

Results on Characterizations of Plateaued Functions in Arbitrary Characteristic

Sihem Mesnager^{1,2,3}, Ferruh Özbudak^{4,5}, and Ahmet Sinak^{5,6}(✉)

¹ Department of Mathematics, University of Paris VIII, Saint-Denis, France
smesnager@univ-paris8.fr

² LAGA, UMR 7539, CNRS, University of Paris XIII, Villetaneuse, France

³ Telecom ParisTech, Paris, France

⁴ Department of Mathematics, Middle East Technical University, Ankara, Turkey

⁵ Institute of Applied Mathematics, Middle East Technical University,
Ankara, Turkey

{ozbudak,ahmet.sinak}@metu.edu.tr

⁶ Department of Mathematics and Computer Sciences,
Necmettin Erbakan University, Konya, Turkey

Abstract. Bent and plateaued functions play a significant role in cryptography since they can have various desirable cryptographic properties. In this work, we first provide the characterizations of plateaued functions in terms of the moments of their Walsh transforms. Next, we generalize the characterizations of Boolean bent and plateaued functions in terms of their second-order derivatives to arbitrary characteristic. Moreover, we present a new characterization of plateaued functions in terms of fourth power moments of their Walsh transforms. Furthermore, we give a new proof of the characterization of vectorial bent functions. Finally, we present the characterizations of vectorial s -plateaued functions in terms of moments of their Walsh transforms and the zeros of their second-order derivatives.

Keywords: Bent functions · Plateaued functions · Vectorial functions

1 Introduction

The functions over a binary field are called *Boolean* functions. Boolean bent functions are a special type of Boolean functions. These functions were introduced by Rothaus in [26], generalized to p -ary bent functions by Kumar et al. in [19] and further studied in [14, 15, 17, 27]. Plateaued functions over a binary field are a generalization of Boolean bent functions. They were introduced and initially studied by Zheng and Zhang in [28]. The Walsh-Hadamard spectrum is an important tool to define and design plateaued functions. Some plateaued functions have low Hadamard transform, which provides protection against fast correlation attacks and linear cryptanalysis. In addition to the useful properties of bent functions such as high nonlinearity, resiliency, low additive autocorrelation, high algebraic degree and satisfy propagation criteria, some plateaued

functions may have the other desirable cryptographic properties such as balancedness and correlation immunity. On the other hand, plateaued functions include three significant classes of Boolean functions: the well-known bent functions (called 0-plateaued functions), the near-bent functions (called 1-plateaued functions) and the semi-bent functions (called 2-plateaued functions). Boolean plateaued functions have been widely studied (for example, see in [1, 6–8, 18, 20–22, 29]) due to their cryptographic properties. A complete survey on Boolean plateaued functions was given by Mesnager in [24].

In characteristic 2, 0-plateaued functions and 2-plateaued functions exist when n is even, while 1-plateaued functions exist when n is odd. Therefore, Boolean plateaued functions were generalized to p -ary plateaued functions (for example, see in [11]). Recently, Mesnager [23] characterized p -ary plateaued functions in terms of the moments of their Walsh transforms. Moreover, in characteristic p , she established a link between the fourth power moment and the derivative. More recently, interesting characterizations of plateaued functions in characteristic 2 (different from those exhibited (in characteristic p) in [23]) have been provided (without proofs) by Carlet in [3].

In this paper, we are motivated by [7, 23] and our results are valid in arbitrary characteristic. After presenting the basic tools in Sect. 2, we give in Sect. 3 the characterizations of plateaued functions in terms of the moments of their Walsh transforms. In Sect. 4, we generalize the characterizations of bent and plateaued functions in characteristic 2 given in [7] to arbitrary characteristic. Moreover, we present a new characterization of plateaued functions in terms of the fourth power moments of their Walsh transforms. In Sect. 5, we furthermore provide a link between the balancedness of the first-order derivatives of vectorial bent functions and the number of zeros of their second-order derivatives. Finally, Sect. 6 gives the characterizations of vectorial s -plateaued functions in terms of the moments of their Walsh transforms and the number of zeros of their second-order derivatives.

2 Preliminaries

We denote the finite field with p^n elements by \mathbb{F}_{p^n} where p is a prime number and n is a positive integer. The set of nonzero elements of \mathbb{F}_{p^n} is denoted by $\mathbb{F}_{p^n}^*$. Notice that the finite field \mathbb{F}_{p^n} can be seen as an n -dimensional vector space over \mathbb{F}_p and denoted by \mathbb{F}_p^n . The *trace* function of $\alpha \in \mathbb{F}_{p^n}$ over \mathbb{F}_p is defined as $\text{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$. In this paper, the *absolute trace* of α over \mathbb{F}_p is denoted by $\text{Tr}_p^{p^n}(\alpha)$. Let f be a function from \mathbb{F}_{p^n} to \mathbb{F}_p and ϵ_p be a *primitive p -th root of unity* in \mathbb{C} . The *sign* function of f from \mathbb{F}_p^n to \mathbb{C} is denoted by χ_f defined as $\chi_f(x) = \epsilon_p^{f(x)}$ for all $x \in \mathbb{F}_p^n$. The Fourier transform $\hat{\chi}_f$ of the function χ_f is defined as

$$\begin{aligned} \hat{\chi}_f : \mathbb{F}_p^n &\rightarrow \mathbb{C} \\ \omega &\mapsto \hat{\chi}_f(\omega) = \sum_{x \in \mathbb{F}_p^n} \chi_f(x) \epsilon_p^{-\omega \cdot x}, \end{aligned}$$

called the *Walsh transform* of f at $w \in \mathbb{F}_p^n$, where “ \cdot ” is any scalar product in \mathbb{F}_p^n . As the notion of Walsh transform concerns a scalar product, it is suitable to take the isomorphism between the scalar product “ \cdot ” in \mathbb{F}_p^n and the trace of the product $\omega \cdot x = \text{Tr}_p^{p^n}(\omega x)$ in \mathbb{F}_{p^n} . Thus, the Walsh transform of f at $\omega \in \mathbb{F}_{p^n}$ can be given as

$$\widehat{\chi}_f(\omega) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{f(x) - \text{Tr}_p^{p^n}(\omega x)}.$$

A function f is called *bent* if $|\widehat{\chi}_f(\omega)| = p^{\frac{n}{2}}$ for all $\omega \in \mathbb{F}_{p^n}$, and f is called *s-plateaued* if $|\widehat{\chi}_f(\omega)| \in \left\{0, p^{\frac{n+s}{2}}\right\}$ for all $\omega \in \mathbb{F}_{p^n}$ and a fixed integer $0 \leq s \leq n$. It is obvious that bent functions are 0-plateaued functions. The following equation is known as the *Parseval identity*:

$$\sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi}_f(\omega)|^2 = p^{2n}. \quad (1)$$

The following tools were previously introduced in the literature (for example, see in [4] and [23]). The below Lemma is useful to prove some results in the next sections.

Lemma 1. *Let f be an s -plateaued function from \mathbb{F}_{p^n} to \mathbb{F}_p . Then for $\omega \in \mathbb{F}_{p^n}$, $|\widehat{\chi}_f(\omega)|$ takes p^{n-s} times the value $p^{\frac{n+s}{2}}$ and $p^n - p^{n-s}$ times the value 0.*

For a non-negative integer i , the moment of Walsh transforms of f is defined as

$$S_i(f) = \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi}_f(\omega)|^{2i}.$$

It is obvious that $S_0(f) = p^n$ and $S_1(f) = p^{2n}$ by (1). For every integer A and every non-negative integer i , the following equation holds

$$\sum_{\omega \in \mathbb{F}_{p^n}} \left(|\widehat{\chi}_f(\omega)|^2 - A\right)^2 |\widehat{\chi}_f(\omega)|^{2i} = S_{i+2}(f) - 2AS_{i+1}(f) + A^2 S_i(f). \quad (2)$$

The derivative of f at $a \in \mathbb{F}_{p^n}$ is the map $\mathcal{D}_a f$ from \mathbb{F}_{p^n} to \mathbb{F}_p defined as

$$\mathcal{D}_a f(x) = f(x + a) - f(x), \quad \forall x \in \mathbb{F}_{p^n}.$$

Let F be a vectorial function from \mathbb{F}_{p^n} to \mathbb{F}_{p^m} . The derivative of F at $a \in \mathbb{F}_{p^n}$ is the map $\mathcal{D}_a F$ from \mathbb{F}_{p^n} to \mathbb{F}_{p^m} defined as

$$\mathcal{D}_a F(x) = F(x + a) - F(x), \quad \forall x \in \mathbb{F}_{p^n}.$$

3 Characterizations of Plateaued Functions

In this section, our results are originated from [23]. We give the characterizations of s -plateaued functions via the sequence of even moments of their Walsh transforms. The following seems to be more practical than [23, Theorem 1] in some applications.

Theorem 1. *Let f be a function from \mathbb{F}_{p^n} to \mathbb{F}_p . Let s be an integer with $0 \leq s \leq n$ and $i, j \in \mathbb{Z}^+$. Then the followings are equivalent:*

1. f is s -plateaued for $s > 0$.
2. $S_i(f)S_j(f) = S_{i+1}(f)S_{j-1}(f)$ for all $i \geq 1$ and $j \geq 2$.

Moreover, f is bent if and only if (2) holds for all $i, j \in \mathbb{Z}^+$.

Proof. Suppose that f is s -plateaued for $s > 0$. By Lemma 1, it is easily seen that

$$S_i(f)S_j(f) = S_{i+1}(f)S_{j-1}(f), \quad \forall i \geq 1, j \geq 2.$$

Conversely, for $j = i + 2$ and $A = \frac{S_{i+1}(f)}{S_i(f)}$ in (2), the proof is the same as the proof of [23, Theorem 1]. \square

In fact, Theorem 1 is equivalent to [23, Theorem 1], which can be shown as follows.

Corollary 1. *Let f be a function from \mathbb{F}_{p^n} to \mathbb{F}_p . Then the followings are equivalent:*

1. $S_i(f)S_i(f) = S_{i+1}(f)S_{i-1}(f)$ for all $i \geq 2$.
2. $S_i(f)S_j(f) = S_{i+1}(f)S_{j-1}(f)$ for all $i, j \geq 2$.

Proof. Suppose that (1) holds. Without loss of generality, we may assume $i < j$ and fix $i \geq 2$. We proceed by induction on j . For $j = i + 1$ and $j = i + 2$, then (2) trivial holds. Let $j = i + 3$. From (1), we get

$$\begin{aligned} S_{i+1}(f)S_{i+1}(f) &= S_{i+2}(f)S_i(f), \\ S_{i+2}(f)S_{i+2}(f) &= S_{i+3}(f)S_{i+1}(f). \end{aligned}$$

It follows that $S_i(f)S_{i+3}(f) = S_{i+1}(f)S_{i+2}(f)$. Then, (2) holds for $j = i + 3$. For $j = i + k$, assume that (2) holds. We then have

$$\begin{aligned} S_i(f)S_{i+k}(f) &= S_{i+1}(f)S_{i+k-1}(f), \\ S_{i+k-1}(f)S_{i+k+1}(f) &= S_{i+k}(f)S_{i+k}(f). \end{aligned}$$

It follows that $S_i(f)S_{i+k+1}(f) = S_{i+1}(f)S_{i+k}(f)$. Therefore, (2) holds for $j = i + k + 1$. The converse is obvious for $j = i$. \square

For a function f from \mathbb{F}_{p^n} to \mathbb{F}_p , Mesnager in [23] showed that $S_2(f) \geq p^{3n}$ and also

$$S_2(f) = p^{3n} \text{ if and only if } f \text{ is bent.} \quad (3)$$

We deduce that, for a bent function f , the sequence $S_i(f)$ is a simple geometric sequence.

Corollary 2. *Let f be a function from \mathbb{F}_{p^n} to \mathbb{F}_p . If f is a bent function, then for all $i \in \mathbb{N}$*

$$S_i(f) = p^{(i+1)n}. \quad (4)$$

Proof. By (1) and (3), $S_1(f) = p^{2n}$ and $S_2(f) = p^{3n}$, respectively. By Theorem 1, we get $S_i(f) = \frac{S_{i-1}(f)^2}{S_{i-2}(f)} = p^{(i+1)n}$ for all $i \geq 3$, recursively. Thus, (4) holds for all $i \in \mathbb{N}$. \square

We also deduce from (3) the following characterization of s -plateaued functions via the moments of their Walsh transforms.

Theorem 2. *Let f be a function from \mathbb{F}_{p^n} to \mathbb{F}_p and s be an integer with $1 \leq s \leq n$. Then*

$$f \text{ is } s\text{-plateaued if and only if } S_2(f) = p^{3n+s} \text{ and } S_3(f) = p^{4n+2s}.$$

Proof. Assume that f is s -plateaued. By (2) with $A = p^{n+s}$ and $i = 0$,

$$\begin{aligned} \sum_{\omega \in \mathbb{F}_{p^n}} (|\widehat{\chi}_f(\omega)|^2 - p^{n+s})^2 &= S_2(f) - 2p^{n+s}S_1(f) + p^{2n+2s}S_0(f) \\ &= (p^n - p^{n-s})(-p^{n+s})^2 \end{aligned} \quad (5)$$

where the last equality of (5) follows from Lemma 1. Therefore, $S_2(f) = p^{3n+s}$ from (5) and $S_3(f) = \frac{S_2(f)^2}{S_1(f)} = p^{4n+2s}$ by Theorem 1.

Conversely, suppose that $S_2(f) = p^{3n+s}$ and $S_3(f) = p^{4n+2s}$. By (2) with $A = p^{n+s}$ and $i = 1$, we get the following:

$$\sum_{\omega \in \mathbb{F}_{p^n}} (|\widehat{\chi}_f(\omega)|^2 - p^{n+s})^2 |\widehat{\chi}_f(\omega)|^2 = S_3(f) - 2p^{n+s}S_2(f) + p^{2n+2s}S_1(f) = 0.$$

Therefore, $|\widehat{\chi}_f(\omega)| \in \left\{0, p^{\frac{n+s}{2}}\right\}$ for all $\omega \in \mathbb{F}_{p^n}$, which implies that f is s -plateaued. \square

We deduce that, for an s -plateaued function f , the sequence $S_i(f)$ is also a simple geometric sequence.

Corollary 3. *Let f be a function from \mathbb{F}_{p^n} to \mathbb{F}_p and s be an integer with $1 \leq s \leq n$. If f is an s -plateaued function, then for all $i \in \mathbb{Z}^+$*

$$S_i(f) = p^{(i+1)n+(i-1)s}. \quad (6)$$

Proof. By Theorem 2, $S_2(f) = p^{3n+s}$ and $S_3(f) = p^{4n+2s}$. By Theorem 1, we get

$$S_i(f) = \frac{S_{i-1}(f)^2}{S_{i-2}(f)} = p^{(i+1)n+(i-1)s}$$

for all $i \geq 4$, recursively. Thus, (6) holds for all $i \in \mathbb{Z}^+$. \square

4 Characterizations of Bent and Plateaued Functions

The characterizations of bent and plateaued functions in characteristic 2 in terms of the second-order derivatives were firstly given by Carlet and Prouff in [7]. We provide the generalization of their characterizations for any characteristic p as the following.

Theorem 3. *Let f be a function from \mathbb{F}_{p^n} to \mathbb{F}_p and s be an integer with $0 \leq s \leq n$. Then, f is s -plateaued if and only if*

$$\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)} = \theta, \quad \forall x \in \mathbb{F}_{p^n} \quad (7)$$

with $\theta = p^{n+s}$. In particular, f is bent if and only if $\theta = p^n$ for $s = 0$.

Proof. For a function f ,

$$\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)} = \sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{f(x+a+b)-f(x+a)-f(x+b)+f(x)} = \theta, \quad \forall x \in \mathbb{F}_{p^n}$$

if and only if

$$\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{f(x+a+b)-f(x+a)-f(x+b)} = \theta \epsilon_p^{-f(x)}, \quad \forall x \in \mathbb{F}_{p^n}. \quad (8)$$

Let $a_1 = x + a$ and $b_1 = x + b$ for $a_1, b_1 \in \mathbb{F}_{p^n}$. Thus, (8) is equivalent to

$$\sum_{a_1, b_1 \in \mathbb{F}_{p^n}} \epsilon_p^{f(a_1+b_1-x)-f(a_1)-f(b_1)} = \theta \epsilon_p^{-f(x)}, \quad \forall x \in \mathbb{F}_{p^n}. \quad (9)$$

Let the left-hand side of (9) be $G_1(x)$ and its right-hand side be $G_2(x)$ for all $x \in \mathbb{F}_{p^n}$, i.e., $G_1(x) = G_2(x)$ for all $x \in \mathbb{F}_{p^n}$. We recall the following well-known property of the Fourier transform: for a function G from \mathbb{F}_{p^n} to \mathbb{C} ,

$$G(x) = 0 \quad \forall x \in \mathbb{F}_{p^n} \quad \text{if and only if} \quad \widehat{G}(\omega) = \sum_{x \in \mathbb{F}_{p^n}} G(x) \epsilon_p^{-\text{Tr}_p^{p^n}(\omega x)} = 0, \quad \forall \omega \in \mathbb{F}_{p^n}$$

where \widehat{G} is the Fourier transform of G . Then, for all $\omega \in \mathbb{F}_{p^n}$ the Fourier transforms of G_1 and G_2 are equal:

$$\widehat{G}_1(\omega) = \sum_{x \in \mathbb{F}_{p^n}} G_1(x) \epsilon_p^{-\text{Tr}_p^{p^n}(\omega x)} = \sum_{x \in \mathbb{F}_{p^n}} G_2(x) \epsilon_p^{-\text{Tr}_p^{p^n}(\omega x)} = \widehat{G}_2(\omega).$$

The Fourier transform \widehat{G}_1 of G_1 at $\omega \in \mathbb{F}_{p^n}$ can be computed in terms of $\widehat{\chi}_f$ as the following:

$$\begin{aligned} \widehat{G}_1(\omega) &= \sum_{x \in \mathbb{F}_{p^n}} G_1(x) \epsilon_p^{-\text{Tr}_p^{p^n}(\omega x)} = \sum_{x \in \mathbb{F}_{p^n}} \sum_{a_1, b_1 \in \mathbb{F}_{p^n}} \epsilon_p^{f(a_1+b_1-x)-f(a_1)-f(b_1)} \epsilon_p^{-\text{Tr}_p^{p^n}(\omega x)} \\ &= \sum_{a_1 \in \mathbb{F}_{p^n}} \epsilon_p^{-f(a_1)-\text{Tr}_p^{p^n}(\omega a_1)} \sum_{b_1 \in \mathbb{F}_{p^n}} \epsilon_p^{-f(b_1)-\text{Tr}_p^{p^n}(\omega b_1)} \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{f(a_1+b_1-x)-\text{Tr}_p^{p^n}(-\omega(a_1+b_1-x))} \\ &= (-\widehat{\chi}_f)(\omega)(-\widehat{\chi}_f)(\omega)\widehat{\chi}_f(-\omega). \end{aligned}$$

Similarly, for all $\omega \in \mathbb{F}_{p^n}$

$$\widehat{G}_2(\omega) = \sum_{x \in \mathbb{F}_{p^n}} G_2(x) \epsilon_p^{-\text{Tr}_p^{p^n}(\omega x)} = \sum_{x \in \mathbb{F}_{p^n}} \theta \epsilon_p^{-f(x)-\text{Tr}_p^{p^n}(\omega x)} = \theta(-\widehat{\chi}_f)(\omega).$$

Recall that for all $\omega \in \mathbb{F}_{p^n}$

$$(-\widehat{\chi}_f)(\omega) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{-f(x) - \text{Tr}_p^{p^n}(\omega x)} = \overline{\sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{f(x) + \text{Tr}_p^{p^n}(\omega x)}} = \overline{\sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{f(x) - \text{Tr}_p^{p^n}(-\omega x)}} = \overline{\widehat{\chi}_f(-\omega)}.$$

Then for all $\omega \in \mathbb{F}_{p^n}$

$$\widehat{\chi}_f(-\omega) \overline{\widehat{\chi}_f(-\omega)} \widehat{\chi}_f(-\omega) = \theta \overline{\widehat{\chi}_f(-\omega)}.$$

Therefore, (7) holds if and only if $|\widehat{\chi}_f(\omega)|^2 \in \{0, \theta\}$ for all $\omega \in \mathbb{F}_{p^n}$ where $\theta = p^{n+s}$. In particular, for $s = 0$, (7) holds if and only if $|\widehat{\chi}_f(\omega)|^2 = p^n$ for all $\omega \in \mathbb{F}_{p^n}$. \square

Theorem 3 can be rewritten as the following.

Corollary 4. *Let f be a function from \mathbb{F}_{p^n} to \mathbb{F}_p and s be an integer with $0 \leq s \leq n$. Then, f is s -plateaued if and only if*

$$\sum_{a, b, x \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)} = p^{2n+s}.$$

We remember a link between the second-order derivatives and the fourth power moments of the Walsh transforms in characteristic p in the following Proposition (see [23, Proposition 1], [16, Theorem 10] and in [13]).

Proposition 1. *Let f be a function from \mathbb{F}_{p^n} to \mathbb{F}_p . Then*

$$S_2(f) = \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi}_f(\omega)|^4 = p^n \sum_{a, b, x \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)}.$$

We deduce a new characterization of s -plateaued functions in terms of the fourth power moments of their Walsh transforms.

Theorem 4. *Let f be a function from \mathbb{F}_{p^n} to \mathbb{F}_p and s be an integer with $0 \leq s \leq n$. Then, f is s -plateaued if and only if*

$$S_2(f) = \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi}_f(\omega)|^4 = p^{3n+s}.$$

In particular, f is bent if and only if $S_2(f) = p^{3n}$.

Proof. By Corollary 4 and Proposition 1, f is s -plateaued if and only if

$$S_2(f) = \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi}_f(\omega)|^4 = p^n \sum_{a, b, x \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)} = p^{3n+s}.$$

\square

Notice that Theorem 2 is also a direct corollary of Theorem 4. Let us introduce an example of quadratic s -plateaued functions.

Example 1. Let p be an odd prime and $n \geq 2$ be an integer. Let f be an arbitrary \mathbb{F}_p -quadratic form from \mathbb{F}_{p^n} to \mathbb{F}_p defined as

$$f(x) = \text{Tr}_p^{p^n} (a_0 x^2 + a_1 x^{p+1} + a_2 x^{p^2+1} + \cdots + a_{\lfloor \frac{n}{2} \rfloor} x^{p^{\lfloor \frac{n}{2} \rfloor + 1}}).$$

The radical of f given by

$$W = \{x \in \mathbb{F}_{p^n} : f(x+y) = f(x) + f(y), \forall y \in \mathbb{F}_{p^n}\}$$

is an \mathbb{F}_p -linear subspace of \mathbb{F}_{p^n} . Let $\dim_{\mathbb{F}_p} W = s$. It follows from [9, the proof of Theorem 4.1] that for all $\omega \in \mathbb{F}_{p^n}$

$$|\widehat{\chi}_f(\omega)|^2 = 0 \quad \text{or} \quad p^{2s} \sum_{y_1, \dots, y_{n-s} \in \mathbb{F}_p} \sum_{z_1, \dots, z_{n-s} \in \mathbb{F}_p} \epsilon_p^{H(y_1, \dots, y_{n-s}) - H(z_1, \dots, z_{n-s})}$$

where $H(x_1, \dots, x_{n-s}) = \frac{1}{2}(x_1^2 + \cdots + x_{n-s-1}^2 + dx_{n-s}^2)$ and $d \in \mathbb{F}_p^*$. For each pair y_i and z_i where $i = 1, \dots, n-s$, it is easy to see that

$$\sum_{y_i, z_i \in \mathbb{F}_p} \epsilon_p^{\frac{1}{2}(y_i^2 - z_i^2)} = \sum_{t_{i1}, t_{i2} \in \mathbb{F}_p} \epsilon_p^{\frac{1}{2}(t_{i1}t_{i2})} = \sum_{t_{i2} \in \mathbb{F}_p} \left(\sum_{t_{i1} \in \mathbb{F}_p} \epsilon_p^{\frac{1}{2}t_{i1}} \right) = p.$$

Therefore, we conclude that $|\widehat{\chi}_f(\omega)|^2 \in \{0, p^{n+s}\}$ for all $\omega \in \mathbb{F}_{p^n}$. Moreover, [10, Proposition 5.8] gives an algorithm to construct a such quadratic form f with radical W of dimension s with $0 \leq s \leq n-1$. In fact, this algorithm holds for any finite field \mathbb{F}_q where q is a prime power. Hence, for each odd prime p , integers $n \geq 2$ and s with $0 \leq s \leq n-1$, there exists a quadratic p -ary s -plateaued function f from \mathbb{F}_{p^n} to \mathbb{F}_p . For example, for $p = 3$ and $n = 5$, we provide the following s -plateaued functions:

- $f_1(x) = \text{Tr}_3^{3^5}(x^2 + x^4 + 2x^{10})$ is the quadratic 0-plateaued function,
- $f_2(x) = \text{Tr}_3^{3^5}(x^2 + x^4 + x^{10})$ is the quadratic 1-plateaued function,
- $f_3(x) = \text{Tr}_3^{3^5}(\xi x^2 + x^4 + 2x^{10})$ is the quadratic 2-plateaued function,
- $f_4(x) = \text{Tr}_3^{3^5}(\xi^2 x^2 + 2x^4 + \xi^{28} x^{10})$ is the quadratic 3-plateaued function and
- $f_5(x) = \text{Tr}_3^{3^5}(x^2 + 2x^4 + 2x^{10})$ is the quadratic 4-plateaued function

where ξ is a primitive element of \mathbb{F}_{3^5} with $\xi^5 + 2\xi + 1 = 0$.

5 Characterization of Vectorial Bent Functions

The present section provides a new proof of characterization of vectorial bent functions given in [23]. The vectorial bent function is defined as the following.

Definition 1. Let F be a vectorial function from \mathbb{F}_{p^n} to \mathbb{F}_{p^m} . For every $\lambda \in \mathbb{F}_{p^m}^*$, the component function f_λ from \mathbb{F}_{p^n} to \mathbb{F}_p is defined as $f_\lambda(x) = \text{Tr}_p^{p^m}(\lambda F(x))$ for all $x \in \mathbb{F}_{p^n}$. Then, F is called *vectorial bent* if f_λ is bent for all $\lambda \in \mathbb{F}_{p^m}^*$.

In [25, Theorem 2.3], vectorial bent functions were characterized by using their derivatives: A vectorial function F is bent if and only if $\mathcal{D}_a F$ is balanced for all $a \in \mathbb{F}_{p^n}^*$. Recently, Mesnager characterized the vectorial bent functions in [23, Theorem 6] by using the number of zeros of second-order derivatives: A vectorial function F is bent if and only if

$$\mathfrak{N}(F) = |\{(a, b, x) \in \mathbb{F}_{p^n}^3 : \mathcal{D}_b \mathcal{D}_a F(x) = 0\}| = p^{3n-m} + p^{2n} - p^{2n-m}.$$

It would be interesting to prove directly that $\mathcal{D}_a F$ is balanced for all $a \in \mathbb{F}_{p^n}^*$ if and only if $\mathfrak{N}(F) = p^{3n-m} + p^{2n} - p^{2n-m}$ without using the bentness of vectorial function F . Before proving it, we start with a well-known result.

Lemma 2. *Let x_1, x_2, \dots, x_m be positive real numbers such that $x_1 + x_2 + \dots + x_m = n$. We then have*

$$x_1^2 + x_2^2 + \dots + x_m^2 \geq \frac{n^2}{m} \quad (10)$$

and the equality in (10) holds if and only if $x_1 = x_2 = \dots = x_m$.

The following Lemma is similar to Proposition 1, items (1) and (2) in [5], but it is valid in arbitrary characteristic.

Lemma 3. *Let G be a vectorial function from \mathbb{F}_{p^n} to \mathbb{F}_{p^m} . Then*

$$|\{(x_1, x_2) \in \mathbb{F}_{p^n}^2 : G(x_1) = G(x_2)\}| \geq p^{2n-m} \quad (11)$$

and the equality in (11) holds if and only if G is balanced.

Proof. Let $A_j = \{x \in \mathbb{F}_{p^n} : G(x) = y_j \in \mathbb{F}_{p^m}\}$ and $z_j = |A_j|$ for $j \in \{1, \dots, p^m\}$. Then we have

$$|\{(x_1, x_2) \in \mathbb{F}_{p^n}^2 : G(x_1) = G(x_2)\}| = \left| \bigcup_{j=1}^{p^m} \{(x_1, x_2) \in \mathbb{F}_{p^n}^2 : x_1, x_2 \in A_j\} \right| = \sum_{j=1}^{p^m} |A_j|^2 = \sum_{j=1}^{p^m} z_j^2.$$

By Lemma 2, for $\sum_{j=1}^{p^m} z_j = p^n$ and $z_j \geq 0$, we get $\sum_{j=1}^{p^m} z_j^2 \geq p^{2n-m}$. Thus, (11) holds. Notice that G is balanced if and only if $z_1 = z_2 = \dots = z_{p^m}$. The final assertion also follows from Lemma 2. \square

Proposition 2. *Let F be a vectorial function from \mathbb{F}_{p^n} to \mathbb{F}_{p^m} . Then*

$$\mathcal{D}_a F \text{ is balanced for all } a \in \mathbb{F}_{p^n}^* \iff \mathfrak{N}(F) = p^{3n-m} + p^{2n} - p^{2n-m} \quad (12)$$

where $\mathfrak{N}(F) = |\{(a, b, x) \in \mathbb{F}_{p^n}^3 : \mathcal{D}_b \mathcal{D}_a F(x) = 0\}|$.

Proof. The second-order derivative of F at $(a, b) \in \mathbb{F}_{p^n}^2$ is

$$\mathcal{D}_b \mathcal{D}_a F(x) = F(x + a + b) + F(x) - F(x + b) - F(x + a).$$

Notice that for $(a, b, x) \in \mathbb{F}_{p^n}^3$, $\mathcal{D}_b \mathcal{D}_a F(x) = 0$ if and only if

$$\mathcal{D}_a F(x) = \mathcal{D}_a F(x + b). \quad (13)$$

First, for $n = m$, let us prove that $\mathcal{D}_a F$ is balanced for all $a \in \mathbb{F}_{p^n}^*$ if and only if $\mathfrak{N}(F) = 2p^{2n} - p^n$. For $a = 0$, it is easy to see that (13) holds for all $b, x \in \mathbb{F}_{p^n}$ since $\mathcal{D}_a F$ is zero map. Then, $|\{(0, b, x) \in \mathbb{F}_{p^n}^3 : \mathcal{D}_b \mathcal{D}_a F(x) = 0\}| = p^{2n}$. For $a \neq 0$, by Lemma 3, the number of pairs $(b, x) \in \mathbb{F}_{p^n}^2$ satisfying (13) is equal to p^n if and only if $\mathcal{D}_a F$ is balanced. Then, $|\{(a, b, x) \in \mathbb{F}_{p^n}^3 : a \neq 0, \mathcal{D}_b \mathcal{D}_a F(x) = 0\}| = p^{2n} - p^n$. Therefore, $\mathcal{D}_a F$ is balanced for all $a \in \mathbb{F}_{p^n}^*$ if and only if $\mathfrak{N}(F) = 2p^{2n} - p^n$.

Now, let $n \neq m$. For $a = 0$, we get $|\{(0, b, x) \in \mathbb{F}_{p^n}^3 : \mathcal{D}_b \mathcal{D}_a F(x) = 0\}| = p^{2n}$. For $a \neq 0$, by Lemma 3, the number of pairs $(b, x) \in \mathbb{F}_{p^n}^2$ satisfying (13) is equal to p^{2n-m} if and only if $\mathcal{D}_a F$ is balanced. Then, $|\{(a, b, x) \in \mathbb{F}_{p^n}^3 : a \neq 0, \mathcal{D}_b \mathcal{D}_a F(x) = 0\}| = (p^n - 1)p^{2n-m}$. Thus, (12) holds. \square

In [23, Corollary 1], F is vectorial bent if and only if $\mathfrak{N}^*(F) = (p^n - 1)(p^{2n-m} - p^n)$ where

$$\mathfrak{N}^*(F) = |\{(a, b, x) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n} : \mathcal{D}_b \mathcal{D}_a F(x) = 0\}|.$$

Then, $\mathcal{D}_a F$ is balanced for all $a \in \mathbb{F}_{p^n}^*$ if and only if $\mathfrak{N}^*(F) = (p^n - 1)(p^{2n-m} - p^n)$. This can be easily seen by Lemma 3.

6 Characterizations of Vectorial s -Plateaued Functions

In this section, we are interested in a special class of vectorial plateaued functions, which are called *vectorial s -plateaued* functions where $s \in \mathbb{N}$. We provide their characterizations in terms of the moments of their Walsh transforms and the number of zeros of their second-order derivatives.

The notion of vectorial plateaued functions in characteristic 2 were defined by Carlet in [2]. This can be given in arbitrary characteristic.

Definition 2. Let F be a vectorial function from \mathbb{F}_{p^n} to \mathbb{F}_{p^m} . For every $\lambda \in \mathbb{F}_{p^m}^*$, the component function f_λ from \mathbb{F}_{p^n} to \mathbb{F}_p is defined as $f_\lambda(x) = \text{Tr}_p^{p^m}(\lambda F(x))$ for all $x \in \mathbb{F}_{p^n}$. Then, F is called *vectorial plateaued* if f_λ is plateaued for all $\lambda \in \mathbb{F}_{p^m}^*$.

The notion of vectorial s -plateaued functions in arbitrary characteristic can be given as the following (for example, see in [12]).

Definition 3. Let F be a vectorial function from \mathbb{F}_{p^n} to \mathbb{F}_{p^m} and s be an integer with $0 \leq s \leq n$. For every $\lambda \in \mathbb{F}_{p^m}^*$, the component function f_λ from \mathbb{F}_{p^n} to \mathbb{F}_p is defined as $f_\lambda(x) = \text{Tr}_p^{p^m}(\lambda F(x))$ for all $x \in \mathbb{F}_{p^n}$. Then, F is called *vectorial s -plateaued* if f_λ is s -plateaued with the same amplitude s for all $\lambda \in \mathbb{F}_{p^m}^*$.

Notice that F is said to be *vectorial s -plateaued* if and only if f_λ is s -plateaued with the same amplitude s for all $\lambda \in \mathbb{F}_{p^m}^*$.

We can extract from Theorem 2 the following characterization of vectorial s -plateaued functions.

Theorem 5. *Let F be a vectorial function from \mathbb{F}_{p^n} to \mathbb{F}_{p^m} . Then, F is a vectorial s -plateaued function if and only if*

$$\sum_{\lambda \in \mathbb{F}_{p^m}^*} S_2(f_\lambda) = p^{3n+s}(p^m - 1) \quad \text{and} \quad \sum_{\lambda \in \mathbb{F}_{p^m}^*} S_3(f_\lambda) = p^{4n+2s}(p^m - 1). \quad (14)$$

Proof. Suppose that F is vectorial s -plateaued. By Theorem 2 for all $\lambda \in \mathbb{F}_{p^m}^*$, f_λ is s -plateaued if and only if $S_2(f_\lambda) = p^{3n+s}$ and $S_3(f_\lambda) = p^{4n+2s}$. Thus, (14) holds.

Conversely, suppose that (14) holds. By (2) with $A = p^{n+s}$ and $i = 1$, for all $\lambda \in \mathbb{F}_{p^m}^*$

$$D_\lambda = \sum_{\omega \in \mathbb{F}_{p^n}} (|\widehat{\chi}_{f_\lambda}(\omega)|^2 - p^{n+s})^2 |\widehat{\chi}_{f_\lambda}(\omega)|^2 = S_3(f_\lambda) - 2p^{n+s}S_2(f_\lambda) + p^{2(n+s)}S_1(f_\lambda).$$

Then by (1) and (14),

$$\sum_{\lambda \in \mathbb{F}_{p^m}^*} D_\lambda = p^{4n+2s}(p^m - 1) - 2p^{n+s}p^{3n+s}(p^m - 1) + p^{2n+2s}p^{2n}(p^m - 1) = 0.$$

Since $D_\lambda \geq 0$ and $\sum_{\lambda \in \mathbb{F}_{p^m}^*} D_\lambda = 0$, we get $D_\lambda = 0$ for every $\lambda \in \mathbb{F}_{p^m}^*$. Then, for every $\lambda \in \mathbb{F}_{p^m}^*$, $|\widehat{\chi}_{f_\lambda}(\omega)| \in \left\{0, p^{\frac{n+s}{2}}\right\}$ for all $\omega \in \mathbb{F}_{p^n}$. Therefore, F is vectorial s -plateaued function. \square

For a vectorial function F , the relation between the sum of $S_2(f_\lambda)$ for all $\lambda \in \mathbb{F}_{p^m}^*$ and $\mathfrak{N}(F)$ was given by Mesnager in [23] as follows.

Proposition 3. *Let F be a vectorial function from \mathbb{F}_{p^n} to \mathbb{F}_{p^m} . Then*

$$\sum_{\lambda \in \mathbb{F}_{p^m}^*} S_2(f_\lambda) = p^{n+m}\mathfrak{N}(F) - p^{4n}$$

where $\mathfrak{N}(F) = |\{(a, b, x) \in \mathbb{F}_{p^n}^3 : \mathcal{D}_b \mathcal{D}_a F(x) = 0\}|$.

We conclude the following characterization of vectorial s -plateaued functions.

Theorem 6. *Let F be a vectorial function from \mathbb{F}_{p^n} to \mathbb{F}_{p^m} . Then, F is vectorial s -plateaued if and only if $S_3(f_\lambda) = p^{4n+2s}$ for all $\lambda \in \mathbb{F}_{p^m}^*$ and*

$$\mathfrak{N}(F) = p^{3n-m} + p^{2n+s} - p^{2n+s-m}$$

where $\mathfrak{N}(F) = |\{(a, b, x) \in \mathbb{F}_{p^n}^3 : \mathcal{D}_b \mathcal{D}_a F(x) = 0\}|$.

Proof. By Proposition 3 and Theorem 5, we get $p^{3n+s}(p^m - 1) = p^{n+m}\mathfrak{N}(F) - p^{4n}$. Thus, we obtain

$$\mathfrak{N}(F) = p^{3n-m} + p^{2n+s} - p^{2n+s-m}.$$

Conversely, by Proposition 3, we get

$$\sum_{\lambda \in \mathbb{F}_{p^m}^*} S_2(f_\lambda) = p^{n+m}(p^{3n-m} + p^{2n+s} - p^{2n+s-m}) - p^{4n} = p^{3n+s}(p^m - 1).$$

By assumption, $\sum_{\lambda \in \mathbb{F}_{p^m}^*} S_3(f_\lambda) = p^{4n+2s}(p^m - 1)$. Therefore, by Theorem 5, F is vectorial s -plateaued functions. \square

Let us give an example of vectorial quadratic s -plateaued functions.

Example 2. Let p be an odd prime, $m \geq 2$ and $r \geq 2$ be integers and $q = p^m$. Let f be an arbitrary \mathbb{F}_q -quadratic form from \mathbb{F}_{q^r} to \mathbb{F}_q given by

$$f(x) = \text{Tr}_q^{q^r}(a_0x^2 + a_1x^{q+1} + a_2x^{q^2+1} + \cdots + a_{\lfloor \frac{r}{2} \rfloor}x^{q^{\lfloor \frac{r}{2} \rfloor+1}).$$

As in Example 1, by [9, 10], we have an algorithm to construct f with radical

$$W = \{x \in \mathbb{F}_{q^r} : f(x+y) = f(x) + f(y), \forall y \in \mathbb{F}_{q^r}\} \quad (15)$$

of prescribed dimension s over \mathbb{F}_q for each given integer s with $0 \leq s \leq r-1$. For $\lambda \in \mathbb{F}_{p^m}^*$, the component function g_λ from \mathbb{F}_{p^n} to \mathbb{F}_p given by $g_\lambda(x) = \text{Tr}_p^{p^m}(\lambda f(x))$ is an \mathbb{F}_p -quadratic form with radical

$$W_\lambda = \{x \in \mathbb{F}_{p^n} : g_\lambda(x+y) = g_\lambda(x) + g_\lambda(y), \forall y \in \mathbb{F}_{p^n}\} \quad (16)$$

where $n = mr$. For a \mathbb{F}_q -quadratic form f on \mathbb{F}_{q^r} and $\lambda \in \mathbb{F}_q^*$, the radical W in (15) is the set of the roots of the equation

$$a_0x + a_1x^q + (a_1x)^{q^{-1}} + a_2x^{q^2} + (a_2x)^{q^{-2}} + \cdots + a_{\lfloor \frac{r}{2} \rfloor}x^{q^{\lfloor \frac{r}{2} \rfloor}} + \left(a_{\lfloor \frac{r}{2} \rfloor}x\right)^{q^{-\lfloor \frac{r}{2} \rfloor}} \quad (17)$$

in \mathbb{F}_{q^r} and W_λ in (16) is the set of the roots of the equation

$$\lambda a_0x + \lambda a_1x^q + (\lambda a_1x)^{q^{-1}} + \lambda a_2x^{q^2} + (\lambda a_2x)^{q^{-2}} + \cdots + \lambda a_{\lfloor \frac{r}{2} \rfloor}x^{q^{\lfloor \frac{r}{2} \rfloor}} + \left(\lambda a_{\lfloor \frac{r}{2} \rfloor}x\right)^{q^{-\lfloor \frac{r}{2} \rfloor}} \quad (18)$$

(for example, see [10, Lemma 2.1]). As $\lambda \in \mathbb{F}_q^*$, it is easy to observe from (17) and (18) that $W = W_\lambda$. Therefore, we obtain vectorial s -plateaued function F from \mathbb{F}_{p^n} to \mathbb{F}_{p^m} (notice that $F(x) = f(x)$ for all $x \in \mathbb{F}_{p^n}$). This shows existence of an algorithm to construct vectorial s -plateaued functions F for any integer s with $0 \leq s \leq r-1$. For example, if $p = 3$, $m = 2$ and $n = 6$, then

- $f_1(x) = \text{Tr}_{32}^{36}(x^2 + x^{10})$ is the vectorial 0-plateaued function and
- $f_2(x) = \text{Tr}_{32}^{36}(x^2 + 2x^{10})$ is the vectorial 1-plateaued function.

Example 3. Let p be an odd prime and n be a positive even integer. Let f_1 and f_2 be the quadratic p -ary s_1 -plateaued and s_2 -plateaued functions from \mathbb{F}_{p^n} to \mathbb{F}_p with $s_1 \neq s_2$, respectively. For any $\theta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, a function F given as

$$F(x) = f_1(x) + \theta f_2(x)$$

is the vectorial plateaued function from \mathbb{F}_{p^n} to \mathbb{F}_{p^2} , but it is not the vectorial s -plateaued function for any integer s . This shows that the vectorial plateaued functions are strictly more general than the vectorial s -plateaued function for any s .

7 Conclusion

This paper studies the characterizations of (vectorial) bent and plateaued functions in arbitrary characteristic. First, we provide the results on characterizations of bent and plateaued functions. Next, we generalize their characterizations in characteristic 2 in terms of the second-order derivatives given in [7] to arbitrary characteristic. Moreover, we present a new characterization of plateaued functions in terms of fourth power moments of their Walsh transforms. Furthermore, we give a direct proof between the balancedness of the first-order derivatives of vectorial bent functions and the number of zeros of their second-order derivatives. Lastly, we present the characterizations of vectorial s -plateaued functions.

Acknowledgment. The third author is partially supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK)-BİDEB 2211 program.

References

1. Cao, X., Chen, H., Mesnager, S.: Further results on semi-bent functions in polynomial form. *J. Adv. Math. Commun. (AMC)* (To appear)
2. Carlet, C.: Vectorial boolean functions for cryptography. *Boolean Models Methods Math. Comput. Sci. Eng.* **134**, 398–469 (2010)
3. Carlet, C.: On the properties of vectorial functions with plateaued components and their consequences on APN functions. In: El Hajji, S., Nitaj, A., Carlet, C., Souidi, E.M. (eds.) *Codes, Cryptology, and Information Security. LNCS*, vol. 9084, pp. 63–73. Springer, Heidelberg (2015)
4. Carlet, C., Ding, C.: Highly nonlinear mappings. *Spec. Issue Complex. Issues Coding Crypt. J. Complex.* **20**(2–3), 205–244 (2004)
5. Carlet, C., Ding, C.: Nonlinearities of S-boxes. *Finite Fields Appl.* **13**(1), 121–135 (2007)
6. Carlet, C., Mesnager, S.: On semi-bent boolean functions. *IEEE Trans. Inf. Theory* **58**(5), 3287–3292 (2012)
7. Carlet, C., Prouff, E.: On plateaued functions and their constructions. In: Johansson, T. (ed.) *FSE 2003. LNCS*, vol. 2887, pp. 54–73. Springer, Heidelberg (2003)
8. Cohen, G., Mesnager, S.: On constructions of semi-bent functions from bent functions. *J. Contemp. Math.* **625**, 141–154 (2014). *Discrete Geometry and Algebraic Combinatorics*, American Mathematical Society
9. Çakçak, E., Özbudak, F.: Curves related to coulter’s maximal curves. *Finite Fields Appl.* **14**(1), 209–220 (2008)
10. Çakçak, E., Özbudak, F.: Some Artin-Schreier type function fields over finite fields with prescribed genus and number of rational places. *J. Pure Appl. Algebra* **210**(1), 113–135 (2007)

11. Çeşmelioglu, A., Meidl, W.: A construction of bent functions from plateaued functions. *Des. Codes Crypt.* **66**(1–3), 231–242 (2013)
12. Çeşmelioglu, A., Meidl, W.: Non weakly regular bent polynomials from vectorial quadratic functions. In: *Topics in Finite Fields-Proceedings of Fq11*, Contemporary Mathematics, AMS, vol. 632, pp. 83–94 (2015)
13. Dobbertin, H., Helleseht, T., Kumar, P.V., Martinsen, H.M.: Ternary m-sequences with three-valued cross-correlation function: new decimations of Welch and Niho type. *IEEE Trans. Inf. Theory* **47**(4), 1473–1481 (2001)
14. Helleseht, T., Kholosha, K.: Monomial and quadratic bent functions over the finite field of odd characteristic. *IEEE Trans. Inf. Theory* **52**(5), 2018–2032 (2006)
15. Helleseht, T., Kholosha, A.: On the dual of monomial quadratic p -ary bent functions. In: Golomb, S.W., Gong, G., Helleseht, T., Song, H.-Y. (eds.) *SSC 2007*. LNCS, vol. 4893, pp. 50–61. Springer, Heidelberg (2007)
16. Helleseht, T., Rong, C., Sandberg, D.: New families of almost perfect nonlinear power mappings. *IEEE Trans. Inf. Theory* **45**(2), 475–485 (1999)
17. Hou, X.-D.: p -ary and q -ary versions of certain results about bent functions and resilient functions. *Finite Fields Appl.* **10**(4), 566–582 (2004)
18. Khoo, G.: A new characterization of semi-bent and bent functions on finite fields. *Des. Codes Crypt.* **38**(2), 279–295 (2006)
19. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. *J. Comb. Theory Ser. A* **40**(1), 90–107 (1985)
20. Mesnager, S.: Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials. *IEEE Trans. Inf. Theory* **57**(11), 7443–7458 (2011)
21. Mesnager, S.: Semi-bent functions with multiple trace terms and hyperelliptic curves. In: Hevia, A., Neven, G. (eds.) *LatinCrypt 2012*. LNCS, vol. 7533, pp. 18–36. Springer, Heidelberg (2012)
22. Mesnager, S.: Semi-bent functions from oval polynomials. In: Stam, M. (ed.) *IMACC 2013*. LNCS, vol. 8308, pp. 1–15. Springer, Heidelberg (2013)
23. Mesnager, S.: Characterizations of plateaued and bent functions in characteristic p . In: Schmidt, K.-U., Winterhof, A. (eds.) *SETA 2014*. LNCS, vol. 8865, pp. 72–82. Springer, Heidelberg (2014)
24. Mesnager, S.: On semi-bent functions and related plateaued functions over the Galois field F_{2^n} . In: Koç, Ç.K. (ed.) *Open Problems in Mathematics and Computational Science*, pp. 243–273. Springer International Publishing, Switzerland (2014)
25. Nyberg, K.: Perfect nonlinear S-boxes. In: Davies, D.W. (ed.) *EUROCRYPT 1991*. LNCS, vol. 547, pp. 378–386. Springer, Heidelberg (1991)
26. Rothaus, O.S.: On bent functions. *J. Comb. Theory Ser. A* **20**(3), 300–305 (1976)
27. Tan, Y., Yang, J., Zhang, X.: A recursive construction of p -ary bent functions which are not weakly regular. In: *IEEE International Conference on Information Theory and Information Security (ICITIS)*, pp. 156–159 (2010)
28. Zheng, Y., Zhang, X.-M.: Plateaued functions. In: Varadharajan, V., Mu, Y. (eds.) *ICICS 1999*. LNCS, vol. 1726, pp. 284–300. Springer, Heidelberg (1999)
29. Zheng, Y., Zhang, X.-M.: Relationships between bent functions and complementary plateaued functions. In: Song, J.S. (ed.) *ICISC 1999*. LNCS, vol. 1787, pp. 60–75. Springer, Heidelberg (2000)

Cryptography and Information Security in the Balkans
Second International Conference, BalkanCryptSec
2015, Koper, Slovenia, September 3-4, 2015, Revised
Selected Papers

Pasalic, E.; Knudsen, L.R. (Eds.)

2016, VIII, 207 p. 19 illus., Softcover

ISBN: 978-3-319-29171-0