Differential Properties of $x \mapsto x^{2^t-1}$

Céline Blondeau, Anne Canteaut, and Pascale Charpin

***Abstract*—We provide an extensive study of the differential properties of the functions $x \mapsto x^{2^t-1}$ over $\mathbb{F}_{2^n}$, for $1 < t < n$. We notably show that the differential spectra of these functions are determined by the number of roots of the linear polynomials $x^{2^t} + bx^2 + (b+1)x$ where b varies in $\mathbb{F}_{2^n}$. We prove a strong relationship between the differential spectra of $x \mapsto x^{2^t-1}$ and $x \mapsto x^{2^s-1}$ for $s = n - t + 1$. As a direct consequence, this result enlightens a connection between the differential properties of the cube function and of the inverse function. We also determine the complete differential spectra of $x \mapsto x^7$ by means of the value of some Kloosterman sums, and of $x \mapsto x^{2^t-1}$ for $t \in \{\lfloor n/2 \rfloor, \lceil n/2 \rceil + 1, n-2\}$.**

***Index Terms*—APN function, block cipher, differential cryptanalysis, differential uniformity, Kloosterman sum, linear polynomial, monomial, permutation, power function, S-box.**

I. Introduction

DIFFERENTIAL cryptanalysis is the first statistical attack proposed for breaking iterated block ciphers. Its publication [4] then gave rise to numerous works which investigate 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 [23]. Most notably, finding appropriate S-boxes which guarantee that the cipher using them resist differential attacks is a major topic for the last twenty years, see, e.g., [7], [9], [10], [12], [17].

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 a few power functions for which we can prove that they have a 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[18] and they do not belong to a large class: they correspond to the exponents defined by Welch [11], [15], by Niho [14], [19], by Dobbertin [16], by Bracken and Leander [8], and to the inverse function [22]. It is worth noticing that some of these functions seem to have different structures because they do not share the same differential spectrum. For instance, for a quadratic power function or a Kasami function, the differential spectrum has only two values, *i.e.*, the number of occurrences of each differential belongs to $\{0, \delta\}$ for some δ[5]. The inverse function has a very different behavior since its differential spectrum has three values, namely 0, 2 and 4 and, for each input difference, there is exactly one differential which is satisfied four times.

However, when classifying all functions with a low differential uniformity, it can be noticed that the family of all power functions $x \mapsto x^{2^t-1}$ over $\mathbb{F}_{2^n}$, with $1 < t < n$, contains several functions with a low differential uniformity. Most notably, it includes the cube function and the inverse function, and also $x \mapsto x^{2^{(n+1)/2}-1}$ for n odd, which is the inverse of a quadratic function. At a first glance, this family of exponents may be of very small relevance because the involved functions have distinct differential spectra. Then, they are expected to have distinct structures. For this reason, one of the motivations of our study was to determine whether some link could be established between the differential properties of the cube function and of the inverse function. Our work then answers positively to this question since it exhibits a general relationship between the differential spectra of $x \mapsto x^{2^t-1}$ and $x \mapsto x^{2^{n-t+1}-1}$ over $\mathbb{F}_{2^n}$. We also determine the complete differential spectra of some other exponents in this family.

The rest of the paper is organized as follows. Section II recalls some definitions and some general properties of the differential spectrum of monomial functions. Section III then focuses on the differential spectra of the monomials $x \mapsto x^{2^t-1}$. First, the differential spectrum of any such function is shown to be determined by the number of roots of a family of linear polynomials. Then, we exhibit a symmetry property for the exponents in this family: it is proved that the differential spectra of $x \mapsto x^{2^t-1}$ and $x \mapsto x^{2^{n-t+1}-1}$ over $\mathbb{F}_{2^n}$ are closely related. In Section V, we determine the whole differential spectrum of $x \mapsto x^7$ over $\mathbb{F}_{2^n}$. It is expressed by means of some Kloosterman sums, and explicitly computed using the work of Carlitz [13]. We then derive the differential spectra of $x \mapsto x^{2^{n-2}-1}$. Further, we study the functions $x \mapsto x^{2^{\lfloor n/2 \rfloor}-1}$ and $x \mapsto x^{2^{\lceil n/2 \rceil+1}-1}$. We finally end up with some conclusions. An extended version of this paper can be found in [6].

II. Preliminaries

A. 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 univariate degree at

Manuscript received July 23, 2010; revised May 31, 2011; accepted July 12, 2011. Date of current version December 07, 2011. This paper was presented in part at Finite Fields and their Applications (Fq10), Ghent, Belgium, July 2011.

The authors are with the SECRET project-team, INRIA Paris-Rocquencourt Domaine de Voluceau, B.P. 105 78153 Le Chesnay Cedex, France (e-mail: celine.blondeau@inria.fr; anne.canteaut@inria.fr; pascale.charpin@inria.fr).

Communicated by K. Martin, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2011.2169129

most 2^n-1. The *algebraic degree* of F is the maximal Hamming weight of the 2-ary expansions of its exponents

$$\deg\left(\sum_{i=0}^{2^n-1}\lambda_i X^i\right)=\max\{wt(i)\mid \lambda_i\neq 0\}$$

where $\lambda_i\in\mathbb{F}_{2^n}$ and wt denotes the *Hamming weight*. In this paper, we will identify a polynomial of $\mathbb{F}_{2^n}[X]$ with the corresponding function over $\mathbb{F}_{2^n}$.

Boolean functions are also involved in this paper and are generally of the form

$$x\in\mathbb{F}_{2^n}\mapsto Tr(P(x))\in\mathbb{F}_2$$

where P is any function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^n}$ and where Tr denotes the *absolute trace* on $\mathbb{F}_{2^n}$, *i.e.,*

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

In the whole paper, $\#E$ is the cardinality of any set E.

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 [22], [23].

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

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 $\mathbb{F}_{2^n}$, which will be denoted by F_d when necessary. In the case of such a power function, the differential properties can be analyzed 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

$$\delta(a,b)=\delta(1,b/a^d)\text{ for all }a\neq 0.$$

Then, when $F:x\mapsto x^d$ is a monomial function, the differential characteristics of F 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 $F(x)=x^d$ be a power function on $\mathbb{F}_{2^n}$. We denote by ω_i the number of output differences b that occur i times

$$\omega_i=\#\{b\in\mathbb{F}_{2^n}|\delta(b)=i\}.\tag{1}$$

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

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

Obviously, the differential spectrum satisfies

$$\sum_{k=0}^{2^n}\omega_k=2^n\ \text{ and }\ \sum_{k=2}^{2^n}(k\times\omega_k)=2^n\tag{2}$$

where $\omega_i=0$ for i odd.

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.

C. General Properties on the Differential Spectrum

Studying $\delta(b)$ for special values of b may give us at least a lower bound on $\delta(F_d)$. So we first focus on $\delta(0)$.

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

Proof: Note that $s=1$ if and only if F_d is a permutation. Obviously, x is a solution of $x^d+(x+1)^d=0$ if and only if

$$\left(\frac{x+1}{x}\right)^d=1\text{ that is }x+1=xz\text{ with }z^d=1$$

since $x\mapsto(x+1)/x$ is a permutation over $\mathbb{F}_{2^n}\setminus\{0,1\}$. As there are exactly $s-1$ such $z\neq 0$, the proof is completed. ■

There is an immediate consequence of Lemma 1 for specific values of d.

Proposition 1: Let $d\geq 3$ such that d divides 2^n-1. Then $\delta(F_d)=\delta(0)=d-1$. In particular, if $d=2^t-1$ with $\gcd(t,n)=t$ then $\delta(F_d)=\delta(0)=2^t-2$.

Proof: Since $\gcd(d,2^n-1)=d$, $\delta(0)=d-1$ from Lemma 1. But the polynomial $x^d+(x+1)^d+b$ has degree $d-1$ for any b, so that $\delta(b)\leq d-1$. We conclude that $\delta(F_d)=d-1$. Now, let $d=2^t-1$ with $\gcd(t,n)=t$. Then $\gcd(d,2^n-1)=2^t-1$ so that $\delta(0)=2^t-2$. As previously we conclude that $\delta(F_d)=2^t-2$. ■

The previous remarks combined with our simulation results point out that $\delta(0)$ and $\delta(1)$ play a very particular role in the differential spectra of power functions. This leads us to investigate the properties of the differential spectrum restricted to the values $\delta(b)$ with $b\notin\mathbb{F}_2$.

Definition 4: Let F be a power function on $\mathbb{F}_{2^n}$. We say that F has the same restricted differential spectrum as an APN function when

$$\delta(b) \le 2 \text{ for all } b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2 .$$

For the sake of simplicity, we will say that F is *locally-APN*.

This definition obviously generalizes the APN property. For instance, the *inverse* function over $\mathbb{F}_{2^n}$ is locally-APN for any n, while it is APN for odd n only. Another infinite class of locally-APN functions is exhibited in Section V-B.

III. The Differential Spectrum of $x \mapsto x^{2^t-1}$

From now on, we investigate the differential spectra of the following specific monomial functions

$$G_t : x \mapsto x^{2^t-1},\ 2 \le t \le n-1, \text{ over } \mathbb{F}_{2^n}. \tag{3}$$

Note that such a function has algebraic degree t.

A. Link With Linear Polynomials

Theorem 1: Let $G_t(x) = x^{2^t-1}$ defined by (3). Then

$$G_t(x+1) + G_t(x) + 1 = \frac{(x^{2^{t-1}}+x)^2}{x^2+x}. \tag{4}$$

Consequently, for any $b \in \mathbb{F}_{2^n} \setminus \{1\}$, $\delta(b)$ is the number of roots in $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$ of the linear polynomial

$$P_b(x) = x^{2^t} + bx^2 + (b+1)x$$

and we have

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

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

Proof: To prove (4) we simply check

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

Thus, $\delta(1)$ is directly deduced and it corresponds to the number of roots of $P_1(x) = (x^{2^{t-1}}+x)^2$. Let $b \in \mathbb{F}_{2^n} \setminus \{1\}$. Then $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ is a solution of $D_1(G_t(x)) = b$ if and only if it is a solution of

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

or equivalently if it is a root of the linear polynomial

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

The values $x=0$ and $x=1$ are counted in $\delta(1)$ (as solutions of $D_1(G_t(x)) = 1$), while $P_b(0) = P_b(1) = 0$ for any b. So, we get that, if $b \neq 1$, the number of roots of P_b in $\mathbb{F}_{2^n}$ is equal to $(\delta(b)+2)$. Because the set of all roots of a linear polynomial is a linear space, we deduce that

$$\forall b \in \mathbb{F}_{2^n} \setminus \{1\},\ \ \delta(b) = 2^r - 2 \text{ with } r \le t.$$

Moreover, by raising P_b to the 2^{n-t}th power, we get that any root of P_b is also a root of

$$b' x^{2^{n-t+1}} + (b'+1)x^{2^{n-t}} + x$$

with $b' = b^{2^{n-t}}$. This then implies that $\delta(b) = 2^r - 2$ with $r \le n-t+1$. Finally, for $b=0$, $P_0(x) = x^{2^t}+x$, implying that $\delta(0) = 2^{\gcd(t,n)} - 2$, which naturally corresponds to Lemma 1. ∎

Remark 1: As a first easy corollary, we recover the following well-known form of the differential spectrum of the inverse function, $G_{n-1} : x \mapsto x^{2^{n-1}-1}$ 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 following corollary is a direct consequence of Theorem 1.

Corollary 1: Let $G_t(x) = x^{2^t-1}$ over $\mathbb{F}_{2^n}$ with $2 \le t \le n-1$. Then, its differential uniformity is of the form either $2^r - 2$ or 2^r for some $2 \le r \le n$. Moreover, if $\delta(G_t) = 2^r$ for some $r > 1$, then this value appears only once in the differential spectrum, *i.e.*, $\omega_{2^r} = 1$, and it corresponds to the value of $\delta(1)$, implying $\delta(G_t) = 2^{\gcd(t-1,n)}$.

B. Equivalent Formulations

In Theorem 1, we exhibited some tools for the computation of the differential spectra of functions $x \mapsto x^{2^t-1}$. The problem boils down to the determination of the roots of a linear polynomial whose coefficients depend on $b \in \mathbb{F}_{2^n}$. There are equivalent formulations that we are going to develop now. The first one is obtained by introducing another class of linear polynomials over $\mathbb{F}_{2^n}$. For any subspace E of $\mathbb{F}_{2^n}$, we define its *dual* as follows:

$$E^\perp = \{\, x \mid Tr(xy) = 0,\ \forall\, y \in E \,\}.$$

Also, we denote by $\mathcal{I}m(F)$ the image set of any function F.

Lemma 2: Let $t, s \ge 2$ and $s = n-t+1$. Let us consider the linear applications

$$P_{t,b}(x) = x^{2^t} + bx^2 + (b+1)x,\ \ b \in \mathbb{F}_{2^n}.$$

Then the dual of $\mathcal{I}m(P_{t,b})$ is the set of all α satisfying $P^*_{t,b}(\alpha) = 0$, where

$$P^*_{t,b}(x) = x^{2^s} + (b+1)^2x^2 + bx.$$

Note that $P^*_{t,b}$ is called the *adjoint* application of $P_{t,b}$.

Proof: By definition, $\mathcal{I}m(P_{t,b})^\perp$ consists of all α such that $Tr(\alpha P_{t,b}(x)) = 0$ for all $x \in \mathbb{F}_{2^n}$. We have

$$\begin{aligned}Tr(\alpha P_{t,b}(x)) &= Tr(\alpha x^{2^t}) + Tr(b\alpha x^2) + Tr(\alpha(b+1)x)\\ &= Tr(\alpha^{2^{n-t+1}}x^2 + b\alpha x^2 + \alpha^2(b+1)^2x^2)\\ &= Tr(x^2(\alpha^{2^s} + \alpha^2(b+1)^2 + \alpha b)).\end{aligned}$$

Hence, α belongs to the dual of the image of $P_{t,b}$ if and only if $\alpha^{2^s} + \alpha^2(b+1)^2 + \alpha b = 0$, *i.e.*, α is a root of $P^*_{t,b}$, completing the proof. ∎

The following theorem gives an equivalent formulation of the quantity r which is presented in Theorem 1.

Theorem 2: Notation is as in Lemma 2. Then

$$\dim Ker(P_{t,b}) = \dim Ker(P^*_{t,b}).$$

Consequently, this dimension can be determined by solving $P_{t,b}(x) = 0$ or equivalently by solving

$$x^{2^s} + (b+1)^2 x^2 + bx = 0, \quad \text{where } s = n - t + 1.$$

Proof: Let κ be the dimension of the image set of $P_{t,b}$. It is well-known that $n = \kappa + \dim Ker(P_{t,b})$. On the other hand, Lemma 2 shows that α is in the dual of the image of $P_{t,b}$ if and only if $P^*_{t,b}(\alpha) = 0$. We deduce that

$$n - \kappa = \dim Ker(P^*_{t,b}) = \dim Ker(P_{t,b})$$

completing the proof. ∎

Now, we discuss a different point of view, using an equivalent linear system.

Theorem 3: For any $2 \le t < n$, we define the following equation:

$$E_b : x^{2^t} + bx^2 + (b+1)x = 0, \; b \in \mathbb{F}_{2^n}.$$

Let N_b be the number of solutions of E_b in $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$. Let M_b be the number of solutions in $\mathbb{F}^*_{2^n}$ of the system

$$\left.\begin{array}{rcl} y^{2^{t-1}} + \cdots + y^2 + y(b+1) & = & 0 \\ Tr(y) & = & 0 \end{array}\right\}.$$

Then $N_b = 2 \times M_b$.

Proof: We simply write

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

which is equal to

$$\begin{aligned} &= (x^2+x)^{2^{t-1}} + \cdots + (x^2+x) + b(x^2+x) \\ &= y^{2^{t-1}} + y^{2^{t-2}} + \cdots y^2 + y(b+1), \text{ with } y = x^2 + x. \end{aligned}$$

We are looking at the number of solutions of E_b which are not in $\mathbb{F}_2$. So, it is equivalent to compute the number of nonzero solutions y of

$$y^{2^{t-1}} + y^{2^{t-2}} + \cdots y^2 + y(b+1) = 0$$

such that the equation $x^2 + x + y = 0$ has solutions. This last condition holds if and only if $Tr(y) = 0$, providing two distinct solutions $x_1, x_2 = x_1 + 1$ such that $x_i^2 + x_i = y$, completing the proof. ∎

Remark 2: In Theorem 3, b takes any value while P_b is defined for $b \neq 1$ in Theorem 1. For all $b \neq 1$, we have clearly $N_b = \delta(b)$. If $b = 1$, $P_1(x) = x^{2^t} + x^2$ and the number of roots of P_1 in $\mathbb{F}_{2^n}$ is equal to

$$N_1 + 2 = 2^{\gcd(t-1,n)} = \delta(1).$$

Therefore, we have $M_1 = \frac{\delta(1)}{2} - 1$.

IV. Property of Symmetry

Recall that $G_t(x) = x^{2^t - 1}$. Now, we are going to examine some symmetries between the differential spectra of G_t and G_s where $t, s \ge 2$ and $s = n - t + 1$. In the list of properties below, notation is conserved as soon it is defined. Recall that

$$P^*_{t,b}(x) = x^{2^s} + x^2(b+1)^2 + xb$$

is the adjoint polynomial of $P_{t,b}(x) = x^{2^t} + bx^2 + (b+1)x$. Thus, both polynomials have a kernel with the same dimension (see Lemma 2 and Theorem 2). It is worth noticing that this dimension is at least 1 since $P_{t,b}(0) = P_{t,b}(1) = 0$. In this section we want to prove the following theorem.

Theorem 4: For any ν with $2 \le \nu \le n-1$, we define

$$S^i_\nu = \{\, b \mid \dim Ker(P_{\nu,b}) = i \,\} \text{ with } 1 \le i \le \nu \,.$$

Then, for any $s, t \ge 2$ with $t = n - s + 1$ and for any i, we have $\#S^i_s = \#S^i_t$.

We begin by proving two lemmas.

Lemma 3: Let $s, t \ge 2$ with $t = n - s + 1$. Let π be the permutation of $\mathbb{F}^*_{2^n} \times \mathbb{F}_{2^n}$ defined by

$$\pi(a,b) = \left(a^{2^s}, \frac{ab}{a^{2^s}} + 1 \right) .$$

Then, for any (a,b) in $\mathbb{F}^*_{2^n} \times \mathbb{F}_{2^n}$, $(\alpha, \beta) = \pi(a,b)$ satisfies

$$P^*_{s,\beta}(\alpha) = P^*_{t,b}(a) \,.$$

Proof: First, we clearly have that π is a permutation of $\mathbb{F}^*_{2^n} \times \mathbb{F}_{2^n}$. Indeed, $\pi\left(\mathbb{F}^*_{2^n} \times \mathbb{F}_{2^n}\right) \subset \mathbb{F}^*_{2^n} \times \mathbb{F}_{2^n}$ and one can define the inverse of π as follows:

$$\pi^{-1}(\alpha,\beta) = \left(\alpha^{2^{n-s}}, \frac{\alpha(\beta+1))}{\alpha^{2^{n-s}}} \right) .$$

Actually, $(\alpha^{2^{n-s}})^{2^s} = \alpha$ and it can be checked that

$$\pi(\pi^{-1}(\alpha,\beta)) = \left(\alpha, \frac{\alpha^{2^{n-s}} \alpha(\beta+1)}{\alpha \alpha^{2^{n-s}}} + 1 \right) = (\alpha, \beta).$$

Then, by using that $(\beta+1)^2 = \frac{a^2 b^2}{a^{2^{s+1}}}$ and $s + t = n + 1$, we deduce that

$$\begin{aligned} P^*_{s,\beta}(\alpha) &= (a^{2^s})^{2^t} + (a^{2^s})^2 (\beta+1)^2 + (a^{2^s})\beta \\ &= a^2 + a^2 b^2 + ab + a^{2^s} \\ &= P^*_{t,b}(a) \,. \end{aligned}$$

∎

Lemma 4: Let $s, t \ge 2$ with $t = n - s + 1$. Let $b \in \mathbb{F}_{2^n}$ and let $a \in \mathbb{F}^*_{2^n}$ such that $P^*_{t,b}(a) = 0$. Then $\dim Ker(P^*_{t,b}) = \dim Ker(P^*_{s,\beta})$, where $\beta = 1 + ab/a^{2^s}$.

Proof: Recall that $P^*_{t,b}(x) = x^{2^s} + x^2(b+1)^2 + xb$. We know that for any $b \notin \mathbb{F}_2$ there is $a \in \mathbb{F}_{2^n} \setminus \{0,1\}$ such that $P^*_{t,b}(a) = 0$. This is because $\dim Ker(P_{t,b}) = \dim Ker(P^*_{t,b})$ (see Theorem 2) and $\{0,1\}$ is included in the kernel of $P_{t,b}$. Moreover, $P^*_{t,b}(1) = b^2 + b = 0$ if and only if $b \in \mathbb{F}_2$.

We treat the case $a = 1$ separately, a case where $P^*_{t,b}(a) = 0$ for $b \in \mathbb{F}_2$ only. In this case, Lemma 3 leads to $P^*_{s,\beta}(1) = 0$ too where $\beta = b + 1$, since $\pi(1, b) = (1, b + 1)$. And we have for $b = 0$

$$P^*_{t,0}(x) = x^{2^s} + x^2 = P_{s,1}(x)$$

and for $b = 1$

$$P^*_{t,1}(x) = x^{2^s} + x = P_{s,0}(x).$$

Thus, we conclude: for $a = 1$, if b is such that $P^*_{t,b}(1) = 0$ then $\beta = b + 1$ and $\dim Ker(P^*_{t,b}) = \dim Ker(P_{s,\beta}) = \dim Ker(P^*_{s,\beta})$ where the last equality comes from Theorem 2.

Now, we suppose that $a \notin \mathbb{F}_2$. With $x = ay$, the equation $P^*_{t,b}(x) = 0$ is equivalent to

$$a^{2^s} y^{2^s} + a^2 y^2 (b+1)^2 + ayb = 0$$

which is

$$a^{2^s}\left(y^{2^s} + \frac{a^2(b+1)^2}{a^{2^s}} y^2 + y\frac{ab}{a^{2^s}}\right) = 0.$$

We can set

$$\beta = \frac{a^2(b+1)^2}{a^{2^s}} \text{ and } \beta + 1 = \frac{ab}{a^{2^s}}$$

since

$$\frac{a^2(b+1)^2}{a^{2^s}} + 1 = \frac{ab}{a^{2^s}}$$

is equivalent to

$$a^{2^s} + a^2(b+1)^2 + ab = 0, \ i.e., P^*_{t,b}(a) = 0.$$

We have proved that $P^*_{t,b}(x) = 0$ is equivalent to

$$P_{s,\beta}(y) = y^{2^s} + \beta y^2 + (\beta+1)y = 0.$$

Therefore, $\dim Ker(P_{s,\beta}) = \dim Ker(P^*_{t,b})$. But $\dim Ker(P_{s,\beta}) = \dim Ker(P^*_{s,\beta})$, by Theorem 2, completing the proof. ∎

Proof of Theorem 4: Recall that

$$S^i_\nu = \{ \ b \in \mathbb{F}_{2^n} \mid \dim Ker(P_{\nu,b}) = i \ \} \ .$$

Then, we want to show that, for any i, $\#S^i_t = \#S^i_s$. For any $2 \le \nu \le n-1$ and for any $1 \le i \le \nu$, we define

$$\mathcal{E}^i_\nu = \{(a,b) \in \mathbb{F}^*_{2^n} \times \mathbb{F}_{2^n} | P^*_{\nu,b}(a) = 0, \ \dim Ker(P_{\nu,b}) = i\}.$$

From Theorem 2, we know that $\dim Ker(P_{\nu,b}) = \dim Ker(P^*_{\nu,b})$. Then

$$\mathcal{E}^i_\nu = \{(a,b) \in \mathbb{F}^*_{2^n} \times \mathbb{F}_{2^n} | P^*_{\nu,b}(a) = 0, \ \dim Ker(P^*_{\nu,b}) = i\}.$$

For any $b \in S^i_\nu$ there are $2^i - 1$ nonzero a in $Ker(P^*_{\nu,b})$ and then $2^i - 1$ pairs (a,b), for a fixed b, in $\mathcal{E}^i_\nu$ so that

$$\#\mathcal{E}^i_\nu = (2^i - 1)\#S^i_\nu \ . \tag{5}$$

We use Lemma 3. Recall that π is the permutation of $\mathbb{F}^*_{2^n} \times \mathbb{F}_{2^n}$ defined by

$$\pi(a,b) = \left(a^{2^s}, \frac{ab}{a^{2^s}} + 1\right).$$

Then, we have

$$\begin{aligned}
\mathcal{E}^i_t &= \{(a,b) \in \mathbb{F}^*_{2^n} \times \mathbb{F}_{2^n} | P^*_{t,b}(a) = 0, \dim Ker(P^*_{t,b}) = i\} \\
\mathcal{E}^i_s &= \{(\alpha,\beta) \in \mathbb{F}^*_{2^n} \times \mathbb{F}_{2^n} | P^*_{s,\beta}(\alpha) = 0, \dim Ker(P^*_{s,\beta}) = i\} \\
&= \{(\alpha,\beta) = \pi(a,b), (a,b) \in \mathcal{E}^i_t\} \ .
\end{aligned}$$

Indeed, any (α, β) is as follows specified from (a,b). We have $P^*_{s,\beta}(\alpha) = P^*_{t,b}(a)$ from Lemma 3. Moreover, according to Lemma 4, $\dim Ker(P^*_{t,b}) = \dim Ker(P^*_{s,\beta})$, where β is calculated from a and b, for any a such that $P^*_{t,b}(a) = 0$.

In other terms, to any pair $(a,b) \in \mathcal{E}^i_t$ corresponds a unique pair $(\alpha,\beta) \in \mathcal{E}^i_s$. We finally get that $\#\mathcal{E}^i_s = \#\mathcal{E}^i_t$ and it directly follows from (5) that $\#S^i_s = \#S^i_t$, completing the proof. ∎

Now we are going to explain Theorem 4, in terms of the differential spectra of G_t and G_s, $s,t \ge 2$ with $t = n - s + 1$. Actually, we can deduce from the previous theorem that both functions G_t and G_s have the same restricted differential spectrum, *i.e.,* the multisets $\{\delta(b), b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2\}$ are the same for both functions.

Corollary 2: We denote by $\delta_\nu(b)$, $b \in \mathbb{F}_{2^n}$, the quantities $\delta(b)$ corresponding to $G_\nu : x \mapsto x^{2^\nu - 1}$. Then, for any $s,t \ge 2$ with $t = n - s + 1$, we have

$$\begin{aligned}
\delta_s(0) &= \delta_t(1) - 2 = 2^{\gcd(t-1,n)} - 2 \\
\delta_s(1) &= \delta_t(0) + 2 = 2^{\gcd(t,n)}
\end{aligned}$$

and we have equality between both following multisets:

$$\{\delta_s(b), b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2\} = \{\delta_t(b), b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2\} \tag{6}$$

implying that G_t is locally-APN if and only if G_s is locally-APN (in the sense of Definition 4). Moreover, G_t and G_s have the same differential spectrum if and only if

$$\gcd(s,n) = \gcd(t,n) = 1$$

which can hold for odd n only.

Proof: Since $s = n - t + 1$, we clearly have

$$\gcd(s,n) = \gcd(t-1,n) \text{ and } \gcd(s-1,n) = \gcd(t,n).$$

Thus, applying Theorem 1, we get

$$\delta_s(0) = 2^{\gcd(s,n)} - 2 = 2^{\gcd(t-1,n)} - 2 = \delta_t(1) - 2$$

and

$$\delta_s(1) = 2^{\gcd(s-1,n)} = 2^{\gcd(t,n)} = \delta_t(0) + 2.$$

Moreover, we have

$$\begin{aligned}(P_{t,1}(x))^{2^{s-1}} &= \left(x^{2^t} + x^2\right)^{2^{s-1}} = x + x^{2^s} = P_{s,0}(x)\\ (P_{t,0}(x))^{2^s} &= \left(x^{2^t} + x\right)^{2^s} = x^{2^s} + x^2 = P_{s,1}(x)\end{aligned}$$

implying that $\{\dim Ker(P_{t,0}), \dim Ker(P_{t,1})\}$ is equal to $\{\dim Ker(P_{s,0}), \dim Ker(P_{s,1})\}$. We deduce from Theorem 4 that

$$\begin{aligned}&\#\{\, b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2 \mid \dim Ker(P_{t,b}) = i \,\}\\ &= \#\{\, b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2 \mid \dim Ker(P_{s,b}) = i \,\}.\end{aligned}$$

Equality (6) is then a direct consequence of Theorem 1, since

$$\{\delta_\nu(b), b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2\} = \{2^{\kappa(b)} - 2, \kappa(b) = \dim Ker(P_{\nu,b})\}.$$

Now, we note that $\delta_s(0) = \delta_t(0)$ if and only if $\delta_s(1) = \delta_t(1)$. Thus, G_t and G_s have the same differential spectrum if and only if $\delta_s(0) = \delta_t(0)$. Since

$$\delta_s(0) = 2^{\gcd(s,n)} - 2 \text{ and } \delta_t(0) = 2^{\gcd(t,n)} - 2$$

this holds if and only if $\gcd(t,n) = \gcd(s,n) = 1$. It cannot hold when n is even, because in this case either s or t is even too.

Using Definition 4, the last statement is obviously derived. ■

The previous result implies that, if G_t is APN over $\mathbb{F}_{2^n}$, then G_s is locally-APN. Moreover, the differential spectrum of G_s can be completely determined as shown by the following corollary.

Corollary 3: Let n and $t < n$ be two integers such that $G_t : x \mapsto x^{2^t-1}$ is APN over $\mathbb{F}_{2^n}$. Let $s = n - t + 1$. Then:

- if n is odd, both G_t and G_s are APN permutations;
- if n is even, G_t is not a permutation and G_s is a differentially 4-uniform permutation (locally-APN) with the following differential spectrum: $\omega_4 = 1$, $\omega_2 = 2^{n-1} - 2$ and $\omega_0 = 2^{n-1} + 1$.

Proof: From Theorem 1, we deduce that, if F is APN, then $\delta_t(b) \in \{0, 2\}$ for all $b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$; moreover, $\gcd(n, t-1) = 1$ and $\gcd(n,t) \in \{1, 2\}$ since $\delta_t(1) = 2$ and $\delta_t(0) \in \{0, 2\}$.

If n is odd, $\gcd(n,t) = 1$ is then the only possible value, implying that $\delta_t(0) = 0$. It follows that $\delta_s(0) = 0$, $\delta_s(1) = 2$ and $\delta_s(b) \in \{0, 2\}$ for all $b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$. In other words, both G_t and G_s are APN permutations.

If n is even, it is well-known that G_t is not a permutation (see, e.g., [2]). More precisely, we have here $\gcd(n,t) = 2$ since t and $t-1$ cannot be both coprime with n. Then, we deduce that $\delta_s(0) = 0$ and $\delta_s(1) = 4$. The differential spectrum of G_s directly follows from Corollary 2. ■

Example 1: Notation is as in Corollary 3. For $t = 2$, we have $G_t(x) = x^3$. It is well-known that G_2 is an APN function over $\mathbb{F}_{2^n}$ for any n. Since $s = n - 1$, $G_s(x)$ is equivalent to the inverse function and it is also well-known that the inverse function is APN for odd n. For even n, $\delta(G_{n-1}) = 4$ and the differential spectrum is computed in Remark 1.

Corollary 4: Let n and $t < n$ be two integers such that $G_t : x \mapsto x^{2^t-1}$ is differentially 4-uniform. Then, n is even and G_t is a permutation with the following differential spectrum: $\omega_4 = 1$, $\omega_2 = 2^{n-1} - 2$ and $\omega_0 = 2^{n-1} + 1$. Moreover, for $s = n - t + 1$, G_s is APN.

Proof: From Corollary 1, we deduce that $\delta(G_t) = 4$ implies $\gcd(n, t-1) = 2$ and $\omega_4 = 1$. In particular, n is even. Since $\gcd(n, t-1)$ and $\gcd(n,t)$ cannot be both equal to 2, we also deduce that that G_t is a permutation. Its differential spectrum is then derived from (2). Moreover, we have $\delta_s(0) = 2$ and $\delta_s(1) = 2$, implying that G_s is APN. ■

V. Specific Classes

In this section, we apply the results of Section III to the study of the differential spectrum of $G_t : x \mapsto x^{2^t-1}$, for special values of t.

A. Function $x \mapsto x^7$

We first focus on $G_3 : x \mapsto x^7$ over $\mathbb{F}_{2^n}$, *i.e.*, $t = 3$. In this case, we determine the complete differential spectrum of the function. Actually, we show that this differential spectrum is related to some Kloosterman sum, which has an explicit expression found by Carlitz [13].

Definition 5: Let $K(1)$ be the Kloosterman sum

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

extended to 0 assuming that $(-1)^{Tr(x^{-1})} = 1$ for $x = 0$.

Theorem 5: Let $G_3 : x \mapsto x^7$ over $\mathbb{F}_{2^n}$ with $n \geq 2$. Then, its differential spectrum is given by:

- If n is odd

$$\begin{aligned}\omega_6 &= \frac{2^{n-2}+1}{6} - \frac{K(1)}{8}\\ \omega_4 &= 0\\ \omega_2 &= 2^{n-1} - 3\omega_6\\ \omega_0 &= 2^{n-1} + 2\omega_6.\end{aligned}$$

- If n is even

$$\begin{aligned}\omega_6 &= \frac{2^{n-2}-4}{6} + \frac{K(1)}{8}\\ \omega_4 &= 1\\ \omega_2 &= 2^{n-1} - 3\omega_6 - 2\\ \omega_0 &= 2^{n-1} + 2\omega_6 + 1.\end{aligned}$$

where $K(1)$ is the Kloosterman sum defined as in Definition 5. In particular, G_3 is differentially 6-uniform for all $n \geq 6$.

Remark 3: An explicit formula for $K(1)$ is due to Carlitz [13, Formula (6.8)] for $n \geq 3$

$$K(1) = 1 + \frac{(-1)^{n-1}}{2^{n-1}} \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^i \binom{n}{2i} 7^i.$$

To prove this theorem, we need some preliminary results. We first recall some basic results on cubic equations.

Lemma 5: [3] The cubic equation $x^3 + ax + b = 0$, where $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}^*$ has a unique solution in $\mathbb{F}_{2^n}$ if and only if $Tr(a^3/b^2) \neq Tr(1)$. In particular, if it has three distinct roots in $\mathbb{F}_{2^n}$, then $Tr(a^3/b^2) = Tr(1)$.

Proposition 2: [20, Appendix] Let $f_a(x) = x^3 + x + a$ and

$$M_i = \#\{\, a \in \mathbb{F}_{2^n}^* \mid f_a(x) = 0 \text{ has } i \text{ solutions in } \mathbb{F}_{2^n} \,\}.$$

Then, we have for odd $n > 1$

$$M_0 = \frac{2^n + 1}{3},\ M_1 = 2^{n-1} - 1,\ M_3 = \frac{2^{n-1} - 1}{3}$$

and for even n

$$M_0 = \frac{2^n - 1}{3},\ M_1 = 2^{n-1},\ M_3 = \frac{2^{n-1} - 2}{3}.$$

Now we are going to solve the equations $P_b(x) = 0$ (see Theorem 1) by solving a system of equations, including a cubic equation, thanks to the equivalence presented in Theorem 3.

Theorem 6: Let $n \geq 2$ and

$$P_b(x) = x^8 + bx^2 + (b+1)x,\ b \in \mathbb{F}_{2^n} \setminus \{1\}.$$

The number ν_0 of $b \in \mathbb{F}_{2^n} \setminus \{1\}$ such that P_b has no roots in $\mathbb{F}_{2^n} \setminus \{0,1\}$ is given by

$$\nu_0 = \frac{2^n + (-1)^{n+1}}{3} + 2^{n-2} + (-1)^n \frac{K(1)}{4}$$

where $K(1)$ is the Kloosterman sum defined as in Definition 5.

Proof: Let $b \in \mathbb{F}_{2^n} \setminus \{1\}$ with $n \geq 4$. According to Theorem 3 we know that the number (denoted by N_b) of roots in $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$ of P_b is twice the number of roots in $\mathbb{F}_{2^n}^*$ of the following system where $\beta = b + 1$

$$\begin{cases} Q_\beta(y) &= y^3 + y + \beta = 0 \\ Tr(y) &= 0. \end{cases} \tag{7}$$

Since $\beta \neq 0$, $Q_\beta(y) \neq 0$ for $y \in \mathbb{F}_2$. Then, for any $\beta \neq 0$, the following situations may occur:

- Q_β has no root in $\mathbb{F}_{2^n}$. In this case, $N_b = 0$.
- Q_β has a unique root $y \in \mathbb{F}_{2^n}$. From Lemma 5, this occurs if and only if $Tr(\beta^{-1}) \neq Tr(1)$. In this case, $N_b = 0$ if $Tr(y) = 1$ and $N_b = 2$ if $Tr(y) = 0$.
- Q_β has three roots $y_1, y_2, y_3 \in \mathbb{F}_{2^n}$. Since these roots are roots of a linear polynomial of degree 4 then $y_3 = y_1 + y_2$, implying $Tr(y_3) = Tr(y_1) + Tr(y_2)$. Then, at least one y_i is such that $Tr(y_i) = 0$. It follows that, in this case, N_b is either 6 or 2.

Let us define B as the cardinality of

$$\{\beta \in \mathbb{F}_{2^n}^*,\ Q_\beta \text{ has a unique root } y \in \mathbb{F}_{2^n} \text{ and } Tr(y) = 1\}.$$

From the previous discussion, we have

$$\begin{aligned}\nu_0 &= \#\{\beta \in \mathbb{F}_{2^n}^*,\ \ Q_\beta \text{ has no root in } \mathbb{F}_{2^n}\} + B \\ &= \frac{2^n + (-1)^{n+1}}{3} + B\end{aligned}$$

where the last equality comes from Proposition 2. Let us now compute the value of B.

$$\begin{aligned}B = \#\{&(y^3 + y) \in \mathbb{F}_{2^n}^*,\ \ Tr\left(\frac{1}{y^3 + y}\right) \neq Tr(1) \\ &\text{and } Tr(y) = 1\}\end{aligned}$$

by using that $\beta = y^3 + y$. But, we have

$$\frac{1}{y^3+y} = \frac{1+y^2}{y^3+y} + \frac{y^2+y}{y^3+y} + \frac{y}{y^3+y} = \frac{1}{y} + \frac{1}{y+1} + \frac{1}{y^2+1}$$

implying that

$$Tr\left(\frac{1}{y^3+y}\right) = Tr\left(\frac{1}{y}\right).$$

Therefore

$$B = \#\{(y^3 + y) \in \mathbb{F}_{2^n}^*,\ Tr\left(\frac{1}{y}\right) \neq Tr(1) \text{ and } Tr(y) = 1\}.$$

Now, we clearly have that $(y^3 + y) = 0$ if and only if $y \in \mathbb{F}_2$. Moreover, two distinct elements y_1 and y_2 in $\mathbb{F}_{2^n} \setminus \mathbb{F}_2$ with $Tr(y_1^{-1}) \neq Tr(1)$ and $Tr(y_2^{-1}) \neq Tr(1)$ satisfy $(y_1^3 + y_1) \neq (y_2^3 + y_2)$ (otherwise, Q_β with $\beta = y_1^3 + y_1$ has at least 2 roots in $\mathbb{F}_{2^n}$). Therefore, we deduce that

$$B = \#\{y \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2,\ \ Tr\left(\frac{1}{y}\right) \neq Tr(1) \text{ and } Tr(y) = 1\}.$$

If n is odd, we deduce that

$$B = \#\{y \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2,\ \ Tr\left(\frac{1}{y}\right) = 0 \text{ and } Tr(y) = 1\}.$$

If n is even, we deduce that

$$\begin{aligned}B &= \#\{y \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2,\ \ Tr\left(\frac{1}{y}\right) = 1 \text{ and } Tr(y) = 1\} \\ &= \#\{y \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2, Tr(y) = 1\} - \#\{y \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2 \\ &\qquad Tr\left(\frac{1}{y}\right) = 0 \text{ and } Tr(y) = 1\} \\ &= 2^{n-1} - \#\{y \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2,\ \ Tr\left(\frac{1}{y}\right) = 0 \\ &\qquad \text{and } Tr(y) = 1\}\ .\end{aligned}$$

On the other hand, by definition of the Kloosterman sum $K(1)$, we have

$$\begin{aligned}K(1)-2 &= \sum_{x\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2}(-1)^{Tr(x^{-1}+x)}\\ &= -2\#\{x\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2, Tr(x^{-1}+x)=1\}+2^n-2\\ &= -4\#\{x\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2,\ Tr(x^{-1})=0\\ &\qquad \text{and } Tr(x)=1\}+2^n-2.\end{aligned}$$

Thus

$$\#\{x\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2, Tr(x^{-1})=0 \text{ and } Tr(x)=1\}=2^{n-2}-\frac{K(1)}{4}.$$

We then deduce that, for any n

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

It follows that

$$\nu_0=\frac{2^n+(-1)^{n+1}}{3}+2^{n-2}+(-1)^n\frac{K(1)}{4}.$$

It can be checked that this formula also holds for $n=2$ (resp. $n=3$) since $K(1)=4$ (resp. $K(1)=-4$). ■

Proof of Theorem 5: In accordance with (2), we obtain the differential spectrum of G_3 as soon as we are able to solve the following system:

$$\begin{aligned}\omega_0+\omega_2+\omega_4+\omega_6 &= 2^n\\ 2\omega_2+4\omega_4+6\omega_6 &= 2^n.\end{aligned} \tag{8}$$

Now, we apply Theorem 1 and we recall first that $\delta(b)\in\{0,2,6\}$ for any $b\in\mathbb{F}_{2^n}\setminus\{1\}$. Moreover, we know that $\omega_0=\nu_0$ as defined in Theorem 6.

Since $t=3$, $\gcd(t-1,n)$ equals 1 for odd n and 2 otherwise. Then, if n is even then $\delta(1)=4$ else $\delta(1)=2$. Thus, $\omega_4=1$ for even n and $\omega_4=0$ otherwise. From the second equation of (8), we get

$$\omega_2=2^{n-1}-3\omega_6-2\omega_4$$

and using the first equation of (8)

$$\omega_6=2^n-\omega_0-\omega_2-\omega_4=2^{n-1}-\omega_0+\omega_4+3\omega_6$$

leading to

$$\omega_6=-2^{n-2}+\frac{\omega_0-\omega_4}{2}.$$

Finally, we deduce from Theorem 6 that, for odd n

$$\begin{aligned}\omega_6 &= -2^{n-2}+\frac{\omega_0}{2}=-2^{n-3}+\frac{2^n+1}{6}-\frac{K(1)}{8}\\ &=\frac{2^{n-2}+1}{6}-\frac{K(1)}{8}\end{aligned}$$

and for even n

$$\begin{aligned}\omega_6 &= -2^{n-2}+\frac{\omega_0-1}{2}=-2^{n-3}+\frac{2^n-1}{6}+\frac{K(1)}{8}-\frac{1}{2}\\ &=\frac{2^{n-2}-4}{6}+\frac{K(1)}{8}.\end{aligned}$$

Finally, it can be proved that $\omega_6\geq 1$ for any $n\geq 6$, implying that G_3 is differentially 6-uniform. Actually, it has been proved in [21, Th. 3.4] that

$$-2^{\frac{n}{2}+1}+1\leq K(1)\leq 2^{\frac{n}{2}+1}+1$$

implying that $\omega_6>0$ when $n>5$. It is worth noticing that G_3 is APN when $n=5$ since its inverse is the quadratic APN permutation $x\mapsto x^9$. When $n=4$, G_3 is locally-APN, and not APN, since it corresponds to the inverse function over $\mathbb{F}_{2^4}$. ■

By combining the previous theorem and Corollary 2, we deduce the differential spectrum of $G_{n-2}: x\mapsto x^{2^{n-2}-1}$ over $\mathbb{F}_{2^n}$.

Corollary 5: Let $G_{n-2}: x\mapsto x^{2^{n-2}-1}$ over $\mathbb{F}_{2^n}$ with $n\geq 6$. Then, we have:

- If $\gcd(n,3)=1$, G_{n-2} is differentially 6-uniform and for any $b\in\mathbb{F}_{2^n}$, $\delta(b)\in\{0,2,6\}$. Moreover, its differential spectrum is given by:

$$\begin{aligned}\omega_6 &= \begin{cases}\frac{2^{n-2}+1}{6}-\frac{K(1)}{8}, & \text{for odd } n\\ \frac{2^{n-2}-4}{6}+\frac{K(1)}{8}, & \text{for even } n\end{cases}\\ \omega_2 &= 2^{n-1}-3\omega_6\\ \omega_0 &= 2^{n-1}+2\omega_6.\end{aligned}$$

- If 3 divides n, G_{n-2} is differentially 8-uniform and for any $b\in\mathbb{F}_{2^n}$, $\delta(b)\in\{0,2,6,8\}$. Moreover, its differential spectrum is given by

$$\begin{aligned}\omega_8 &= 1\\ \omega_6 &= \begin{cases}\frac{2^{n-2}-5}{6}-\frac{K(1)}{8}, & \text{for odd } n\\ \frac{2^{n-2}-10}{6}+\frac{K(1)}{8}, & \text{for even } n\end{cases}\\ \omega_2 &= 2^{n-1}-3\omega_6-4\\ \omega_0 &= 2^{n-1}+2\omega_6+3.\end{aligned}$$

Proof: Let $(\omega_0',\omega_2',\omega_4',\omega_6')$ denote the differential spectrum of G_3 over $\mathbb{F}_{2^n}$. We apply Corollary 2 (with $s=3$). Then, if $\gcd(3,n)=1$, $\delta_3(0)=0$ and $\delta_{n-2}(1)=2$. Otherwise, $\delta_3(0)=6$ and $\delta_{n-2}(1)=8$. Moreover, in both cases, $\delta_3(1)=4$ for n even and $\delta_3(1)=2$ for n odd. It follows that:

- For $\gcd(3,n)=1$, n odd, we have $(\delta_3(0),\delta_3(1))=(0,2)$ and $(\delta_{n-2}(0),\delta_{n-2}(1))=(0,2)$. Then, $\omega_i=\omega_i'$ for all i.
- For $\gcd(3,n)=1$, n even, we have $(\delta_3(0),\delta_3(1))=(0,4)$ and $(\delta_{n-2}(0),\delta_{n-2}(1))=(2,2)$. Then, $\omega_0=\omega_0'-1$, $\omega_4=\omega_4'-1$ and $\omega_2=\omega_2'+2$.
- For $\gcd(3,n)=3$, n odd, we have $(\delta_3(0),\delta_3(1))=(6,2)$ and $(\delta_{n-2}(0),\delta_{n-2}(1))=(0,8)$. Then, $\omega_8=1$, $\omega_6=\omega_6'-1$, $\omega_2=\omega_2'-1$ and $\omega_0=\omega_0'+1$.

- For $\gcd(3,n)=3$, n even, we have $(\delta_3(0),\delta_3(1))=(6,4)$ and $(\delta_{n-2}(0),\delta_{n-2}(1))=(2,8)$. Then, $\omega_8=1$, $\omega_6=\omega'_6-1$, $\omega_4=\omega'_4-1$, $\omega_2=\omega'_2+1$ and $\omega_0=\omega'_0$.

The result finally follows from Theorem 5. ■

B. Exponents $2^{\lfloor n/2 \rfloor}-1$

We are going to determine the differential uniformity of G_t for $t=\lfloor n/2 \rfloor$. We first consider the case where n is even. Note that in this case, G_t is not a permutation since $2^n-1=(2^t-1)(2^t+1)$.

Theorem 7: Let n be an even integer, $n>4$ and $G_t(x)=x^{2^t-1}$ for $t=\frac{n}{2}$. Then G_t is locally-APN. More precisely

$$\delta(G_t)=2^t-2 \text{ and } \delta(b)\le 2,\ \forall\, b\in \mathbb{F}_{2^n}\setminus\mathbb{F}_2.$$

Moreover, the differential spectrum of G_t is:
- If $n\equiv 0 \bmod 4$, then

$$\begin{aligned}\omega_{2^t-2}&=1\\ \omega_i&=0,\ \forall\, i,\ 2<i<2^t-2\\ \omega_2&=2^{n-1}-2^{t-1}+1\\ \omega_0&=2^{n-1}+2^{t-1}-2.\end{aligned}$$

- If $n\equiv 2 \bmod 4$

$$\begin{aligned}\omega_{2^t-2}&=1\\ \omega_i&=0,\ \forall\, i,\ 4<i<2^t-2\\ \omega_4&=1\\ \omega_2&=2^{n-1}-2^{t-1}-1\\ \omega_0&=2^{n-1}+2^{t-1}-1.\end{aligned}$$

Proof: From Theorem 1, we obtain directly $\delta(0)=2^t-2$. Also, $\delta(1)=2$ if t is even and $\delta(1)=4$ otherwise.

Now, for all $b\notin\mathbb{F}_2$, we have to determine the number of roots in $\mathbb{F}_{2^n}$ of $P_b(x)=x^{2^t}+bx^2+(b+1)x$ or, equivalently, the number of roots of

$$\left(P_b(x)\right)^{2^t}=x+b^{2^t}x^{2^{t+1}}+(b+1)^{2^t}x^{2^t}.$$

If x is a root of P_b then $x^{2^t}=bx^2+(b+1)x$. So, $P_b(x)=0$ implies

$$\begin{aligned}\left(P_b(x)\right)^{2^t}&=x+b^{2^t}(x^{2^t})^2+(b^{2^t}+1)x^{2^t}\\ &=x+b^{2^t}(bx^2+(b+1)x)^2\\ &\quad+(b^{2^t}+1)(bx^2+(b+1)x)\\ &=b^{2^t+2}x^4+(b^{2^t+2}+b^{2^t+1}+b^{2^t}+b)x^2\\ &\quad+(b^{2^t+1}+b^{2^t}+b)x.\end{aligned}$$

Thus, we get a linear polynomial of degree 4 which has at least the roots 0 and 1. Hence, this polynomial has τ roots where τ is either 4 or 2, including $x=0$ and $x=1$. Therefore, for any $b\notin\mathbb{F}_2$, $\delta(b)\le 2$ since $\delta(b)\le\tau-2$. We deduce that G_t is locally-APN.

We also proved that $\omega_i=0$ unless $i\in\{0,2,2^t-2\}$ when t is even and $i\in\{0,2,4,2^t-2\}$ otherwise. Moreover $\omega_{2^t-2}=\omega_4=1$. According to (2), we have for t even

$$2^n=\omega_0+\omega_2+\omega_{2^t-2}=\omega_0+\omega_2+1$$

and

$$2^n=2\omega_2+(2^t-2)\omega_{2^t-2}=2\omega_2+(2^t-2).$$

So, we get $\omega_2=2^{n-1}-2^{t-1}+1$ and conclude with $\omega_0=2^n-\omega_2-1$. We proceed similarly for odd t, with the following equalities derived from (2)

$$2^n=\omega_0+\omega_2+2 \text{ and } 2^n=2\omega_2+2^t+2$$

■

and we directly deduce a property on the corresponding class of linear polynomials.

Corollary 6: Let $n=2t$ and consider the polynomials over $\mathbb{F}_{2^n}$

$$x^{2^t}+bx^2+(b+1)x \text{ and } x^{2^{t+1}}+bx^2+(b+1)x.$$

Then, for any $b\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2$, these polynomials have either 2 or 4 roots in $\mathbb{F}_{2^n}$.

According to Corollary 2, the differential spectrum of $x\mapsto x^{2^{\frac{n}{2}}-1}$ determines the differential spectrum of $x\mapsto x^{2^{\frac{n}{2}+1}-1}$

Theorem 8: Let n be an even integer $n>4$ and $G_{t+1}(x)=x^{2^{t+1}-1}$ for $t=\frac{n}{2}$. Then, G_{t+1} is locally-APN. It is differentially 2^t-uniform and its differential spectrum is

$$\begin{aligned}\omega_{2^t}&=1\\ \omega_i&=0,\ \forall\, i,\ 2<i<2^t\\ \omega_2&=2^{n-1}-2^{t-1}\\ \omega_0&=2^{n-1}+2^{t-1}-1\ .\end{aligned}$$

Moreover, G_{t+1} is a permutation if and only if $n\equiv 0 \bmod 4$.

Proof: First, since $n=2t$, we have $\gcd(t+1,n)=1$ if t is even (*i.e.*, $n\equiv 0 \bmod 4$) and $\gcd(t+1,n)=2$ if t is odd (*i.e.*, $n\equiv 2 \bmod 4$). Here $s=t+1$.

Let $(\omega'_i)_{0\le i\le 2^n}$ (resp. $(\omega_i)_{0\le i\le 2^n}$) denote the differential spectrum of G_t (resp. G_{t+1}) over $\mathbb{F}_{2^n}$.
- For $n\equiv 0 \bmod 4$, we have $(\delta_t(0),\delta_t(1))=(2^t-2,2)$ and $(\delta_s(0),\delta_s(1))=(0,2^t)$. Thus, $\omega_0=\omega'_0+1$, $\omega_2=\omega'_2-1$, $\omega_{2^t-2}=\omega'_{2^t-2}-1$ and $\omega_{2^t}=1$.
- For $n\equiv 2 \bmod 4$, we have $(\delta_t(0),\delta_t(1))=(2^t-2,4)$ and $(\delta_s(0),\delta_s(1))=(2,2^t)$. Thus, $\omega_2=\omega'_2+1$, $\omega_4=\omega'_4-1$, $\omega_{2^t-2}=\omega'_{2^t-2}-1$ and $\omega_{2^t}=1$.

The differential spectrum of G_{t+1} is then directly deduced by combining the previous formulas with the values of ω'_i computed in Theorem 7. ■

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

Theorem 9: Let n be an odd integer, $n > 3$. Let $G_t(x) = x^{2^t-1}$ with $t = (n-1)/2$. Then, G_t is a permutation and for all $b \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$ we have $\delta(b) \in \{0, 2, 6\}$. Moreover:

- If $n \equiv 0 \bmod 3$, then $\delta(G_t) = 8$, 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 $\delta(G_t) \leq 6$ and the differential spectrum satisfies $\omega_i = 0$ for all $i \notin \{0, 2, 6\}$.

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

$$P_b(x) = x^{2^t} + bx^2 + (b+1)x$$

or, equivalently, the number of roots of

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

Set $c = b^{2^{t+1}}$ and $Q_b(x) = (P_b(x))^{2^{t+1}}$. If x is a root of P_b then $x^{2^t} = bx^2 + (b+1)x$. So, $P_b(x) = 0$ implies

$$\begin{aligned} Q_b(x) &= x + c(x^{2^t})^4 + (c+1)(x^{2^t})^2 \\ &= x + c(bx^2 + (b+1)x)^4 \\ &\quad + (c+1)(bx^2 + (b+1)x)^2 \\ &= cb^4x^8 + (c(b+1)^4 + (c+1)b^2)x^4 \\ &\quad + (c+1)(b^2+1)x^2 + x\,. \end{aligned}$$

Since Q_b has degree 8, it has either 8 or 4 or 2 solutions. In other terms, $\delta(b) \in \{0, 2, 6\}$. ■

VI. Conclusion

In this work, we point out that the family of all power functions

$$\{\, G_t : x \mapsto x^{2^t-1} \text{ over } \mathbb{F}_{2^n},\ 1 < t < n\} \tag{9}$$

has interesting differential properties. In particular, we give several results about the functions with a low differential uniformity within family (9). We exhibit some infinite classes of functions G_t such that $\delta(G_t) = 6$, including the functions G_3 over $\mathbb{F}_{2^n}$ (see Theorem 5). Moreover, our simulations show that, from $n > 16$, all power functions F with $4 \leq \delta(F) \leq 6$, which are not quadratic, Kasami or Bracken-Leander exponents (and their inverses), belong to family (9).

The functions such that $\delta(G_t) \leq 4$ can be differentially 4-uniform for even n only (see Corollary 4). We have shown that, for exponents of the form $2^t - 1$, the APN property imposes many conditions of the value of t. In particular, it is easy to prove, using Theorem 1 that such exponent must satisfy $\gcd(t, n) = 2$ for even n and $\gcd(t, n) = \gcd(t-1, n) = 1$ for odd n. Another condition can be derived from the recent result by Aubry and Rodier [1] who proved the following theorem.

Theorem 10: [1, Theorem 9] Let $G_t : x \mapsto x^{2^t-1}$ over $\mathbb{F}_{2^n}$ with $t \geq 3$. If $7 \leq 2^t - 1 < 2^{n/4} + 4.6$ then $\delta(G_t) > 4$.

Thanks to Corollary 2, we can extend this result as follows.

Corollary 7: Let $G_t : x \mapsto x^{2^t-1}$ over $\mathbb{F}_{2^n}$ with $3 \leq t \leq n-2$. If $\delta(G_t) \leq 4$, then

$$\log_2(2^{\frac{n}{4}} + 5.6) \leq t \leq n + 1 - \log_2(2^{\frac{n}{4}} + 5.6)\,.$$

Proof: Let $s = n - t + 1$ so that $3 \leq s \leq n-2$. In this proof, we denote by $\delta_t(b)$ (resp. $\delta_s(b)$) the quantities $\delta(b)$ corresponding to G_t (resp. G_s).

From Theorem 10, we know that $\delta(G_t) \leq 4$ implies

$$2^{n/4} + 4.6 \leq 2^t - 1,\ i.e, t \geq \log_2(2^{\frac{n}{4}} + 5.6).$$

We consider now the function G_s. Note that, from Theorem 1, $\delta(G_t) \leq 4$ implies $\delta_t(0) \in \{0, 2\}$ and $\delta_t(1) \in \{2, 4\}$. Moreover, we obtain directly from Corollary 2 :

- $\delta_s(b) \leq 4$, for any $b \notin \mathbb{F}_2$.
- $\delta_s(0) \in \{0, 2\}$ and $\delta_s(1) \in \{2, 4\}$.

Thus, $\delta(G_s) \leq 4$ and, applying Theorem 10 again, we get

$$s \geq \log_2(2^{\frac{n}{4}} + 5.6),\ \ i.e.,\ n + 1 - \log_2(2^{\frac{n}{4}} + 5.6) \geq t.$$

■

We now concentrate on APN functions belonging to the family (9). Some are well-known as the inverse permutation for n odd ($t = n-1$) and the quadratic function $x \mapsto x^3$ ($t = 2$). There is also the function G_t for $t = (n+1)/2$ with n odd, because this function is the inverse of the quadratic function $x \mapsto x^{2^{(n+1)/2}+1}$. Recall that x^{2^i+1} is an APN function over $\mathbb{F}_{2^n}$ if and only if $\gcd(n, i) = 1$ and we have obviously $\gcd(n, (n+1)/2) = 1$ (for odd n). We conjecture that these three functions are the only APN functions within family (9).

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

If the previous conjecture holds then there are some consequences for the functions of (9) which are differentially 4-uniform. From Corollary 4, we can say that such a function G_t is a function over $\mathbb{F}_{2^n}$ with n even. Moreover G_s, $s = n - t + 1$, is APN. If the conjecture holds then $s = 2$ ($t = n-1$) is the only one possibility. So, in this case we could conclude that the inverse function is the only one differentially 4-uniform function of family (9).

References

[1] Y. Aubry and F. Rodier, *Arithmetic, Geometry, Cryptography, and Coding Theory 2009,* ser. Contemporary Mathematics, vol. 521, AMS, 2010, pp. 1–8..

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

[3] E. Berlekamp, H. Rumsey, and G. Solomon, "On the solution of algebraic equations over finite fields," *Inf. Contr.*, vol. 12, no. 5, pp. 553–564, Oct. 1967.

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

[5] C. Blondeau, A. Canteaut, and P. Charpin, "Differential properties of power functions," *Int. J. Inf. Coding Theory*, vol. 1, no. 2, pp. 149–170, 2010.

[6] C. Blondeau, A. Canteaut, and P. Charpin, "Differential Properties of $x \mapsto x^{2^t-1}$ (Extended Version)," Research Rep. INRIA, RR-inria-00616674 [Online]. Available: http://www.inria.fr/rrrt/

[7] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "New families of quadratic almost perfect nonlinear trinomials and multinomials," *Finite Fields Appl.*, vol. 14, no. 3, pp. 703–714, 2008.

[8] C. Bracken and G. Leander, "A highly nonlinear differentially 4-uniform power mapping that permutes fields of even degree," *Finite Fields Appl.*, vol. 16, pp. 231–242, 2010.
[9] K. Browning, J. Dillon, M. McQuistan, and A. Wolfe, "An APN permutation in dimension six," in *Finite Fields: Theory and Applications – FQ9*. Providence, RI: AMS, 2010, vol. 518, Contemporary Mathematics, pp. 33–42.
[10] L. Budaghyan, C. Carlet, and A. Pott, "New classes of almost bent and almost perfect nonlinear polynomials," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 1141–1152, Mar. 2006.
[11] A. Canteaut, P. Charpin, and H. Dobbertin, "Binary m-sequences with three-valued crosscorrelation: A proof of Welch conjecture," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 4–8, Jan. 2000.
[12] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Designs, Codes, Cryptogr.*, vol. 15, no. 2, pp. 125–156, 1998.
[13] L. Carlitz, "Kloosterman sums and finite field extensions," *Acta Arithmetica*, vol. XVI, no. 2, pp. 179–183, 1969.
[14] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: The Niho case," *Inf. Comput.*, vol. 151, no. 1-2, pp. 57–72, 1999.
[15] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: The Welch case," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1271–1275, Apr. 1999.
[16] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: A new class for n divisible by 5," in *Proc. Finite Fields and Applications Fq5*, Augsburg, Germany, 2000, pp. 113–121.
[17] Y. Edel, G. Kyureghyan, and A. Pott, "A new APN function which is not equivalent to a power mapping," *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 744–747, Feb. 2006.
[18] F. Hernando and G. McGuire, "Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions," *J. Algebra*, vol. 343, no. 1, pp. 78–92, Oct. 2011.
[19] H. Hollmann and Q. Xiang, "A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences," *Finite Fields Appl.*, vol. 7, no. 2, pp. 253–286, 2001.
[20] P. Kumar, T. Helleseth, A. Calderbank, and A. Hammons, "Large families of quaternary sequences with low correlation," *IEEE Trans. Inf. Theory*, vol. IT-42, no. 2, pp. 579–592, Feb. 1996.
[21] G. Lachaud and J. Wolfmann, "The weights of the orthogonal of the extended quadratic binary Goppa codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 3, pp. 686–692, Mar. 1990.
[22] K. Nyberg, "Differentially uniform mappings for cryptography," in *Proc. Advances in Cryptology–EUROCRYPT'93*, 1993, vol. 765, Lecture Notes in Computer Science, pp. 55–64.
[23] K. Nyberg and L. Knudsen, "Provable security against differential cryptanalysis," in *Proc. Advances in Cryptology–CRYPTO'92*, 1993, vol. 740, Lecture Notes in Computer Science, pp. 566–574.

Céline Blondeau is a Ph.D. student at INRIA, the French National Institute for Research in Computer Science, within the SECRET team. She is working on symmetric cryptography.

Anne Canteaut received the French engineer's degree from the École Nationale Supérieure de Techniques Avancées in 1993 and the Ph.D. degree in computer science from the University of Paris VI in 1996. Since 1997, she has been a researcher at the French National Research Institute in Computer Science (INRIA) in Rocquencourt. She is currently Director of Research and the scientific head of the SECRET research team at INRIA. Her current research interests include cryptography and coding theory.

Dr. Canteaut has served on program committees for several international conferences such as Crypto, FSE and Eurocrypt. She served on the Editorial Board of the IEEE TRANSACTIONS ON INFORMATION THEORY (from 2005 to 2008).

Pascale Charpin received the Ph.D. degree and the Doctorate in Sciences (Theoretical Computer Science) from the University of Paris VII, France, in 1982 and 1987, respectively. She was with the Department of Mathematics at the University of Limoges, France, from 1973 to 1982. From 1982 to 1989, she has worked at the University of Paris VI. She is currently Director of Research at INRIA, the French National Institute for Research in Computer Science, in Rocquencourt. She was the scientific head of the group CODES (coding and cryptography) in this institute from 1995 to 2002. Her research interests include finite algebra, algorithmic and applications to coding (error-correcting coding and cryptology). Dr. Charpin served on the Editorial Board of the IEEE TRANSACTIONS ON COMPUTERS (from 2000 to 2004) and serves on the Editorial Board of *Designs, Codes and Cryptography* (from 2002).