Differential properties of power functions

Céline Blondeau, Anne Canteaut and Pascale Charpin
SECRET Project-Team - INRIA Paris-Rocquencourt
Domaine de Voluceau - B.P. 105 - 78153 Le Chesnay Cedex - France
celine.blondeau@inria.fr, anne.canteaut@inria.fr, pascale.charpin@inria.fr

***Abstract*—Some properties of the differential spectra of power functions, *i.e.*, monomials mappings on $\mathbb{F}_{2^n}$, are investigated. We focus in particular on functions with a small differential uniformity and on some infinite families of power functions.**

I. Introduction

Differential cryptanalysis is the first statistical attack proposed for breaking iterated block ciphers. Its presentation [1] then gave rise to numerous works which investigate the security offered by different types of functions with respect to differential attacks. This security is quantified by the so-called *differential uniformity* of the Substitution box used in the cipher. Most notably, finding appropriate S-boxes which guarantee that the cipher using them resists differential attacks is a major topic for the last fifteen years. Power permutations, *i.e.*, monomial permutations, form a class of suitable candidates since they usually have a lower implementation cost in hardware. However, using power permutations which are optimal for differential cryptanalysis might not be suitable in a cryptographic context.

One reason is that generally such permutations on $\mathbb{F}_{2^n}$ are not known for n even (which is obviously the case in most applications). Actually the nonexistence of APN permutations for even n was conjectured, until the recent announcement of such mappings for $n = 6$ by Dillon [2]. A second important point is that optimal functions usually correspond to extremal objects, which possess very strong algebraic structures. Then, optimal functions might introduce some unsuitable weaknesses within a cipher. Some examples of such weaknesses have been exploited in cryptanalysis, for instance in [3]–[5]. For all these reasons, it is important to find some functions which have an almost optimal differential uniformity. Also, the security of the underlying cipher is affected by some other properties related to the behavior of the function when an input difference is fixed, besides its differential uniformity. For instance, we have pointed out in [6] that the whole differential spectrum of a power permutation may influence its security regarding some variants of differential cryptanalysis, especially truncated differential attacks.

In this context, our purpose is then to investigate the differential properties, namely the whole differential spectrum, of power functions, with a particular interest in functions which have a low differential uniformity. This paper is the continuation of a recent work [6], where we focused on differentially 4-uniform power permutations.

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

II. Definitions and basic properties

In the whole paper, $\#E$ denotes the cardinality of any set E. The paper investigates some properties of functions from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^m}$, $m \geq 1$. It mainly focuses on the case $m = n$ and $m = 1$ (Boolean functions).

A. Differential characteristics of a function

The resistance of a cipher to differential attacks and to its variants is quantified by some properties of the *derivatives* of its S-box, in the sense of the following definition. It is worth noticing that this definition is general: it deals with mappings from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^m}$ for any $m \geq 1$.

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

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

The resistance to differential cryptanalysis is related to the following quantities.

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

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

Then, the *differential uniformity* of F is

$$\delta(F) = \max_{a \neq 0,\ b \in \mathbb{F}_{2^n}} \delta(a,b).$$

Those functions for which $\delta(F) = 2$ are said to be *almost perfect nonlinear (APN)*.

B. Differential spectrum of power functions

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 $\mathbb{F}_{2^n}$. This power function will be denoted by F_d. Power functions are very popular S-boxes for symmetric ciphers since they have a relatively low implementation complexity in hardware environments. Studying their resistance to differential attacks is then of great interest. In the case of a power function, $F_d(x) = x^d$, the differential properties can be analysed more easily since, for any nonzero $a \in \mathbb{F}_{2^n}$, the equation $(x+a)^d + x^d = b$ can be written

$$a^d \left(\left(\frac{x}{a} + 1 \right)^d + \left(\frac{x}{a} \right)^d \right) = b,$$

implying that $\delta(a,b) = \delta(1, b/a^d)$ for all $a \neq 0$. Then, if $F_d : x \mapsto x^d$ is a monomial function, the differential characteristics

of F_d are determined by the values $\delta(1,b)$, $b \in \mathbb{F}_{2^n}$. From now on, this quantity $\delta(1,b)$ is denoted by $\delta(b)$.

Since

$$\#\{b \in \mathbb{F}_{2^n} | \delta(a,b) = i\} = \#\{b \in \mathbb{F}_{2^n} | \delta(b) = i\} \quad \forall a \neq 0,$$

the *differential spectrum* of F can be defined as follows.

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

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

The *differential spectrum* of F_d is the set of ω_i:

$$\mathbb{S} = \{\omega_0, \omega_2, ..., \omega_{\delta(F)}\}.$$

A power function F is said *differentially* 2*-valued* if and only if for any $b \in \mathbb{F}_{2^n}$, we have $\delta(b) \in \{0, \kappa\}$ (and then only two ω_i are not zero in $\mathbb{S}$). It is known that $\kappa = 2^r$ for some $r > 1$. Note that APN functions are differentially 2-valued with $\kappa = 2$ (see an extensive study in [6, Section 5]).

There are basic transformations which preserve $\mathbb{S}$.

Lemma 1: Let $F_d(x) = x^d$ and $F_e(x) = x^e$. If there exists k such that $e = 2^k d \bmod 2^n - 1$ or if $\gcd(2^n - 1, d) = 1$ and $e = d^{-1}$ then F_d and F_e have the same differential spectrum.

Now, we wish to point out that, besides the differential uniformity, the whole differential spectrum of the S-box affects the resistance of the cipher to differential attacks.

Suppose for instance that a cipher involves a differentially 4-uniform function. If ω_4 is large, the probability of having $\delta(a,b) = 4$ for a fixed input difference a is not negligible. This affects the security of the corresponding cipher. Indeed, an obvious strategy for finding a good differential characteristic for the whole cipher consists in chaining several one-round differentials with $\delta(a,b) = 4$. This is usually much easier when there are some degrees of freedom in the choice of the output difference. So when n is even, the power permutations which offer the best resistance to differential cryptanalysis are the differentially 4-uniform S-boxes with ω_4 small. A fortiori $\omega_4 = 1$ is the best value. In this context, the inverse function has the best possible differential spectrum when n is even.

III. General properties of the differential spectrum

In order to evaluate $\delta(F_d)$ we study $\delta(b)$ for special values of b. In this section, we denote by $\mathcal{S}_d(b)$ the set formed by the solutions of

$$(x+1)^d + x^d = b. \tag{1}$$

We here focus on $b \in \mathbb{F}_2$.

Lemma 2: Let d be such that $\gcd(d, 2^n - 1) = s$. Then $\delta(0) = s - 1$. In particular $s = 1$ if and only if $\delta(0) = 0$.

The next result is partly in [7, Chapter V].

Lemma 3: Let k be any integer such that $k \geq 1$. Consider the trinomial over $\mathbb{F}_2$

$$P(x) = x^{2^k} + x + 1.$$

Then all irreducible factors of $P(x)$ have degrees $2s$ dividing $2k$ with $s = \gcd(2s, k)$. Consequently, $x^{2^s} + x + 1$ divides $P(x)$ for all such s.

Now, we denote by α a primitive element in $\mathbb{F}_{2^n}$.

Theorem 1: Let $F_d : x \mapsto x^d$ be a power function over $\mathbb{F}_{2^n}$. Let $b \in \mathbb{F}_2$. Assume that, no $\alpha^i \in \mathcal{S}_d(b)$, with $i > 0$, is a root of $x^{2^k} + x + 1$ for some $k \geq 1$. Then, $\mathcal{S}_d(b) \setminus \mathbb{F}_2$ consists of some elements α^i where i describes an even number of cyclotomic cosets modulo $(2^n - 1)$.

Proof: Let us define the set

$$\mathcal{E} = \{i,\ 1 \leq i \leq 2^n - 2,\ \ \alpha^i \in \mathcal{S}_d(b)\}.$$

For any $x \in \mathcal{S}_d(b)$, $(1 + x)$ belongs to $\mathcal{S}_d(b)$ too. In other words, $i \in \mathcal{E}$ if and only if its Zech logarithm $Z(i) \in \mathcal{E}$ where the Zech logarithm is defined by $\alpha^{Z(i)} = \alpha^i + 1$. Since $\mathcal{E}$ is a union of cyclotomic cosets modulo $(2^n - 1)$, we have

$$\mathcal{E} = \bigcup_{i \in \mathcal{I}} \left[Cl(i) \cup Cl(Z(i)) \right],$$

for some set $\mathcal{I}$. Then, $\mathcal{E}$ contains an odd number of cyclotomic coset if and only if it contains some element i such that $Cl(i) = Cl(Z(i))$, which means that we have $\alpha^{2^k i} = \alpha^i + 1$ for some k. But this is impossible, by hypothesis. ■

We later prove, using Lemma 3, that the hypothesis of Theorem 1 is satisfied in many cases.

Proposition 1: The hypothesis of Theorem 1, say $\mathcal{H}$, is satisfied in the following cases.

(i) When n is odd, $\mathcal{S}_d(1) \setminus \mathbb{F}_2$ and $\mathcal{S}_d(0)$ satisfy $\mathcal{H}$.

(ii) When $n = 2m$ and m is prime: if 3 divides d then $\mathcal{S}_d(1) \setminus \mathbb{F}_2$ otherwise $\mathcal{S}_d(0)$ satisfies $\mathcal{H}$.

Proof: Set $E_b(x) = x^d + (x+1)^d + b$, $b \in \mathbb{F}_2$. When n is odd, it is impossible to have an i such that $\alpha^{2^k i} + \alpha^i + 1 = 0$, since for any $i > 0$

$$Tr(\alpha^{2^k i} + \alpha^i + 1) = Tr(1) = 1.$$

Now, we consider even n, $n = 2m$. Suppose that there is i such that $\alpha^{2^k i} + \alpha^i + 1 = 0$ and $\alpha^i \in \mathcal{S}_d(b)$ for some k and some $b \in \mathbb{F}_2$. As previously explained (see Lemma 3), we can suppose that k is the smallest integer such that this property holds for i. Hence α^i is a root of an irreducible polynomial $P(x)$ of degree $2k$, which is a factor of $x^{2^n} + x$. Thus $2k$ divides $2m$; further k divides m with $1 \leq k < m$ (see Lemma 3). Note that $k \neq m$ since $x^{2m} \neq x + 1$ for any $x \in \mathbb{F}_{2^n}$. Hence, when m is prime the only possibility is $k = 1$.

The case $k = 1$ corresponds to the trinomial $x^2 + x + 1$ which always divides $x^{2^n} + x$ for even n. If $\gcd(d, 3) = 1$, then $x^2 + x + 1$ divides $E_1(x)$ and we have

$$E_1(0) = E_1(1) = 0 \text{ and } x^d + x^{2d} + 1 = 0 \text{ when } x \in \mathbb{F}_4 \setminus \mathbb{F}_2,$$

implying $\delta(1) \geq 4$. On the other hand $x^2 + x + 1$ does not divide $E_0(x)$ since in this case $x^d + x^{2d} \neq 0$ unless $x \in \mathbb{F}_2$. If $\gcd(d, 3) = 3$ then $x^2 + x + 1$ divides $E_0(x)$ and does not divide $E_1(x)$. ■

And, the hypothesis $\mathcal{H}$ could imply some bound on $\delta(b)$. For instance, we deduce directly:

Corollary 1: Let s be the smallest divisor of n such that $3 \leq s \leq n$.

If n and d are such that $\mathcal{S}_d(1) \setminus \mathbb{F}_2$ satisfies $\mathcal{H}$, then either $\delta(1) = 2$ or $\delta(1) \geq 2 + 2s$. If n and d are such that $\mathcal{S}_d(0)$ satisfies $\mathcal{H}$ then either $\delta(0) = 0$ or $\delta(0) \geq 2s$.

IV. Some general issues

With our numerical results, several interesting problems appeared (see, for instance, our tables in [6]). In a cryptographic context, the functions F_d which have a small differential uniformity are of most interest and, therefore, provided many works (see, for instance, [8] and [9] and their references). We first prove a general property for non-bijective functions. Furthermore, we obtain a surprising result concerning the bijective functions. Notably, we prove that *the differentially* 4*-uniform functions are permutations when* n *is odd.*

Proposition 2: Assume that n is odd and d is such that $\gcd(d, 2^n - 1) = s$ with $s > 1$. Then $s \neq 2^i + 1$ for any $i > 0$. Consequently F_d cannot be differentially 2-valued. Moreover, if 3 divides n then $\delta(F_d) \geq 6$, otherwise $\delta(F_d) \geq 10$.

Proof: From Lemma 2, $\delta(0) = s - 1$. Since n is odd, $\gcd(2^i + 1, 2^n - 1) = 1$ for any i. Thus one cannot have $s = 2^i + 1$ for some i. Therefore $\delta(b)$ cannot take two values $\{0, \kappa\}$, with $\kappa = 2^i$ for some i.

Now we use Proposition 1. Note that we have proved that $s \notin \{3, 5, 9, \dots\}$. If 3 divides n then two irreducible polynomials of degree 3 could have their roots in $\mathcal{S}_d(0)$ so that $\delta(0) \geq 6$. Otherwise, $\delta(0) \geq 10$ since two irreducible polynomials of degree 5 could have their roots in $\mathcal{S}_d(0)$. ■

Corollary 2: Consider any exponent d such that $\delta(F_d) \leq 6$. Then we have:

(i) Assume that n is odd. Then F_d is a permutation when
- $\delta(F_d) \leq 4$;
- $\delta(F_d) = 6$ with $\gcd(3, n) = 1$.

When $\gcd(3, n) = 3$ and $\delta(F_d) = 6$ either 7 divides d or F_d is a permutation. Morever, if $\delta(F_d) \leq 6$, then $\delta(1) = 2$, implying that $\omega_2 \neq 0$.

(ii) Let $n = 2m$ with m odd. Assume that $\gcd(3, d) = 1$. Then $\delta(F_d) \in \{4, 6\}$ and $\delta(1) = 4$ and
- if $\delta(F_d) = 4$ then F_d is a permutation;
- if $\delta(F_d) = 6$ and $\gcd(3, n) = 1$ then F_d is a permutation.

When $\gcd(3, n) = 3$ and $\delta(F_d) = 6$ either 7 divides d or F_d is a permutation.

Proof: Let n be odd. Then $\mathcal{S}_d(1) \setminus \mathbb{F}_2$ and $\mathcal{S}_d(0)$ satisfy $\mathcal{H}$ (Proposition 1). According to Corollary 1, if $\delta(F_d) \leq 6$ then $\delta(1) = 2$ so that $\omega_2 \neq 0$. Moreover $\delta(0) = 0$ or $\delta(0) = 6$ (since $\delta(F_d) \leq 6$).

Let $s = \gcd(2^n - 1, d)$. Since $\delta(0) = s - 1$, if F_d is not a permutation then $\delta(0) = 6$ ($s = 7$), implying $\delta(F_d) = 6$, which is possible only if 3 divides n.

Now, assume that $n = 2m$ with m odd. Since 3 divides $2^n - 1$, if $\gcd(3, d) = 3$ then F_d is not a permutation. Also, we know that if F_d is APN then $\gcd(3, d) = 3$. Thus, with our hypothesis $\delta(F_d) \in \{4, 6\}$ and $\delta(1) = 4$ (see the proof of Proposition 1).

Let $s = \gcd(2^n - 1, d)$; so $s \in \{1, 5, 7\}$, but $s = 5$ is impossible since $\gcd(2^n - 1, 5) = 1$ as soon as m is odd. Hence $s = 1$ when $\delta(F_d) = 4$, implying that F_d is a permutation. If $\delta(F_d) = 6$ then F_d is a permutation unless $s = 7$ which is possible only if 3 divides n. ■

The existence of *differentially* 2*-valued* functions is related to the problem of *finding* b *such that* $\delta(b) = 2$. We think that such b exists for almost all d. In [6], the following conjecture is given but for permutations only.

Conjecture 1: Any power function x^d which is not APN and is differentially 2-valued is such that d is either a quadratic exponent or a Kasami exponent, up to any equivalence which preserves the differential spectrum.

This conjecture is corroborated by the results on the scarcity of such functions, which we presented in [6]. Actually, it can be proved that power permutations over $\mathbb{F}_{2^n}$ which are differentially 2-valued do not exist for many sets of parameters. Using the new results presented here, we can strengthen our conjecture, especially when n is odd.

Corollary 3: Let d be such that F_d is not APN. Then for odd n, F_d is not differentially 2-valued
- when F_d is not a permutation;
- when $\delta(F_d) = 4$.

For even n, F_d is not differentially 2-valued when $\gcd(2^n - 1, d) = 3$.

V. On exponents $d = 2^t - 1$

Now, we investigate the differential spectra of the power functions $G_t : x \mapsto x^{2^t - 1}$ over $\mathbb{F}_{2^n}$.

Theorem 2: Let $G_t(x) = x^{2^t - 1}$, $2 \leq t \leq n - 1$. Then,

$$G_t(x + 1) + G_t(x) + 1 = \frac{(x^{2^{t-1}} + x)^2}{x^2 + x}. \tag{2}$$

Consequently, for any $b \in \mathbb{F}_{2^n}^*$, $\delta(b)$ is determined by the number of roots in $\mathbb{F}_{2^n}$ of the linearized polynomial

$$P_b(X) = X^{2^t} + bX^2 + (b + 1)X.$$

And we have

$$\begin{aligned} \delta(0) &= 2^{\gcd(t,n)} - 2 \\ \delta(1) &= 2^{\gcd(t-1,n)} \\ \text{for any } \ b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2, \ \ \delta(b) &= 2^r - 2 \end{aligned}$$

for some r with $1 \leq r \leq \min(t, n - t + 1)$.

Proof: To prove (2) we simply compute

$$(x^2 + x)(1 + x^d + (1 + x)^d), \ d = 2^t - 1.$$

Thus, $\delta(1)$ is directly deduced, while $\delta(0)$ is obtained from Lemma 2. Let $b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$. Then $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ is a solution of $(x + 1)^d + x^d = b$ if and only if it is a solution of

$$(x^{2^{t-1}} + x)^2 = (b + 1)x(x + 1).$$

The proof is completed, since P_b is linear. ■

We now show how the previous theorem enables us to determine the differential uniformity and some properties of the

differential spectrum of $G_t : x \mapsto x^{2^t-1}$ for some particular cases.

Remark 1: As a first easy corollary, we recover the following well-known form of the differential spectrum of the inverse mapping, $G_{n-1} : x \mapsto x^{2^{n-1}-1}$ over $\mathbb{F}_{2^n}$. Actually, the previous theorem applied to $t = n-1$ leads to $\delta(0) = 0$ and $\delta(1) = 2$ when n is odd and $\delta(1) = 4$ when n is even. For all $b \notin \mathbb{F}_2$, $\delta(b) \in \{0, 2\}$. Therefore, we have

- if n is odd, $\delta(G_{n-1}) = 2$ and $\omega_0 = 2^{n-1}, \omega_2 = 2^{n-1}$;
- if n is even, $\delta(G_{n-1}) = 4$ and $\omega_0 = 2^{n-1} + 1$, $\omega_2 = 2^{n-1} - 2, \omega_4 = 1$.

The family of power functions $G_t : x \mapsto x^{2^t-1}$ then contains several APN functions: the inverse permutation for n odd ($t = n-1$), the quadratic function $x \mapsto x^3$ ($t = 2$) and also the function

$$x \mapsto x^{2^{\frac{n+1}{2}}-1} \quad \text{for } n \text{ odd}$$

which is the inverse of the quadratic mapping

$$x \mapsto x^{2^{\frac{n+1}{2}}+1}.$$

Moreover, we raise the following conjecture.

Conjecture 2: Let $G_t(x) = x^{2^t-1}$, $2 \le t \le n-1$. If G_t is APN then either $t = 2$ or n is odd and $t \in \{\frac{n+1}{2}, n-1\}$.

We now study some specific subclasses of the previous family $G_t : x \mapsto x^{2^t-1}$. An example is G_7 for which we are able to give the complete differential spectrum (the proof, which is long and highly technical is not given here).

A. Exponent $d = 2^t - 1$ with $t = \lfloor n/2 \rfloor$

We now show that we are able to determine the differential uniformity of G_t in the case $t = \lfloor n/2 \rfloor$. We first consider the case n even. Note that in this case, $G_{n/2}$ is not a permutation.

Theorem 3: Let n be an even integer, $n > 4$. Let $G_{n/2} : x \mapsto x^{2^{n/2}-1}$. Then $\delta(G_{n/2}) = 2^{n/2} - 2$ and the differential spectrum of $G_{n/2}$ is:

- if $n \equiv 0 \bmod 4$,

$$\begin{aligned} \omega_{2^{n/2}-2} &= 1 \\ \omega_i &= 0 \text{ for all } 2 < i < 2^{n/2} - 2 \\ \omega_2 &= 2^{n-1} - 2^{n/2-1} + 1 \\ \omega_0 &= 2^{n-1} + 2^{n/2-1} - 2 \end{aligned}$$

- if $n \equiv 2 \bmod 4$,

$$\begin{aligned} \omega_{2^{n/2}-2} &= 1 \\ \omega_i &= 0 \text{ for all } 4 < i < 2^{n/2} - 2 \\ \omega_4 &= 1 \\ \omega_2 &= 2^{n-1} - 2^{n/2-1} - 1 \\ \omega_0 &= 2^{n-1} + 2^{n/2-1} - 1 \end{aligned}$$

Proof: From Theorem 2, we have $\delta(0) = 2^{n/2} - 2$ and $\delta(1) = 2$ if $n/2$ is odd and $\delta(1) = 4$ if $n/2$ is even. Now, for all $b \notin \mathbb{F}_2$, we have to determine the number of roots in $\mathbb{F}_{2^n}$ of $P_b(X) = X^{2^{n/2}} + bX^2 + (b+1)X$. Any root of P_b is also a root of

$$\begin{aligned} Q_b(X) &= P_b(X)^{2^{n/2}} + b^{2^{n/2}} P_b(X)^2 + (b^{2^{n/2}} + 1) P_b(X) \\ &= X^{2^n} + b^{2^{n/2}} X^{2^{n/2}+1} + (b^{2^{n/2}} + 1) X^{2^{n/2}} \\ &\quad + b^{2^{n/2}} X^{2^{n/2}+1} + b^{2^{n/2}} b^2 X^4 + b^{2^{n/2}} (b^2+1) X^2 \\ &\quad + (b^{2^{n/2}} + 1) X^{2^{n/2}} + (b^{2^{n/2}} + 1) b X^2 \\ &\quad + (b^{2^{n/2}} + 1)(b+1) X \\ &= b^{2^{n/2}} b^2 X^4 + \left[b^{2^{n/2}} (b^2+1) + (b^{2^{n/2}} + 1) b \right] X^2 \\ &\quad + \left[(b^{2^{n/2}} + 1)(b+1) + 1 \right] X \end{aligned}$$

Since Q_b is a linearized polynomial of degree 4, it has either 4 or 2 roots. The whole differential spectrum is derived by using that $\sum_{i=0}^{n} i\omega_i = 2^n$ and $\sum_{i=0}^{n} \omega_i = 2^n$. ∎

In the case where n is odd, the differential uniformity of G_t, with $t = \frac{n-1}{2}$, can be determined.

Theorem 4: Let n be an odd integer, $n > 3$. Let

$$G_{\frac{n-1}{2}} : x \mapsto x^{2^{\frac{n-1}{2}}-1}.$$

Then, $G_{\frac{n-1}{2}}$ is a permutation. And we have

- if $n \equiv 0 \bmod 3$, then $\delta(G_{\frac{n-1}{2}}) = 8$, and the differential spectrum satisfies $\omega_i = 0$ for all $i \notin \{0, 2, 6, 8\}$ and $\omega_8 = 1$.
- if $n \not\equiv 0 \bmod 3$, then $\delta(G_{\frac{n-1}{2}}) \le 6$ and the differential spectrum satisfies $\omega_i = 0$ for all $i \notin \{0, 2, 6\}$.

Proof: From Theorem 2, we have $\delta(0) = 0$ and $\delta(1) = 8$ if 3 divides n and $\delta(1) = 2$ otherwise. Now, for all $b \notin \mathbb{F}_2$, we have to determine the number of roots in $\mathbb{F}_{2^n}$ of

$$P_b(X) = X^{2^{\frac{n-1}{2}}} + bX^2 + (b+1)X.$$

We use that any root of P_b is a root of Q_b defined as follows where $c = b^{2^{\frac{n+1}{2}}}$:

$$\begin{aligned} Q_b(X) &= P_b(X)^{2^{\frac{n+1}{2}}} + cP_b(X)^4 + (c+1)P_b(X)^2 \\ &= X^{2^n} + cX^{2^{\frac{n+3}{2}}} + (c+1)X^{2^{\frac{n+1}{2}}} \\ &\quad + cX^{2^{\frac{n+3}{2}}} + cb^4X^8 + c(b^4+1)X^4 \\ &\quad + (c+1)X^{2^{\frac{n+1}{2}}} + (c+1)b^2X^4 \\ &\quad + (c+1)(b^2+1)X^2 \\ &= cb^4X^8 + \left[c(b^4+1) + (c+1)b^2 \right] X^4 \\ &\quad + (c+1)(b^2+1)X^2 + X \end{aligned}$$

The result then follows from the fact that Q_b has degree 8, and then it has either 8 or 4 or 2 solutions. ∎

B. Exponent $d = 2^t - 1$ with $t = n/3,\ n = 3m$

The technique used for proving Theorem 3 also applies to the case where t corresponds to some other large divisor of n, but the upper bound on the differential uniformity of the function increases when t decreases. We then only give an example corresponding to the case $t = n/3$.

Theorem 5: Let $n = 3m$ with $m > 1$. Let

$$G_{n/3} : x \mapsto x^{2^{n/3}-1}.$$

Then $\delta(G_{n/3}) = 2^{n/3} - 2$ and we have

- if $n \equiv 3 \bmod 9$, the differential spectrum satisfies $\omega_i = 0$ for all $i \notin \{0, 2, 6, 8, 2^{n/3}-2\}$, $\omega_8 = 1$ and $\omega_{2^{n/3}-2} = 1$.
- if $n \equiv 0 \bmod 9$, the differential spectrum satisfies $\omega_i = 0$ for all $i \notin \{0, 2, 6, 2^{n/3} - 2\}$.

Proof: From Theorem 2, we have $\delta(0) = 2^{n/3} - 2$ and $\delta(1) = 8$ if $n \equiv 3 \bmod 9$ and $\delta(1) = 2$ otherwise. Now, for all $b \notin \mathbb{F}_2$, we have to determine the number of roots in $\mathbb{F}_{2^n}$ of $P_b(X) = X^{2^{n/3}} + bX^2 + (b+1)X$. We use that any root of P_b is a root of Q_b defined as follows where $c = b^{2^{2n/3}}$ and $d = b^{2^{n/3}}$:

$$\begin{aligned}
Q_b(X) &= P_b(X)^{2^{2n/3}} \\
&= X + cX^{2^{2n/3+1}} + (c+1)X^{2^{2n/3}} \\
&= X + c[d^2X^{2^{n/3+2}} + (d^2+1)X^{2^{n/3+1}}] \\
&\quad +(c+1)[dX^{2^{n/3+1}} + (d+1)X^{2^{n/3}}] \\
&= X + c[d^2(bX^2 + (b+1)X)^4 \\
&\quad +(d^2+1)(bX^2 + (b+1)X)^2] \\
&\quad +(c+1)[d(b^2X^4 + (b^2+1)X^2) \\
&\quad +(d+1)(bX^2 + (b+1)X)]
\end{aligned}$$

The result then follows from the fact that Q_b has degree 8, and then it has either 8 or 4 or 2 solutions. ■

C. Exponent $d = 7$

We now focus on $G_t : x \mapsto x^{2^t-1}$ for $t = 3$, *i.e.*, $x \mapsto x^7$, and we completely determine its differential spectrum.

Theorem 6: Let $F_7 : x \mapsto x^7$ over $\mathbb{F}_{2^n}$. Then, F_7 is differentially 6-uniform and its differential spectrum is given by:

- if n is odd,

$$\begin{aligned}
\omega_6 &= \frac{2^n+1}{24} - \frac{1}{8}\left(\frac{1-i\sqrt{7}}{2}\right)^n - \frac{1}{8}\left(\frac{1+i\sqrt{7}}{2}\right)^n \\
\omega_4 &= 0 \\
\omega_2 &= 2^{n-1} - 3\omega_6 \\
\omega_0 &= 2^{n-1} + 2\omega_6;
\end{aligned}$$

- if n is even:

$$\begin{aligned}
\omega_6 &= \frac{2^n-13}{24} - \frac{1}{8}\left(\frac{1-i\sqrt{7}}{2}\right)^n - \frac{1}{8}\left(\frac{1+i\sqrt{7}}{2}\right)^n \\
\omega_4 &= 1 \\
\omega_2 &= 2^{n-1} - 3\omega_6 - 2 \\
\omega_0 &= 2^{n-1} + 2\omega_6 + 1.
\end{aligned}$$

The proof of this theorem relies on the following lemma where we characterize the values of b such that the linearized polynomial

$$P_b(X) = X^8 + bX^2 + (b+1)X$$

has all its 8 roots in $\mathbb{F}_{2^n}$.

Lemma 4: Let $P_b(X) = X^8 + bX^2 + (b+1)X$ and let $(p_n)_{n\geq 4}$ be the sequence of polynomials which are recursively defined by

$$p_n(X) = X^{2^{n-4}} p_{n-2}(X) + (X^{2^{n-4}} + 1)p_{n-3}(X) \qquad (3)$$

$$\text{with} \quad p_4(X) = X, \quad p_5(X) = X^2 + 1, \quad p_6(X) = X^5.$$

Then, we have:

- if all roots of P_b lie in $\mathbb{F}_{2^n}$, then b belongs to $\mathbb{F}_{2^n}$ and b is a root of $m_n = \gcd(p_{n+1}, p_n)$;
- if b is a root of $m_n = \gcd(p_{n+1}, p_n)$ in its splitting field, then b belongs to $\mathbb{F}_{2^n}$ and all roots of P_b lie in $\mathbb{F}_{2^n}$.

VI. Conclusions

Functions with a small differential uniformity are of great interest for the design of symetric cryptographic primitives as they guarantee the best resistance to differential attacks in most practical cases. But, besides the differential uniformity, the whole differential spectrum of its Substitution boxes affects the security of a cipher. In this context, we have studied the case of power functions with small differential uniformity. We have also exhibited some properties and conjectures on the differential spectra of several infinite families of power functions. In particular, we have investigated the power function of the form $x \mapsto x^{2^t-1}$.

References

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[2] J. Dillon, "APN polynomials: An update," in *Fq9, the 9th International Conference on Finite Fields and Applications*, Dublin, Ireland, July 2009, invited talk.

[3] T. Jakobsen and L. Knudsen, "The interpolation attack on block ciphers," in *Fast Software Encryption - FSE'97*, ser. Lecture Notes in Computer Science, vol. 1267. Springer-Verlag, 1997.

[4] N. Courtois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations," in *Advances in Cryptology - ASIACRYPT'02*, ser. Lecture Notes in Computer Science, vol. 2501. Springer-Verlag, 2002, pp. 267–287.

[5] A. Canteaut and M. Videau, "Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis," in *Advances in Cryptology - EUROCRYPT 2002*, ser. Lecture Notes in Computer Science, vol. 2332. Springer-Verlag, 2002, pp. 518–533.

[6] C. Blondeau, A. Canteaut, and P. Charpin, "Differential properties of power functions," *Int. J. Inform. and Coding Theory*, vol. 1, no. 2, pp. 149–170, 2010, special Issue dedicated to Vera Pless.

[7] S. Golomb, *Shift register sequences*. Aegean Park Press, 1982.

[8] T. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy, "On almost perfect nonlinear functions," *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 4160–4170, Sep. 2006.

[9] Y. Aubry and F. Rodier, "Differentially 4 uniform functions," *arXiv:0907.1734*, July 2009, research-report.