More Differentially 6-uniform Power Functions

Céline Blondeau and Léo Perrin
celine.blondeau@aalto.fi
perrin.leo@gmail.com

Aalto University,
Department of Information and Computer Science

Paper presented at WCC 2013, including some corrections.

Abstract. We provide the differential spectra of differentially 6-uniform functions among the family of power functions $x \mapsto x^{2^t-1}$ defined in $\mathbb{F}_{2^n}$. We show that the functions $x \mapsto x^{2^t-1}$ when $t = \frac{n-1}{2}$, $\frac{n+3}{2}$ with odd n and when $t = \frac{kn+1}{3}, \frac{(3-k)n+2}{3}$ with $kn \equiv 2 \mod 3$ have differential spectra similar to the one of the function $x \mapsto x^7$ which belongs to the same family. To provide the differential spectra for these functions, a recent result of Helleseth and Kholosha regarding the number of roots of polynomials of the form $x^{2^t+1} + x + a$ is used. A discussion regarding the non-linearity and the algebraic degree of this family of exponents is provided.
Keywords: Differential uniformity, Differential spectrum, Kloosterman sum, Power function, Roots of trinomial, $x \mapsto x^{2^t-1}$, Dickson polynomial.

1 Introduction

Differential cryptanalysis is the first statistical attack proposed for breaking iterated block ciphers. Its publication [BS91] then gave rise to numerous works which investigated the security offered by different types of functions regarding differential attacks. This security is quantified by the so-called *differential uniformity* of the Substitution box used in the cipher [NK93]. Most notably, finding appropriate S-boxes which guarantee that the cipher using them resists differential attacks has been a major topic for the last twenty years.

Power functions, *i.e.*, monomial functions, form a class of suitable candidates since they usually have a lower implementation cost in hardware. Also, their particular algebraic structure makes the determination of their differential properties easier. However, there are only few power functions with proved low differential uniformity. Up to equivalence, there are two large families of such functions: a subclass of the quadratic power functions (a.k.a. Gold functions) and a subclass of the so-called Kasami functions. Both of these families contain some permutations which are APN over $\mathbb{F}_{2^n}$ for odd n and differentially 4-uniform for even n. The other known power functions with a low differential uniformity correspond to "sporadic" cases in the sense that the corresponding exponents vary with n [HM11] and they do not belong to a large class: they correspond to the exponents defined by Welch [Dob99b,CCD00], by Niho [Dob99a,HX01],

by Dobbertin [Dob00], by Bracken and Leander [BL10], and to the inverse function [Nyb93].

If the conjecture of [BCC10] concerning the list of monomials differentially 4-uniform is true, we can consider that the differential spectrum of all power functions differentially 4-uniform have been provided in the past. For some cryptographic applications, using a differentially 6-uniform power function instead of a differentially 2- or 4-uniform does not drastically reduce the security of the cipher. Power functions differentially 6-uniform can then present some cryptographic interest in particular if non-linear and algebraic properties are also relatively good for cryptographic applications.

Simulations of [BCC11] show that, for $17 \leq n \leq 31$, all power functions differentially 6-uniform belong to the family $G_t(x) = x^{2^t-1}$. In [BCC11], properties of the differential spectra of such functions were investigated. In particular, it was shown that the differential spectrum of the power function $G_t(x) = x^{2^t-1}$ and the one of the power function $G_s(x)$ with $s = n - t + 1$ are related to each other. In the same paper, the differential spectrum of the power functions $x \mapsto x^7$ and $x \mapsto x^{2^{n-2}-1}$ on the field $\mathbb{F}_{2^n}$ is extracted.

In this paper, we give explicit formulas for the differential spectrum of G_t when n is odd and $t = \frac{n-1}{2}$, $\frac{n+3}{2}$, or when $kn \equiv 2 \mod 3$ ($k = 1$ or $k = 2$) and $t = \frac{kn+1}{3}$, $\frac{(3-k)n+2}{3}$. All of these functions are differentially 6-or 8-uniform. We show in particular that their differential spectrum, which can be expressed in term of the Kloostermann sum, is similar to the one of the function $G_3(x) = x^7$. While computing the differential spectrum of the function x^7, an important result of [BRS67] regarding the number of roots of the polynomial $x^3 + x + a$ was used. In this paper, as the degree of the derivative depends on t, we use a generalisation of this result published recently by Helleseth and Kholosha [HK08,HK10]. Differential spectrum provided in Theorem 3 and 5 are proofs of Conjecture 8.9 and 8.10 proposed in [Blo11]. A relation between derivative of monomials and reversed Dickson polynomials is also mentioned in this paper.

The following of this paper is organised as follows. In Section 2, definitions and results relevant to this work are recalled. While in Section 3, the functions G_t with $t = \frac{kn+1}{3}$ and $t = \frac{(3-k)n+2}{3}$ are studied, Section 4 presents the differential spectra of the functions G_t with $t = \frac{n-1}{2}$ and $\frac{n+3}{2}$. In Section 5, a discussion regarding the inverse of these functions G_t, their algebraic degree and their nonlinearity is given. Section 6 concludes this paper.

2 Preliminary

2.1 Functions over $\mathbb{F}_{2^n}$ and their derivatives

Any function F from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^n}$ can be expressed uniquely as a univariate polynomial in $\mathbb{F}_{2^n}[x]$ of degree at most $2^n - 1$. The *algebraic degree* of F, denoted by $deg(F)$, is the maximal Hamming weight of the 2-ary expansions of its exponents. In this paper, we identify a polynomial of $\mathbb{F}_{2^n}[x]$ with the corresponding function over $\mathbb{F}_{2^n}$.

In the following, we denote by **Tr** the *absolute trace* on $\mathbb{F}_{2^n}$, *i.e.,*

$$\mathbf{Tr}(\beta) = \beta + \beta^2 + \cdots + \beta^{2^{n-1}}, \ \beta \in \mathbb{F}_{2^n}.$$

In the whole paper, $\#E$ is the cardinality of any set E. To simplify the notation, we also denote by $\mathcal{F}$ the set $\mathbb{F}_{2^n} \backslash \{0, 1\}$.

The resistance of a cipher to differential attacks and to its variants is quantified by some properties of the *derivatives* of its S(ubstitution)-box, in the sense of the following definition.

Definition 1. *Let F be a function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^m}$. For any $a \in \mathbb{F}_{2^n}$, the* derivative of F with respect to a *is the function D_aF from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^m}$ defined by*

$$D_aF(x) = F(x + a) + F(x), \ \ \forall x \in \mathbb{F}_{2^n}.$$

The resistance to differential cryptanalysis is related to the following quantities, introduced by Nyberg and Knudsen [NK93,Nyb93].

Definition 2. *Let F be a function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^n}$. For any a and b in $\mathbb{F}_{2^n}$, we denote*

$$\delta(a, b) = \#\{x \in \mathbb{F}_{2^n}, \ D_aF(x) = b\}.$$

The differential uniformity *of F is $\delta(F) = \max_{a \neq 0, \ b \in \mathbb{F}_{2^n}} \delta(a, b)$. Functions for which $\delta(F) = 2$ are said to be* almost perfect non-linear (APN).

In this paper, we focus on the case where the S-box is a power function, *i.e.,* a monomial function on $\mathbb{F}_{2^n}$. In other words, $F(x) = x^d$ over $\mathbb{F}_{2^n}$. In the case of such a power function, the differential properties can be analysed more easily since, for all $a \neq 0$, $\delta(a, b) = \delta(1, b/a^d)$. Then, when $F : x \mapsto x^d$ is a monomial function, the differential characteristics of F are determined by the values $\delta(b) = \delta(1, b)$, $b \in \mathbb{F}_{2^n}$. The *differential spectrum* of F can be defined as follows.

Definition 3. *Let $F(x) = x^d$ be a power function on $\mathbb{F}_{2^n}$. We denote by ω_i the number of output differences b that occur i times:*

$$\omega_i = \#\{b \in \mathbb{F}_{2^n} \mid \delta(b) = i\}.$$

The differential spectrum of F_d is the set of the ω_i: $\mathbb{S} = \{\omega_0, \omega_2, ..., \omega_{\delta(F)}\}$.

Obviously, the differential spectrum satisfies

$$\sum_{i=0}^{\delta(F)} \omega_i = 2^n \ \text{ and } \ \sum_{i=2}^{\delta(F)} (i \times \omega_i) = 2^n, \tag{1}$$

where $\omega_i = 0$ for odd i.

As explained in [HMAL09], derivatives of monomial $F_d : x \mapsto x^d$ are linked with the Dickson polynomial D_d (see [Dic96] for definition). We have $(x+1)^d + x^d = D_d(1, x^2+x)$. In the following we denote by RD_d the resulting one variable polynomial $RD_d(x) = D_d(1, x)$.

As $b = 0$ and $b = 1$ correspond to the cyclotomic classes of order one, they are often particular cases. In the following we say that a function F is *locally differentially λ-uniform* if $\delta(b) \leq \lambda$ for $b \neq 0, 1$. We define the *restricted differential spectrum* as the sequence of values $\omega'_i = \#\{b \neq 0, 1 \mid \delta(b) = i\}$.

It is well-known that some basic transformations preserve $\mathbb{S}$. In particular, if F is a permutation, its inverse has the same differential spectrum as F.

2.2 General properties of $x \mapsto x^{2^t-1}$

In [BCC11], different properties of the differential spectra of the functions $G_t(x) = x^{2^t-1}$, defined in the field $\mathbb{F}_{2^n}$, were investigated. In particular it was shown that the quantities $\delta(b)$ can be computed as follows:

$$\delta(0) = 2^{\gcd(t,n)} - 2, \ \delta(1) = 2^{\gcd(t-1,n)}, \text{ and } \forall b \neq 0, 1 \ \ \delta(b) = N_b - 2, \tag{2}$$

were N_b is the number of roots of the linear polynomial $P_b(x) = x^{2^t} + bx^2 + (b+1)x$ over $\mathbb{F}_{2^n}$. The problem of determining the restricted differential spectrum of the function G_t is then equivalent to the problem of finding the number of roots of the linear polynomial P_b for $b \in \mathcal{F}$. In particular $\omega'_i \neq 0$ if and only if $i = 2^r - 2$ for some r. As 0 and 1 are simple roots of this polynomial, by setting $y = x^2 + x$, we obtain that N_b, $b \in \mathcal{F}$, is equal to twice the number of roots of the following system (see Theorem 3 of [BCC11]) in $\mathbb{F}_{2^n}^*$:

$$E_b : \ \begin{cases} Q(y) &= by \\ \mathbf{Tr}(y) &= 0 \end{cases}, \ Q(y) = \sum_{i=0}^{t-1} y^{2^i}. \tag{3}$$

In [Göl12], the reversed Dickson polynomials when $d = 2^t - 1$ are studied. Assuming $y \neq 0$, we notice that $RD_{2^t-1}(y) = Q(y)/y$.

In [BCC11], it is shown that the restricted differential spectrum of the functions G_t and G_s with $s = n - t + 1$ are equal. Only the values $\delta(0)$ and $\delta(1)$ can differ and are defined by (2). The function G_s is called the *symmetric* of G_t.

When n and t are co-prime, the function G_t is a permutation. In Theorem 7 of [KS12], the inverse of the exponent $2^t - 1$ is extracted. In the following, when G_t is invertible, we denote by τ the inverse of $2^t - 1 \mod 2^n - 1$:

$$\tau = \sum_{i=0}^{t^{-1}-1 \mod n} 2^{ti} \mod 2^n - 1. \tag{4}$$

In [BCC11], a complete definition of the differential spectrum of the function $G_3(x) = x^7$ is provided. As this function is differentially 6-uniform, and the value of ω_4 is determined only by $\delta(1)$, the complete differential spectrum can be derived from ω_6. Using (1), we have $\omega_2 = 2^{n-1} - 3\omega_6 - 2\omega_4$ and $\omega_0 = 2^{n-1} + 2\omega_6 + \omega_4$. In Theorem 5 of [BCC11], it is shown that:

$$\text{if } n \text{ is odd, } \omega_6 = \frac{2^{n-2}+1}{6} - \frac{K(1)}{8}, \omega_4 = 0,$$
$$\text{if } n \text{ is even, } \omega_6 = \frac{2^{n-2}-4}{6} + \frac{K(1)}{8}, \omega_4 = 1,$$

where $K(1)$ is the Kloosterman sum defined by

$$K(1) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(x^{-1}+x)}, \tag{5}$$

with the convention that $(-1)^{\mathbf{Tr}(x^{-1})} = 1$ for $x = 0$. To express the differential spectrum of the function x^7, a result from [Car79] which gives the number of roots of the polynomial x^3+x+a, was used. In this paper, results are derived using a generalisation of [HK08] concerning the number of roots of the polynomial $\mathcal{L}_a(x) = x^{2^t+1} + x + a$ in $\mathbb{F}_{2^n}$.

Theorem 1. *(Theorem 1 of [HK08]) Let t be a positive integer such that $t \leq n$ and $\gcd(t, n) = 1$. For any $a \in \mathbb{F}_{2^n}^*$, the polynomial $\mathcal{L}_a(x) = x^{2^t+1} + x + a$ has either none, one or three roots in $\mathbb{F}_{2^n}$. Further $\mathcal{L}_a$ has exactly one zero in $\mathbb{F}_{2^n}$, namely x_0, if and only if $\mathbf{Tr}\left((1 + x_0^{-1})^\tau\right) = 1$. Let $M_i = \#\{a \in \mathbb{F}_{2^n}^* \mid \mathcal{L}_a \text{ has } i \text{ roots}\}$.*

$$\text{For } n \text{ odd}, \quad M_0 = \frac{2^n+1}{3}, M_1 = 2^{n-1} - 1, M_3 = \frac{2^{n-1}-1}{3}.$$
$$\text{For } n \text{ even}, \quad M_0 = \frac{2^n-1}{3}, M_1 = 2^{n-1}, \qquad M_3 = \frac{2^{n-1}-2}{3}.$$

3 Functions $x \mapsto x^{2^t-1}$ when $t = (kn + 1)/3$

In this section, we focus on field $\mathbb{F}_{2^n}$ where n is not a multiple of 3. We define $k = 1, 2$ such that $kn \equiv 2 \bmod 3$. We are interested in the computation of the differential spectra of the functions G_t and G_s with t and s as follows:

$$t = \frac{kn+1}{3}, \quad s = \frac{(3-k)n+2}{3}.$$

Notice that k is chosen such that t and s are integer values. For this value of t, the function G_t is a permutation (which is not always the case of the function G_s). The inverse of $2^t - 1$ modulo $2^n - 1$, which we denote by τ, can be computed easily from (4) as $\tau = 1 + 2^t + 2^{2t}$.

To derive the differential spectrum of these functions, we provide a different formulation of (3). The following result will be used when rewriting the system.

Lemma 1. *If $n \not\equiv 0 \mod 3$, then $L_1(x) = x + x^{2^t} + x^{2^{2t}}$ has only one root $x = 0$.*

Proof. This lemma is a direct consequence of Proposition 2 of [HK10]. This polynomial has only one root zero if and only if $\mathcal{L}_1(z) = z^{2^t+1}+z+1$ ($z = x^{2^t-1}$) is irreducible. Using the same notation as in the original paper, we notice that if $n \not\equiv 0 \mod 3$, we have $C_n(1) = 1$ and $Z_n(1) = 1$. As $\gcd(t, n) = 1$, $\mathcal{L}_1$ is irreducible. □

Theorem 2. *Let $\beta = 1 + b^{-1}$. For $b \neq 1$ (if $b = 0$ then $\beta = 1$), the number of solutions of $G_t(x) + G_t(x+1) = b$ is equal to twice the number of solutions of this system:*

$$\begin{cases} \mathcal{L}_\beta(v) = v^{2^t+1} + v + \beta &= 0, \\ \mathbf{Tr}(v^\tau) &= 0. \end{cases} \tag{6}$$

Proof. For the sake of simplification, we present the proof for $b \neq 0$. Let $Q(y)$ be the polynomial of (3). Summing $Q(y)^{2^{it}}$ for $i = 0, 1, 2$ gives:

$$Q(y) + Q(y)^{2^t} + Q(y)^{2^{2t}} = \sum_{i=0}^{kn} y^{2^i} = k \times \mathbf{Tr}(y) + y^{2^{kn}} = y.$$

From Lemma 1, $\sum_{i=0}^{2}(Q(y) + (by))^{2^{it}} = 0$ if and only if $Q(y) + by = 0$. Thus, (3) has the same number of solutions as:

$$(1+b)y + (by)^{2^t} + (by)^{2^{2t}} = 0 \text{ and } \mathbf{Tr}(y) = 0. \tag{7}$$

Using the substitution $z = by$, the equation $(1+b)y + (by)^{2^t} + (by)^{2^{2t}} = 0$ of (7) is equivalent to $L_\beta(z) = 0$ where $\beta = 1 + b^{-1}$ and $L_\beta(z) = z^{2^{2t}} + z^{2^t} + \beta z$. The linear polynomial L_β can be decomposed as

$$L_\beta(z) = z \cdot \left(z^{(2^t-1)(2^t+1)} + z^{2^t-1} + \beta\right) = z \cdot \mathcal{L}_\beta(z^{2^t-1}),$$

where $\mathcal{L}_\beta(x) = x^{2^t+1} + x + \beta$. Thus, $L_\beta(z) = 0$ and $z \neq 0, 1$ is equivalent to $\mathcal{L}_\beta(z^{2^t-1}) = 0$. Furthermore, if it holds that $L_\beta(z) = 0$ we have $z^{2^{2t}} + z^{2^t} + z + y = 0$. Thus, $\mathbf{Tr}(z) = \mathbf{Tr}(y)$ so the trace condition of (7) is equivalent to $\mathbf{Tr}(z) = 0$. If we let $v = z^{2^t-1}$, as we remove the trivial solution $y = 0$, (7) has exactly one more root than (6) meaning the same number of solutions as $G_t(x) + G_t(x+1) + b = 0$. □

Using this theorem, we derive the differential spectrum of the function G_t.

Theorem 3. *Let $G_t \in \mathbb{F}_{2^n}[x]$, with $t = \frac{kn+1}{3}$ and $k = 1$ or 2 depending of n. The function G_t is differentially 6-uniform. Let $K(1)$ as defined in (5), its differential spectrum $\{\omega_0, \omega_2, \omega_4, \omega_6\}$ is determined as follows:*

$$\begin{aligned} &\text{if } n \equiv \pm 1 \bmod 6, \quad \omega_6 = \frac{2^{n-2}+1}{6} - \frac{K(1)}{8}, \quad \omega_4 = 0, \\ &\text{if } n \equiv \pm 2 \bmod 6, \quad \omega_6 = \frac{2^{n-2}-4}{6} + \frac{K(1)}{8}, \quad \omega_4 = 1. \end{aligned}$$

In both cases, $\omega_2 = 2^{n-1} - 3\omega_6 - 2\omega_4$ and $\omega_0 = 2^{n-1} + 2\omega_6 + \omega_4$.

Proof. We first compute the value of $\delta(0)$ and $\delta(1)$ separately. As G_t is a permutation we have $\delta(0) = 0$. The value of $\delta(1)$ depends on the value of n modulo 6: if $n \equiv \pm 2 \mod 6$, $\delta(1) = 4$ and $\omega_4 = 1$, if $n \equiv \pm 1 \mod 6$, $\delta(1) = 2$ and $\omega_4 = 0$.

According to Theorem 2, the differential spectrum of G_t can be computed by studying the number of roots of (6). According to Theorem 1, as $\gcd(t,n)=1$, $\mathcal{L}_\beta$ can only have $0,1$ or 3 roots; meaning that for $b \neq 1$, $\delta(b) = 0,2,6$. By determining the number of $\beta \in \mathbb{F}_{2^n}^*$ ($b \neq 1$) such that (6) does not have any roots, we can derive the complete differential spectrum (see. (1)). The number of b such that $G_t(x)+G_t(x+1)=b$ is irreducible is equal to the number of β such that the system has no solution and is denoted by ω_0. We notice that:

- If $\mathcal{L}_\beta$ has three roots, v_1, v_2 and v_3, since $v_1^\tau, v_2^\tau, v_3^\tau$ are roots of L_β, we have $v_1^\tau + v_2^\tau + v_3^\tau = 0$ and at least one of them is such that $\mathbf{Tr}(v_i^\tau) = 0$. Therefore if $\mathcal{L}_\beta$ has three roots, (6) has a least one solution.
- According to Theorem 1, v_0 is the unique root of some $\mathcal{L}_\beta$ if and only if $\mathbf{Tr}\big((1+v_0^{-1})^\tau\big) = 1$.

From these observations, we deduce that (6) has no solution if and only if $\mathcal{L}_\beta$ is irreducible or if $\mathcal{L}_\beta$ has one root v such that $\mathbf{Tr}(v^\tau) \neq 0$ and $\mathbf{Tr}\left((1+v_0^{-1})^\tau\right) = 1$. As M_0 corresponds to the number of β such that the system has no roots, we have:

$$\omega_0 = M_0 + \#\{v \in \mathcal{F}, \mathbf{Tr}(v^\tau) = 1, \mathbf{Tr}\big((1+v^{-1})^\tau\big) = 1\}.$$

Since $x \mapsto x^\tau$ is a permutation, using a similar method to [BCC11] by separating with regards to the parity of n, we obtain that the set on the right is of size $2^{n-2} + (-1)^n K(1)/4$.

This is not as easy as mentioned. For now we only can conjecture this result.

This allows us to conclude that

$$\omega_0 = \frac{2^n + (-1)^{n+1}}{3} + 2^{n-2} + (-1)^n \frac{K(1)}{4}.$$

The complete differential spectrum can be computed using (1). □

Using the differential spectrum of the function G_t, the differential spectrum of the symmetric function G_s, $s = \frac{(3-k)n+2}{3}$ can be derived easily (Theorem 4 of [BCC11]). Notice that in that case G_s is a permutation if and only if $n \equiv \pm 1 \mod 6$ ($\delta(0) = 0$). If $n \equiv \pm 2 \mod 6$, we have $\delta(0) = 2$. In all cases we have $\delta(1) = 2$ and the function G_s is differentially 6-uniform.

4 Functions $x \mapsto x^{2^t-1}$ when $t = (n-1)/2$

In this section, we focus on field $\mathbb{F}_{2^n}$ with odd n. Theorem 9 of [BCC11] states that the permutation $G_t(x) = x^{2^t-1}$ with $t = \frac{n-1}{2}$ is locally differentially 6-uniform. The symmetric of this function is the function G_s with $s = \frac{n+3}{2}$. In this section, we provide the complete differential spectrum of these functions. Theorem 5 shows that their differential spectrum is similar to the one of the function $G_3(x) = x^7$.

In comparison with the previous section, a direct reduction of the problem to a system similar to (6) does not lead easily to the derivation of the differential spectrum.

As $\gcd(\frac{n-1}{2}, n) = 1$, the functions $G_t : x \mapsto x^{2^t-1}$ studied in this section are permutations. As the differential spectrum of a function is equal to the differential spectrum of its inverse, we study the differential spectrum of the function $\Gamma_t : x \mapsto x^\tau$ with $\tau = -2 - 2^{t+1}$. In this section, a property of the reversed Dickson polynomial when $d = 2^{t+1} - 1$ is used to derive the differential spectrum.

Theorem 4. *Let $b \neq 1$ and let $\beta = b^{1-2^t}$. The number of roots of $\Gamma_t(x)+\Gamma_t(x+1) = b$ is equal to twice the number of roots of:*

$$\begin{cases} \mathcal{L}_\beta(v) = v^{2^{t}+1} + v + \beta = 0, \\ \mathbf{Tr}(v) = 1 + \mathbf{Tr}(\beta). \end{cases} \tag{8}$$

Proof. We denote by $\delta(b)$ the number of roots of $\Gamma_t(x) + \Gamma_t(x+1) = b$. By rewriting and simplifying the equation $(x+1)^\tau + x^\tau = b$, we obtain that the number of roots of $\Pi_c(x) = x^{2^t}+x+1+c(x^2+x)^{2^t+1}$, where $c = b^{2^{n-1}}$ is $\delta(b)+2$. By setting $y = x+x^2$, this number of roots is equal to twice the number of roots of

$$\chi_c(y) = cy^{2^t+1} + \sum_{i=0}^{t-1} y^{2^i} + 1 = 0 \text{ and } \mathbf{Tr}(y) = 0,$$

which has as many solutions as:

$$y^{-2^t}\left(\chi_c(y) + \chi_c(y)^{2^{t+1}}\right) = c^{2^{t+1}} y^{2^t+1} + cy + 1 = 0 \text{ and } \mathbf{Tr}(cy^{2^t+1}) = 1.$$

At last, if we let $v = yc^{2-2^{t+1}}$ and $\beta = c^{1-2^{t+1}} (= b^{1-2^t})$, we obtain the result. Notice that when v is a root of $\mathcal{L}_\beta$, the condition $\mathbf{Tr}(v^{2^t+1}) = 1$ can be written as $\mathbf{Tr}(v) = 1 + \mathbf{Tr}(\beta)$. □

As before, Theorem 1 gives us the number of solutions of this system if we do not take the condition over the trace into account. Before determining the differential spectrum we introduce the following lemma.

Lemma 2. *Let $\Lambda(l) = \sum_{i=1}^{t} l^{2^i-1}$ be a function of $\mathbb{F}_{2^n}$. The set of the x being the unique roots of polynomial $\mathcal{L}_\beta$ for some β is equal to the image of $\mathcal{F}_0 = \{x \in \mathcal{F} \mid \mathbf{Tr}(x) = 0\}$ by the function $l \mapsto 1/\Lambda(l)$.*

Proof. From [HK08], $\mathcal{L}_\beta$ has 0, 1 or 3 roots. Let β be such that $\mathcal{L}_\beta$ has 3 roots. We denote by x one of the roots. As $\mathcal{L}_\beta$ has 3 roots, it exists $\gamma \in \mathcal{F}$ such that $y = \gamma x$ is also a root of $\mathcal{L}_\beta$. Thus, $x^{2^t+1} + x = (\gamma \cdot x)^{2^t+1} + \gamma \cdot x$. After simplification, we obtain that $x^{2^t} = (1+\gamma)/(1+\gamma^{2^t+1})$. By setting $\gamma = \alpha^{2^{t+1}-2}$, we have $x^{2^t} = (\alpha^2 + \alpha^{2^{t+1}})/(\alpha + \alpha^2)$. By setting $l = \alpha + \alpha^2$, we obtain:

$$\mathcal{L}_\beta(x) = \mathcal{L}_\beta(y) = 0, \quad (x \neq y) \;\Leftrightarrow\; \exists l \in \mathcal{F}_0, x^{2^t} = \Lambda(l) = \sum_{i=1}^{t} l^{2^i-1}.$$

Therefore, $\{x \mid \mathcal{L}_\beta(x) = 0 \text{ and } \mathcal{L}_\beta \text{ has 3 roots}\} = \mathcal{I}m_\Lambda(\mathcal{F}_0)$. By contradiction we can prove that the inverse of $\Lambda(l)$ is never in $\mathcal{I}m_\Lambda(\mathcal{F}_0)$ for $l \in \mathcal{F}_0$ and as Λ is injective, the conclusion comes from $|\mathcal{I}m_\Lambda(\mathcal{F}_0)| = |\mathcal{I}m_{1/\Lambda}(\mathcal{F}_0)| = |\mathcal{F}_0| = |\mathcal{F}|/2$, meaning that $\mathcal{F} = \mathcal{I}m_\Lambda(\mathcal{F}_0) \dot\cup \mathcal{I}m_{1/\Lambda}(\mathcal{F}_0)$. We can conclude by noticing that $\mathcal{F} = \{x \mid \mathcal{L}_\beta(x) = 0 \text{ and } \mathcal{L}_\beta \text{ has 3 roots}\} \dot\cup \{x \mid \mathcal{L}_\beta(x) = 0 \text{ and } \mathcal{L}_\beta \text{ has 1 root}\}$. □

Using the notation of [Göl12] we remark that $\Lambda + 1$ corresponds to the reversed Dickson polynomial $RD_{2^{t+1}-1}$. The fact that Λ is an injection can be seen by observing that $x^{2^{t+1}-1}$ is APN, which implies that $RD_{2^{t+1}-1}$ is an injection on $\mathcal{F}_0$.

Theorem 5. *Let n be odd and $t = \frac{n-1}{2}$. The functions G_t and Γ_t are locally differentially 6-uniform (differentially 6 or 8-uniform depending of n). Let $K(1)$ be as defined in (5), the differential spectrum $\{\omega_0, \omega_2, \omega_4, \omega_6, \omega_8\}$ of these functions is:*

$$\text{if } n \equiv \pm 1 \bmod 6, \quad \omega_8 = 0, \quad \omega_6 = \frac{2^{n-2}+1}{6} - \frac{K(1)}{8},$$
$$\text{if } n \equiv 3 \bmod 6, \quad \omega_8 = 1, \quad \omega_6 = \frac{2^{n-2}-5}{6} - \frac{K(1)}{8}.$$

In both cases, $\omega_4 = 0$, $\omega_2 = 2^{n-1} - 3\omega_6 - 4\omega_8$ and $\omega_0 = 2^{n-1} + 2\omega_6 + 3\omega_8$.

Proof. From Theorem 9 of [BCC11] we know that these functions are differentially 6-uniform. If $n \equiv 3 \mod 6$ we have $\delta(1) = 8$ and $\omega_8 = 1$, otherwise $\delta(1) = 2$. In this theorem it is also proved that for $b \neq 1$ we have $\delta(b) \leq 6$. Like in Section 3, to determine the differential spectrum, we compute the number ω_0 of β such that (8) has no solutions. We notice that:

- If $\mathcal{L}_\beta$ has three roots v_1, v_2, v_3, we have $v_1^\tau + v_2^\tau + v_3^\tau = 0$. After some computations we deduce that $\mathbf{Tr}(v_1 + v_2 + v_3) = 1 + \mathbf{Tr}(\beta)$, and that the system has at least one solution.
- If v is the unique roots of $\mathcal{L}_\beta$, by Lemma 2 we know that $\exists l \in \mathcal{F}_0$ such that $v = 1/\Lambda(l)$. We can show that $\mathbf{Tr}(\Lambda(l)^{-1-2^t}) = 1 + \mathbf{Tr}\big((l \cdot \Lambda(l))^{-1}\big)$.

From these observations, we deduce that (8) has no root if and only if $\mathcal{L}_\beta$ is irreducible or if $\mathcal{L}_\beta$ has one root v such that $\mathbf{Tr}(v^{2^t+1}) \neq 1$. Hence, we have the following expression:

$$\omega_0 = M_0 + \#\{v \in \mathcal{F}, \exists l \in \mathcal{F}, v = 1/\Lambda(l), \mathbf{Tr}(l) = 0, \mathbf{Tr}\big((l\Lambda(l))^{-1}\big) = 1\}.$$

If $\mathbf{Tr}(l) = 0$ then $\mathbf{Tr}(l \cdot \Lambda(l)) = 0$ and $\lambda : l \mapsto l \cdot \Lambda(l)$ is a permutation of $\mathcal{F}_0$ so by setting $l' = \lambda(l)$, we have

$$\omega_0 = M_0 + \#\{l' \in \mathcal{F}, \mathbf{Tr}(l') = 0, \mathbf{Tr}(l'^{-1}) = 1\}.$$

We know from [BCC11] that the size of this set for odd n is $2^{n-2} - K(1)/4$. Thus, we know that ω_0 is such that: $\omega_0 = \dfrac{2^n+1}{3} + 2^{n-2} - \dfrac{K(1)}{4}$. The complete differential spectrum can be computed using (1). □

Using the differential spectrum of the function G_t, the differential spectrum of the symmetric function G_s with $s = \frac{(n+3)}{2}$ can be derived easily (Theorem 4 of [BCC11]). Notice that G_s is a permutation if and only if $n \not\equiv 0 \mod 3$ ($\delta(0) = 0$). If $n \equiv 0 \mod 3$, we have $\delta(0) = 2$. In all cases $\delta(1) = 2$. We conclude that the function G_s is differentially 6-uniform.

5 Overview on the function $x \mapsto x^{2^t-1}$

Among monomials with exponents $2^t - 1$ ($t = 2, \cdots, n-1$), several have good differential properties, as for instance the Gold function $G_2(x) = x^3$ and the inverse function $G_{n-2}(x) = x^{2^{n-2}-1}$. In [BCC11] it is conjectured that only few G_t are APN (equivalent to known APN). When n is even, it has been proved recently in [Göl12] that this conjecture is true and only $G_2(x) = x^3$ is APN. Proving the case n odd of Conjecture 1 of [BCC11] is still an open problem. In [BCC11] and in this article, the differential uniformity and the differential spectrum for different values of t have been extracted. These functions, resumed in Table 1, are locally differentially 2-or 6-uniform meaning that for $b \neq 0, 1$ $\delta(b) \leq 2$ or 6. Other functions among the family $x \mapsto x^{2^t-1}$ can be proved locally differentially 6-uniform. Nevertheless these functions present less cryptographic interest since their differential uniformity increases with the dimension of the field.

Theorem 6. *Let $G_t : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with $n \equiv 0 \mod 3$ and $t = \frac{n}{3}, \frac{2n}{3}, \frac{n}{3} + 1, \frac{2n}{3} + 1$. The function G_t is differentially 2^t-uniform or $(2^t - 2)$-uniform. For $b \neq 0, 1$ we have $\delta(b) \leq 6$.*

In Table 1, we give the list of functions G_t proved locally differentially 2- or 6-uniform. As the algebraic degree is also a criteria when designing a block cipher, in the same table, we resume the algebraic degree of the functions G_t their symmetric G_s and, when they exist, their inverses. When the function is not invertible the degree is denoted by $'*'$. The differential uniformity and the permutation property depend of the value of n modulo 2, 3, 6 or 9. Restricted differential uniformity is denoted by $\Delta = \max_{b \neq 0,1} \delta(b)$. Algebraic degree of the inverse of the function G_t has been computed using (4).

As actual block ciphers are designed using many iterations of the non-linear layer, using a function differentially 6-uniform instead of a differentially 2-or 4-uniform does not influence directly the security of the cipher in regards to differential cryptanalysis. Nevertheless, degree of the function or its inverse is important to insure some security against algebraic attacks. For the locally differentially 6-uniform ones, we notice that the algebraic degrees are related to each other. For instance, in some cases, we have $deg(G^{-1}_{(n-1)/2}) = deg(G_{(jn+2)/3})$. As proved in this paper, all these functions have a similar differential spectrum and the question of equivalence of these functions can be raised. As the CCZ and the EA equivalence [CCZ98,Car10] preserve the Walsh spectrum, experiments have been done to compute the non-linearity and the Walsh spectrum of the functions

t, $deg(G_t)$	s, $deg(G_s)$	$deg(G_t^{-1})$	$deg(G_s^{-1})$	Δ	$\delta(G_t)$	$\delta(G_s)$	Spectrum
2	$n-1$	$(*, \frac{n+1}{2})$	$n-1$	2	2	(2,4)	Gold/Inverse
$\frac{n+1}{2}$	$\frac{n+1}{2}$	2	2	2	2	2	Inverse of x^{2^t+1}
$\frac{n}{2}$	$\frac{n}{2}+1$	$*$	$\frac{n+2}{2}$	2	$2^{n/2-2}$	$2^{n/2}$	[BCC11]
3	$n-2$	$(*, \frac{jn+1}{3})$	$\frac{n-1}{2}$	6	6	(6,8)	[BCC11]
$\frac{kn+1}{3}$	$\frac{(3-k)n+2}{3}$	3	$(*, 3)$	6	6	6	Theorem 3
$\frac{n-1}{2}$	$\frac{n+3}{2}$	$n-2$	$(*, \frac{jn+2}{3})$	6	(6,8)	6	Theorem 5
$\frac{kn}{3}$	$\frac{(3-k)n+3}{3}$	$*$	$(*, \frac{jn+3}{3})$	6	$2^{n/3}-2$	$2^{n/3}$	Spectrum not proved

Table 1. Differential Uniformity and Algebraic degree of the function $G_t(x) = x^{2^t-1}$, their symmetric G_s and their inverses G_t^{-1} and G_s^{-1}. We have $\Delta = \max_{b \neq 0,1} \delta(b)$ and $1 \leq k, j \leq 2$.

G_t in $\mathbb{F}_{2^n}$ for $n < 18$. While for small n some functions have the same Walsh spectrum, this property is not true anymore for larger n. Among the different properties observed when computing the non-linearity, we notice that two symmetric functions G_t and G_s with related differential spectrum do not necessary have the same non-linearity. These experimental results show that in general the functions are not affine equivalent.

Notice that the function G_s with $s = \frac{n+3}{2}$ when $n \equiv \pm 1 \mod 6$ has large algebraic degree and its inverse too. As it is well known that if the degree of the function is too small or too large the cipher can be sensitive to algebraic attacks, this function can be a relatively good candidate for the Sbox of a block cipher.

Simulation over monomials G_t for $(n \leq 31)$ shows that almost all functions G_t locally differentially 6-uniform are of a form in Table 1. From the simulation of [BCC11], we have argument to conjecture that for $n > 16$, all power functions differentially 6-uniform are of the form $x \mapsto x^{2^t-1}$. If both of these conjectures are true, the classification of differentially 6-uniform power functions is almost complete.

6 Conclusion

Studying the properties of power functions is of great interest for the security of symmetric cryptographic primitives. As the differential spectrum of known families of APN and differentially 4-uniform power functions have already been studied, further investigations on power functions lead naturally to the study of the differentially 6-uniform ones. In [BCC11], it was conjectured that a large number of differentially 6-uniform power functions are such that $G_t(x) = x^{2^t-1}$ in $\mathbb{F}_{2^n}[X]$. While the differential spectrum when $t = 3$ and $t = n-2$ was already

presented in [BCC11], in this paper we present the differential spectrum of the functions G_t for other values of t: $t = \frac{n-1}{2}$, $t = \frac{n+3}{2}$, $t = \frac{kn+1}{3}$ and $t = \frac{(3-k)n+2}{3}$ when t is an integer value and $k = 1, 2$. While these differential spectra are similar to the one of the function x^7, the algebraic degrees of some of these functions and of their inverses can provide better candidate for the S-boxes of a block cipher.

7 Acknowledgements

The authors wish to thank the anonymous reviewers for helpful comments and would like to thank Pascale Charpin for the advices provided when writing this article. The work of Léo Perrin is partly supported by an Erasmus Thesis scholarship.

References

BCC10. C. Blondeau, A. Canteaut, and P. Charpin. Differential properties of power functions. *Int. J. Inform. and Coding Theory*, 1(2):149–170, 2010. Special Issue dedicated to Vera Pless.

BCC11. C. Blondeau, A. Canteaut, and P. Charpin. Differential Properties of $x \mapsto x^{2^t-1}$. *IEEE Transactions on Information Theory*, 57(12):8127–8137, 2011.

BL10. C. Bracken and G. Leander. A highly nonlinear differentially 4-uniform power mapping that permutes fields of even degree. *Finite Fields and Their Applications*, 16:231–242, 2010.

Blo11. C. Blondeau. *La cryptanalyse différentielle et ses généralisations*. PhD thesis, Université Pierre et Marie Curie, Paris, France, 2011.

BRS67. E.R. Berlekamp, H. Rumsey, and G. Solomon. On the solution of algebraic equations over finite fields. *Inform. Contr.*, 12(5):553–564, 1967.

BS91. E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.

Car79. L. Carlitz. Explicit evaluation of certain exponential sums. *Mathematica Scandinavica*, 44:5–16, 1979.

Car10. C. Carlet. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, chapter Vectorial Boolean Functions for Cryptography, pages 398–469. Cambridge University Press, 2010.

CCD00. A. Canteaut, P. Charpin, and H. Dobbertin. Binary m-sequences with three-valued crosscorrelation: A proof of Welch conjecture. *IEEE Transactions on Information Theory*, 46(1):4–8, 2000.

CCZ98. C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

Dic96. L. E. Dickson. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *Annals of Mathematics*, 11(1/6):65–120, 1896.

Dob99a. H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case. *Information and Computation*, 151(1-2):57–72, 1999.

Dob99b. H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, 1999.

Dob00. H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: a new class for n divisible by 5. In *Proceedings of Finite Fields and Applications Fq5*, pages 113–121. Springer-Verlag, 2000.

Göl12. F. Göloğlu. A note on "differential properties of $x \mapsto x^{2^t-1}$ ". *IEEE Transactions on Information Theory*, 58(11):6986–6988, 2012.

HK08. T. Helleseth and A. Kholosha. On the equation $x^{2^l+1} + x + a = 0$ over $GF(2^k)$. *Finite Fields and Their Applications*, 14(1):159–176, 2008.

HK10. T. Helleseth and A. Kholosha. $x^{2^l+1} + x + a$ and related affine polynomials over $GF(2^k)$. *Cryptography and Communications*, 2(1):85–109, 2010.

HM11. F. Hernando and G. McGuire. Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. *Journal of Algebra*, 343(1):78–92, 2011.

HMAL09. X.-D. Hou, G. L. Mullen, Sellers J. A., and Yucas J. L. Reversed Dickson polynomials over finite fields. *Finite Fields and Their Applications*, 15(6):748–773, 2009.

HX01. H.D.L. Hollmann and Q. Xiang. A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. *Finite Fields and their Applications*, 7(2):253–286, 2001.

KS12. G. Kyureghyan and V. Suder. On inverses of APN exponents. In *ISIT 2012*, pages 1207–1211. IEEE, 2012.

NK93. K. Nyberg and L.R. Knudsen. Provable security against differential cryptanalysis. In *CRYPTO'92*, volume 740 of *LNCS*, pages 566–574. Springer-Verlag, 1993.

Nyb93. K. Nyberg. Differentially uniform mappings for cryptography. In *EUROCRYPT'93*, volume 765 of *LNCS*, pages 55–64. Springer-Verlag, 1993.