Mediterr. J. Math. (2024) 21:116
https://doi.org/10.1007/s00009-024-02660-x
1660-5446/24/030001-24
published online May 8, 2024

Mediterranean Journal of Mathematics

On Second-Order Derivatives of Boolean Functions and Cubic APN Permutations in Even Dimension

Augustine Musukwa, Massimiliano Sala, Irene Villa and Marco Zaninelli

Abstract. The big APN problem is one of the most important challenges in the theory of Boolean functions, i.e. finding a new APN permutation in even dimension. Among this class of functions, those with the lowest possible degree are cubic. Yet, none has been found so far. In this paper, we introduce new parameters for Boolean functions and for vectorial Boolean functions, mostly derived from the behavior of their second-order derivatives. These parameters are invariant under extended affine equivalence, and they are particularly relevant for small-degree functions. They allow studying bent, semi-bent and APN functions of degrees two and three. In particular, they allow tackling the big APN problem for cubic permutations. Notably, we focus on the case of dimension 8, providing some computational results.

Mathematics Subject Classification. 06E30, 94A60, 14G50.

Keywords. (Vectorial) Boolean functions, cubic Boolean functions, APN, EA-invariant.

1. Introduction

A vectorial Boolean function is a map that takes in input a sequence of bits (of fixed length) and it outputs another sequence of bits (of fixed length). These functions play an important role in many fields. In cryptography, they can be used to represent all inner layers of a block cipher. In particular, they can represent its confusion layer and therefore cryptographic properties of these functions directly influence the security of a block cipher, see [11, Section 3.2]. In the study of cryptographically significant vectorial Boolean functions, APN functions play an important role. Introduced by Nyberg in [23], these provide optimal resistance to the well-known differential attack presented by Biham and Shamir in [3], as well as to its many variations,

see e.g. [19,25]. More precisely, given a vectorial Boolean function F that takes n bits and returns n bits, that is, $F : \mathbb{F}^n \to \mathbb{F}^n$ with $\mathbb{F} = \mathbb{F}_2 = \{0, 1\}$, we say that F is APN if, for any $a, b \in \mathbb{F}^n$ with a nonzero, the equation $F(x)+F(x+a) = b$ admits at most two solutions. Many important problems of APN functions are still unsolved.

The so-called big APN problem consists of finding an APN permutation for even dimension $n \geq 8$, or better an infinity class, see [11, p. 478]. Few non-existence results are known. For example, for $n = 4$ no APN permutation exists [17]. We also know from [6] that an APN permutation in even dimension cannot have quadratic components nor partially-bent components. As a consequence, among APN permutations (n even), those with the lowest possible degree are cubic. Regardless of the effort of many researchers (see e.g. [8–10,18,24]), no such function has been found and it may even not exist.

Other open problems concern the classification of known APN functions into equivalence classes. To attack this problem, it is essential to find new invariants, that is, properties or parameters that remain unchanged while applying an equivalence relation.

In this work, we first study Boolean functions, that is $f : \mathbb{F}^n \to \mathbb{F}$, and we introduce a few parameters, notably an integer $\mathcal{M}(f)$ related to the behavior of its second-order derivatives. We show that $\mathcal{M}(f)$ provides useful information on f; in particular, it characterizes partially bent functions and bent functions of degrees 2 and 3. Interestingly, $\mathcal{M}(f)$ is invariant under extended affine equivalence. We also generalize $\mathcal{M}$ to vectorial Boolean functions, $F : \mathbb{F}^n \to \mathbb{F}^n$, obtaining a parameter that is invariant under extended affine equivalence. We use $\mathcal{M}(F)$ to characterize quadratic and cubic APN functions. When dealing with permutations, $\mathcal{M}(F)$ turns out to be a powerful tool, especially in the case n even. Finally, we focus on cubic APN permutations in dimension eight and provide some computational results.

This paper is organized as follows:

- Sect. 2 presents terminologies and some useful known results both for Boolean functions and vectorial Boolean functions.
- In Sect. 3, we deal with Boolean functions. We introduce the parameters $\mathfrak{m}(f)$, which depends on the first derivative of f, and $\mathcal{M}(f)$, which depends on the second-order derivative. We also introduce a new notion of nonlinearity, *variable maximal functions*. Such functions cannot be reduced to fewer variables via an affine transformation. We used the mentioned parameters to characterize partially bent, semi-bent and bent functions of degrees 2 and 3.
- In Sect. 4, we extend the parameter $\mathcal{M}$ introduced in Sect. 3 to vectorial Boolean functions. We restrict to considering functions F of degrees 2 and 3. We show a connection between the fourth power moment of the Walsh transform of F and the value $\mathcal{M}(F)$. Then, we use $\mathcal{M}(F)$ for the characterization of APN functions, in particular APN permutations. We also present some computational results on $\mathcal{M}(F)$ when F is not APN or when F has higher degree.

- Finally, Sect. 5 presents some computational results related to APN permutations, in particular on possible cubic APN permutations over $\mathbb{F}^8$. As final results, we present a list of functions in eight variables and we prove that, up to EA-equivalence, at least 85 components of a cubic APN permutation must belong to this list.

2. Preliminaries

We provide here some notions related to (vectorial) Boolean functions, useful to understand the results presented in the following sections. We refer the interested reader to [2,7,11,13,14,21,26] for a more extensive presentation of vectorial Boolean functions and their properties.

Set $\mathbb{N}$ to be the set of natural numbers and, when not specified, let n be any positive integer. With $\mathbb{F}$ we denote the finite field with two elements (0 and 1), and with $\mathbb{F}^n$ the vector space of dimension n over $\mathbb{F}$. The element $0_n \in \mathbb{F}^n$ is the vector with all zero entries, and the element $e_i \in \mathbb{F}^n$, for $1 \leq i \leq n$, is the vector with only one nonzero component in the i-th position. Given a finite set A, $|A|$ denotes its size.

A *vectorial Boolean function* is a map F from $\mathbb{F}^n$ to $\mathbb{F}^m$, for some positive integers n, m. This is also called an (n, m)-*function*. When $m = 1$, the function is usually called a *Boolean function*, and with B_n we denote the set of all Boolean functions from $\mathbb{F}^n$ to $\mathbb{F}$. An (n, m)-function F can be seen as a vector of Boolean functions, that is, $F = (f_1, \ldots, f_m)$ where $f_1, \ldots, f_m$ are $(n, 1)$-functions called the *coordinates* of F. Given a nonzero $\lambda = (\lambda_1, \ldots, \lambda_m) \in \mathbb{F}^m$, the λ-*component* of F is the Boolean function $F_\lambda = \lambda \cdot F = \sum_{i=1}^{m} \lambda_i f_i$. With $\mathrm{Im}(F)$, we denote the image set of the function F.

A vectorial Boolean function admits different representations. The algebraic normal form (ANF) of an (n, m)-function is its representation as a polynomial with coefficients in $\mathbb{F}^m$, that is, the ANF of $F \in \mathbb{F}^m[x_1, \ldots, x_n]$ is

$$F(x_1, \ldots, x_n) = \sum_{I \subseteq \mathcal{P}} a_I \prod_{i \in I} x_i,$$

where $\mathcal{P} = \{1, \ldots, n\}$ and $a_I \in \mathbb{F}^m$. The *algebraic degree* of F, denoted $\deg(F)$, corresponds to the value $\max_{a_I \neq 0_m} |I|$ and it coincides with the maximum degree of the component functions of F. If $\deg(F) \leq 1$ and $F(0_n) = 0_m$, then F is called *linear*, F is *affine* if $\deg(F) \leq 1$, *quadratic* if $\deg(F) \leq 2$ and *cubic* if $\deg(F) \leq 3$. These same definitions apply also to Boolean functions.

In this work, we are interested in studying $(n, 1)$-functions and (n, n)-functions. In the following, we present further properties of these functions.

2.1. On Boolean Functions

Here we present some definitions and fundamental properties related to Boolean functions.

For a positive integer n, consider $f \in B_n$. The *Hamming weight* of f is given by $\mathrm{w}(f) = |\{x \in \mathbb{F}^n \mid f(x) = 1\}|$, and we say that f is *balanced* if $\mathrm{w}(f) = 2^{n-1}$. All non-constant affine functions are balanced. The *distance* between f and g is $d(f,g) = \mathrm{w}(f+g)$ and the *nonlinearity* of f is $\mathcal{N}(f) = \min_{\alpha \in A_n} d(f,\alpha)$, where A_n is the set of all affine Boolean functions in n variables.

The *Walsh transform* of f is the function $\mathcal{W}_f$ from $\mathbb{F}^n$ to $\mathbb{Z}$ (set of integers), defined as $\mathcal{W}_f(a) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x)+a\cdot x}$ for all $a \in \mathbb{F}^n$. We define $\mathcal{F}(f)$ as $\mathcal{F}(f) = \mathcal{W}_f(0_n) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x)} = 2^n - 2\mathrm{w}(f)$. Observe that f is balanced if and only if $\mathcal{F}(f) = 0$.

The nonlinearity of f can also be expressed as $\mathcal{N}(f) = 2^{n-1} - \frac{1}{2}\mathcal{L}(f)$, where $\mathcal{L}(f) = \max_{a \in \mathbb{F}^n} |\mathcal{W}_f(a)|$. The function f is called *bent* if $\mathcal{N}(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$ (this happens only for n even). The lowest possible value for $\mathcal{L}(f)$ is $2^{\frac{n}{2}}$, and the bent functions are precisely those that meet this bound with equality. There are other equivalent characterizations of bent functions. For example, as reported in [11], f is bent if and only if $\mathcal{W}_f(a) = \pm 2^{\frac{n}{2}}$ for any $a \in \mathbb{F}^n$. Therefore, a bent Boolean function cannot be balanced. For n odd, a function f is called *semi-bent* if $\mathcal{N}(f) = 2^{n-1} - 2^{\frac{n-1}{2}}$.

Set $a, b \in \mathbb{F}^n$. The *first-order derivative*, or simply the derivative, of f in the direction of a is defined by $D_a f(x) = f(x+a) + f(x)$, and its *second-order derivative* at a and b is $D_b D_a f(x) = f(x) + f(x+b) + f(x+a) + f(x+a+b)$. Notice that

$$D_{a_1+a_2} f(x) = D_{a_1} f(x) + D_{a_2} f(x + a_1). \tag{2.1}$$

The following result is well-known, see for instance [11] Theorem 12.

Theorem 1. *A function $f \in B_n$ is bent if and only if $D_a f$ is balanced for any nonzero $a \in \mathbb{F}^n$.*

Two functions $f, g \in B_n$ are said to be *affine equivalent* if there exists an affine automorphism $\varphi : \mathbb{F}^n \to \mathbb{F}^n$ such that $f = g \circ \varphi$; in which case we write $f \sim_A g$. The functions f and g are called *extended affine equivalent* (EA-equivalent) if there exist two Boolean functions h, ℓ such that $f = h + \ell$ with ℓ affine and $h \sim_A g$. Observe that both relations are equivalence relations. The nonlinearity, the weight, the balancedness and the algebraic degree are affine invariants. The nonlinearity is also an EA-invariant, same as the algebraic degree when the function has degree strictly greater than one. There are many other invariants for these equivalences; for example in [15] Dillon considers properties of the derivatives to determine the affine inequivalence.

The following well-known theorems characterize quadratic Boolean functions up to affine equivalence, see for example [21] and [14].

Theorem 2. *Consider $f \in B_n$ with $\deg(f) = 2$. Then*

(i) $f \sim_A x_1x_2 + \cdots + x_{2k-1}x_{2k} + x_{2k+1}$ with $k \leq \lfloor \frac{n-1}{2} \rfloor$ if f is balanced,
(ii) $f \sim_A x_1x_2 + \cdots + x_{2k-1}x_{2k} + c$, with $k \leq \lfloor \frac{n}{2} \rfloor$ and $c \in \mathbb{F}$, if f is not balanced.

Theorem 3. *Let f be a quadratic Boolean function denoted as in Theorem 2. Then we have $\mathcal{W}_f(a) \in \{0, \pm 2^{n-k}\}$, for $a \in \mathbb{F}^n$, and $\mathcal{N}(f) = 2^{n-1} - 2^{n-k-1}$.*

Remark 4. Notice that, for n even and $k = \frac{n}{2}$, then f in Theorem 2 is bent. Obviously, this cannot happen for balanced functions.

An element $a \in \mathbb{F}^n$ is called a *linear structure* of $f \in B_n$ if $D_a f$ is constant. We denote by $V(f)$ the set of all linear structures of f and we call it the *linear space* of f. Observe that $V(f)$ is a vector space, since $D_{a+b}f(x) = D_a f(x) + D_b f(x+a)$. A function f is *partially-bent* if there exists a linear subspace W of $\mathbb{F}^n$ such that the restriction of f to W is affine and the restriction of f to any complementary subspace U of W, $W \oplus U = \mathbb{F}^n$, is bent. It is worth noticing that $W = V(f)$ and the dimension of U must be even, see [6]. Moreover, from Theorem 2, any quadratic function is partially-bent.

2.2. On Vectorial Boolean Functions

We present some basic definitions related to cryptographic vectorial Boolean functions, in particular (n,n)-functions. Some of the definitions given for Boolean functions in Subsect. 2.1 can be extended to vectorial functions. For example, given F an (n,n)-function, the first-order derivative of F at a, for $a \in \mathbb{F}^n$, is defined by $D_a F(x) = F(x+a) + F(x)$. The definition of second-order derivative is extended in a similar way. A function $F : \mathbb{F}^n \to \mathbb{F}^n$ is called a *permutation* if $\{F(u) \mid u \in \mathbb{F}^n\} = \mathbb{F}^n$. Equivalently, F is a permutation if and only if all its (nonzero) components are balanced, see for instance [11] Proposition 35. Additionally, F is called *strongly plateaued* if all its (nonzero) component functions are partially bent.

Definition 5. Define $\delta_F(a,b) = |\{x \in \mathbb{F}^n \mid D_a F(x) = b\}|$, for $a, b \in \mathbb{F}^n$ and F an (n,n)-function. The *differential uniformity of F is*

$$\delta(F) = \max_{a,b \in \mathbb{F}^n, a \neq 0_n} \delta_F(a,b),$$

and it always satisfies $\delta(F) \geq 2$. A function with $\delta(F) = 2$ is called *Almost Perfect Nonlinear (APN)*.

Two (n,n)-functions F, G are said to be *EA-equivalent* if $F = A_1 \circ G \circ A_2 + A$ with A_1 and A_2, respectively, a linear and an affine permutation of $\mathbb{F}^n$ and A an affine transformation of $\mathbb{F}^n$. The differential uniformity is invariant under EA-equivalence.

The k-th power moment of the Walsh transform of a function $f \in B_n$ is defined by

$$L_k(f) = \sum_{a \in \mathbb{F}^n} |\mathcal{W}_f(a)|^k.$$

For an (n,n)-function F, we define the k-th power moment of its Walsh transform by

$$L_k(F) = \sum_{\lambda \in \mathbb{F}^n \setminus \{0_n\}} L_k(F_\lambda).$$

Next, we state a result in which APN functions are characterized by the fourth power moment of their Walsh transform, see for instance [11] Theorem 25.

Theorem 6. *Let F be a function from $\mathbb{F}^n$ to itself. Then*

$$L_4(F) \geq 2^{3n+1}(2^n - 1).$$

Moreover, F is APN if and only if the equality holds.

For $f \in B_n$, the following relation is known, see for example [1],

$$L_4(f) = \sum_{a \in \mathbb{F}^n} W_f(a)^4 = 2^n \sum_{a \in \mathbb{F}^n} \mathcal{F}^2(D_a f). \tag{2.2}$$

3. Two Parameters for Boolean Functions

In this section, we introduce two parameters $\mathfrak{m}(f)$ and $\mathcal{M}(f)$ related to the derivatives of a Boolean function f. With these parameters, we can characterize partially bent functions and bent functions of degrees 2 and 3. Moreover, we show that these parameters are invariant under some equivalence relations.

Recall that, given $n \in \mathbb{N}$ and $f \in B_n$, the linear structure of f is the set $V(f) = \{a \in \mathbb{F}^n \mid \deg(D_a f) = 0\}$. We introduce the following notation,

$$Z(f) = \{a \in \mathbb{F}^n \mid D_a f = 0\}, \text{ and } U(f) = \{a \in \mathbb{F}^n \mid D_a f = 1\},$$

where, for $g \in B_n$ and $c \in \mathbb{F}$, with $g = c$, we indicate that g is constantly equal to c.

Remark 7. Notice that, if $U(f) \neq \emptyset$, then f is balanced since $f \sim_A g(x_1, \ldots, x_{n-1}) + x_n$.

Definition 8. For a Boolean function f on n variables, we define $\mathfrak{m}(f) = |Z(f)| - |U(f)|$.

We present some properties of the parameters introduced.

Proposition 9. *Consider $f \in B_n$, for $n \in \mathbb{N}$. Then $V(f) = Z(f) \cup U(f)$, where $Z(f)$ is a vector space and $U(f)$ is either a coset of $Z(f)$ or the empty set. Moreover,*

- $\mathfrak{m}(f) = 0$ *and* $|V(f)| = 2|Z(f)|$, *if* $U(f) \neq \emptyset$,
- $\mathfrak{m}(f) = |V(f)| = |Z(f)| \neq 0$, *otherwise.*

Proof. From the definition of $V(f)$, $Z(f)$ and $U(f)$, we trivially verify that $V(f) = Z(f) \cup U(f)$. Notice that the union is a disjoint union. The element 0_n always belongs to $Z(f)$. Moreover, from Eq. (2.1), for any $a_1, a_2 \in Z(f)$, the element $a_1 + a_2$ belongs to $Z(f)$. So, $Z(f)$ is a vector space. Suppose now that $U(f) \neq \emptyset$. For any $a \in U(f)$, we show in the following that $a + Z(f) = U(f)$. For $b \in Z(f)$, set $c = a + b$. Then, from Eq. (2.1), $D_c f = 1$ and $c \in U(f)$. This implies that $a + Z(f) \subseteq U(f)$. Conversely, for $e \in U(f)$, we have $D_{a+e} f = 0$ and $a + e \in Z(f)$, so $e = a + (a + e) \in a + Z(f)$. Hence $U(f) \subseteq a + Z(f)$. The last two conditions follow immediately. □

By Theorem 1, we deduce the following corollary.

Corollary 10. *If $f \in B_n$ is bent, then $\mathfrak{m}(f) = 1$.*

To study the invariance of the parameters introduced, with respect to the affine equivalence relation, we make use of the following result.

Lemma 11. *For $n \in \mathbb{N}$, let $g_1, g_2 \in B_n$ be affine equivalent functions. In particular, let $g_1(x) = g_2(Mx + w)$, with $w \in \mathbb{F}^n$ and M an invertible linear function over $\mathbb{F}^n$. For simplicity, we write Mx or $M \cdot x$ to indicate $M(x)$. Then, for any $a \in \mathbb{F}^n$, $a \neq 0_n$, we have $D_a g_1 \sim_A D_{M \cdot a} g_2$.*

Proof. For $a \in \mathbb{F}^n$, we have

$$\begin{aligned} D_a g_1(x) &= g_1(x + a) + g_1(x) = g_2(M \cdot (x + a) + w) + g_2(Mx + w) \\ &= g_2(Mx + Ma + w) + g_2(Mx + w) = D_{M \cdot a} g_2(Mx + w). \end{aligned}$$

This implies $D_a g_1 \sim_A D_{M \cdot a} g_2$. □

Theorem 12. *The values $|Z(\cdot)|$, $|U(\cdot)|$ and $\mathfrak{m}(\cdot)$ are invariant under affine equivalence.*

Proof. Consider two affine equivalent functions $g_1, g_2 \in B_n$ as in Lemma 11. By the mentioned lemma, for any $a \in \mathbb{F}^n$ we have that $a \in Z(g_1)$ if and only if $M \cdot a \in Z(g_2)$. The same is true for $U(\cdot)$. From this, we can easily deduce the theorem. □

Remark 13. Notice that, if we restrict to consider Boolean functions f such that $\mathfrak{m}(f) = 1$, the parameters are also invariant under EA-equivalence. That is, for $f, g \in B_n$ EA-equivalent such that $\mathfrak{m}(f) = \mathfrak{m}(g) = 1$, then it holds $|Z(f)| = |Z(g)|$ and $|U(f)| = |U(g)|$. For general values of $\mathfrak{m}(\cdot)$, this is not satisfied. Indeed, consider $g = f + \ell$ where ℓ is a linear function given by $\ell(x) = x \cdot u$ with $u \in \mathbb{F}^n$. It is straightforward to verify that $V(f) = V(g)$. We have two cases to analyze.

- Assume $U(f) = \emptyset$ ($\mathfrak{m}(f) \neq 0$). Then if $u \in Z(f)^\perp$ we have $U(g) = \emptyset$, $Z(f) = Z(g)$ and $\mathfrak{m}(f) = \mathfrak{m}(g)$, otherwise we have $U(g) \neq \emptyset$ and $\mathfrak{m}(g) = 0$.
- Assume $U(f) = a + Z(f)$ ($\mathfrak{m}(f) = 0$). Then if $u \in Z(f)^\perp$ and $u \cdot a = 1$ we have $U(g) = \emptyset$ and $\mathfrak{m}(g) \neq 0$, otherwise we have $U(g) \neq \emptyset$ and $\mathfrak{m}(g) = 0$. Moreover, $Z(g) = Z(f)$ and $U(g) = U(f)$ if and only if $u \in Z(f)^\perp$ and $u \cdot a = 0$.

Note. *In the rest of the article, with abuse of notation, for $f \in B_n$ we write that $f \sim_A g \in B_r$, with $r < n$, in the sense that $f \sim_A g$ with $g \in B_n$ a Boolean function in which only r variables appear. So g can be also viewed as a Boolean function in B_r. In this context, we write $\mathfrak{m}^r(g)$ to indicate the parameter $\mathfrak{m}(g)$ computed considering g as a function in B_r. We operate similarly for $Z^r(g)$ and $U^r(g)$.*

Related to the note above, we introduce the following definition.

Definition 14. Given $f \in B_n$, we define $\mathrm{var}(f)$ as the smallest integer k in $\{0, \ldots, n\}$ such that there exists $g \in B_k$ with $f \sim_A g$. If $\mathrm{var}(f) = n$ we say that f is *variable maximal*. Given $f \in B_n$, we indicate with $\bar{f}$ an affine equivalent Boolean function such that $f \sim_A \bar{f} \in B_k$ for $k = \mathrm{var}(f)$.

Remark 15. The case $\mathrm{var}(f) = 0$ corresponds to the case f constant.

Proposition 16. *Consider $f \in B_n$, then $|Z(f)| = 2^{n-\mathrm{var}(f)}$.*

Proof. Recall that $Z(f)$ is a vector space. Hence, we want to show that $\dim Z(f) = n - \mathrm{var}(f)$. Set $k = \mathrm{var}(f)$, $\ell = \dim Z(f)$ and $\{a_1, \ldots, a_\ell\}$ a basis of $Z(f)$. Set L to be a linear permutation such that $L(e_i) = a_i$, for $1 \leq i \leq \ell$, and consider the map $f' = f \circ L \sim_A f$. Therefore, for $1 \leq i \leq \ell$, we have $f'(x + e_i) + f'(x) = f(L(x) + a_i) + f(L(x))$ is the constant zero function, implying that the variables $x_1, \ldots, x_\ell$ do not appear in the map f'. Hence, $f' \in B_{n-\ell}$ and $k \leq n - \ell$. On the other side, since $\mathrm{var}(f) = k$ and $f \sim_A \bar{f} \in B_k$, then every linear combination of $e_{k+1}, \ldots, e_n$ belongs to $Z(f')$. This implies that $|Z(f)| = |Z(f')| \geq 2^{n-k}$ and $\ell \geq n - k$. This concludes the proof. □

Corollary 17. *A bent Boolean function f is variable maximal.*

In the following, we analyze Boolean functions of a particular form, called in [22] *splitting functions*. We recall their definition.

Definition 18. We say that $f \in B_n$ is a *splitting function* if $f \sim_A f_1(x_1, \ldots, x_k) + f_2(x_{k+1}, \ldots, x_n)$ for some positive $k < n$, $f_1 \in B_k$ and $f_2 \in B_{n-k}$.

Proposition 19. *Consider a splitting function $f \in B_n$ and $1 \leq k \leq n-1$, $f_1 \in B_k$ and $f_2 \in B_{n-k}$ such that $f \sim_A f_1(x_1, \ldots, x_k) + f_2(x_{k+1}, \ldots, x_n)$.*

Set $|Z^k(f_1)| = 2^r$ and $|Z^{n-k}(f_2)| = 2^s$ with $0 \leq r \leq k$ and $0 \leq s \leq n-k$. Then we have the following

$$Z(f) = \begin{cases} 2^{r+s+1} & \text{if and only if } U^k(f_1), U^{n-k}(f_2) \neq \emptyset, \\ 2^{r+s} & \text{otherwise;} \end{cases}$$

$$U(f) = \begin{cases} 2^{r+s+1} & \text{if and only if } U^k(f_1), U^{n-k}(f_2) \neq \emptyset, \\ 0 & \text{if and only if } U^k(f_1), U^{n-k}(f_2) = \emptyset, \\ 2^{r+s} & \text{otherwise.} \end{cases}$$

Proof. Consider an element $a \in \mathbb{F}^n$ as $a = (a_1, a_2)$ with $a_1 \in \mathbb{F}^k$ and $a_2 \in \mathbb{F}^{n-k}$. Then we have $D_a f = D_{a_1} f_1 + D_{a_2} f_2$. Since f_1 and f_2 do not have common variables, in order for $D_a f$ to be constant, both $D_{a_1} f_1$ and $D_{a_2} f_2$ have to be constant. Therefore, $Z(f) = Z^k(f_1) \times Z^{n-k}(f_2) \cup U^k(f_1) \times U^{n-k}(f_2)$ and $U(f) = U^k(f_1) \times Z^{n-k}(f_2) \cup Z^k(f_1) \times U^{n-k}(f_2)$. Hence, we have $|Z(f)| = |Z^k(f_1)| \cdot |Z^{n-k}(f_2)| + |U^k(f_1)| \cdot |U^{n-k}(f_2)|$ and $|U(f)| = |U^k(f_1)| \cdot |Z^{n-k}(f_2)| + |Z^k(f_1)| \cdot |U^{n-k}(f_2)|$. The proof follows by substituting the values for every case. □

Theorem 20. *Consider $f \in B_n$ such that $f \sim_A f_1(x_1, \ldots, x_k) + f_2(x_{k+1}, \ldots, x_n)$, with $1 \leq k \leq n-1$ ($f_1 \in B_k$ and $f_2 \in B_{n-k}$). Then we have $\mathfrak{m}(f) = \mathfrak{m}^k(f_1)\mathfrak{m}^{n-k}(f_2)$.*

Proof. Let r, s be as in Proposition 19. We deduce that $\mathfrak{m}(f) = |Z(f)| - |U(f)|$ is nonzero (and equal to 2^{r+s}) if and only if $U^k(f_1), U^{n-k}(f_2) = \emptyset$. This corresponds to the case $\mathfrak{m}^k(f_1), \mathfrak{m}^{n-k}(f_2) \neq 0$. In particular, we have $\mathfrak{m}^k(f_1) = 2^r$ and $\mathfrak{m}^{n-k}(f_2) = 2^s$. Hence we conclude the proof. □

Proposition 21. *Consider $f \in B_n$ and set $k = \mathrm{var}(f)$. Three cases are possible.*

1. *$k = 0$ if and only if $\mathfrak{m}(f) = 2^n$.*
2. *If $1 \leq k \leq n-1$, then* $\mathfrak{m}(f) = \begin{cases} 0 & \text{if } \mathfrak{m}^k(\bar{f}) = 0, \\ 2^{n-k} & \text{if } \mathfrak{m}^k(\bar{f}) = 1. \end{cases}$
3. *If $k = n$, then $\mathfrak{m}(f) = 0, 1$.*

Moreover, if $\mathfrak{m}(f) = 0$ then f is balanced, if $\mathfrak{m}(f) = 1$ then f is variable maximal.

Proof. First, consider that the condition $\mathfrak{m}(f) = 0$ is equivalent to $U(f) \neq \emptyset$. This implies that if $\mathfrak{m}(f) = 0$, the map f is balanced. If we assume $\mathfrak{m}(f) = 1$, this implies $|Z(f)| = 1$ and $|U(f)| = 0$. So by Proposition 16, f is variable maximal.

Set now $k = \mathrm{var}(f)$ and $f \sim_A \bar{f} \in B_k$. From Theorem 20, we have $\mathfrak{m}(f) = \mathfrak{m}^k(\bar{f}) \cdot 2^{n-k}$. Clearly, $k = 0$ if and only if the function f is constant, which is equivalent to $\mathfrak{m}(f) = 2^n$. Now consider $k \geq 1$. From Proposition 16 we have that $|Z(f)| = 2^{n-k}$, so either $\mathfrak{m}^k(\bar{f}) = 0$ and $\mathfrak{m}(f) = 0$ or $\mathfrak{m}^k(\bar{f}) = 1$ and $\mathfrak{m}(f) = 2^{n-k}$. No other case is possible. □

Remark 22. The statement "if $\mathfrak{m}(f) = 0$ then f is balanced" presented in Proposition 21 cannot be turned into an if and only if condition. Indeed, there are balanced functions $f \in B_n$ such that $\mathfrak{m}(f) \neq 0$, that is, such that $U(f) = \emptyset$. For example, the function $f = x_1x_2x_4 + x_1x_2 + x_2x_3x_4 + x_2x_4 + x_3x_4 \in B_4$ is balanced with $Z(f) = \{0_4\}$ and $U(f) = \emptyset$ ($\mathfrak{m}(f) = 1$).

Fact. *In B_4, there are no balanced functions f such that $\mathfrak{m}(f) > 1$, that is, $U(f) = \emptyset$ and $Z(f)$ contains at least two elements. This result was obtained with a computer search.*

Remark 23. Clearly the above fact is not true in greater dimensions. If we consider the function f from Remark 22, but as an element of B_5, then f is still balanced, $U(f) = \emptyset$ but $Z(f) = \{0, e_5\}$ and $\mathfrak{m}^5(f) = 2$.

We consider now the case of quadratic Boolean functions.

Proposition 24. *Let $f \in B_n$ be a function with $\deg(f) \leq 2$. Then*

$$\mathfrak{m}(f) = \begin{cases} 0 & \text{if and only if } f \text{ is balanced}, \\ 2^n & \text{if and only if } f \text{ is constant}, \\ 2^{n-2k} & \text{otherwise}, \end{cases}$$

where $2k = \mathrm{var}(f)$.

Proof. We analyze the different cases based on the degree of f. We have already seen that $\mathfrak{m}(f) = 2^n$ if and only if f is constant ($\deg(f) = 0$). If $\deg(f) = 1$, then f is balanced and $|Z(f)| = |U(f)| = 2^{n-1}$, so $\mathfrak{m}(f) = 0$.

If $\deg(f) = 2$, then by Theorem 2, we know that $f \sim_A g_1 = x_1x_2 + \cdots + x_{2k-1}x_{2k} + x_{2k+1}$, with $1 \leq k \leq \lfloor (n-1)/2 \rfloor$, if f is balanced, and $f \sim_A g_2 = x_1x_2 + \cdots + x_{2k-1}x_{2k} + c$, with $1 \leq k \leq \lfloor n/2 \rfloor$ and $c \in \mathbb{F}$, if f is not balanced. If f is balanced then $e_{2k+1} \in U(g_1)$ so $\mathfrak{m}(f) = \mathfrak{m}(g_1) = 0$. If

f is not balanced then $\mathrm{var}(f) = \mathrm{var}(g_2) = 2k$ and, for $b = (b_1, \ldots, b_n) \in \mathbb{F}^n$, $D_b g_2(x) = b_1 x_2 + b_2 x_1 + \cdots + b_{2k-1} x_{2k} + b_{2k} x_{2k-1}$. Clearly, $U(g_2) = \emptyset$ and, from Proposition 21, $\mathfrak{m}(f) = \mathfrak{m}(g_2) = 2^{n-2k}$. This concludes the proof. □

Now, we apply the notions introduced above to the derivatives of a Boolean function f. From this, we define a new parameter for Boolean functions. In the next subsection, we extend this parameter to vectorial Boolean functions and use it to characterize quadratic and cubic APN functions.

Definition 25. For $a \in \mathbb{F}^n$ and $f \in B_n$ with $n \in \mathbb{N}$, we consider the sets $Z_a(f) = Z(D_a f)$ and $U_a(f) = U(D_a f)$, hence $\mathfrak{m}(D_a f) = |Z_a(f)| - |U_a(f)|$. We define

$$\mathcal{M}(f) = \sum_{a \in \mathbb{F}^n \setminus \{0_n\}} \mathfrak{m}(D_a f).$$

Proposition 26. *Let $f \in B_n$. Then, for all $a \in \mathbb{F}^n$, $Z_a(f)$ is a vector space of positive dimension, and $U_a(f)$ is either a coset of $Z_a(f)$ or the empty set.*

Proof. Using Proposition 9, we only need to show that $Z_a(f)$ has nonzero dimension. Clearly, 0_n is in $Z_a(f)$. Observe that if $a = 0_n$ then $Z_a(f) = \mathbb{F}^n$ and if $a \neq 0_n$, then we have $D_a D_a f(x) = 0$, implying that $\{0_n, a\} \subseteq Z_a(f)$. So the dimension of $Z_a(f)$ is at least 1. □

We study now the behavior of the second-order derivative (and the mentioned parameters) when an extended affine transformation is applied.

Theorem 27. *Consider $g_1, g_2 \in B_n$ affine equivalent as in Lemma 11. Then $|Z_a(g_1)| = |Z_{M \cdot a}(g_2)|$ and $|U_a(g_1)| = |U_{M \cdot a}(g_2)|$. Hence, the parameter $\mathcal{M}(\cdot)$ is invariant under affine transformation. Moreover, the same is true if we consider EA-equivalent functions.*

Proof. From Lemma 11, we have that $D_a g_1 \sim_A D_{M \cdot a} g_2$. From the fact that also their second derivatives are affine equivalent, that is, there exists a linear permutation N such that $D_b D_a g_1 \sim_A D_{N \cdot b} D_{M \cdot a} g_2$, we can easily deduce that the two pairs of sets have the same cardinality. It follows that $\mathcal{M}(g_1) = \mathcal{M}(g_2)$.

Consider now $f \in B_n$ and $g = f + \ell$, where $\ell \in B_n$ is an affine function. Notice that $D_a D_b f = D_a D_b g$ for any $a, b \in \mathbb{F}^n$, and so $\mathfrak{m}(D_a f) = \mathfrak{m}(D_a g)$ for any $a \in \mathbb{F}^n$. Hence $\mathcal{M}(f) = \mathcal{M}(g)$ and the mentioned parameters are EA-invariant. □

The rest of this section is restricted to functions of degree at most three.

Proposition 28. *Let $f \in B_n$ be a function with $\deg(f) \in \{2, 3\}$. Then, for any $a \in \mathbb{F}^n$ we have*

$$\mathfrak{m}(D_a f) = \begin{cases} 0, & \text{if and only if } D_a f \text{ is balanced,} \\ 2^n, & \text{if and only if } D_a f \text{ is constant,} \\ 2^{n-j}, & \text{otherwise,} \end{cases}$$

where $j < n$ is a positive even integer.

Proof. Since $\deg(f) \in \{2,3\}$ we have $\deg(D_a f) \in \{0,1,2\}$. From Proposition 24, we only need to show that $j < n$. Proposition 26 tells us that $Z_a(f)$ has always positive dimension, so $\mathfrak{m}(D_a f) \neq 1$. This concludes the proof. □

Remark 29. Notice that, if we remove the restriction on the degree of f, then $\mathfrak{m}(D_a f) = 0$ implies that $D_a f$ is balanced but not vice versa. Moreover, j is not necessarily an even integer, but it still satisfies the restriction $1 \leq j \leq n-1$. This is obtained by using Proposition 21.

Proposition 30. *For any partially bent function $f \in B_n$ with $\deg(f) = 2,3$, we have $\mathcal{M}(f) = 2^n(2^k - 1)$, where $k = \dim V(f)$.*

Proof. For any partially bent function f, $D_a f$ is constant if and only if $a \in V(f)$ and $D_a f$ is balanced if and only if $a \notin V(f)$. Recall that all quadratic functions are partially bent. We know, from Proposition 28, that $\mathfrak{m}(D_a f) = 0$ if and only if $D_a f$ is balanced and $\mathfrak{m}(D_a f) = 2^n$ if and only if $D_a f$ is a constant. Thus, for any quadratic function f or any cubic partially bent function f with $k = \dim V(f)$, we have

$$\mathcal{M}(f) = \sum_{a \in \mathbb{F}^n \setminus \{0_n\}} \mathfrak{m}(D_a f) = \sum_{a \in V(f) \setminus \{0_n\}} \mathfrak{m}(D_a f) = 2^n(2^k - 1).$$

□

If a function f is bent, then $\dim V(f) = 0$ and so, by Proposition 30, $\mathcal{M}(f) = 0$. Thus, we have the following corollary.

Corollary 31. *Let $f \in B_n$ be a quadratic or cubic function. Then f is bent if and only if $\mathcal{M}(f) = 0$.*

Observe that Corollary 31 can also be deduced from Theorem 1 and Proposition 28. When f is of general degree, we can deduce the following.

Proposition 32. *Let $f \in B_n$ be such that $\mathcal{M}(f) = 0$. Then f is bent and n is even.*

Proof. Assume $\mathcal{M}(f) = 0$, so for any $a \in \mathbb{F}^n$, $a \neq 0_n$, $\mathfrak{m}(D_a f) = 0$. From Proposition 21, we know that this implies that $D_a f$ is balanced for any nonzero $a \in \mathbb{F}^n$, that is, f must be bent and n is an even integer. □

We now study the value of $\mathcal{M}(\cdot)$ for splitting functions.

Proposition 33. *Consider $f \in B_n$ such that $f \sim_A f_1(x_1, \ldots, x_k) + f_2(x_{k+1}, \ldots, x_n)$ ($f_1 \in B_k$, $f_2 \in B_{n-k}$). Then $\mathcal{M}(f) = \mathcal{M}^k(f_1)\mathcal{M}^{n-k}(f_2) + 2^{n-k}\mathcal{M}^k(f_1) + 2^k\mathcal{M}^{n-k}(f_2)$.*

Proof. We consider an element $a \in \mathbb{F}^n$ as $a = (a_1, a_2) \in \mathbb{F}^k \times \mathbb{F}^{n-k}$. Then, from Theorem 20, we deduce the following relation:

$$\begin{aligned}\mathcal{M}(f) &= \sum_{a \neq 0_n} \mathfrak{m}(D_a f) = \sum_{(a_1,a_2) \neq 0_n} \mathfrak{m}(D_{a_1} f_1 + D_{a_2} f_2) \\ &= \sum_{(a_1,a_2) \neq 0_n} \mathfrak{m}^k(D_{a_1} f_1)\mathfrak{m}^{n-k}(D_{a_2} f_2)\end{aligned}$$

$$
\begin{aligned}
&= \sum_{a_1 \neq 0_k} \sum_{a_2 \neq 0_{n-k}} \mathfrak{m}^k(D_{a_1} f_1)\mathfrak{m}^{n-k}(D_{a_2} f_2) + \mathfrak{m}^{n-k}(D_{0_{n-k}} f_2) \sum_{a_1 \neq 0_k} \mathfrak{m}^k(D_{a_1} f_1) \\
&\quad + \mathfrak{m}^k(D_{0_k} f_1) \sum_{a_2 \neq 0_{n-k}} \mathfrak{m}^{n-k}(D_{a_2} f_2) \\
&= \mathcal{M}^k(f_1)\mathcal{M}^{n-k}(f_2) + 2^{n-k}\mathcal{M}^k(f_1) + 2^k \mathcal{M}^{n-k}(f_2).
\end{aligned}
$$

□

In the following, we give some lower bounds for the parameter $\mathcal{M}(\cdot)$.

Proposition 34. *For $f \in B_n$ with $k = \mathrm{var}(f)$, we have*

$$\mathcal{M}(f) = 2^n \cdot (2^{n-k} - 1) + \mathcal{M}^k(\bar{f}) \cdot 2^{2(n-k)} \geq 2^n \cdot (2^{n-k} - 1).$$

Proof. Consider $\bar{f}$ as in Definition 14, that is, $f \sim_A \bar{f} \in B_k$. Using Proposition 33, we deduce the following relation,

$$
\begin{aligned}
\mathcal{M}(f) = \mathcal{M}(\bar{f}) &= \mathcal{M}^k(\bar{f})\mathcal{M}^{n-k}(0) + 2^{n-k}\mathcal{M}^k(\bar{f}) + 2^k \mathcal{M}^{n-k}(0) \\
&= \mathcal{M}^k(\bar{f}) \cdot (2^{n-k}(2^{n-k} - 1) + 2^{n-k}) + 2^k \cdot 2^{n-k}(2^{n-k} - 1) \\
&= \mathcal{M}^k(\bar{f}) \cdot 2^{2(n-k)} + 2^n \cdot (2^{n-k} - 1).
\end{aligned}
$$

□

Recalling that f is balanced if and only if $\bar{f}$ is balanced, we have the following corollary.

Corollary 35. *If f is not variable maximal ($k = \mathrm{var}(f) < n$), then*

1. $\mathcal{M}(f) \geq 2^n$;
2. $\mathcal{M}(f) = 2^n$ *if and only if* $\bar{f}$ *is bent and* $\mathrm{var}(f) = n - 1$ *with n odd;*
3. *if f is balanced then* $\mathcal{M}(f) \geq 2^n \cdot (2^{n-k} - 1) + 2^{2(n-k)} \geq 2^n + 4$.

Proposition 36. *For an even positive integer n, consider $f \in B_n$ a balanced function with* $\deg(f) \leq 3$. *Then* $\mathcal{M}(f) \geq 4$.

Proof. Assume $\mathcal{M}(f) = \sum_{a \neq 0_n} \mathfrak{m}(D_a f) \leq 3$. From Proposition 28, we know that $\mathfrak{m}(D_a f) \in \{0, 2^n, 2^{n-j}\}$, with $j < n$ a positive even integer. Hence, $n - j \neq 0$ and, since n is even, $n - j \neq 1$. Therefore, $\mathfrak{m}(D_a f) \neq 1, 2$ and so $\mathcal{M}(f) \notin \{1, 2, 3\}$. From the previous results, we also have that, since f is balanced, $\mathcal{M}(f) \neq 0$. This concludes the proof. □

Lemma 37. *Let $f \in B_n$, with n odd, be quadratic. Then* $\dim V(f) \geq 1$ *and equality holds if and only if f is semi-bent.*

Proof. From Theorem 2, observe that

$$|V(f)| = |\{c = (c_1, \ldots, c_n) \in \mathbb{F}^n \mid c_1 = \cdots = c_{2i} = 0, i \leq (n-1)/2\}|.$$

It follows that $|V(f)| = 2^{n-2i}$. Since n is odd, we must have $\dim V(f) \geq 1$. We observe, from Theorem 3, that f is semi-bent if and only if $f \sim_A x_1x_2 + \cdots + x_{n-2}x_{n-1} + x_n$ or $f \sim_A x_1x_2 + \cdots + x_{n-2}x_{n-1} + c$, with $c \in \mathbb{F}$. From this, we deduce that f is semi-bent if and only if $\dim V(f) = 1$. □

By Proposition 28 and Lemma 37, the following corollary holds.

Corollary 38. *For n odd, a quadratic Boolean function $f \in B_n$ is semi-bent if and only if $\mathcal{M}(f) = 2^n$.*

We conclude this section with the study of $\mathcal{M}(f)$ for a particular splitting function f.

Proposition 39. *Let $n \in \mathbb{N}$ be even and consider $f \in B_n$ a cubic function. If $f \sim_A g(x_1) + h(x_2, \ldots, x_n)$, then there exist two distinct nonzero elements $a, b \in \mathbb{F}^n$ such that $D_a f$ and $D_b f$ are not balanced. Moreover, we have that $\mathcal{M}(f) > 2^n + 1$.*

Proof. Given Lemma 11 and Theorem 27, we can consider without loss of generality $f = g(x_1) + h(x_2, \ldots, x_n)$. Set $a = e_1$, then $D_a f$ is constant, hence it is not balanced. If $D_b f$ is balanced for every $b \in \mathbb{F}^n$, $b \neq 0_n, a$, then we have that $D_c h_{\restriction \mathbb{F}^{n-1}}$ is balanced for every $c \in \mathbb{F}^{n-1} \setminus \{0_{n-1}\}$. That is, $h \in B_{n-1}$ is bent. This is not possible since $n-1$ is odd. Therefore, there must exist another element $b \in \mathbb{F}^n \setminus \{0_n, a\}$ such that $D_b f$ is not balanced. From Theorem 28, we have that $\mathcal{M}_a(f) = 2^n$ and $\mathcal{M}_b(f) = 2^{n-j}$, for a positive integer $j < n$. So, $\mathcal{M}(f) \geq 2^n + 2$. □

4. APN Functions and Their Second-Order Derivatives

We move now to study vectorial Boolean functions. In particular, we extend the parameters introduced for Boolean functions and we use them to characterize APN maps of low degree.

Definition 40. For a function $F : \mathbb{F}^n \to \mathbb{F}^n$ with $n \in \mathbb{N}$, define

$$\mathcal{M}(F) = \sum_{\lambda \in \mathbb{F}^n \setminus \{0_n\}} \mathcal{M}(F_\lambda).$$

It will be clear from the context whether the parameter $\mathcal{M}(\cdot)$ is applied to Boolean functions, Definition 25, or to vectorial Boolean functions, above definition.

We prove in the following the invariance of this quantity.

Theorem 41. *The value $\mathcal{M}$ is invariant under EA-transformation.*

Proof. Consider two EA-equivalent (n, n)-functions F and G. Set $F = A_1 \circ G \circ A_2 + A$, where A_1 is a linear permutation, A_2 is an affine permutation and A is an affine transformation (of $\mathbb{F}^n$). We prove that $\mathcal{M}(F) = \mathcal{M}(G)$ in three steps.

1. Consider $G' = F + A$. Then a coordinate of G' is of the form $G'_\lambda = \lambda \cdot G' = \lambda \cdot (F + A) = \lambda \cdot F + \lambda \cdot A = F_\lambda + \varphi$, for $\varphi \in A_n$. Since F_λ is EA-equivalent to G'_λ, then applying Theorem 27, we have $\mathcal{M}(F) = \mathcal{M}(G')$.
2. Consider $G' = F \circ A_2$. Then $G'_\lambda(x) = \lambda \cdot G'(x) = \lambda \cdot F(A_2(x)) = F_\lambda(A_2(x))$. Similarly as before, we obtain $\mathcal{M}(F) = \mathcal{M}(G')$.
3. Consider $G' = A_1 \circ F$. Since A_1 is a linear permutation of $\mathbb{F}^n$, then there exists a permutation σ of $\mathbb{F}^n$ such that $G'_\lambda = (A_1 \circ F)_\lambda = F_{\sigma(\lambda)}$. Therefore, $\mathcal{M}(F) = \mathcal{M}(G')$.

Combining these three results, we complete the proof. □

Remark 42. Notice that, in general, the parameter $\mathcal{M}$ is not invariant under CCZ-equivalence, see [12] for the definition of CCZ-equivalence. For example, if we consider the two CCZ-equivalent permutations, defined over $\mathbb{F}_{2^5}$, $F(x) = x^3$ and $F'(x) = x^{11}$, we have $\mathcal{M}(F) = 240$ and $\mathcal{M}(F') = 360$.

We establish a connection between the fourth power moment of the Walsh transform and the value $\mathcal{M}(F)$, and consequently derive a characterization of quadratic and cubic APN functions based on the latter quantity.

First, we consider two known results and their proofs, to prepare the background for our subsequent arguments (see for instance page 140 in [11]).

Lemma 43. *For $n \in \mathbb{N}$, consider F an (n, n)-function. Then*

$$\begin{aligned} L_4(F) &= 2^n \sum_{\lambda \in \mathbb{F}^n \setminus \{0_n\}} \sum_{a,b,x \in \mathbb{F}^n} (-1)^{D_a D_b F_\lambda(x)} \\ &= 2^{2n} \sum_{a,b \in \mathbb{F}^n} |\{x \in \mathbb{F}^n \mid D_a D_b F(x) = 0_n\}| - 2^{4n}. \end{aligned}$$

Proof. Given Eq. (2.2), we have

$$\begin{aligned} L_4(F) &= \sum_{\lambda \in \mathbb{F}^n \setminus \{0_n\}} L_4(F_\lambda) = 2^n \sum_{\lambda \in \mathbb{F}^n \setminus \{0_n\}} \sum_{a \in \mathbb{F}^n} \mathcal{F}^2(D_a F_\lambda) \\ &= 2^n \sum_{\lambda \in \mathbb{F}^n \setminus \{0_n\}} \sum_{a,x,y \in \mathbb{F}^n} (-1)^{D_a F_\lambda(x) + D_a F_\lambda(y)} \\ &= 2^n \sum_{\lambda \in \mathbb{F}^n \setminus \{0_n\}} \sum_{a,b,x \in \mathbb{F}^n} (-1)^{D_a D_b F_\lambda(x)} \\ &= 2^n \sum_{\lambda \in \mathbb{F}^n} \sum_{a,b,x \in \mathbb{F}^n} (-1)^{\lambda \cdot D_a D_b F(x)} - 2^n \cdot 2^{3n} \\ &= 2^{2n} \sum_{a,b \in \mathbb{F}^n} |\{x \in \mathbb{F}^n \mid D_a D_b F(x) = 0_n\}| - 2^{4n}, \end{aligned}$$

where the equation in the second line is obtained by substituting $y = x + b$. □

From Lemma 43, observe that, for any function $F : \mathbb{F}^n \to \mathbb{F}^n$, we have

$$L_4(F) = 2^n \sum_{\lambda,a,b \in \mathbb{F}^n, \lambda \neq 0_n} \mathcal{F}(D_a D_b F_\lambda). \tag{4.1}$$

So, by Theorem 6 and Eq. (4.1), we deduce the following result, which relates an APN function to its second-order derivatives.

Theorem 44. *For $F : \mathbb{F}^n \to \mathbb{F}^n$, we have that*

$$\sum_{\lambda,a,b \in \mathbb{F}^n, \lambda \neq 0_n} \mathcal{F}(D_a D_b F_\lambda) \geq 2^{2n+1}(2^n - 1).$$

Moreover, F is APN if and only if the equality holds.

We use now the above-mentioned notation to present our results.

Lemma 45. *Let $F : \mathbb{F}^n \to \mathbb{F}^n$ be a function of* $\deg(F) \in \{2, 3\}$. *Then*

$$L_4(F) = 2^{3n}(2^n - 1) + 2^{2n}\mathcal{M}(F).$$

Proof. For $a, b, \lambda \in \mathbb{F}^n$, if $\deg(D_a D_b F_\lambda) = 1$, then $\sum_{x\in\mathbb{F}^n}(-1)^{D_a D_b F_\lambda(x)} = 0$. Hence, by Lemma 43, we have

$$\begin{aligned}
L_4(F) &= 2^n \sum_{\lambda\in\mathbb{F}^n\setminus\{0_n\}} \sum_{a,b,x\in\mathbb{F}^n} (-1)^{D_a D_b F_\lambda(x)} \\
&= 2^n \sum_{\lambda\in\mathbb{F}^n\setminus\{0_n\}} \sum_{b\in\mathbb{F}^n} \sum_{x,a\in\mathbb{F}^n \mid \deg(D_a D_b F_\lambda)=0} (-1)^{D_a D_b F_\lambda(x)} \\
&= 2^n \sum_{\lambda\in\mathbb{F}^n\setminus\{0_n\}} \sum_{b\in\mathbb{F}^n} 2^n \sum_{a\in\mathbb{F}^n \mid \deg(D_a D_b F_\lambda)=0} (-1)^{D_a D_b F_\lambda(0)} \\
&= 2^{2n} \sum_{\lambda\in\mathbb{F}^n\setminus\{0_n\}} \sum_{b\in\mathbb{F}^n} \left(\sum_{a\in\mathbb{F}^n \mid D_a D_b F_\lambda=0} (-1)^0 + \sum_{a\in\mathbb{F}^n \mid D_a D_b F_\lambda=1} (-1)^1 \right) \\
&= 2^{2n} \sum_{\lambda\in\mathbb{F}^n\setminus\{0_n\}} \sum_{b\in\mathbb{F}^n} (|\{a \in \mathbb{F}^n \mid D_a D_b F_\lambda = 0\}| - |\{a \in \mathbb{F}^n \mid D_a D_b F_\lambda = 1\}|) \\
&= 2^{2n} \sum_{\lambda\in\mathbb{F}^n\setminus\{0_n\}} |\{a \in \mathbb{F}^n \mid D_a D_0 F_\lambda = 0\}| + 2^{2n} \sum_{\lambda,b\in\mathbb{F}^n\setminus\{0_n\}} \mathfrak{m}(D_b F_\lambda) \\
&= 2^{2n} \sum_{\lambda\in\mathbb{F}^n\setminus\{0_n\}} 2^n + 2^{2n}\mathcal{M}(F) = 2^{3n}(2^n - 1) + 2^{2n}\mathcal{M}(F).
\end{aligned}$$

□

Given the equality presented in Lemma 45, we have that, for quadratic and cubic functions F, all the relations involving $L_4(F)$ can be translated into relations involving $\mathcal{M}(F)$.

Theorem 46. *Let $F : \mathbb{F}^n \to \mathbb{F}^n$ be a function with* $\deg(F) \in \{2, 3\}$. *Then*

$$\mathcal{M}(F) \geq 2^n(2^n - 1).$$

Moreover, F is APN if and only if the equality holds.

Proof. From Theorem 6 and Lemma 45, we have

$$2^{3n}(2^n - 1) + 2^{2n}\mathcal{M}(F) \geq 2^{3n+1}(2^n - 1)$$

from which we deduce that $\mathcal{M}(F) \geq 2^n(2^n - 1)$ and equality holds if and only if F is APN. □

Corollary 47. *An APN function $F : \mathbb{F}^n \to \mathbb{F}^n$ with* $\deg(F) \in \{2, 3\}$ *has at most $2^n - 1$ pairs (a, λ) $(a, \lambda \neq 0_n)$ such that $D_a F_\lambda$ is constant.*

Proof. Recall that $\mathfrak{m}(D_a F_\lambda) = 2^n$ if $D_a F_\lambda$ is constant. Therefore, Theorem 46 implies this result. □

Remark 48. Note that this bound follows also from the result in [16, Theorem 1], which indicates that, for a w-APN (n, n)-function F, every nonzero derivative $D_a F$ admits at most one constant component $D_a F_\lambda$, $\lambda \neq 0_n$. We recall that an (n, n)-function F is *weakly APN* (w-APN) if for any $a \in \mathbb{F}^n \setminus \{0_n\}$

the image set of the derivative D_aF is such that $|\mathrm{Im}(D_aF)| > 2^{n-2}$. So an APN function is weakly APN. However, observe that [16, Theorem 1] holds for any degree.

From Proposition 30, we deduce the following corollary.

Corollary 49. *Let $F : \mathbb{F}^n \to \mathbb{F}^n$ be a strongly plateaued function with* $\deg(F) = 2, 3$. *Then*

$$\mathcal{M}(F) = 2^n \sum_{\lambda \in \mathbb{F}^n \setminus \{0_n\}} (2^{\dim V(F_\lambda)} - 1). \tag{4.2}$$

Example 50. Let $F(x_1, x_2, x_3) = (f_1, f_2, f_3)$ where $f_1 = x_1x_3 + x_2x_3 + x_1$, $f_2 = x_2x_3 + x_1 + x_2$ and $f_3 = x_1x_2 + x_1 + x_2 + x_3$ are all in B_3. One can verify that all components are quadratic, then compute $\dim V(F_\lambda)$ and, using Corollary 49, obtain $\mathcal{M}(F) = 2^3 \cdot (2^3 - 1) = 56$. Therefore, by Theorem 46, we conclude that F is an APN function. Moreover, all components are balanced, implying that F is an APN permutation.

We want to stress that we are interested in the parameter $\mathcal{M}(F)$ from a theoretical point of view. In particular, we are interested in studying the parameter $\mathcal{M}$ related to APN permutations.

The following result basically coincides with Proposition 3.2 in [6].

Theorem 51. *For an APN permutation $F : \mathbb{F}^n \to \mathbb{F}^n$ every nonzero component F_λ is such that $\mathfrak{m}(F_\lambda) = 0, 1$ and $Z(F_\lambda) = \{0_n\}$.*

Proof. Consider F an APN permutation and recall that the APN property implies that for any nonzero $a \in \mathbb{F}^n$, $|\mathrm{Im}(D_aF)| = 2^{n-1}$. Assume there exists $a, \lambda \in \mathbb{F}^n \setminus \{0_n\}$ such that $a \in Z(F_\lambda)$, that is, $D_aF_\lambda = 0$. Up to an affine transformation, we can assume that F_λ is the first component of $F = (f_1, \ldots, f_n)$, i.e. $F_\lambda = f_1$. Hence $D_aF = (0, D_af_2, \ldots, D_af_n)$ and $|\mathrm{Im}(D_aF)| = 2^{n-1}$ implies $0_n \in \mathrm{Im}(D_aF)$. This is not possible since F is a permutation. Therefore, $Z(F_\lambda) = \{0_n\}$ and $\mathfrak{m}(F_\lambda) = 0, 1$. □

Combining this result with Proposition 16, we deduce the following.

Corollary 52. *Every nonzero component of an APN permutation is variable maximal.*

Fact. *Set F to be the APN permutation in six variables presented by Dillon in [4]. The function has 7 nonzero components F_λ such that $\mathfrak{m}(F_\lambda) = 0$. In the other cases we have $\mathfrak{m}(F_\lambda) = 1$.*

Remark 53. Theorem 51 implies that, given F an APN permutation, every nonzero component F_λ admits at most one constant derivative. Combining this with the result mentioned in Remark 48, we have that, for any $\alpha \neq 0_n$, there exists at most one $\beta \neq 0_n$ such that $D_\alpha F_\beta = 1$ or $D_\beta F_\alpha = 1$.

We now restrict to the case of pure cubic APN permutations in even dimension, where pure cubic means that all the nonzero components are of degree three.

Table 1. The value of $\mathcal{M}(F)$ for some APN power functions $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with $\deg(F) > 3$

n	F	Name	$\mathcal{M}(F)$	$2^n(2^n-1)$	n	F	Name	$\mathcal{M}(F)$	$2^n(2^n-1)$
5	x^{15}	Inverse	1916	992	8	x^{57}	Kasami	130330	65280
7	x^{63}	Inverse	32258	16256	9	x^{255}	Inverse	522242	261632
	x^{57}	Kasami	32274			x^{241}	Kasami	522242	

Proposition 54. *For n a positive even integer, consider $F : \mathbb{F}^n \to \mathbb{F}^n$ an APN permutation of degree 3. Then either one of the following two conditions is satisfied.*

1. *Every nonzero component F_λ is such that $\mathcal{M}(F_\lambda) = 2^n$.*
2. *There are two distinct nonzero components F_λ, F_γ such that $\mathcal{M}(F_\lambda) < 2^n$ and $\mathcal{M}(F_\gamma) \leq 2^n$.*

Proof. From Theorem 3.3 in [6], we know that F cannot have partially-bent components, implying that any nonzero component F_λ must have degree 3 and so, F is pure cubic. Set $\lambda \in \mathbb{F}^n$ be such that $\mathcal{M}(F_\lambda) = \min_{\gamma \in \mathbb{F}^n \setminus \{0_n\}} \mathcal{M}(F_\gamma)$. From Theorem 46, we have that $\mathcal{M}(F_\lambda) \leq 2^n$. If $\mathcal{M}(F_\lambda) = 2^n$, then we are in the first case, hence for any nonzero $\gamma \in \mathbb{F}^n$ $\mathcal{M}(F_\gamma) = 2^n$.

Assume otherwise that $\mathcal{M}(F_\lambda) < 2^n$. Moreover, assume that for any $\gamma \in \mathbb{F}^n$, $\gamma \neq 0_n, \lambda$, we have $\mathcal{M}(F_\gamma) > 2^n$. Therefore,

$$\begin{aligned} 2^n(2^n-1) =& \mathcal{M}(F) = \sum_{\gamma \neq 0_n} \mathcal{M}(F_\gamma) = \mathcal{M}(F_\lambda) + \sum_{\gamma \neq 0_n, \lambda} \mathcal{M}(F_\gamma) \\ \geq& \mathcal{M}(F_\lambda) + \sum_{\gamma \neq 0_n, \lambda} (2^n+1) = \mathcal{M}(F_\lambda) + (2^n-2)(2^n+1) \end{aligned}$$

Implying that $\mathcal{M}(F_\lambda) \leq 2^n(2^n-1) - (2^n-2)(2^n+1) = 2$.

From Proposition 36, we know that this is not possible. Therefore, there must exists at least another component of F satisfying the restriction. □

Remark 55. From Proposition 39, we can deduce that a function F as in the above proposition cannot have all but two components that are (equivalent to) splitting functions of the form $g(x_1) + h(x_2, \ldots, x_n)$.

4.1. Computational Analysis On (n, n)-Functions of Higher Degree

We present here some computational results obtained using the Magma Algebra package [5].

We have mainly studied the parameter $\mathcal{M}$ for quadratic and cubic functions. We now consider functions of higher degree and we analyze the behavior of this parameter. We recall to the reader that we can identify the vector space $\mathbb{F}^n$ with the finite field $\mathbb{F}_{2^n}$ of 2^n elements. Therefore, we can consider (n, n)-functions also as functions from $\mathbb{F}_{2^n}$ to itself. These functions can be represented as polynomials over $\mathbb{F}_{2^n}$ of degree at most $2^n - 1$. In the following computations, we use this representation.

Table 1 shows the value of $\mathcal{M}(F)$ for some known APN power functions.

Table 2. The value of $\mathcal{M}(F)$ for some non-APN power functions $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with $\deg(F) > 3$

n	F	$\mathcal{M}(F)$	F	$\mathcal{M}(F)$	n	F	$\mathcal{M}(F)$	F	$\mathcal{M}(F)$
6	x^{15}	8154	x^{27}	35280	8	x^{23}	130036	x^{43}	130098
	x^{23}	8402	x^{31}	7938		x^{51}	1101600	x^{29}	130104
7	x^{15}	32258	x^{29}	32282		x^{85}	4211712	x^{15}	130050
						x^{87}	130172	x^{27}	130292

Table 3. All possible values of $\mathcal{M}(f)$, for $f \in B_8$ with $\deg(f) \leq 3$

0	384	552	720	888	1056	1296	1584	2016	2496	3456	6912	16128
192	408	576	744	912	1080	1344	1632	2064	2688	3648	7488	22272
240	432	600	768	936	1104	1392	1680	2112	2784	3792	8064	65280
288	456	624	792	960	1152	1440	1728	2208	2880	3840	8448	
312	480	648	816	984	1200	1488	1824	2256	3024	4416	8832	
336	504	672	840	1008	1224	1512	1872	2304	3072	4800	9984	
360	528	696	864	1032	1248	1536	1920	2352	3264	5376	11520	

We compare the value $\mathcal{M}(F)$ with the quantity $2^n(2^n - 1)$. Indeed, we know from Theorem 46 that a function of degree two or three is APN if and only if $\mathcal{M}(F) = 2^n(2^n - 1)$. Clearly, this is not true for functions of higher degree. Notice that, for the inverse function over $\mathbb{F}_{2^n}$ with $n = 7, 9$, we have $\mathcal{M}(F) = 2 \cdot (2^n - 1)^2$.

Table 2 shows the value of $\mathcal{M}(F)$ for some power functions that are not APN.

5. On Cubic APN Permutations over $\mathbb{F}^8$

It is known that there are no cubic APN permutations in dimension six, see for example Theorem 5.4 in [6]. We study here the case of a possible cubic APN permutation in dimension eight. Indeed, to our knowledge it is still not known whether such a function exists. As mentioned earlier, every nonzero component of a cubic APN permutation must have degree 3. Moreover, from Proposition 54, we know that at least two components f_1, f_2 are such that $\mathcal{M}(f_1), \mathcal{M}(f_2) \leq 2^n$.

We consider the work done in [20], where the author classifies cubic Boolean functions (not considering linear and constant terms) up to linear equivalence and affine equivalence. There are listed 3796971 classes for the linear equivalence and 20748 classes for the affine equivalence. Since $\mathcal{M}(\cdot)$ is EA-invariant (see Theorem 27), we consider the second list and compute the value $\mathcal{M}(f)$ for the representative f of each class. We obtain a list of 87 different possible values for $\mathcal{M}(f)$, see Table 3.

Table 4. All possible values of $\mathcal{M}(f)$ for $f \in B_8$, with $\deg(f) = 3$, f balanced and with at most 2 constant derivatives

192	408	528	648	768	888	1008	1200	1536	1920	2496	3264	8832
288	432	552	672	792	912	1032	1248	1584	2016	2688	3456	
336	456	576	696	816	936	1056	1344	1632	2112	2784	3648	
360	480	600	720	840	960	1104	1440	1728	2208	2880	4800	
384	504	624	744	864	984	1152	1512	1824	2304	3072	8064	

Notice that the value $2^n = 256$ is not displayed in the table. So the first case mentioned in Proposition 54 cannot happen.

Since we are interested in the components of a cubic APN permutation, we can restrict our search with the following observations.

- The value $\mathcal{M}(f) = 65280$ corresponds to the constant function.
- No cubic Boolean function has value $\mathcal{M}(f) = 16128$.
- We are interested only in functions f equivalent to balanced maps, that is, there must exist an affine map ℓ such that $f + \ell$ is balanced.
- Finally, functions with more than three constant derivatives cannot be components of an APN permutation. Indeed, this would lead to having a component with a derivative constantly null.

With the above observations, we restrict the number of possible values for $\mathcal{M}(f)$ to 61, see Table 4.

Notice that the only value smaller than 2^n is $\mathcal{M}(f) = 192$. In Table 5, we list the representatives of the classes (equivalent to balanced maps) such that $\mathcal{M}(f) = 192$.

From Table 4, we know that, for F a cubic APN permutation in eight variables, $\mathcal{M}(F_\lambda) = 192$ or $\mathcal{M}(F_\lambda) \geq 288$. Set Λ to be the set of λ's such that $\mathcal{M}(F_\lambda) \leq 2^n$. We now focus on the size of this set Λ.

Theorem 56. *Let F be a cubic APN permutation in 8 variables and let Λ be the set $\{\lambda \in \mathbb{F}^n \mid \mathcal{M}(F_\lambda) \leq 2^n\}$. Then the size of Λ is between 85 and 252.*

Proof. We first prove that $|\Lambda| \geq 85$. Since F is a cubic APN map, Theorem 46 holds.

$$\begin{aligned} 2^n(2^n-1) = \sum_{\lambda \neq 0_n} \mathcal{M}(F_\lambda) &= 192 \cdot |\Lambda| + \sum_{\lambda \notin \Lambda \cup \{0_n\}} \mathcal{M}(F_\lambda) \\ &\geq 192 \cdot |\Lambda| + (2^n - 1 - |\Lambda|) \cdot 288 \\ &= 2^n \cdot 288 - 288 - |\Lambda| \cdot (288 - 192). \end{aligned}$$

Therefore, it follows that $|\Lambda| \geq \frac{2^n(288-2^n+1)-288}{288-192} = \frac{2^n(33)}{96} - 3 = 85$. Furthermore, we claim that Λ contains at most $2^n - 4$ elements. Clearly, $|\Lambda| \leq 2^n - 2$, and if $|\Lambda| = 2^n - 2$ then $2^n(2^n-1) = 192 \cdot (2^n-2) + \mathcal{M}(F_\gamma)$, with $\gamma \notin \Lambda \cup \{0_n\}$, and this equation would imply $\mathcal{M}(F_\gamma) = 16512$, which is not possible, see Table 4. Similarly, we can discard the case $|\Lambda| = 2^n - 3$. Indeed, $2^n(2^n-1) = 192 \cdot (2^n-3) + \mathcal{M}(F_\gamma) + \mathcal{M}(F_\delta)$, and so $\mathcal{M}(F_\gamma) + \mathcal{M}(F_\delta) = 16704$. But no two values in Table 4 sum to 16704. □

Table 5. List of functions f in B_8 (up to EA-equivalence) equivalent to balanced functions with $\mathcal{M}(f) \leq 2^n$

No.	function f	$\mathcal{M}(f)$
1	$x_1x_2 + x_1x_3x_4 + x_1x_5x_6 + x_1x_7x_8 + x_2x_3x_7 + x_2x_3 + x_3x_6 + x_3x_8 + x_4x_5 + x_4x_7 + x_5x_6$	192
2	$x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_2x_7 + x_1x_3x_8 + x_1x_3 + x_1x_4x_8 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5x_7 + x_2x_5 + x_2x_6 + x_3x_6 + x_3x_7 + x_4x_6 + x_6x_7x_8$	192
3	$x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_2x_7 + x_1x_2 + x_1x_3x_8 + x_1x_3 + x_1x_4x_8 + x_1x_7 + x_2x_5x_7 + x_2x_5 + x_2x_8 + x_3x_6 + x_4x_5 + x_6x_7x_8$	192
4	$x_1x_2x_4 + x_1x_4x_5 + x_1x_5x_7 + x_1x_8 + x_2x_3x_7 + x_2x_5 + x_3x_4x_5 + x_3x_6$	192
5	$x_1x_2x_4 + x_1x_5x_7 + x_1x_8 + x_2x_3x_4 + x_2x_7 + x_3x_6 + x_4x_5$	192
6	$x_1x_2x_4 + x_1x_4 + x_1x_8 + x_2x_5x_7 + x_2x_6 + x_3x_4 + x_3x_5 + x_3x_7x_8$	192
7	$x_1x_2x_4 + x_1x_5 + x_1x_6 + x_1x_8 + x_2x_5x_7 + x_2x_6 + x_3x_5 + x_3x_7x_8 + x_4x_7$	192
8	$x_1x_2x_4 + x_1x_4 + x_1x_5 + x_1x_6 + x_1x_8 + x_2x_5x_7 + x_2x_5 + x_2x_6 + x_3x_6 + x_3x_7x_8 + x_4x_7$	192

The same argument as in the proof cannot be extended for the other values of $|\Lambda|$. For example, consider the case $|\Lambda| = 2^n - 4$. There must exist $\gamma, \delta, \epsilon \notin \Lambda \cup \{0_n\}$ such that $\mathcal{M}(F_\gamma)+\mathcal{M}(F_\delta)+\mathcal{M}(F_\epsilon) = 2^n(2^n-1)-192\cdot(2^n-4) = 16896$. This is possible with $\mathcal{M}(F_\gamma) = 768,\ \mathcal{M}(F_\delta) = \mathcal{M}(F_\epsilon) = 8064$.

Remark 57. Theorem 56 implies that, up to EA-equivalence, at least 85 components of a cubic permutation in eight variables must belong to Table 5, as already displayed in [20].

Acknowledgements

The results in this paper appear partially in the last author's MSc thesis and in the first author's PhD thesis, both supervised by the second author. The first author acknowledges the support from Ripple's University Blockchain Research Initiative. The third author is a member of the INdAM Research Group GNSAGA.

Author contributions The results in this paper appear partially in MZ's MSc thesis and in AM's PhD thesis, both supervised by MS. IV improved the results and structered the manuscript, toghether with MS. AM, MS and IV reviewed the manuscript.

Funding Open access funding provided by Università degli Studi di Trento within the CRUI-CARE Agreement.

Data Availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The second author is an Editorial Board Member of Mediterranean Journal of Mathematics

References

[1] Berger, T.P., Canteaut, A., Charpin, P., Laigle-Chapuy. Y.: On almost perfect nonlinear functions over $\mathbb{F}_2^n$. IEEE Trans. Inf. Theory **52**(9), 4160–4170 (2006)

[2] Beth, T., Ding, C.: On almost perfect nonlinear permutations. In: Advances in Cryptology—EUROCRYPT '93. vol. 765, pp. 65–76. Springer, Berlin, Heidelberg (1993)

[3] Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)

[4] Browning, K., Dillon, J., Kibler, R., McQuistan, M.: APN polynomials and related codes. J. Combin. Inf. Syst. Sci **34**, 135–159 (2009)

[5] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system I: the user language. J. Symb. Comput. **24**, 235–265 (1997)

[6] Calderini, M., Sala, M., Villa, I.: A note on APN permutations in even dimension. Finite Fields Their Appl. **46**, 1–6 (2017)

[7] Canteaut, A.: Cryptographic functions and design criteria for block ciphers. In: Rangan C.P., Ding C. (eds) Progress in Cryptology—INDOCRYPT 2001. INDOCRYPT 2001. Lecture Notes in Computer Science, vol. 2247, pp. 1–16. Springer, Berlin, Heidelberg (2001)

[8] Canteaut, A., Duval, S., Perrin, L.: A generalisation of Dillon's APN permutation with the best known differential and nonlinear properties for all fields of size 2^{4k+2}. IEEE Trans. Inf. Theory **63**(11), 7575–7591 (2017)

[9] Canteaut, A., Perrin, L., Tian, S.: If a generalised butterfly is APN then it operates on 6 bits. Cryptogr. Commun. **11**, 1147–1164 (2019)

[10] Carlet, C.: Open questions on nonlinearity and on APN functions. In: Koç, Ç., Mesnager, S., Savaş, E. (eds) Arithmetic of Finite Fields. WAIFI 2014. Lecture Notes in Computer Science, vol. 9061. Springer, Cham (2015)

[11] Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge (2021)

[12] Carlet, C., Charpin, P., Zinoviev. V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**(2), 125–156 (1998)

[13] Chee, S., Lee, S., Kim K.: Semi-bent functions. In: Pieprzyk, J., Safavi-Naini, R. (eds.) Advances in Cryptology-ASIACRYPT'94. Proceedings of the 4th International Conference on the Theory and Applications of Cryptology, vol. 917, pp. 107–118. Springer, Wollongong (1994)

[14] Cusick, T. W., Stanica, P.: Chapter 6 - special types of Boolean functions. In: Thomas, W.C., Pantelimon, S., (eds.), Cryptographic Boolean Functions and Applications (Second Edition), Academic Press, pp. 109–142 (2017)

[15] Dillon, J. F.: Elementary Hadamard difference sets. Proceedings of Sixth S-E Conference of Combinatorics, Graph Theory, and Computing, Utility Mathematics, Winnipeg, pp. 237–249 (1975)

[16] Fontanari, C., Pulice, V., Rimoldi, A., Sala, M.: On weakly APN functions and 4-bit S-Boxes. Finite Fields Their Appl. **18**(3), 522–528 (2012)

[17] Hou, X.-D.: Affinity of permutations of $\mathbb{F}_2^n$. Discrete Appl. Math. **154**(2), 313–325 (2006)

[18] Idrisova, V.: On an algorithm generating 2-to-1 APN functions and its applications to "the big APN problem". Cryptogr. Commun. **11**, 21–39 (2019)

[19] Knudsen, L.: Truncated and higher order differentials. In: 2nd International Workshop on Fast Software Encryption (FSE 1994), pp. 196–211. Springer-Verlag, Leuven (1994)

[20] Langevin, P.: Classification of RM(3,8)/RM(1,8). http://langevin.univ-tln.fr/project/rm832/rm832.html

[21] MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. Elsevier, New York (1977)

[22] Musukwa, A., Sala, M., Villa, I., Zaninelli, M.: On cryptographic properties of cubic and splitting Boolean functions. Applicable Algebra in Engineering, Communication and Computing, pp. 1–17 (2022)

[23] Nyberg, K.: Differentially uniform mappings for cryptography. Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg (1993)

[24] Perrin, L., Udovenko, A., Biryukov, A.: Cryptanalysis of a theorem: decomposing the only known solution to the big APN problem. In: Robshaw, M., Katz, J. (eds) Advances in Cryptology—CRYPTO 2016. CRYPTO 2016. Lecture Notes in Computer Science, vol 9815. Springer, Berlin (2016)

[25] Wagner, D.: The boomerang attack. In: International Workshop on Fast Software Encryption. pp. 156-17. Springer, Berlin (1999)

[26] Wu, C., Feng, D.: Boolean Functions and Their Applications in Cryptography. Springer, New York (2016)

Augustine Musukwa
Mzuzu University
P/Bag 201, Luwinga
Mzuzu 2
Malawi

e-mail: augustinemusukwa@gmail.com

Augustine Musukwa, Massimiliano Sala, Irene Villa and Marco Zaninelli
University of Trento
Via Sommarive, 14
38123 Povo
Trento
Italy

e-mail: irene1villa@gmail.com

Massimiliano Sala
e-mail: maxsalacodes@gmail.com

Marco Zaninelli
e-mail: zaninelli.marco21@gmail.com

Irene Villa
University of Genova
Via Dodecaneso, 35
16146 Genoa
Italy

Marco Zaninelli
University of Pennsylvania
209 South 33rd Street
Philadelphia
PA19104
USA

Received: January 12, 2024.
Revised: April 17, 2024.
Accepted: April 19, 2024.