 + \beta^2 \bar{x}^{12} + \bar{x}^4 x + \beta^2 \bar{x}^3 + \beta \bar{x}^{2^{m-2}+1} + \\ &\quad + x^3 + \beta^2 x^{2^{m-2}+1} + \beta^2 \bar{x}^{12} + \beta \bar{x}^4 x + x^{12} + \beta^2 \bar{x} x^4 = \\ &= \beta^2 x^3 + \beta \bar{x}^3 + \bar{x} x^4 + \beta^2 \bar{x}^4 x. \end{aligned}$$

Hence, $L_1(G_1(x) + P_0(x)) = L_1(F_l(x)) =$

$$= \beta^2 x^3 + \beta \bar{x}^3 + \beta^2 \bar{x}^4 x + \bar{x} x^4 + \beta^2 N(x) + \beta N^2(x),$$

and $L_1(F_l(x)) + L_2(x) = F_{l_0}(x)$. Therefore F_{l_0} and F_l are EA-equivalent. $\square$

Theorem 4 shows that F_l and F_{l_0} are EA-equivalent. Since the APN property is preserved under CCZ-equivalence, and EA-equivalence is a special case of CCZ-equivalence, we obtain the following corollary.

Corollary 1. *Let $m \geq 5$ be an odd integer such that $3 \nmid m$, let $n = 2m$, and let $i = m - 2$. Let β be a primitive element of $\mathbb{F}_4$. Then the function*

$$\begin{aligned} F_l(x) &= x^3 + \beta x^{2^i+1} + \beta^2 \bar{x}^3 + \bar{x}^{2^i+1} + \beta N(x) + \\ &\quad + \beta^2 N^{2^{m-2}}(x) + \beta^2 N^{2^{m-1}}(x), \end{aligned} \quad (12)$$

where $\bar{x} = x^{2^m}$, and $N(x) = x\bar{x}$, is APN over $\mathbb{F}_{2^n}$.

Now, when we have shown that F_l is APN, we need the following auxiliary lemmas to prove the same for F_1 .

Since m is odd, $3 \nmid (2^m - 1)$, cubing is a bijection of $\mathbb{F}_{2^m}^*$, and $\beta, \beta^2 \notin \mathbb{F}_{2^m}^*$.

Lemma 2. *Let $c \in \mathbb{F}_{2^m}^*$, $f(X) = X^3 + X + c \in \mathbb{F}_{2^m}[X]$, and let $T^2 + cT + 1$ be its resolvent, with roots τ, τ^{-1} (whose product is 1 by Viète's formula) in $\mathbb{F}_2$. If f has a root in $\mathbb{F}_{2^m}$, then τ is a cube in $\mathbb{F}_{2^{2m}}^*$.*

Proof. Let $X_0 \in \mathbb{F}_{2^m}$ be a root of f , and let Y be a root of $T^2 + X_0T + 1$. Then Y^{-1} is also a root of the quadratic since its constant term is 1, and the two roots have product 1. Their sum is X_0 , therefore

$$X_0^3 + X_0 = (Y + Y^{-1})^3 + (Y + Y^{-1}) = Y^3 + Y^{-3}.$$

Since X_0 is a root of f , we get $Y^3 + Y^{-3} = c$, meaning that Y^3 is a root of the resolvent $T^2 + cT + 1$, hence $Y^3 \in \{\tau, \tau^{-1}\}$. Thus τ or τ^{-1} is the cube of $Y \in \mathbb{F}_{2^{2m}}^*$. Since τ and τ^{-1} are simultaneously cubes or non-cubes, τ is a cube in $\mathbb{F}_{2^{2m}}^*$. $\square$

Lemma 3. *Let $n = 2m$ with m odd and $3 \nmid m$. Then for every $a \in \mathbb{F}_{2^n}^*$,*

$$\beta^2 a^3 + \beta \bar{a}^3 + a\bar{a} + 1 \neq 0. \quad (13)$$

Proof. Since $\gcd(2^m - 1, 2^m + 1) = 1$, the group $\mathbb{F}_{2^n}^*$ is the internal direct product of the unit circle $\mathcal{U}$ and $\mathbb{F}_{2^m}^*$; accordingly, write $a = \nu\mu$ with $\nu \in \mathcal{U}$ and $\mu \in \mathbb{F}_{2^m}^*$. Then $\bar{a} = \nu^{-1}\mu$, and (13) becomes

$$\begin{aligned} &(\beta^2 \nu^3 + \beta \bar{\nu}^3) \mu^3 + \mu^2 + 1 = 0, \\ &\left(\frac{1}{\mu}\right)^3 + \frac{1}{\mu} + \beta^2 \nu^3 + \beta \bar{\nu}^3 = 0. \end{aligned}$$

Set $X := \frac{1}{\mu} \in \mathbb{F}_{2^m}$, and $c := \beta^2 \nu^3 + \beta \bar{\nu}^3$. A cubic $X^3 + X + c = 0$ has roots iff its resolvent $T^2 + cT + 1$ admits $\beta^2 \nu^3$ as a root, since $\beta^2 \nu^3 + (\beta^2 \nu^3)^{-1} = c$. According to Lemma 2, the polynomial $X^3 + X + c = 0$ has a root in $\mathbb{F}_{2^m}$ if and only if $\beta^2 \nu^3$ is a cube in $\mathbb{F}_{2^m}^*$. Since $3 \nmid m$, the latter never occurs. $\square$

We are now ready to prove the APN-ness of the functions F_1 . We consider F_1 and F_l as switching neighbours of one another, and verify that the conditions for preserving APN-ness are preserved.

Theorem 5. *Let $m \geq 5$ be an odd integer such that $3 \nmid m$, $n = 2m$, and $i = m - 2$. Let β be a primitive element of $\mathbb{F}_4$. Then the function*

$$\begin{aligned} F_1(x) &= x^3 + \beta x^{2^i+1} + \beta^2 \bar{x}^3 + \bar{x}^{2^i+1} + \\ &\quad + \beta \sum_{j=1}^{m-3} N^{2^j}(x) + N^{2^{m-2}}(x) + N^{2^{m-1}}(x), \end{aligned} \quad (14)$$

where $\bar{x} = x^{2^m}$, and $N(x) = x\bar{x}$, is APN over $\mathbb{F}_{2^n}$.

Proof. Let $A = A(a, x) = a^3(x^2 + x)$, $B = B(a, x) = a^{2^i+1}(x^{2^i} + x)$, and $C = C(a, x) = a^{2^m+1}(x^{2^m} + x)$, where $i = m - 2$. For $a \in \mathbb{F}_{2^n}^*$, denote by $\Delta_a F(x) = F(ax) + F(ax + a) + F(a)$ the derivative of F in direction a . Then, the corresponding derivatives of the functions F_l and F_1 are

$$\begin{aligned} \Delta_a F_l(x) &= A + \beta B + \beta^2 \bar{A} + \bar{B} + \beta C + \\ &\quad + \beta^2 (C^{2^{m-2}} + C^{2^{m-1}}), \end{aligned} \quad (15)$$

$$\begin{aligned} \Delta_a F_1(x) &= A + \beta B + \beta^2 \bar{A} + \bar{B} + \beta C + \\ &\quad + \beta^2 (C^{2^{m-2}} + C^{2^{m-1}}) + \beta \text{tr}_1^m(C). \end{aligned} \quad (16)$$

Since $C \in \mathbb{F}_{2^m}$, we have $\text{tr}_1^m(C) \in \mathbb{F}_2$.

Let $\text{tr}_1^m(C) = 0$, then $\Delta_a F_l(x) = \Delta_a F_1(x)$. Since F_l is APN (Corollary 1), we know that $\Delta_a F_l(x) = 0$ has at most two solutions for all $a \in \mathbb{F}_{2^n}^*$.

Let $\text{tr}_1^m(C) = 1$, then $\Delta_a F_1(x) = 0$ is equivalent to $\Delta_a \overline{F_1}(x) = \beta$, i.e.

$$A + \beta B + \beta^2 \overline{A} + \overline{B} + \beta C + \beta^2 (C^{2^{m-2}} + C^{2^{m-1}}) = \beta. \quad (17)$$

Since $\Delta_a F_l$ is linear and F_l is APN, every preimage has size at most two. Hence, equation (17) also has at most two solutions (which makes at most 4 solutions for $\Delta_a F_1$ in total). Therefore, F_1 can fail to be APN only if there exist solutions of (17) satisfying $\text{tr}_1^m(C) = 1$.

Using the decomposition of (17) with respect to the basis $\{1, \beta\}$ of $\mathbb{F}_{2^{2m}}$ over $\mathbb{F}_{2^m}$, we obtain

$$\begin{cases} C = \beta^2 A + \beta \overline{A} + 1, \\ \beta^2 B + \beta \overline{B} = C^{2^{m-2}} + C^{2^{m-1}}. \end{cases} \quad (18)$$

Raising the second equation to the fourth power yields

$$\begin{cases} \beta^2 A + \beta \overline{A} + C = 1, \\ \beta^2 B^4 + \beta \overline{B}^4 = C + C^2. \end{cases} \quad (19)$$

Let $x = x_0 + \beta x_1$ with $x_0, x_1 \in \mathbb{F}_{2^m}$ and $a^3 = a_0 + \beta a_1$. Then $x_1 = x + \bar{x}$ and $C = a\bar{a}x_1$, while $x^2 + x = (x_0^2 + x_0 + x_1^2) + \beta(x_1^2 + x_1)$ and $\bar{x} + x^4 = (x_0 + x_0^4 + x_1) + \beta(x_1 + x_1^4)$. The $\mathbb{F}_{2^m}$ -component (the coefficient of 1 in the basis $\{1, \beta\}$) of an element $y = y_0 + \beta y_1$ is $y_0 = \text{tr}_m^n(\beta^2 y)$. Taking that component of the first equation of (19) (whose left side is $\text{tr}_m^n(\beta^2 A) + C$) gives

$$a_0(x_0^2 + x_0) = (a_0 + a_1)x_1^2 + (a_1 + a\bar{a})x_1 + 1. \quad (20)$$

For the second equation, $B^4 = a^{4(2^i+1)}(x^{2^m} + x^4) = \bar{a}a^4(\bar{x} + x^4)$. Denote $N := a\bar{a}$, then $\bar{a}a^4 = a^3N$, and, since $N \in \mathbb{F}_{2^m}$, the coordinates of a^3N are Na_0, Na_1 . Its 1-component equals $Na_0(x_0 + x_0^4 + x_1) + Na_1(x_1 + x_1^4)$. Equating to $C + C^2 = Nx_1 + N^2x_1^2$ and dividing by N we get

$$a_0(x_0^4 + x_0) = a_1x_1^4 + Nx_1^2 + (a_0 + a_1 + 1)x_1. \quad (21)$$

Set $w = x_0^2 + x_0$, so $x_0^4 + x_0 = w + w^2$. From (20), $a_0w = R$ with $R = (a_0 + a_1)x_1^2 + (a_1 + N)x_1 + 1$. Multiplying (21) by a_0 gives $a_0^2(w + w^2) = a_0R + R^2 = a_0(a_1x_1^4 + Nx_1^2 + (a_0 + a_1 + 1)x_1)$. We use the relative-norm identity

$$\begin{aligned} N^3 &= a^3 \overline{a^3} = (a_0 + \beta a_1)(a_0 + \beta^2 a_1) = \\ &= a_0^2 + a_0 a_1 (\beta + \beta^2) + \beta^3 a_1^2 = a_0^2 + a_0 a_1 + a_1^2, \end{aligned}$$

and collect the powers of x_1 in $a_0R + R^2 = a_0(a_1x_1^4 + Nx_1^2 + (a_0 + a_1 + 1)x_1)$, s.t.

$$N^3x_1^4 + (N^3 + N^2 + a_0N)x_1^2 + a_0(a_0 + N + 1)x_1 + (a_0 + 1) = 0.$$

Since $x_1 = C/N$, multiplying by N gives

$$\begin{aligned} Q(C) &:= C^4 + (N^2 + N + a_0)C^2 + \\ &+ a_0(a_0 + N + 1)C + N(a_0 + 1) = 0, \end{aligned} \quad (22)$$

as $a \neq 0, a_0 \neq 0$. Let $S = a_0 + N + 1$, then $Q(1) = S^2$, and $Q(N) = NS^2$, meaning that $\{1, N\}$ are roots of (22) iff $S = 0$. By lemma 3, we know that $S \neq 0$ for every $a \in \mathbb{F}_{2^n}^*$.

With $a_0, S \neq 0$ assume C_0 is a root of (22). If $C_0 = 0$, then $\text{tr}_1^m(C_0) = 0$, so assume $C_0 \neq 0$. Since $S \neq 0$, we also know that $C_0 \neq 1, C_0 \neq N$. Collecting powers of a_0 in (22) gives

$$\begin{aligned} C_0 a_0^2 + (C_0 + 1)(C_0 + N) a_0 + \\ + (C_0^4 + (N^2 + N)C_0^2 + N) = 0. \end{aligned} \quad (23)$$

Read this as a quadratic in a_0 ; its leading coefficient C_0 and middle coefficient $(C_0 + 1)(C_0 + N)$ are nonzero (since $S \neq 0$). By the solvability criterion,

$$\text{tr}_1^m \left(\frac{C_0 (C_0^4 + (N^2 + N)C_0^2 + N)}{((C_0 + 1)(C_0 + N))^2} \right) = 0.$$

Clearing denominators gives us the identity

$$\begin{aligned} \frac{C_0 (C_0^4 + (N^2 + N)C_0^2 + N)}{((C_0 + 1)(C_0 + N))^2} &= C_0 + \\ &+ \frac{C_0}{(C_0 + 1)^2} + \frac{NC_0}{(C_0 + N)^2}, \end{aligned} \quad (24)$$

where

$$\begin{aligned} \frac{C_0}{(C_0 + 1)^2} &= \frac{1}{C_0 + 1} + \left(\frac{1}{C_0 + 1} \right)^2; \\ \frac{NC_0}{(C_0 + N)^2} &= \frac{N}{C_0 + N} + \left(\frac{N}{C_0 + N} \right)^2. \end{aligned}$$

Each of them is of the form $(\cdot) + (\cdot)^2$, which has trace 0. Taking the trace of (24), therefore, leaves us only with $\text{tr}_1^m C_0 = 0$. Meaning that for every solution C_0 of Q (22), its trace must be equal to 0. Therefore, (17) has solutions only when $\text{tr}_1^m(C_0) = 0$. Hence, no solution has $\text{tr}_1^m C = 1$, so $\Delta_a F_1(x) = 0$ has at most two solutions in total, and F_1 is APN. $\square$

Note 1. We can see that $F_l(x) + F_1(x) = \beta \text{tr}_1^m(N(x))$. Since we are adding a Boolean function to an existing APN function, families F_l and F_1 are related by a switching construction. Theorem 5 is the first instance of an APN family constructed entirely using the switching construction from an existing family since 2009 [24]. It is also the first instance of a family constructed by switching a non-power family.

In Section IV, we compute the differential spectra of the orthoderivatives of the functions from family F_1 , and observe that they are distinct from those of all known infinite families of APN functions that are defined in that dimension. We can thus conclude that Theorem 5 gives a new infinite family of APN functions. Furthermore, F_l and F_1 generalize two of the six sporadic instances from [25]. We also remark that F_2 and F_3 , discussed in the next section, generalize another two of the six sporadic instances.

B. Infinite families built on $G_2(x)$

In this section, we study families of functions that can be obtained from G_2 by adding perturbation terms in the same way that this was done for G_1 . The resulting functions prove to be much more difficult to handle than the ones obtained from G_1 , and we have not been able to show that they are APN. We have confirmed the APN property of the constructed functions computationally for $n = 10, 14, 22, 26$, and conjecture that the families F_2 and F_3 are APN under the following conditions. Furthermore, we investigate their structure and give some characterizations of their APN-ness. Furthermore, in Section IV, we compute the differential spectra of their orthoderivatives, and observe that they are distinct from those of all known infinite APN families that are defined over the corresponding dimensions, and that they generalize two sporadic instances of APN functions first identified in [25].

Let $m \geq 5$ be a positive odd integer such that $3 \nmid m$, and $n = 2m$. Consider the APN function $G_2(x)$ (7) over $\mathbb{F}_{2^n}$ (BHK for $i = (m-2)^{-1} \pmod n$).

Let $N(x) = x^{2^{m+1}}$ denote the norm map from $\mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^m}$. Set $k = \frac{n-6}{4}$; we construct Frobenius conjugates into the following structured perturbation terms

$$P_2(x) = \beta \sum_{j=1}^k N^{2^j}(x) + \sum_{j=k+1}^{m-1} N^{2^j}(x), \quad (25)$$

$$P_3(x) = \beta^2 N(x) + \sum_{j=1}^k N^{2^j}(x) + \beta \sum_{j=k+1}^{m-1} N^{2^j}(x). \quad (26)$$

Denote $N := N(x)$. Using (25), (26) and BHK (7), we construct the following infinite families of functions

which we conjecture are APN:

$$F_2(x) = x^3 + \beta x^{2^i+1} + \beta^2 \bar{x}^3 + \overline{x^{2^i+1}} + \beta \sum_{j=1}^k N^{2^j} + \sum_{j=k+1}^{m-1} N^{2^j}, \quad (27)$$

$$F_3(x) = x^3 + \beta x^{2^i+1} + \beta^2 \bar{x}^3 + \overline{x^{2^i+1}} + \beta^2 N + \sum_{j=1}^k N^{2^j} + \beta \sum_{j=k+1}^{m-1} N^{2^j}; \quad (28)$$

where $i = (m-2)^{-1} \pmod n$, $\bar{x} = x^{2^m}$, $k = \frac{n-6}{4}$, and β is a primitive element of $\mathbb{F}_4$.

One of the factors contributing to the difficulty of analyzing the functions is the value $i = (m-2)^{-1} \pmod n$, which is given as a multiplicative inverse. To simplify the analysis, we compute the exact value of i in terms of k :

Lemma 4. *Let $n = 2m = 4k + 6$ with m odd. Then the inverse $i = (m-2)^{-1} \pmod n$ is given by*

$$i = \begin{cases} 3k + 4, & \text{for odd } k, \\ k + 1, & \text{for even } k. \end{cases} \quad (29)$$

Proof. Since $i = (m-2)^{-1} \pmod n$, we have $i(m-2) = 1 \pmod{2m}$. Reducing modulo m yields

$$\begin{aligned} im - 2i &= 1 \pmod m, \\ 2i + 1 &= 0 \pmod m, \\ i &= \frac{m-1}{2} \pmod m. \end{aligned}$$

Since i must be odd because m is odd, the unique solution modulo n is $\frac{m-1}{2}$ if $m = 3 \pmod 4$, and $\frac{m-1}{2} + m$ for $m = 1 \pmod 4$. $\square$

For $a \in \mathbb{F}_{2^n}^*$, denote by $\Delta_a F(x) = F(ax) + F(ax + a) + F(a)$ the derivative of F in direction a , and put

$$\begin{aligned} A &= A(a, x) = a^3(x^2 + x), \\ B &= B(a, x) = a^{2^i+1}(x^{2^i} + x), \\ C &= C(a, x) = a^{2^{m+1}}(x^{2^m} + x), \end{aligned}$$

where $i = (m-2)^{-1} \pmod n$. Then we observed the following statements.

Proposition 1. *For every $a \in \mathbb{F}_{2^n}^*$,*

$$\Delta_a F_2(x) = A + \beta B + \beta^2 \bar{A} + \bar{B} + C + \beta^2 h(C) + \text{tr}_1^m(C), \quad (30)$$

$$\Delta_a F_3(x) = A + \beta B + \beta^2 \bar{A} + \bar{B} + C + \beta^2 h(C) + \beta \text{tr}_1^m(C); \quad (31)$$

where $h(C) = \sum_{j=1}^k C^{2^j}$ for $k = \frac{n-6}{4}$.

Since m is odd, $\mathbb{F}_4 \not\subseteq \mathbb{F}_{2^m}$, so $\{1, \beta\}$ is a basis of $\mathbb{F}_{2^{2m}}$ over $\mathbb{F}_{2^m}$; for $y \in \mathbb{F}_{2^{2m}}$ the corresponding coordinates are $\beta^2 y + \beta \bar{y}$ and $y + \bar{y}$. Decomposing (30) and (31) in this basis yields the following characterizations.

Proposition 2. *The function F_2 is APN if and only if, for every $a \in \mathbb{F}_{2^n}^*$, the system*

$$\begin{cases} \beta^2 A + \beta \bar{A} = C + \text{tr}_1^m C, \\ \beta^2 B + \beta \bar{B} = C + h(C) + \text{tr}_1^m C; \end{cases} \quad (32)$$

admits only the trivial solutions $x \in \mathbb{F}_2$.

Proposition 3. *The function F_3 is APN if and only if, for every $a \in \mathbb{F}_{2^n}^*$, the system*

$$\begin{cases} \beta^2 A + \beta \bar{A} = C + \text{tr}_1^m C, \\ \beta^2 B + \beta \bar{B} = C + h(C); \end{cases} \quad (33)$$

admits only the trivial solutions $x \in \mathbb{F}_2$.

The two systems share their first equation and differ only by the term $\text{tr}_1^m(C)$ in the second. In particular, if $\text{tr}_1^m(C) = 0$ then $\Delta_a F_2 = \Delta_a F_3$ and both systems reduce to

$$\begin{cases} C = \beta^2 A + \beta \bar{A}, \\ \beta^2 B + \beta \bar{B} = C + h(C). \end{cases} \quad (34)$$

Conjecture 1. *Let $m \geq 5$ be odd with $3 \nmid m$, $n = 2m$, and $i = (m-2)^{-1} \pmod{n}$. Then the functions F_2 in (27) and F_3 in (28) are APN over $\mathbb{F}_{2^n}$.*

By the computations in the propositions above, Conjecture 1 is equivalent to the following three statements holding for every $a \in \mathbb{F}_{2^n}^*$:

- (i) system (34) has only the solutions $x \in \{0, 1\}$ in the case $\text{tr}_1^m(C) = 0$;
- (ii) the system

$$\begin{cases} \beta^2 A + \beta \bar{A} = C + 1, \\ \beta^2 B + \beta \bar{B} = C + h(C) + 1; \end{cases} \quad (35)$$

- has no solutions with $\text{tr}_1^m C = 1$;
- (iii) the system

$$\begin{cases} \beta^2 A + \beta \bar{A} = C + 1, \\ \beta^2 B + \beta \bar{B} = C + h(C); \end{cases} \quad (36)$$

has no solutions with $\text{tr}_1^m C = 1$.

Here (i) is common to F_2 and F_3 ; the function F_2 is APN if and only if (i) and (ii) hold, and F_3 is APN if and only if (i) and (iii) hold. We note that (ii) and (iii) are not implied by (i): the solution sets of (35) and (36) lie in different fibres of the linear map $x \mapsto$

$A + \beta B + \beta^2 \bar{A} + \bar{B} + C + \beta^2 h(C)$, and may be nonempty or empty independently of one another.

Proposition 4. *Conjecture 1 holds for $n = 10$, $n = 14$, $n = 22$ and $n = 26$; that is, F_2 and F_3 are APN over $\mathbb{F}_{2^{10}}$, $\mathbb{F}_{2^{14}}$, $\mathbb{F}_{2^{22}}$ and $\mathbb{F}_{2^{26}}$. These are all admissible dimensions $n \leq 26$.*

Remark 1. *The technique of Theorem 5 does not extend to $i = (m-2)^{-1}$. There, the right-hand side of the second equation is $C^{2^{m-2}} + C^{2^{m-1}}$, and raising it to the fourth power collapses it to $C + C^2$, while simultaneously $B^4 = a^{2^m+4}(\bar{x} + x^4) = a^3 N(\bar{x} + x^4)$ acquires the coefficient a^3 ; the two effects together produce an equation of degree four in C . Both effects fail for $i = (m-2)^{-1}$.*

First, by Lemma 4 the second equation of (34) involves $h(C)$, and $h(C)^{2^t} = \sum_{j=t+1}^{k+t} C^{2^j}$ is a sum of k terms for every t , so no Frobenius twist reduces it to boundedly many terms. Second, the substitution used for B has no analogue: raising B to a power 2^t transforms its coefficient into $a^{2^t(2^i+1)}$, and this equals $a^3 N^s$ for some integer s precisely when

$$2^t(2^i + 1) \equiv 3 + s(2^m + 1) \pmod{2^n - 1}, \quad (37)$$

which, since $\gcd(2^m - 1, 2^m + 1) = 1$ and the congruence modulo $2^m - 1$ is always solvable in s , is equivalent to $2^t(2^i + 1) \equiv 3 \pmod{2^m + 1}$. For $i = m-2$ this holds with $t = 2$, which is exactly the fourth power used in Theorem 5. For $i = (m-2)^{-1}$, however, (37) has no solution t for $m \in \{7, 11, 13, 17, 19, 23\}$, while for $m = 5$ its only solution is $t = m$, which corresponds to conjugation $B \mapsto \bar{B}$ and hence yields no new relation.

Note 2. *We have $F_2(x) + F_3(x) = \beta^2 \text{tr}_1^m(N(x))$ and $F_L(x) + F_1(x) + F_2(x) + F_3(x) = \text{tr}_1^m(N(x))$. Thus the four functions are related by switching constructions.*

IV. DISTINGUISHING THE NEW FAMILIES VIA ORTHO-DERIVATIVES

To establish that F_1 , F_2 and F_3 are genuinely new, we must show that they are CCZ-inequivalent to all previously known infinite families of APN functions. We use the ortho-derivative differential spectrum introduced in Section II, which is at present the most discriminating invariant that is efficient to compute [26].

Recall that for a quadratic APN function F , the ortho-derivative π_F is defined by (4), and that the multiset $\mathcal{D}_{\pi_F}$ obtained by applying (2) to π_F is invariant under CCZ-equivalence. Two quadratic APN functions with different ortho-derivative differential spectra are

therefore CCZ-inequivalent. We stress that this does not work in the other direction: equality of the spectra is only a necessary condition for equivalence (although in practice, equality of the differential spectra of the ortho-derivatives almost always implies CCZ-equivalence of the corresponding functions, with extremely few exceptions).

Our verification proceeds as follows. The admissible dimensions in our setting are $n = 2m$ with m odd and $3 \nmid m$; the smallest of them are $m = 5, 7, 11$, that is, $n = 10, 14, 22$ (the value $m = 9$ is excluded by $3 \mid 9$). For each such dimension, we compute the ortho-derivative differential spectra of F_1, F_2, F_3 and F_l , and compare them against each other to establish that the functions obtained from the families belong to distinct CCZ-classes. More importantly, for dimension $n = 10$, where we have a full classification of APN functions from the known infinite families available, we compare the ortho-derivative differential spectra to those of the known families, and observe that the ones corresponding to F_1, F_2 and F_3 do not match any instance of a known APN family. In this way, we show that the constructions are new.

Let $m = 5$, then $n = 10$, the four functions constructed in Section III have the following univariate representations over $\mathbb{F}_{2^{10}}$, where β is a primitive element of $\mathbb{F}_4$:

$$\begin{aligned} F_l(x) &= x^3 + \beta x^9 + \beta^2 x^{96} + x^{288} + \beta x^{33} + \beta^2 x^{264} + \beta^2 x^{528}, \\ F_1(x) &= x^3 + \beta x^9 + \beta^2 x^{96} + x^{288} + \beta x^{66} + \beta x^{132} + x^{264} + x^{528}, \\ F_2(x) &= x^3 + \beta x^{129} + \beta^2 x^{96} + x^{36} + \beta x^{66} + x^{132} + x^{264} + x^{528}, \\ F_3(x) &= x^3 + \beta x^{129} + \beta^2 x^{96} + x^{36} + \beta^2 x^{33} + x^{66} + \beta x^{132} + \beta x^{264} + \beta x^{528}. \end{aligned}$$

Table IV lists their ortho-derivative differential spectra, together with those of the two BHK functions G_1 and G_2 that they are built on. All six spectra are pairwise distinct.

To compare the ortho-derivative differential spectra against those of the known infinite families, we refer to Table 4 in [25], which lists representatives and ortho-derivative differential spectra for all known quadratic 3-to-1 APN functions over $\mathbb{F}_{2^{10}}$ at the time of writing. Clearly, the values corresponding to F_1, F_2 , and F_3 are absent in that table. Furthermore, we can see from Table 2 in the same paper, that the ortho-derivative differential spectra of F_1, F_2 and F_3 , in fact, correspond to the functions nos. 6, 4, and 3, respectively, which

are identified in [25] as sporadic instances over $\mathbb{F}_{2^{10}}$ not corresponding to any infinite APN family known at the time.

To the best of our knowledge, the only infinite APN families that have been published since [25] and that can produce functions for $n = 10$ are F19, F21, and F22 from Table III. Family F19 is the construction given in [14], which we have already discussed, and which is equivalent to F_l . As to the functions from families F21 and F22, the authors in [16] under Remark 1 indicate that the instances from these families for dimensions below $n = 12$ are CCZ-equivalent to ones originating from the two constructions being extended in [16], namely the ones given in [13] and [14]. We can thus conclude that the functions F_1, F_2 , and F_3 can not be explained by any previously known infinite family of APN functions. In particular, the family constructed in Theorem 5 is new up to CCZ-equivalence, and generalizes one of the sporadic instances given in [25].

TABLE IV
ORTHO-DERIVATIVE DIFFERENTIAL SPECTRA OVER $\mathbb{F}_{2^{10}}$

$0^{**}637701, 2^{**}313131, 4^{**}80910, 6^{**}14415, 8^{**}1395$	G_1
$0^{**}626541, 2^{**}330336, 4^{**}79515, 6^{**}10230, 8^{**}930$	G_2
$0^{**}634041, 2^{**}320166, 4^{**}78420, 6^{**}13020, 8^{**}1830, 10^{**}60, 12^{**}15$	F_l
$0^{**}636591, 2^{**}316371, 4^{**}78720, 6^{**}13740, 8^{**}1935, 10^{**}165, 12^{**}30$	F_1
$0^{**}632286, 2^{**}322566, 4^{**}78540, 6^{**}12675, 8^{**}1320, 10^{**}165$	F_2
$0^{**}631911, 2^{**}323421, 4^{**}78495, 6^{**}11775, 8^{**}1725, 10^{**}210, 12^{**}15$	F_3

V. CONCLUSION

We have presented the first new infinite family of APN functions obtained using the switching construction since 2009. This is also the first infinite family to be constructed by applying the switching method to a non-power family. We have shown that this new family is CCZ-inequivalent to all previously known infinite families of APN functions, and that it generalizes a previously known sporadic instance over $\mathbb{F}_{2^{10}}$ from [25]. In the process of proving this, we have shown that our family is a switching neighbor of a family EA-equivalent to the construction defined by Li, Zhou, Li, and Qu [14], thereby obtaining an alternative representation for the latter family. More generally, we have shown that both the Li-Zhou-Li-Qu family and our new infinite family can be obtained by adding specific perturbation terms to one of the two families from the Budaghyan-Helleseth-Kaleyski construction [15]. Furthermore, we have computationally identified the form of two more families that can be obtained

from the second Budaghyan-Helleseth-Kaleyski family, observed that these two new families also form a switching pair (in the sense that one can be obtained from the other via the switching construction), and conducted computations that support the conjecture that these families are APN. We have derived conditions that characterize their APN-ness, and have shown that they generalize two further sporadic instances over $\mathbb{F}_{2^{10}}$.

The most immediate open problem is to establish the APN property of the conjectured families F_2 and F_3 . More generally, it would be interesting to determine whether the same norm-derived switching can be applied to other primary APN constructions in even dimension, and to characterize the classes of APN families that admit perturbations of this type. It would also be of interest to determine whether richer combinations of norm and trace terms give rise to additional CCZ-inequivalent families, and whether an analogous mechanism can be developed in odd dimension.

REFERENCES

- [1] E. Biham and A. Shamir, *Differential cryptanalysis of the data encryption standard*. Springer Science & Business Media, 2012.
- [2] K. Nyberg, “Differentially uniform mappings for cryptography,” *Lecture Notes in Computer Science*, vol. 765, pp. 55–64, 1994.
- [3] R. Gold, “Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.),” *IEEE Transactions on Information Theory*, vol. 14, no. 1, pp. 154–156, 1968.
- [4] T. Kasami, “The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes,” *Information & Computation*, vol. 18, no. 4, pp. 369–394, 1971.
- [5] H. Dobbertin, “Almost perfect nonlinear power functions on $\text{GF}(2^n)$: the Welch case,” *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 1271–1275, 1999.
- [6] —, “Almost perfect nonlinear power functions on $\text{GF}(2^n)$: the Niho case,” *Information & Computation*, vol. 151, no. 1, pp. 57–72, 1999.
- [7] Y. Edel, G. Kyureghyan, and A. Pott, “A new apn function which is not equivalent to a power mapping,” *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 744–747, 2006.
- [8] L. Budaghyan, C. Carlet, P. Felke, and G. Leander, “An infinite class of quadratic apn functions which are not equivalent to power mappings,” *2006 IEEE International Symposium on Information Theory*, pp. 2637–2641, 2006. [Online]. Available: <https://api.semanticscholar.org/CorpusID:13915395>
- [9] L. Budaghyan, C. Carlet, and G. Leander, “Two classes of quadratic APN binomials inequivalent to power functions,” *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4218–4229, 2008.
- [10] L. Budaghyan and C. Carlet, “Classes of quadratic APN trinomials and hexanomials and related structures,” *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 2354–2357, 2008.
- [11] C. Bracken, E. Byrne, N. Markin, and G. McGuire, “A few more quadratic APN functions,” *Cryptography and Communications*, vol. 3, no. 1, pp. 43–53, 2011.
- [12] H. Taniguchi, “On some quadratic APN functions,” *Designs, Codes and Cryptography*, vol. 87, no. 9, pp. 1973–1983, 2019.
- [13] F. Göloğlu, “Biprojective almost perfect nonlinear functions,” *IEEE Transactions on Information Theory*, vol. 68, no. 7, pp. 4750–4760, 2022.
- [14] K. Li, Y. Zhou, C. Li, and L. Qu, “Two new families of quadratic APN functions,” *IEEE Transactions on Information Theory*, vol. 68, no. 7, pp. 4761–4769, 2022.
- [15] L. Budaghyan, T. Helleseeth, and N. Kaleyski, “A new family of APN quadrinomials,” *IEEE Transactions on Information Theory*, vol. 66, no. 11, pp. 7081–7087, 2020.
- [16] M. Calderini, K. Li, and I. Villa, “Extending two families of bivariate APN functions,” *Finite Fields and Their Applications*, vol. 88, p. 102190, 2023.
- [17] L. Zheng, H. Kan, Y. Li, J. Peng, and D. Tang, “Constructing new apn functions through relative trace functions,” *IEEE Transactions on Information Theory*, vol. 68, no. 11, pp. 7528–7537, 2022.
- [18] M. Brinkmann and G. Leander, “On the classification of APN functions up to dimension 5,” *Des. Codes Cryptography*, vol. 49, pp. 273–288, 12 2008.
- [19] Y. Yu, N. Kaleyski, L. Budaghyan, and Y. Li, “Classification of quadratic APN functions with coefficients in $\mathbb{F}_2$ for dimensions up to 9,” *Finite Fields and Their Applications*, vol. 68, p. 101733, 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1071579720301027>
- [20] C. Beierle and G. Leander, “New instances of quadratic APN functions,” *IEEE Transactions on Information Theory*, vol. 68, no. 1, pp. 670–678, 2021.
- [21] C. Beierle, P. Langevin, G. Leander, A. Polujan, and S. Rasoolzadeh, “Millions of inequivalent quadratic apn functions in eight variables,” 2025. [Online]. Available: <https://arxiv.org/abs/2508.04644>
- [22] Y. Edel and A. Pott, “A new almost perfect nonlinear function which is not quadratic,” *Cryptology ePrint Archive*, Paper 2008/313, 2008. [Online]. Available: <https://eprint.iacr.org/2008/313>
- [23] L. Budaghyan, C. Carlet, and G. Leander, “Constructing new APN functions from known ones,” *Finite Fields and Their Applications*, vol. 15, no. 2, pp. 150–159, 2009.
- [24] —, “On a construction of quadratic APN functions,” in *2009 IEEE Information Theory Workshop*. IEEE, 2009, pp. 374–378.
- [25] L. Budaghyan, I. Ivkovic, and N. Kaleyski, “Triplicate functions,” *Cryptography and Communications*, vol. 15, no. 1, pp. 35–83, 2023.
- [26] A. Canteaut, A. Couvreur, and L. Perrin, “Recovering or testing extended-affine equivalence,” *IEEE Transactions on Information Theory*, vol. 68, no. 9, pp. 6187 – 6206, 2022.
- [27] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2021.
- [28] K. Li and N. Kaleyski, “Two new infinite families of apn functions in trivariate form,” *IEEE Transactions on Information Theory*, vol. 70, no. 2, pp. 1436–1452, 2023.
- [29] C. Carlet, P. Charpin, and V. Zinoviev, “Codes, bent functions and permutations suitable for DES-like cryptosystems,” *Designs, Codes and Cryptography*, vol. 15, no. 2, pp. 125–156, 1998.
- [30] I. Ivkovic and N. Kaleyski, “tripeq: Algorithms for linear and EA-equivalence of triplicate functions,” <https://github.com/nskal/tripeq>, 2025, gitHub repository. Accessed: 2026-07-23.
- [31] S. Yoshiara, “Equivalences of quadratic APN functions,” *Journal of Algebraic Combinatorics*, vol. 35, no. 3, pp. 461–475, 2012.
- [32] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. The user language*, 1997. [Online]. Available: <https://magma.maths.usyd.edu.au/magma/>
- [33] L. Budaghyan, M. Calderini, C. Carlet, R. S. Coulter, and I. Villa, “Constructing APN functions through isotopic shifts,” *IEEE Transactions on Information Theory*, vol. 66, no. 8, pp. 5299–5309, 2020.

- [34] C. Carlet, “Relating three nonlinearity parameters of vectorial functions and building apn functions from bent functions,” *Designs, Codes and Cryptography*, vol. 59, no. 1-3, pp. 89–109, 2011.
- [35] H. Janwa and R. 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*. Springer, 1993, pp. 180–194.
- [36] T. Beth and C. Ding, “On almost perfect nonlinear permutations,” in *Workshop on the Theory and Application of Cryptographic Techniques*. Springer, 1993, pp. 65–76.
- [37] H. 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*, pp. 113–121, 2001.
- [38] Y. Zhou and A. Pott, “A new family of semifields with 2 parameters,” *Advances in Mathematics*, vol. 234, pp. 43–60, 2013.
- [39] M. Calderini, L. Budaghyan, and C. Carlet, “On known constructions of APN and AB functions and their relation to each other,” *Rad Hrvatske akademije znanosti i umjetnosti: Matematičke znanosti*, no. 546= 25, pp. 79–105, 2021.
- [40] F. Göloğlu and L. Kölsch, “Equivalences of bijective almost perfect nonlinear functions,” *arXiv preprint arXiv:2111.04197*, 2021.
- [41] J. F. Dillon, “APN polynomials and related codes,” in *Banff Conference, Nov. 2006*, 2006.