A note on semi-bent functions with multiple trace terms and hyperelliptic curves

Sihem Mesnager*

Monday 28th November, 2011

Abstract

Semi-bent functions with even number of variables are a class of important Boolean functions whose Hadamard transform takes three values. In this note we are interested in the property of semi-bentness of Boolean functions defined on the Galois field $\mathbb{F}_{2^n}$ (n even) with multiple trace terms obtained via Niho functions and two Dillon-like functions (the first one has been studied by Mesnager and the second one have been studied very recently by Wang, Tang, Qi, Yang and Xu). We subsequently give a connection between the property of semi-bentness and the number of rational points on some associated hyperelliptic curves. We use the hyperelliptic curve formalism to reduce the computational complexity in order to provide a polynomial time and space test leading to an efficient characterization of semi-bentness of such functions (which includes an efficient characterization of the hyperbent functions proposed by Wang et al.). The idea of this approach goes back to the recent work of Lisoněk on the hyperbent functions studied by Charpin and Gong.

Keywords. Boolean function, Walsh-Hadamard transformation, Semi-bent functions, Dickson polynomial, Hyperelliptic curves.

1 Introduction

A number of research works in symmetric cryptography are devoted to problems of resistance of various ciphering algorithms to the fast correlation attacks (on stream ciphers) and to the linear cryptanalysis (on block ciphers). These works analyse various classes of approximating functions and constructions of functions with the best resistance to such approximations. Some general classes of Boolean functions play a central role with this respect: the class of *bent functions* [34], that is, of Boolean functions of an even number of variables that have the maximum possible Hamming distance to the set of all affine functions (see [7] for the relations of bent functions to coding theory), its subclasses of homogeneous bent functions [33] and hyper-bent functions [40], and the generalizations of the notion: semi-bent functions [5], Z-bent functions [9], negabent functions [32], etc.

The paper is devoted to *semi-bent* Boolean functions. The notion of semi-bent function has been introduced by Chee, Lee and Kim [5] at Asiacrypt' 94. These functions had been previously investigated under the name of three-valued almost optimal Boolean functions in [2]. Moreover, they are particular cases of the so-called plateaued functions [41]. Semi-bent functions

*LAGA (Laboratoire Analyse, Géometrie et Applications), UMR 7539, CNRS, Department of Mathematics, University of Paris XIII and University of Paris VIII, 2 rue de la liberté, 93526 Saint-Denis Cedex, France. smesnager@univ-paris8.fr

are widely studied in cryptography because, besides having low Hadamard transform which provides protection against fast correlation attacks [27] and linear cryptanalysis [26], they can possess desirable properties such as low autocorrelation, propagation criteria, resiliency and high algebraic degree. Semi-bent functions have been paid a lot of attention in code division multiple access (CDMA) communication systems for sequence design [15], [17], [18], [19], [21], [22], [4] etc. In fact, highly nonlinear functions correspond to sequences that have low cross-correlation with the m-sequences (maximum-length linear feedback shift -register sequences) represented by an absolute trace function $Tr_1^m(x)$. Semi-bent functions exist for even or odd number of variables. When n is even, the semi-bent functions are those Boolean functions whose Hadamard transform takes values 0 and $\pm 2^{\frac{n+2}{2}}$. They are balanced (up to the addition of a linear function) and have maximal non-linearity among balanced plateaued functions. Results concerning quadratic semi-bent functions with even number of inputs can be found in [4]. Links of semi-bent functions from Dillon and Niho exponents with exponential sums (namely, Kloosterman sums) can be found in [31]. Some constructions of monomial (that is, absolute trace of a power function) semi-bent functions (namely, quadratic functions) have been proposed in [36]. Recently, a large number of infinite classes of semi-bent functions in explicit bivariate (resp. univariate) polynomial have been obtained in [3].

In this paper, functions in univariate representation expressed by means of trace functions via Dillon-like exponents (proposed by the author [30] and very recently by Wang et al. [39]) and Niho exponents with even number of variables are considered. Our main intention is to provide an efficient characterization of the semi-bentness property of the corresponding functions (whose expressions are in polynomial forms with multiple trace terms). To this end, we precise firstly the connection between the semi-bentness property of such functions and some exponential sums involving Dickson polynomials. Next, in the line of the recent works of Lisonek [25], and further of Flori and Mesnager [12], we give a link between the property of semi-bentness and the number of rational points on certain hyperelliptic curves. The paper exploits the connections between semi-bentness property and binary hyperelliptic curves to produce a polynomial complexity test which is of use in constructing semi-bent functions with multiple trace terms.

The paper is organized as follows. In section 2, we fix our main notation and recall the necessary background. In Section 3, we recall some technical results that we need subsequently. Next, in section 4, we investigate the link between the semi-bentness property of some infinite classes of Boolean functions in univariate representation and some exponential sums involving Dickson polynomials. Such a link leads to an exponential time test of semi-bentness. Finally, in section 5, we connect the property of semi-bentness of such functions to hyperelliptic curves and we reformulate the characterization obtained in section 4 in terms of cardinalities of hyperelliptic curves leading to an efficient test (polynomial time and space test) of semi-bentness.

2 Notation and preliminaries

2.1 Boolean functions in polynomial forms

Let n be a positive integer. A Boolean function f on $\mathbb{F}_{2^n}$ is an $\mathbb{F}_2$-valued function on the Galois field $\mathbb{F}_{2^n}$ of order 2^n. The *weight* of f, denoted by $wt(f)$, is the *Hamming weight* of the image vector of f, that is, the cardinality of its support $\{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$.

For any positive integer k, and for any r dividing k, the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$,

denoted by Tr_r^k, is the mapping defined as:

$$\forall x \in \mathbb{F}_{2^k}, \quad Tr_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}} = x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k-r}}$$

In particular, the *absolute trace* over $\mathbb{F}_2$ is the function $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. Recall that, for every integer r dividing k, the trace function Tr_r^k satisfies the transitivity property, that is,

$$Tr_1^k = Tr_1^r \circ Tr_r^k$$

There exist several kinds of possible trace (univariate) representations of Boolean functions which are not necessary unique and use the identification between the vector-space $\mathbb{F}_2^n$ and the field $\mathbb{F}_{2^n}$.
Every non-zero Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion of the form:

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n-1})$$

where Γ_n is the set of integers obtained by choosing one element in each cyclotomic coset of 2 modulo $2^n - 1$ (the most usual choice for j is the smallest element in its cyclotomic class, called the coset leader of the class), $o(j)$ is the size of the cyclotomic coset of 2 modulo $2^n - 1$ containing j, $a_j \in \mathbb{F}_{2^{o(j)}}$ and $\epsilon = wt(f)$ modulo 2 where $wt(f)$ is the *Hamming weight* of the image vector of f, that is, the cardinality of its support $Supp(f) := \{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$.
This trace representation of f is unique and is called its *polynomial form.*

2.2 Walsh transform and semi-bent functions

Let f be a Boolean function on $\mathbb{F}_{2^n}$. Its *"sign" function* is the integer-valued function $\chi_f := (-1)^f$. The *W*alsh Hadamard transform of f is the discrete Fourier transform of χ_f, whose value at $\omega \in \mathbb{F}_{2^n}$ is defined as:

$$\forall \omega \in \mathbb{F}_{2^n}, \quad \widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + Tr_1^n(\omega x)}$$

Bent functions [34] can be defined as:

Definition 1. *A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be bent if $\widehat{\chi_f}(\omega) = \pm 2^{\frac{n}{2}}$, for all $\omega \in \mathbb{F}_{2^n}$.*

Semi-bent functions [5], [6] are defined as:

Definition 2. *For even n, a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be semi-bent if $\widehat{\chi_f}(\omega) \in \{0, \pm 2^{\frac{n+2}{2}}\}$, for all $\omega \in \mathbb{F}_{2^n}$. For odd n, a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be semi-bent if $\widehat{\chi_f}(\omega) \in \{0, \pm 2^{\frac{n+1}{2}}\}$, for all $\omega \in \mathbb{F}_{2^n}$.*

2.3 Dickson polynomial

Recall that the family of binary Dickson polynomials $D_r(X) \in \mathbb{F}_2[X]$ of degree r is defined by

$$D_r(X) = \sum_{i=0}^{\lfloor \frac{r}{2} \rfloor} \frac{r}{r-i} \binom{r-i}{i} X^{r-2i}, \quad r = 2, 3, \cdots$$

Moreover, the family of Dickson polynomials $D_r(X)$ can also be defined by the following recurrence relation:

$$D_{i+2}(X) = XD_{i+1}(X) + D_i(X)$$

with initial values

$$D_0(X) = 0, \quad D_1(X) = X.$$

Now, recall the following properties which we use in the sequel. For any non-zero positive integers r and p, Dickson polynomials satisfy:

1. $\deg(D_r(X)) = r$,
2. $D_{rp}(X) = D_r(D_p(X))$,
3. $D_r(x + x^{-1}) = x^r + x^{-r}$.

The reader can refer to [24] for many useful properties and applications of Dickson polynomials. We give the list of the first six Dickson polynomials:
$D_0(X) = 0$; $D_1(X) = X$; $D_2(X) = X^2$; $D_3(X) = X + X^3$; $D_4(X) = X^4$; $D_5(X) = X + X^3 + X^5$.

From now, $n = 2m$ is an (even) integer. We denote by U the cyclic group of $(2^m + 1)$-st roots of unity that is $\{u \in \mathbb{F}_{2^n} \mid u^{2^m+1} = 1\}$.

3 Background on some technical results

Let R be a subset of representatives of the cyclotomic classes modulo $2^n - 1$ for which each class has the full size n. The author has studied the class of functions whose polynomial form is given by $\sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$ (where $a_r \in \mathbb{F}_{2^m}^\star$ for $r \in R$ and $b \in \mathbb{F}_4^\star$) and proved the following result [31] using the method introduced in [29].

Theorem 3. *(Corollary 3, [31]) Suppose $m := \frac{n}{2}$ odd. Let β a primitive element of $\mathbb{F}_4$ and $R \subseteq E$ where E is a set of representatives of the cyclotomic classes modulo $2^n - 1$ for which each class has the full size n. For $b \in \mathbb{F}_4^\star$ and $a_r \in \mathbb{F}_{2^m}^\star$, we denote by $g_{a_r,b}$ the function defined on $\mathbb{F}_{2^n}$ by $\sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$, and by h_{a_r} the function defined on $\mathbb{F}_{2^m}$ by $h_{a_r}(x) = \sum_{r\in R} Tr_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Then,*

1. *$\sum_{u\in U} \chi\Big(g_{a_r,\beta}(u)\Big) = 1$ if and only if $\sum_{u\in U} \chi\Big(g_{a_r,\beta^2}(u)\Big) = 1$ if and only if,*

$$\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(Tr_1^m(x^{-1}) + h_{a_r}(D_3(x))\Big) = 2^m - 2wt(h_{a_r} \circ D_3) + 4.$$

2. *$\sum_{u\in U} \chi\Big(g_{a_r,1}(u)\Big) = 1$ if and only if*

$$3\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(Tr_1^m(x^{-1}) + h_{a_r}(x)\Big) - 2\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(Tr_1^m(x^{-1}) + h_{a_r}(D_3(x))\Big) = 4 + 2^m + 4wt(h_{a_r} \circ D_3) - 6wt(h_{a_r}).$$

Very recently, Wang et al. have studied (with some restriction) the family of functions whose polynomial form is given by $\sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^4(b' x^{\frac{2^n-1}{5}})$ (where $a_r \in \mathbb{F}_{2^m}^\star$ for $r \in R$ and $b' \in \mathbb{F}_{16}^\star$) and proved the following result [39] using the approach introduced by the author in [29].

Theorem 4. *([39]) Suppose $m := \frac{n}{2} \equiv 2 \pmod 4$. Let $R \subseteq E$ where E is a set of representatives of the cyclotomic classes modulo $2^n - 1$ for which each class has the full size n. For $b' \in \mathbb{F}_{16}^\star$ and $a_r \in \mathbb{F}_{2^m}^\star$, we denote by $g_{a_r,b'}$ the function defined on $\mathbb{F}_{2^n}$ by $\sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^4(b' x^{\frac{2^n-1}{5}})$, and by h_{a_r} the function defined on $\mathbb{F}_{2^m}$ by $\sum_{r\in R} Tr_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Then,*

1. *If b' a primitive element of $\mathbb{F}_{16}$ such that $Tr_1^4(b') = 0$ then, $\sum_{u\in U} \chi\Big(g_{a_r,b'}(u)\Big) = 1$ if and only if,*

$$\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(D_5(x))\Big) = 2$$

2. *If $b' = 1$ then, $\sum_{u\in U} \chi\Big(g_{a_r,1}(u)\Big) = 1$ if and only if*

$$2 \sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(D_5(x))\Big) - 5 \sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(x)\Big) = 4.$$

3. *Assume $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$. If $b' \in \{\beta, \beta^2, \beta^3\beta^4\}$ where β is a primitive 5-th root of unity in $\mathbb{F}_{16}$ then, $\sum_{u\in U} \chi\Big(g_{a_r,b'}(u)\Big) = 1$ if and only if,*

$$\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(D_5(x))\Big) + 5 \sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(x)\Big) = -8.$$

4. *Assume $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$. If b' is a primitive element of $\mathbb{F}_{16}$ such that $Tr_1^4(b') = 1$ then, $\sum_{u\in U} \chi\Big(g_{a_r,b'}(u)\Big) = 1$ if and only if,*

$$3 \sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(D_5(x))\Big) - 5 \sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(x)\Big) = -4.$$

5. *Assume $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$. If $b' \in \{\beta+\beta^2, \beta+\beta^3, \beta^2+\beta^4, \beta^3+\beta^4, \beta+\beta^4, \beta^2+\beta^3\}$ where β is a primitive 5-th root of unity in $\mathbb{F}_{16}$ then, $\sum_{u\in U} \chi\Big(g_{a_r,b'}(u)\Big) = 1$ if and only if,*

$$\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(D_5(x))\Big) = 2.$$

4 Characterizations of semi-bent functions with multiple trace terms by means of exponential sums involving Dickson polynomials

Nonlinear Boolean functions whose restriction to any vector space $u\mathbb{F}_{2^m}$ (where $u \in U$) are linear are sums of Niho power functions, that is (see [10]) of functions of the form:

$$Tr_1^{o((2^m-1)s+1)}\left(a_s x^{(2^m-1)s+1}\right) \text{ with } 1 \le s \le 2^m$$

We can determine the value of $o((2^m-1)s+1))$ precisely (recall that $o(j)$ denotes the size of the cyclotomic coset of 2 modulo 2^n-1 containing j):

Lemma 1. *We have $o((2^m-1)s+1))=m$ if $s=2^{m-1}+1$ (i.e. if $(2^m-1)s+1$ and 2^m+1 are conjugate) and $o((2^m-1)s+1))=n$ otherwise.*

Now, consider four infinite classes of functions with multiple trace terms defined on $\mathbb{F}_{2^n}$. We denote by E the set of representatives of the cyclotomic classes modulo 2^n-1 for which each class has full size n. Let $f_{a_r,b,c}$ $f'_{a_r,b}$, $\tilde{f}_{a_r,b',c}$ and $\tilde{f}'_{a_r,b'}$ be the functions defined on $\mathbb{F}_{2^n}$ whose polynomial form is given by (1), (2), (3) and (4), respectively.

$$f_{a_r,b,c}(x) := \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}}) + Tr_1^m(cx^{2^m+1}) \tag{1}$$

$$f'_{a_r,b}(x) := \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}}) + Tr_1^m(x^{2^m+1}) + Tr_1^n\left(x^{(2^m-1)s+1}\right) \tag{2}$$

$$\tilde{f}_{a_r,b',c}(x) := \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^4(b'x^{\frac{2^n-1}{5}}) + Tr_1^m(cx^{2^m+1}) \tag{3}$$

$$\tilde{f}'_{a_r,b'}(x) := \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^4(b'x^{\frac{2^n-1}{5}}) + Tr_1^m(x^{2^m+1}) + Tr_1^n\left(x^{(2^m-1)s'+1}\right) \tag{4}$$

where $R\subseteq E$, $a_r\in\mathbb{F}_{2^m}^\star$, $b\in\mathbb{F}_4^\star$, $b'\in\mathbb{F}_{16}^\star$, $c\in\mathbb{F}_{2^m}^\star$, $s\in\{1/4,3\}$ and $s'\in\{1/6,3\}$(the fractions $1/4$ and $1/6$ are understood modulo 2^m+1).

Note that $o(r(2^m-1))=n$, $o(\frac{2^n-1}{3})=2$, $o(\frac{2^n-1}{5})=4$, $o(2^m+1)=m$ and $o((2^m-1)s+1)=n$ for $s\in\{1/4,1/6,3\}$. Moreover, note that for a fixed r, the function $x\mapsto Tr_1^n(a_r x^{r(2^m-1)})$ is a Dillon-like function (it is a Dillon function for r co-prime with 2^m+1) and for m odd (resp. m even), the function $x\mapsto Tr_1^m(cx^{2^m+1})+Tr_1^n\left(x^{(2^m-1)s+1}\right)$ (resp. $x\mapsto Tr_1^m(cx^{2^m+1})+Tr_1^n\left(x^{(2^m-1)s'+1}\right)$) is a Niho bent function [10].

Theorem 1 in [3] ensures that the set of functions defined above by (1), (2) , (3) and (4) contains semi-bent functions. Our goal is to provide an efficient characterization of the semi-bentness property of the functions $f_{a_r,b,c}$ $f'_{a_r,b}$, $\tilde{f}_{a_r,b',c}$ and $\tilde{f}'_{a_r,b'}$. The first step is to precise a necessary and sufficient condition on the coefficients for a function of the previous form to be semi-bent. In the following, we exhibit thanks to Proposition 3 a criterion of semi-bentness in terms of exponential sums involving Dickson polynomials for functions in the form (1) and (2).

Theorem 5. *Let $n=2m$ with m odd. Let $b\in\mathbb{F}_4^\star$, β be a primitive element of $\mathbb{F}_4$ and $c\in\mathbb{F}_{2^m}^\star$. Let $f_{a_r,b,c}$ (resp. $f'_{a_r,b}$) be the function defined on $\mathbb{F}_{2^n}$ whose expression is of the form (1) (resp. form (2)). Let h_{a_r} be the related function defined on $\mathbb{F}_{2^m}$ by $h_{a_r}(x)=\sum_{r\in R} Tr_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Then*

1. *$f_{a_r,\beta,c}$ (resp. $f'_{a_r,\beta}$) is semi-bent if and only if, $f_{a_r,\beta^2,c}$ (resp. f'_{a_r,β^2}) is semi-bent, if and only if,*

$$\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(Tr_1^m(x^{-1})+h_{a_r}(D_3(x))\Big) = 2^m - 2wt(h_{a_r}\circ D_3)+4.$$

2. *$f_{a_r,1,c}$ (resp. $f'_{a_r,1}$) is semi-bent if and only if,*

$$\begin{aligned}&3\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(Tr_1^m(x^{-1})+h_{a_r}(x)\Big) - 2\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(Tr_1^m(x^{-1})+h_{a_r}(D_3(x))\Big)\\ &= 4+2^m+4wt(h_{a_r}\circ D_3)-6wt(h_{a_r}).\end{aligned}$$

Remark 1. *Note that one can prove that for every positive integer d such that d is co-prime with $\frac{2^m+1}{3}$, the function defined on $\mathbb{F}_{2^n}$ by $x \mapsto \sum_{r\in R} Tr_1^n(a_r x^{d r(2^m-1)}) + Tr_1^2(\beta x^{\frac{2^n-1}{3}}) + Tr_1^m(c x^{2^m+1})$ is also semi-bent if and only if the condition 1 of Theorem 5 holds.*

In the following, we exhibit thanks to Theorem 4 a criterion of semi-bentness in terms of exponential sums involving Dickson polynomials for functions in the form (3) and (4).

Theorem 6. *Suppose $m := \frac{n}{2} \equiv 2 \pmod 4$. Let $R \subseteq E$ where E is a set of representatives of the cyclotomic classes modulo 2^n-1 for which each class has the full size n. For $b' \in \mathbb{F}_{16}^\star$ and $a_r \in \mathbb{F}_{2^m}^\star$, we denote by $g_{a_r,b'}$ the function defined on $\mathbb{F}_{2^n}$ by $\sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^4(b' x^{\frac{2^n-1}{5}})$, and by h_{a_r} the function defined on $\mathbb{F}_{2^m}$ by $\sum_{r\in R} Tr_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Then,*

1. *If Let b' a primitive element of $\mathbb{F}_{16}$ such that $Tr_1^4(b') = 0$ then, $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) is semi-bent if and only if,*

$$\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(D_5(x))\Big) = 2$$

2. *If $b' = 1$ then, $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) is semi-bent if and only if*

$$2 \sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(D_5(x))\Big) - 5 \sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(x)\Big) = 4.$$

3. *Assume $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$. If $b' \in \{\beta, \beta^2, \beta^3\beta^4\}$ where β is a primitive 5-th root of unity in $\mathbb{F}_{16}$ then, $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) is semi-bent if and only if,*

$$\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(D_5(x))\Big) + 5 \sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(x)\Big) = -8.$$

4. *Assume $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$. If b' is a primitive element of $\mathbb{F}_{16}$ such that $Tr_1^4(b') = 1$ then, $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) is semi-bent if and only if,*

$$3 \sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(D_5(x))\Big) - 5 \sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(x)\Big) = -4.$$

5. *Assume $a_r \in \mathbb{F}_{2^{\frac{m}{2}}}$. If $b' \in \{\beta+\beta^2, \beta+\beta^3, \beta^2+\beta^4, \beta^3+\beta^4, \beta+\beta^4, \beta^2+\beta^3\}$ where β is a primitive 5-th root of unity in $\mathbb{F}_{16}$ then, $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) is semi-bent if and only if,*

$$\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(h_{a_r}(D_5(x))\Big) = 2.$$

Remark 2. *Let β be a primitive element of $\mathbb{F}_{16}$ such that $Tr_1^4(\beta) = 0$ and $c \in \mathbb{F}_{2^m}^\star$. Note that for every positive integer d such that d is co-prime with $\frac{2^m+1}{5}$, the function defined on $\mathbb{F}_{2^n}$ by $x \mapsto \sum_{r\in R} Tr_1^n(a_r x^{d r(2^m-1)}) + Tr_1^4(\beta x^{\frac{2^n-1}{5}}) + Tr_1^m(c x^{2^m+1})$ is also semi-bent if and only if the condition 1 of Theorem 6 holds, according to Proposition 3.17 [39].*

5 Efficient Characterizations of semi-bent functions with multiple trace terms by means of cardinalities of hyperelliptic curves

Theorem 5 and Theorem 6 provide a test of semi-bentness for the functions $f_{a_r,b,c}$ (resp. $f'_{a_r,b}$) of the form (1) (resp. form (2) and for functions $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) of the form (3) (resp. form (4) with exponential complexity. Indeed, suppose R is fixed and m is variable then, for any given sequences of coefficients $a_r \in \mathbb{F}_{2^m}^\star$ (where $r \in R$), checking whether the conditions 1. and 2. of Theorem 5 and Theorem 6 are satisfied require time that is exponential in m (hence it also exponential in n). The aim of this section is to exhibit an efficient characterization of the semi-bentness of such functions. In the following, we shall use the hyperelliptic curve formalism to reduce computational complexity. We will show that semi-bent functions $f_{a_r,b,c}$, $f'_{a_r,b}$, $\tilde{f}_{a_r,b',c}$ and $\tilde{f}'_{a_r,b'}$ can be described in terms of cardinalities of some hyperelliptic curves. To this end, we need some background on hyperelliptic curves as well as results about point counting on such curves over finite fields of characteristic 2.

5.1 Point counting on algebraic curves

In this subsection we give basic definitions for elliptic and hyperelliptic curves as well as results about point counting on such curves over finite fields of characteristic 2. Given a curve E defined on $\mathbb{F}_{2^m}$, $\#E$ means the number of points on it with coordinates in the given finite field $\mathbb{F}_{2^m}$. The main fact about such curves we will use in the next section is that there exist algorithms to compute their cardinalities in polynomial time and space in m.

Classical treatment of the theory of elliptic curves can be found for example in [35, 20]. A more cryptographic oriented point of view, and especially special treatment for even characteristic, can be found for example in [1, 8, 13] An elliptic curve can be defined as follows.

Definition 7. *An elliptic curve E is a smooth projective algebraic curve of genus one with a rational point O_E.*

In more down-to-earth terms, such a curve can be described by a Weierstrass equation of the form:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ ,$$

giving its affine part. There is an additional point at infinity O_E which can be seen as the only non-affine solution to the homogenized equation.

There are many different algorithms to compute the cardinality of elliptic curves. The main result we need has been given by Harley [16]. A complete description of many existing algorithms can be found in Vercauteren's thesis [37] or in [38, 23].

Theorem 8 ([16])**.** *([37]) Let E be an elliptic curve defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the cardinality of E in $O(n^2(\log n)^2 \log\log n)$ time and $O(n^2)$ space.*

The theory of hyperelliptic curves, with a cryptographic point of view, can be found for example in [28, 14, 8, 13]. We can define rather generally an hyperelliptic curve as follows.

Definition 9. *An hyperelliptic curve H is a smooth projective algebraic curve which is a degree 2 covering of the projective line.*

This definition includes the elliptic curves, but it is sometimes understood that an hyperelliptic curve should be of genus $g \geq 2$.

A description of the different types of hyperelliptic curves in even characteristic can be found in [11]. For the cryptographic point of view, the curves are often chosen to be imaginary hyperelliptic curves. This is also the kind of curves we will encounter. Such an hyperelliptic curve of genus g can be described by an affine part given by the following equation:

$$H : y^2 + h(x)y = f(x),$$

where $h(x)$ is of degree $\leq g$ and $f(x)$ is monic of degree $2g + 1$.

The main result about point counting of hyperelliptic curves we use is given by Vercauteren [37].

Theorem 10. *(Theorem 4.4.1 page 135, [37]) Let H be an hyperelliptic curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the cardinality of H in*

$$O(g^3m^3(g^2 + \log^2 m \log\log m) \log gm \log\log gm)$$

bit operations and $O(g^4m^3)$ memory.

A stronger result in terms of spaces is also given for hyperelliptic curves of a special form.

Definition 11. *An Artin-Schreier curve is an hyperelliptic curve whose affine part is given by an equation of the form:*

$$H : y^2 + x^n y = f(x),$$

where $0 \leq n \leq g$ and $f(x)$ is monic of degree $2g + 1$.

Theorem 12. *(Theorem 4.3.1 page 114, [37]) Let H be an Artin-Schreier curve of genus g defined over $\mathbb{F}_{2^m}$. There exists an algorithm to compute the cardinality of H in*

$$O(g^3m^3(g^2 + \log^2 m \log\log m) \log gm \log\log gm)$$

bit operations and $O(g^3m^3)$ memory.

5.2 Efficient criteria of semi-bentness

In the following, we shall use the hyperelliptic curve formalism to reduce computational complexity. The characterizations of semi-bentness given by Theorem 5 can be reformulated in terms of cardinality of hyperelliptic curves.

Theorem 13. *The notations are as in Theorem 5. Moreover, let ${H_{a_r}}^{(1)}$, ${H_{a_r}}^{(2)}$ and ${H_{a_r}}^{(3)}$ be the (affine) curves defined over $\mathbb{F}_{2^m}$ by*

$$\begin{aligned}
{H_{a_r}}^{(1)} &: y^2 + y = \sum_{r\in R} a_r D_r(x),\\
{H_{a_r}}^{(2)} &: y^2 + y = \sum_{r\in R} a_r D_r(x + x^3).\\
{H_{a_r}}^{(3)} &: y^2 + xy = x + x^2 \sum_{r\in R} a_r D_r(x),
\end{aligned}$$

a) If β is a primitive element of $\mathbb{F}_4$, then $f_{a_r,\beta,c}$ (resp. $f'_{a_r,\beta}$) is semi-bent if and only if

$$2\#{H_{a_r}}^{(2)} - \left(\#{H_{a_r}}^{(1)} + \#{H_{a_r}}^{(3)}\right) = -3.$$

b) If $b = 1$, then $f_{a_r,1,c}$ (resp. $f'_{a_r,1}$) is semi-bent if and only if

$$4\#{H_{a_r}}^{(2)} - 5\#{H_{a_r}}^{(1)} + \#{H_{a_r}}^{(3)} = 3.$$

The previous theorem provides a test polynomial in m of semi-bentness. Indeed, all the curves considered in Theorem 13 are also Artin-Schreier curves. So for a fixed subset of indices R, we get a test polynomial in m. However the complexity of the point counting algorithms depends on the genera of the curves, and so on the degrees of the polynomials involved to define them. Denoting by r_{max} the maximal index as above, the genus of ${H_{a_r}}^{(2)}$ is $(3r_{max}-1)/2$, so approximately three times that of the curve ${H_{a_r}}^{(1)}$. Therefore we have to compute the cardinalities of three curves of genera $(3r_{max}-1)/2$, $(r_{max}+1)/2$ and $(r_{max}-1)/2$.

The characterizations of semi-bentness given by Theorem 6 can also be reformulated in terms of cardinality of hyperelliptic curves.

Theorem 14. *The notations are as in Theorem 6. Moreover, let ${H_{a_r}}^{(1)}$, ${H_{a_r}}^{(3)}$, $\tilde{H}_{a_r}^{(2)}$ and $\tilde{H}_{a_r}^{(3)}$ be the (affine) curves defined over $\mathbb{F}_{2^m}$ by*

$$\begin{aligned}
{H_{a_r}}^{(1)} &: y^2+y=\sum_{r\in R} a_r D_r(x),\\
{H_{a_r}}^{(3)} &: y^2+xy=x+x^2\sum_{r\in R} a_r D_r(x),\\
\tilde{H}_{a_r}^{(2)} &: y^2+y=\sum_{r\in R} a_r D_r(x+x^3+x^5),\\
\tilde{H}_{a_r}^{(3)} &: y^2+xy=x+x^2\sum_{r\in R} a_r D_r(x+x^3+x^5).
\end{aligned}$$

1. *If Let b' a primitive element of $\mathbb{F}_{16}$ such that $Tr_1^4(b')=0$ then, $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) is semi-bent if and only if,*
$$\#\tilde{H}_{a_r}^{(2)}-\#\tilde{H}_{a_r}^{(3)}=5.$$
2. *If $b'=1$ then, $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) is semi-bent if and only if*
$$2(\#\tilde{H}_{a_r}^{(2)}-\#\tilde{H}_{a_r}^{(3)})-5(\#{H_{a_r}}^{(1)}-\#{H_{a_r}}^{(3)})=5.$$
3. *Assume $a_r\in\mathbb{F}_{2^{\frac{m}{2}}}$. If $b'\in\{\beta,\beta^2,\beta^3\beta^4\}$ where β is a primitive 5-th root of unity in $\mathbb{F}_{16}$ then, $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) is semi-bent if and only if,*
$$\#\tilde{H}_{a_r}^{(2)}-\#\tilde{H}_{a_r}^{(3)}+5(\#{H_{a_r}}^{(1)}-\#{H_{a_r}}^{(3)})=-10.$$
4. *Assume $a_r\in\mathbb{F}_{2^{\frac{m}{2}}}$. If b' is a primitive element of $\mathbb{F}_{16}$ such that $Tr_1^4(b')=1$ then, $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) if and only if,*
$$3\Big(\#\tilde{H}_{a_r}^{(2)}-\#\tilde{H}_{a_r}^{(3)}\Big)+5\Big(\#{H_{a_r}}^{(3)}-\#{H_{a_r}}^{(1)}\Big)=-10.$$
5. *Assume $a_r\in\mathbb{F}_{2^{\frac{m}{2}}}$. If $b'\in\{\beta+\beta^2,\beta+\beta^3,\beta^2+\beta^4,\beta^3+\beta^4,\beta+\beta^4,\beta^2+\beta^3\}$ where β is a primitive 5-th root of unity in $\mathbb{F}_{16}$ then, $\tilde{f}_{a_r,b',c}$ (resp. $\tilde{f}'_{a_r,b'}$) is semi-bent if and only if,*
$$\#\tilde{H}_{a_r}^{(2)}-\#\tilde{H}_{a_r}^{(3)}=5.$$

For a fixed subset of indices R and given a sequence of coefficients a_r, checking the necessary and sufficient conditions given by Theorem 14 requere a time that is polynomial in m. The previous theorem provides then a test polynomial in m of semi-bentness. However the complexity of the point counting algorithms depends on the genera of the curves. Denoting by r_{max} the maximal index as above, the genus of $\tilde{H}_{a_r}^{(2)}$ is $(5r_{max}-1)/2$, the genus of $\tilde{H}_{a_r}^{(3)}$ is $(5r_{max}+1)/2$, the genus of ${H_{a_r}}^{(1)}$ is $(r_{max}-1)/2$ and the genus of ${H_{a_r}}^{(3)}$ is $(r_{max}+1)/2$. Therefore we have to compute the cardinalities of four curves of genera $(5r_{max}-1)/2$, $(5r_{max}+1)/2$, $(r_{max}-1)/2$ and $(r_{max}+1)/2$.

Remark 3. *Note that Theorem 14 gives naturally an efficient characterization of the family of the hyperbent functions studied very recently by Wang et al [39].*

Acknowledgement. The author thanks Jean-Pierre Flori for his interesting discussion and for the state of the art of points counting on algebraic curves.

References

[1] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original.

[2] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine. On cryptographic properties of the cosets of R(1,m). In *IEEE Transactions on Information Theory, vol. 47*, pages 1494–1513, 2001.

[3] C. Carlet and S. Mesnager. A note on Semi-bent Boolean functions. In *Cryptology ePrint Archive, Report no 486. http://eprint.iacr.org/2010/486.*

[4] P. Charpin, E. Pasalic, and C. Tavernier. On bent and semi-bent quadratic Boolean functions. In *IEEE Transactions on Information Theory, vol. 51, no. 12*, pages 4286–4298, 2005.

[5] S. Chee, S. Lee, and K. Kim. Semi-bent Functions. In *Advances in Cryptology-ASIACRYPT94. Proc. 4th Int. Conf. on the Theory and Applications of Cryptology, Wollongong, Australia. Pieprzyk, J. and Safavi-Naini, R., Eds., Lect. Notes Comp. Sci, vol 917*, pages 107–118, 1994.

[6] J. H. Cheon and S. Chee. Elliptic curves and resilient functions. In *Lecture Notes in Computer Science, vol 2015*, pages 386–397, 2000.

[7] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein. Covering codes. In *North Holland*, 1997.

[8] H. Cohen, G. Frey, and R. Avanzi. *Handbook of elliptic and hyperelliptic curve cryptography.* Discrete mathematics and its applications. Chapman & Hall/CRC, 2006.

[9] H. Dobbertin and G. Leander. Cryptographer Toolkit for Construction of 8-Bit Bent Functions. In *Cryptology ePrint Archive, Report no. 2005/089. Available at http://eprint.iacr.org/2005/089*, 2005.

[10] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit. Construction of bent functions via Niho Power Functions. In *Journal of Combinatorial therory, Serie A 113*, pages 779–798, 2006.

[11] A. Enge. How to distinguish hyperelliptic curves in even characteristic. In *Public-Key Cryptography and Computational Number Theory*, de Gruyter Proceedings in Mathematics. DE GRUYTER, July 2011.

[12] J.P. Flori and S. Mesnager. An efficient characterization of a family of hyperbent functions with multiple trace terms. In *Cryptology ePrint Archive, Report 2011/373, 2011. http://eprint.iacr.org/.*

[13] S. Galbraith. *Mathematics of Public Key Cryptography.* 2011. `http://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html`.

[14] P. Gaudry. Hyperelliptic curves and the HCDLP. In *Advances in elliptic curve cryptography*, volume 317 of *London Math. Soc. Lecture Note Ser.*, pages 133–150. Cambridge Univ. Press, Cambridge, 2005.

[15] R. Gold. Maximal recursive sequences with 3-valued recursive crosscorrelation functions. In *IEEE Transactions on Information Theory 14 (1)*, pages 154–156, 1968.

[16] R. Harley. Asymptotically optimal p-adic point-counting. Email to NMBRTHRY list, December 2002. `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0212&L=nmbrthry&T=0&P=1343`.

[17] T. Helleseth. Some results about the cross-correlation function between two maximal linear sequences. In *Discr. Math, vol. 16*, pages 209–232, 1976.

[18] T. Helleseth. Correlation of m-sequences and related topics. In *Proc. SETA8, Discrete Mathematics and Theoretical Computer Science, C. Ding, T. Helleseth, and H. Niederreiter, Eds. London, U.K.: Springer*, pages 49–66, 1999.

[19] T. Helleseth and P. V. Kumar. Sequences with low correlation. In *Handbook of Coding Theory, Part 3: Applications, V. S. Pless, W. C. Huffman, and R. A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier, chapter. 21*, pages 1765–1853, 1998.

[20] D. Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.

[21] K. Khoo, G. Gong, and D. R. Stinson. A new family of Gold-like sequences. In *IEEE Trans. Inform. Theory Lausanne, Switzerland*, page 181, 2002.

[22] K. Khoo, G. Gong, and D. R. Stinson. A new characterization of semibent and bent functions on finite fields. In *Des. Codes. Cryptogr. vol. 38, no. 2*, pages 279–295, 2006.

[23] R. Lercier, D. Lubicz, and F. Vercauteren. Point counting on elliptic and hyperelliptic curves. In *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl. (Boca Raton), pages 407–453. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[24] R. Lidl, G. L. Mullen, and G. Turnwald. Dickson Polynomials. In *ser.Pitman Monographs in Pure and Applied Mathematics. Reading, MA: Addison-Wesley, vol. 65*, 1993.

[25] P. Lisoněk. An efficient characterization of a family of hyperbent functions. *IEEE Transactions on Information Theory*, 57(9):6010–6014, 2011.

[26] M. Matsui. Linear cryptanalysis method for DES cipher. In *Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science 765*, pages 386–397, 1994.

[27] W. Meier and O. Staffelbach. Fast correlation attacks on stream ciphers. In *Advances in Cryptology, EUROCRYPT'88, Lecture Notes in Computer Science 330*, pages 301–314, 1988.

[28] A. J. Menezes, Y.H. Wu, and R. J. Zuccherato. An elementary introduction to hyperelliptic curves. In *Algebraic aspects of cryptography*, volume 3 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1998.

[29] S. Mesnager. Hyper-bent boolean functions with multiple trace terms. In M. A. Hasan and T. Helleseth, editors, *WAIFI*, volume 6087 of *Lecture Notes in Computer Science*, pages 97–113. Springer, 2010.

[30] S. Mesnager. A new class of bent and hyper-bent Boolean functions in polynomial forms. *Des. Codes Cryptography*, 59(1-3):265–279, 2011.

[31] S. Mesnager. Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials. In *IEEE Transactions on Information Theory. Vol 57, No 11*, pages 7443–7458, 2011.

[32] M.G. Parker and A. Pott. On Boolean Functions Which Are Bent and Negabent. In *Workshop on Sequences, Subsequences, and Consequences (SSC 2007), Los Angeles, USA, 2007. Revised Invited Papers, Golomb, S.W., Gong, G., Helleseth, T., and Song, H.-Y., Eds., Lect. Notes Comp. Sci.*, pages 9–23, 2007.

[33] C. Qu, J. Seberry, and J. Pieprzyk. Homogeneous Bent Functions. In *Discrete Appl. Math.102 no. 1-2*, pages 133–139, 2000.

[34] O.S. Rothaus. On "bent" functions. In *J. Combin.Theory Ser A 20*, pages 300–305, 1976.

[35] J.H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[36] G. Sun and C.Wu. Construction of Semi-Bent Boolean Functions in Even Number of Variables. In *Chinese Journal of Electronics, vol 18, No 2*, 2009.

[37] F. Vercauteren. *Computing zeta functions of curves over finite fields*. PhD thesis, Katholieke Universiteit Leuven, 2003.

[38] F. Vercauteren. Advances in point counting. In *Advances in elliptic curve cryptography*, volume 317 of *London Math. Soc. Lecture Note Ser.*, pages 103–132. Cambridge Univ. Press, Cambridge, 2005.

[39] B. Wang, C. Tang, Y. Qi, Y. Yang, and M. Xu. A New Class of Hyper-bent Boolean Functions with Multiple Trace Terms. In *Cryptology ePrint Archive, Report 2011/600, 2011. http://eprint.iacr.org/.*

[40] A. M. Youssef and G. Gong. Hyper-Bent Functions. In *Advances in Crypology, Eurocrypt'01-LNCS Springer*, pages 406–419, 2001.

[41] Y. Zheng and X. M. Zhang. Plateaued functions. In *Advances in Cryptology-ICICS 1999, vol 1726 Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag*, pages 284–300, 1999.