Polynomials with Linear Structure and Maiorana-McFarland Construction

Pascale Charpin and Sumanta Sarkar
SECRET Project-Team - INRIA Paris-Rocquencourt
Domaine de Voluceau - B.P. 105 - 78153 Le Chesnay Cedex - France
pascale.charpin@inria.fr, sumanta.sarkar@inria.fr

***Abstract*—We study permutations over the finite fields that have linear structures. Our main result is to show the relation between a Maiorana-McFarland function with an affine derivative and a polynomial with a linear structure.**

I. Introduction

Bent functions with affine derivatives, i.e., derivatives of degree at most 1, have been studied in [8] and (extensively) in [2]. In [8], Hou proved that all the 8-variable cubic bent functions have at least one affine derivative. However, the existence of 6-variable cubic bent functions which have no affine derivative was known [13]. So Hou raised the following question: for which dimensions do there exist cubic bent functions which have no affine derivative? This question was resolved in [2] by Canteaut and Charpin. They presented a class of cubic Maiorana-McFarland bent functions on all even dimension m ($m \geq 6$ and $m \neq 8$) which have no affine derivative. In this work, we focus on the characterization of Maiorana-McFarland Boolean functions with affine derivatives. We show that such a function is defined by the existence of a polynomial with a linear structure. More generally, we study permutation polynomials over finite fields with linear structures.

Linear structures have been studied in [3], [4], [7], [9]. In [9], Lai characterizes the Boolean functions which admit linear structures. Dubuc [7] characterized linear structures in terms of the Fourier transform. In [3], Charpin and Kyureghyan studied the polynomials of the form $F(x) = G(x) + \gamma Tr(H(x))$, over $\mathbb{F}_{2^n}$, which are permutations. This was generalized in [4], where $F(x) \in \mathbb{F}_{p^n}[x]$, p is any prime.

In this work, we present a construction of permutations which have linear structures. These permutations transform an hyperplane to another hyperplane and have at least one affine component. We fully characterize the so-called *bilinear polynomials* which have linear structures, proving that they cannot be bijective. Further, we present a class of permutation polynomials which have linear structures. Then we prove our main result in Theorem 5, in which we explain the relation between affine derivatives of a Maiorana-McFarland function and a polynomial with linear structures. Later we present some constructions of Maiorana-McFarland bent functions for both the cases: with affine derivatives and without affine derivatives. Finally, we indicate that Theorem 5 holds (in another form) when some resilient functions are considered.

This paper is an extended abstract. Several results are given without proof or with a shortened proof.

II. Preliminaries

Let $\mathbb{F}_{2^n}$ be the finite field of 2^n elements. For any space E, the set of nonzero elements of E is denoted by E^*. Any polynomial $F(X) \in \mathbb{F}_{2^n}[X]$ defines a function $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ by $x \mapsto F(x)$, which is called the *associated function of* $F(X)$. Through out this work, we identify a polynomial with its associated function. In particular, a *permutation* polynomial over $\mathbb{F}_{2^n}$ defines a bijective function from $\mathbb{F}_{2^n}$ to itself.

On the other hand, a so-called *linearized polynomial* is of the form

$$L(x) = \sum_{k=1}^{n-1} c_k x^{2^k},\ c_k \in \mathbb{F}_{2^n}. \quad (1)$$

It defines a linear function L over $\mathbb{F}_{2^n}$.

Let $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^m}$. For $a \in \mathbb{F}_{2^n}$, the function D_aF given by

$$D_aF(x) = F(x) + F(x + a)$$

is called the *derivative of* F *in the direction of* a. Further, $a \in \mathbb{F}_{2^n}^*$ is said to be a linear structure of F if the function D_aF is constant.

By definition, it is clear that if $a \in \mathbb{F}_{2^n}$ is a linear structure of $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^m}$ then

$$F(x) + F(x + a) = F(0) + F(a), \quad \text{for all } x \in \mathbb{F}_{2^n}. \quad (2)$$

If $F(0) + F(a) = c$, for some $c \in \mathbb{F}_{2^m}$, then a is called *c-linear structure*.

For any k dividing n, the function $Tr_k^n : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^k}$ is defined as

$$Tr_k^n(x) = x + x^{2^k} + x^{2^{2k}} + \ldots + x^{2^{k(n/k-1)}},\ x \in \mathbb{F}_{2^n}.$$

It will be denoted by $Tr(x)$ when $k = 1$. From now on we will only consider functions from $\mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^m}$ for the cases $m = n$ and $m = 1$, (i.e., Boolean function). The following result (also given in [9] with another terminology) characterizes polynomials with linear structure.

Note that the $weight$ of an integer is the Hamming weight of the 2-adic expression of the integer and the $degree$ of a polynomial $F(x)$ defined over $\mathbb{F}_{2^n}$ is the maximum of the weights of the exponents of x in $F(x)$.

Theorem 1: Let $F(x)$ be a function over the field $\mathbb{F}_{2^n}$. We assume that $F(x)$ has degree at least 2. Then $F(x)$ has a linear

978-1-4244-7892-7/10/$26.00 ©2010 IEEE

structure if and only if there is a non-bijective linear function $L(x)$ over $\mathbb{F}_{2^n}$ such that

$$F(x) = G(L(x)) + L_1(x), \tag{3}$$

for some function $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and some linear function $L_1(x)$ over $\mathbb{F}_{2^n}$.

III. Permutations with linear structure

From Theorem 1, we have a precise expression of functions on $\mathbb{F}_{2^n}$ which have a linear structure. To have such an expression is difficult when we impose on such a function to be bijective. We want to exhibit specific properties of this kind of functions.

Lemma 1: If F is a permutation of $\mathbb{F}_{2^n}$ then it cannot have a 0-linear structure.

Lemma 2: Let F be a bijection over $\mathbb{F}_{2^n}$ and denote by F^{-1} the inverse function of F. Then, a is a b-linear structure of F if and only if b is an a-linear structure of F^{-1}.

If F is a permutation then $x \mapsto F(x)+c$ is also a permutation for any constant $c \in \mathbb{F}_{2^n}$. Moreover both functions have the same subspace of linear structures. Thus we can assume that $F(0) = 0$ without any loss of generality.

From now on in this section, F is a permutation on $\mathbb{F}_{2^n}$ such that for some $a \neq 0$,

$$F(0) = 0 \quad \text{and} \quad F(x) + F(x+a) = F(a), \quad \text{for all } x \in \mathbb{F}_{2^n}. \tag{4}$$

To construct such a permutation F by using Theorem 1 is not immediate. However a direct construction is easy as we show now. Recall that the hyperplanes of $\mathbb{F}_{2^n}$ can be described as the set of the $2^n - 1$ subspaces of $\mathbb{F}_{2^n}$

$$H_\beta = \{\ y \mid Tr(\beta y) = 0\ \}, \beta \in \mathbb{F}^*_{2^n}. \tag{5}$$

Taking any $a \in \mathbb{F}^*_{2^n}$:

1) Choose a hyperplane H_β such that $Tr(\beta a) = 1$ ($a \notin H_\beta$).
2) Fix $F(0) = 0$, set $b = F(a)$, $M = \mathbb{F}_{2^n} \setminus \{0, b\}$; set $H_\beta = \{x_1, \ldots, x_{2^{n-1}}\}$, with $x_1 = 0$.
3) For any i, from 2 to 2^{n-1}, consider the pair $(x_i, x_i + a)$, $x_i \in H_\beta$; choose $y_i = F(x_i)$ in M and set $F(x_i + a) = y_i + b$;
4) on each step i replace: $M := M \setminus \{y_i, y_i + b\}$.

At the end, for any pair $(F(x), F(x+a))$, one element will be in and the other outside of $F(H_\beta)$; by construction, F is a permutation satisfying (4). Now we specify such F and its image by means of the hyperplanes of $\mathbb{F}_{2^n}$ as follows.

Theorem 2: Let F be a permutation on $\mathbb{F}_{2^n}$ with $F(0) = 0$. Assume that F has a linear structure $a \in \mathbb{F}^*_{2^n}$. Then, for any $\beta \in \mathbb{F}^*_{2^n}$ such that $Tr(\beta a) = 1$ and for any λ such that $Tr(\lambda F(a)) = 1$, there is a permutation $G_{\beta,\lambda}$ such that

$$G_{\beta,\lambda}(F(H_\beta)) = H_\lambda.$$

Moreover, setting $P_{\beta,\lambda} = G_{\beta,\lambda} \circ F$,

- a is a linear structure of the permutation $P_{\beta,\lambda}$,
- the derivatives of $P_{\beta,\lambda}$ satisfy:
  - if $b \in H_\beta$ then $D_b P_{\beta,\lambda}(x) \in H_\lambda$ for all x;
  - if $b \notin H_\beta$ then $D_b P_{\beta,\lambda}(x) \notin H_\lambda$ for all x.
- the Boolean function $x \mapsto Tr(\lambda P_{\beta,\lambda}(x))$ is affine.

Outline of the proof: The mapping $G_{\beta,\lambda}$ is of the form

$$G_{\beta,\lambda}\ :\ y\ \longmapsto\ y + F(a)Tr(\beta F^{-1}(y) + \lambda y).$$

IV. Functions with(out) linear structure

In this section, we exhibit an infinite class of permutations with linear structure. We begin with a discussion on the existence of linear structures. We first indicate a basic result.

Lemma 3: Let F be a function on $\mathbb{F}_{2^n}$. Then F has a linear structure, say $a \in \mathbb{F}^*_{2^n}$, if and only if a is a linear structure of $x \mapsto \lambda F(x) + L(x)$, for some $\lambda \in \mathbb{F}^*_{2^n}$ and some affine function L on $\mathbb{F}_{2^n}$.

Let i and j be two integers. We say that j *strictly covers* i if $i \neq j$ and, in the binary representation of i and j, every digit of i is less or equal to the corresponding digit of j. In this case we note $i \prec j$.

Theorem 3: Let r and s be integers such that $1 \leq r, s \leq 2^n - 2$. Let $\alpha \in \mathbb{F}_{2^n}$. Then the functions over $\mathbb{F}_{2^n}$

$$F(x) = \lambda(x^r + \alpha x^s) + L(x),\ \lambda \in \mathbb{F}^*_{2^n}, \tag{6}$$

where L be any affine function, has no linear structure unless it is affine.

Proof: Thanks to Lemma 3, we have to study the function $F(x) = x^r + \alpha x^s$ only. If a is a linear structure of F, then using (2), we must have $D_a F(x) = a^r + \alpha a^s$. However,

$$\begin{aligned} D_a F(x) &= x^r + (x+a)^r + \alpha(x^s + (x+a)^s) \\ &= a^r + \alpha a^s + \sum_{0<\ell\prec r} a^{r-\ell} x^\ell + \alpha \sum_{0<\ell\prec s} a^{s-\ell} x^\ell. \end{aligned}$$

Thus we must have

$$P(x) = \sum_{0<\ell\prec r} a^{r-\ell} x^\ell + \alpha \sum_{0<\ell\prec s} a^{s-\ell} x^\ell \equiv 0 \pmod{x^{2^n} + x}. \tag{7}$$

which is impossible unless $P(x)$ is the null polynomial. Let $I_s = \{\ell | 0 < \ell \prec s\}$ and $I_r = \{\ell | 0 < \ell \prec r\}$; note that these sets can be empty.

If $I_s \neq I_r$ then, $P(x)$ has at least one term corresponding to an exponent t of the form $a^k x^t$ with $k = r - t$ or $\alpha a^k x^t$ with $k = s - t$. Since $a \neq 0$ and $\alpha \neq 0$, it is impossible to have $P(x) = 0$ for all x. Note that this case happens notably for $\alpha = 0$ (*i.e., F* is a monomial).

If $I_s = I_r \neq \emptyset$ then $r = s$ and F is a monomial. Finally $I_s = I_r = \emptyset$ is the only possibility, meaning that F is linear. ■

Next we present a result on the associated Boolean function of a quadratic permutation. Recall that a Boolean function f on $\mathbb{F}_{2^n}$ is said to be *balanced* when the set $\{x | f(x) = 1\}$ has cardinality 2^{n-1}.

Theorem 4: Let $F(x)$ be any quadratic polynomial over $\mathbb{F}_{2^n}$. Then F is a permutation if and only if for all $\lambda \in \mathbb{F}_{2^n}$, the associated Boolean function $f_\lambda(x) = Tr(\lambda F(x))$ has a $1-$linear structure.

A. Bilinear polynomials

The polynomials of the form $L_1(x)L_2(x)$, where $L_1(x)$ and $L_2(x)$ are two linear polynomials are called *bilinear polynomial* [10]. In [10], some quadratic permutation polynomials have been identified in the class of bilinear polynomials of the form $xL(x)$. Below we characterize bilinear polynomials with linear structures.

Lemma 4: Let $L_1(x)L_2(x)$ be a bilinear polynomial. Then $a \in \mathbb{F}_{2^n}^*$ is a linear structure of $L_1(x)L_2(x)$ if and only if

$$L_2(a)L_1(x) + L_1(a)L_2(x) = 0, \text{ for all } x \in \mathbb{F}_{2^n}. \qquad (8)$$

Proof: Using (2) we know that $a \in \mathbb{F}_{2^n}^*$ is a linear structure of $L_1(x)L_2(x)$ if and only if for all $x \in \mathbb{F}_{2^n}$

$$L_1(x)L_2(x) + L_1(x+a)L_2(x+a) = L_1(a)L_2(a). \qquad (9)$$

Set $P(x) = D_a(L_1(x)L_2(x))$. We have

$$\begin{aligned} P(x) &= L_1(x)\left(L_2(x) + L_2(x+a)\right) + L_1(a)L_2(x+a) \\ &= L_2(a)L_1(x) + L_1(a)L_2(x) + L_1(a)L_2(a). \end{aligned}$$

Hence, (9) holds if and only if (8) holds, completing the proof. ■

Note that by Theorem 4, we know that quadratic polynomials with linear structures exist, since quadratic permutations exist. For this special class of bilinear polynomial, we are able to give a complete result.

Proposition 1: Define the bilinear polynomial $F(x) = L_1(x)L_2(x)$. Assume that F is strictly bilinear, *i.e.,* it is of degree 2.

Then, the linear structures of F are those $a \in \mathbb{F}_{2^n}^*$ such that $L_1(a) = L_2(a) = 0$. Consequently, if F is a permutation, it has no linear structure.

Proof: From Lemma 4, we know that $a \in \mathbb{F}_{2^n}^*$ is a linear structure of F if and only if (8) holds. Clearly, (8) holds when $L_1(a) = L_2(a) = 0$. In the case where $L_2(a) \neq 0$, we get

$$L_1(x) = \mu L_2(x), \ \mu = \frac{L_1(a)}{L_2(a)}, \text{ for all } x \in \mathbb{F}_{2^n}.$$

This leads to $F(x) = \mu\left(L_2(x)\right)^2$, *i.e.,* linear, if $L_1(a) \neq 0$ and $F(x)$ is the null polynomial otherwise. On the other hand taking $L_1(a) \neq 0$ (at the beginning) we get a similar result and both the two cases contradict that F has degree 2.

So, if (8) holds then $L_2(a) = 0$ and, further, $L_1(a) = 0$. In this case, F cannot be a permutation since $F(a) = 0 = F(0)$, completing the proof. ■

Corollary 1: Let $F(x) = L_1(x)L_2(x) + L_3(x)$ be a function over $\mathbb{F}_{2^n}$, where L_1 and L_2 are linear functions over $\mathbb{F}_{2^n}$ and L_3 is an affine function over $\mathbb{F}_{2^n}$. If L_1 or L_2 is bijective then F does not possess any linear structure.

Proof: If a is a linear structure of F then a is a linear structure of L_1L_2. From Proposition 1, this is possible if and only if $L_1(a) = L_2(a) = 0$. In this case, L_1 and L_2 are not bijective. ■

So we have proved that any quadratic polynomial of the form

$$\sum_{i=1}^{n-1} \lambda_i x^{2^i+1} + \sum_{j=0}^{n-1} \mu_j x^{2^j}, \quad \lambda_i \in \mathbb{F}_{2^n}, \ \mu_j \in \mathbb{F}_{2^n},$$

cannot have any linear structure.

Example 1: Dobbertin [6] introduced a class of quadratic permutation polynomials as $x^{2^{m+1}+1} + x^3 + x$ over $\mathbb{F}_{2^{2m+1}}$. Since $x^{2^{m+1}+1}+x^3+x = x(x^{2^{m+1}}+x^2)+x$, then by Corollary 1, these permutations cannot have any linear structure.

B. A class of permutations with linear structure

In [3], a class of permutation polynomials was presented as follows.

Proposition 2: [3, Lemma 4] Let $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a linear 2-to-1 mapping with kernel $\{0, \alpha\}$ and $H : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. If for some $\gamma \in \mathbb{F}_{2^n}$ the mapping

$$N(x) = L(x) + \gamma Tr(H(x))$$

is a permutation of $\mathbb{F}_{2^n}$, then γ does not belong to the image set of L. Moreover, for such an element γ the mapping $N(x)$ is a permutation if and only if α is a 1-linear structure of $Tr(H(x))$.

Recall a well-known result that the equation $x^2 + ax + b = 0$ has no solution in $\mathbb{F}_{2^n}$ if and only if $Tr\left(\frac{b}{a^2}\right) \neq 0$.

Based on Proposition 2, we are able to construct quadratic permutation polynomial with linear structure.

Proposition 3: For n odd and the integer i such that $1 \leq i \leq n-1$, the quadratic polynomials of the form

$$N(x) = x(x+1) + \gamma Tr(x^{2^i+1}),$$

where $x \in \mathbb{F}_{2^n}$ and $Tr(\gamma) \neq 0$, is a quadratic permutation polynomial over $\mathbb{F}_{2^n}$ with the linear structure 1.

Proof: Let $L(x) = x(x+1)$, then L is a 2-to-1 linear function with kernel $\{0, 1\}$. Since $Tr(\gamma) \neq 0$, it is impossible to have $x^2 + x + \gamma = 0$. Hence γ is not in the image set of L. Now, we have

$$Tr(x^{2^i+1} + (x+1)^{2^i+1}) = Tr(x^{2^i} + x + 1) = Tr(1) = 1,$$

since n is odd, which shows that 1 is a 1-linear structure of $Tr(x^{2^i+1})$. Therefore, by Proposition 2, $N(x)$ is a permutation polynomial over $\mathbb{F}_{2^n}$.

Again, we have for any $x \in \mathbb{F}_{2^n}$:

$$N(x) + N(x+1) = L(1) + \gamma Tr(1) = 0 + \gamma = \gamma.$$

So, 1 is a linear structure of $N(x)$, completing the proof. ■

Remark 1: It has been proved in [3] that for any integer s, $0 \leq s \leq 2^n-2$ such that $s \notin \{2^i, 2^i+2^j\}$ for all integers i and j, the Boolean function $x \mapsto Tr(\delta x^s)$ can never have a linear structure (for any $\delta \in \mathbb{F}_{2^n}$). Therefore, one cannot construct any permutation polynomial having degree more than 2 of the form

$$N(x) = L(x) + \gamma Tr(x^s),$$

where $L(x)$ and γ are as given in Proposition 2.

Moreover such a polynomial $N(x)$ cannot have any linear structure. Indeed, assume that a is a c-linear structure of $N(x)$. Then $N(x) + N(x+a) = c$ for all $x \in \mathbb{F}_{2^n}$. This implies that

$$\begin{aligned} L(x) + \gamma Tr(x^s) + L(x+a) + \gamma Tr((x+a)^s) &= c \\ L(a) + \gamma(Tr(x^s) + Tr((x+a)^s)) &= c \\ Tr(x^s) + Tr((x+a)^s) &= v, \end{aligned}$$

for all $x \in \mathbb{F}_{2^n}$, where $v = \gamma^{-1}(c + L(a))$, implying that a is a linear structure of $Tr(x^s)$.

However, using Proposition 2 again, we are going to construct permutations of higher degree which have a linear structure. Observe that if $H(x)$ has a linear structure a then a is also a linear structure of $Tr(H(x))$. Moreover, if a is a 1-linear structure of $Tr(H(x))$, then

$$N(x) = x(x+a) + \gamma Tr(H(x)),$$

where $Tr(\gamma/a^2) \neq 0$, is a permutation polynomial with the linear structure a.

Lemma 5: Let s and i be two integers such that $1 \leq s \leq 2^n - 2$ and $0 \leq i \leq n-1$. Set

$$H(x) = x^s + x^{2^i}\left(x^s + (x+1)^s + 1\right).$$

Then, 1 is a 1-linear structure of H.

Proposition 4: Let n be odd, $n \geq 5$ and let k be an odd integer such that $1 \leq k \leq n-2$. Let

$$s = 1 + 2^{i_1} + \cdots + 2^{i_k},\ 1 \leq i_1 < \cdots < i_k \leq n-2,$$

i.e., $3 \leq s \leq 2^{n-1} - 1$. Consider the function

$$N(x) = x(x+1) + \gamma Tr(H(x)),$$

where $H(x) = x^s + x^{2^{n-1}}\left(x^s + (x+1)^s + 1\right)$ and $\gamma \in \mathbb{F}_{2^n}^*$ satisfies $Tr(\gamma) = 1$. Then $N(x)$ is a permutation of degree $k+1$ which has 1 as a γ-linear structure.

Proof: Using lemma 5, we have

$$Tr(H(x)) + Tr(H(x+1)) = Tr(1) = 1,$$

for all $x \in \mathbb{F}_{2^n}$. Thus by Proposition 2, N is a permutation. Moreover

$$N(x) + N(x+1) = 0 + \gamma Tr(H(x) + H(x+1)) = \gamma.$$

Now we look at the degree of N. It is clear that

$$H(x) = x^s + \sum_{r \neq 0,\ r \prec s} x^{r + 2^{n-1}}.$$

Note that in $H(x)$, the exponents s and $r + 2^{n-1}$, where $r = s - 2^i$ for some $i \in \{0, i_1, \ldots, i_k\}$, only have the maximum weight, i.e., $k+1$. In total there are $k+2$ exponents of weight $k+1$. Among these $k+2$ exponents, if two exponents belong to the same cyclotomic coset, then they cancel each other in $Tr(H(x))$. Since k is odd and so is $k+2$, therefore, at least one exponent will not be canceled out in $Tr(H(x))$ by some other exponent. Thus the degree of $Tr(H(x))$ is also equal to $k+1$ and hence the degree of $N(x)$ is equal to $k+1$ (the weight of s). ■

V. Maiorana-McFarland bent functions without affine derivative

In [8], Hou proved that all the 8-variable cubic Boolean bent functions have at least one affine derivative. In [2], Canteaut and Charpin presented a family of n-variables, $n \geq 6$ and $n \neq 8$ cubic bent functions which have no affine derivative. Those functions belong to the Maiorana-McFarland class which was extensively studied by Dillon [5, pp. 90-95]. This class is usually called the *class* $\mathcal{M}$ of bent functions. Using our previous results, we propose a more general approach. Boolean functions of class $\mathcal{M}$ are functions of the form

$$f\ :\ (x,y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \quad \mapsto \quad Tr_1^t\left(x\pi(y) + h(y)\right) \qquad (10)$$

where π is a function over $\mathbb{F}_{2^t}$ and h is any function on $\mathbb{F}_{2^t}$.

Lemma 6: Let $n = 2t$. Let us consider a Boolean function f defined by (10). Then, f is a bent function if and only if π is a bijection. In this case, f is said to belong to the class $\mathcal{M}$ of bent functions.

Theorem 5: Let $n = 2t$. Let π be a function over $\mathbb{F}_{2^t}$ of degree ℓ, $1 < \ell \leq t-1$. Let f be a function given by (10) where the degree of h is less than or equal to 2. Then f has no affine derivative if and only if π does not have any linear structure. In this case, if π is a bijection then f is a bent function without affine derivative.

Proof: Note that, since the degree of h is less than or equal to ℓ, the degree of f is exactly $\ell + 1$. Take $a, b \in \mathbb{F}_{2^t}$. Then

$$\begin{aligned} D_{(a,b)}f(x,y) \quad &= Tr_1^t(x\pi(y) + (x+a)\pi(y+b) \\ &\quad + h(y) + h(y+b)) \\ &= Tr_1^t(a\pi(y+b)) + Tr_1^t(x(\pi(y) \\ &\quad + \pi(y+b)) + h(y) + h(y+b)). \end{aligned}$$

It is clear that the degree of $D_{(a,b)}f$ is at most ℓ. If $a \neq 0$, then the term $a\pi(y+b)$ asserts that $D_{(a,b)}f$ is of degree exactly ℓ. In this case, $D_{(a,b)}f$ is not affine.

Let us now investigate for the case $a = 0$. In this case,

$$D_{(0,b)}f(x,y) = Tr_1^t\left(x(\pi(y) + \pi(y+b)) + h(y) + h(y+b)\right).$$

Since $\ell > 1$ and any derivative of h is affine or constant, $D_{(0,b)}f$ is affine if and only if the function $y \mapsto \pi(y) + \pi(y+b)$ is constant, *i.e.,* b is a linear structure of π.

When π is a permutation, f is a bent function belonging to $\mathcal{M}$ (see Lemma 6). ■

By Theorem 5, we are able to construct bent functions of any degree d, $3 \leq d \leq t$ on $\mathbb{F}_{2^n}$ $(n = 2t)$ which have affine derivatives. For example, we obtain the following result directly from Proposition 4.

Corollary 2: Let $n = 2t$ with t odd. Let N be defined as in Proposition 4. Then $f(x,y) = Tr_1^t(xN(y))$ is a bent function of degree $d = k+2$ whose derivative at the point 1 is affine.

On the other hand we can state some general results such as the following which generalizes [2, Lemma 1].

Corollary 3: Let $n = 2t$. Let r and s be integers such that $1 \leq r, s \leq 2^n - 2$. Let $\alpha \in \mathbb{F}_{2^n}$. Assume that $y \mapsto y^r$ has degree $\ell > 1$ and h is any function of degree at most 2. Then the function

$$f\ :\ (x,y) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \quad \mapsto \quad Tr_1^t\left(x(y^r + \alpha y^s) + h(y)\right)$$

does not have any affine derivative. In particular, any function

$$f\ :\ (x,y) \quad \mapsto \quad Tr_1^t\left(xy^{2^i+1}\right) \quad \text{with } \tfrac{t}{\gcd(t,i)} \text{ odd},$$

is a bent function without affine derivatives.

Proof: By Theorem 3, we know that the function $y \mapsto y^r + \alpha y^s$ has no linear structure. Hence we can apply Theorem 5. In particular, we get the class of cubic bent functions without any affine derivative introduced in [2]. Note that $2^i + 1$ is coprime to $2^t - 1$ (*i.e.,* $y \mapsto y^{2^i+1}$ is a permutation) if and only if $t/\gcd(t,i)$ is odd (see for instance [12, Lemma 11.1]). ■

Theorem 5 also has a surprising consequence. By Hou's result [8], we know that all the cubic bent functions of 8 variables have at least one affine derivative. In particular this property holds for bent functions of the form (10) for $t = 4$ and π is a permutation on $\mathbb{F}_{2^4}$. Thus we have:

Corollary 4: Any quadratic permutation over $\mathbb{F}_{2^4}$ has at least one linear structure.

In [2, Section IV], it was proved that a bent function has an affine derivative if and only if its dual has an affine derivative. The dual of a bent function f of the class $\mathcal{M}$ given by (10) is known to be as follows:

$$\tilde{f} \;:\; (x, y) \;\; \mapsto \;\; Tr_1^t \left(y\pi^{-1}(x) + h(\pi^{-1}(x)) \right)$$

(where π is a permutation). Let f be a bent function, defined as in Theorem 5. If π has no linear structure then f has no affine derivative. Thanks to Lemma 2, π^{-1} has no linear structure too; further $\tilde{f}$ has no affine derivative. So we prove, by another way, an instance of the result given in [2].

VI. Cryptographic relevance

So far we have considered functions over the finite field $\mathbb{F}_{2^n}$. Let $\mathbb{F}_2^n$ denote the vector space of 2^n binary n-tuples. The vector space $\mathbb{F}_2^n$ can easily be identified to the field $\mathbb{F}_{2^n}$. This is done by choosing a basis $\{\alpha_1, \ldots, \alpha_n\}$ of the vector space $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Then an element $x \in \mathbb{F}_{2^n}$ can be described as $\sum_{i=1}^n x_i \alpha_i$, i.e., we can identify x to the n-tuple $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$ where each x_i belongs to $\mathbb{F}_2$. The number of nonzero x_i's is the Hamming weight of x denoted by $wt(x)$ and any Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is an n-variable Boolean function.

There are several cryptosystems in which Boolean functions are used. For example, in some LFSR based stream ciphers, a Boolean function is used to combine the outputs of several LFSRs. For secure design purpose, it is required that the output of the Boolean function should not have correlation with a subset of input variables. Otherwise, one can mount the correlation attack [14] by exploiting the statistical dependence between the input variables and the output of the Boolean function. Therefore in order to resist this attack it is required that the Boolean function remains balanced if some input bits are kept constant. From this requirement, the concept of *resiliency* comes.

A Boolean function $g : \mathbb{F}_2^n \to \mathbb{F}_2$ is k-resilient if and only if

$$W_g(\lambda) = \sum_{z \in \mathbb{F}_2^n} (-1)^{f(z) + \lambda \cdot z} = 0$$

for all $\lambda \in \mathbb{F}_2^n$ such that $wt(\lambda) \leq k$, where $\lambda \cdot z$ denotes the usual dot product over $\mathbb{F}_2^n$.

There are several constructions of resilient functions. There is one construction, introduced in [1, Proposition 4.2], which is quite similar to the Maiorana-McFarland construction of bent functions.

Proposition 5: [1] Let k be an integer such that $0 \leq k \leq n - r - 2$. Let $G : \mathbb{F}_2^r \to \mathbb{F}_2^{n-r}$ be any function such that $wt(G(y)) \geq k + 1$ for all $y \in \mathbb{F}_2^r$. Then the Boolean function $f : \mathbb{F}_2^{n-r} \times \mathbb{F}_2^r \to \mathbb{F}_2$ given by

$$f(x, y) =< x, G(y) >_{n-r} + H(y)$$

is a k-resilient function of n variables, where $H : \mathbb{F}_2^r \to \mathbb{F}_2^{n-r}$ is any function and $< \cdot, \cdot >_{n-r}$ is the dot product on $\mathbb{F}_2^{n-r}$.

Noting the similarity between the construction of resilient function in Proposition 5 and the construction of Maiorana-McFarland bent functions, we can easily extend Theorem 5 in the case of resilient functions as follows.

Theorem 6: Let $G : \mathbb{F}_2^r \to \mathbb{F}_2^{n-r}$ be any function of degree ℓ, $1 < \ell \leq r - 1$ such that $wt(G(x)) \geq k + 1$ for all $x \in \mathbb{F}_2^r$. Then the k-resilient function of degree more than 2

$$f : \mathbb{F}_2^{n-r} \times \mathbb{F}_{2^r} \to \mathbb{F}_2 \text{ given by } f(x, y) =< x \cdot G(y) >_{n-r}$$

does not possess any affine derivative if and only if G does not have any linear structure.

Acknowledgment

The authors would like to thank the anonymous reviewer whose comments have improved this paper.

References

[1] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On Correlation-Immune Functions", in *Proc. CRYPTO*, ser. Lecture Notes in Computer Science, vol. 576. Springer-Verlag, 1992, pp. 86-100.

[2] A. Canteaut and P. Charpin, "Decomposing Bent Functions", *IEEE Trans. Inf. Theory*, vol. 49, no. 8, pp. 2004-2019, 2003.

[3] P. Charpin and G. M. Kyureghyan, "On a Class of Permutation Polynomials over $\mathbb{F}_{2^n}$". in *Proc. SETA*, ser. Lecture Notes in Computer Science, vol. 5203. Springer-Verlag, 2008, pp. 368-376.

[4] P. Charpin and G. M. Kyureghyan, When does $G(x) + \gamma Tr(H(x))$ permute $\mathbb{F}_{2^n}$? *Finite Fields and Their Applications*, vol. 15, no. 5, pp. 615-632, in press.

[5] J.Dillon, "Elementary Hadamard Difference sets," Ph.D. dissertation, Univ. of Maryland, 1974.

[6] H. Dobbertin, "Almost Perfect Nonlinear Power Functions on $GF(2^n)$: The Welch Case", *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1271–1275, 1999.

[7] S. Dubuc, "Characterization of linear structures", *Des. Codes Cryptography* vol. 22, pp. 33–45, 2001.

[8] X.-D. Hou, "Cubic bent functions", *Discrete Maths.*, vol. 189, pp. 149–161, 1998.

[9] X. Lai, "Additive and linear structures of cryptographic functions", in Proc. FSE, ser. Lecture Notes in Computer Science, vol. 1008, Springer-Verlag, 1995, pp. 75–85.

[10] Y. Laigle-Chapuy, A note on a class of quadratic permutations over F_{2^n}, in *Proc. AAECC 17*, ser. Lecture Notes in Computer Science, 4851, Springer-Verlag, 2007, pp. 130–137.

[11] R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and its Applications*, vol. 20, second edition, Cambridge University Press, 1997.

[12] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Kluwer Academic Publishers, 1987.

[13] O. S. Rothaus, "On bent functions", *J. Comb. Theory Ser. A* vol. 20, pp. 300-305, 1976.

[14] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications", *IEEE Trans. Inf. Theory*, vol. 30, no. 5, pp. 776–780, 1984.