On propagation characteristics of resilient functions

Pascale Charpin, Enes Pasalic

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

On propagation characteristics of resilient functions

Pascale Charpin — Enes Pasalic

N° 4537

Septembre 2002

THÈME 2

ISSN 0249-6399 ISRN INRIA/RR--4537--FR+ENG

INRIA
ROCQUENCOURT

On propagation characteristics of resilient functions

Pascale Charpin* , Enes Pasalic†

Thème 2 — Génie logiciel
et calcul symbolique
Projet Codes

Rapport de recherche n° 4537 — Septembre 2002 — 27 pages

Abstract: In this paper we derive several important results towards a better understanding of propagation characteristics of resilient Boolean functions. We first introduce a new upper bound on nonlinearity of a given resilient function depending on the propagation criterion. We later show that a large class of resilient functions admit a linear structure; more generally, we exhibit some divisibility properties concerning the Walsh-spectrum of the derivatives of any resilient function. We prove that, fixing the order of resiliency and the degree of propagation criterion, a high algebraic degree is a necessary condition for construction of functions with good autocorrelation properties. We conclude by a study of the main constructions of resilient functions. We notably show how to avoid linear structures when a linear concatenation is used and when the recursive construction introduced in [13] is chosen.

Key-words: Boolean functions, nonlinearity, propagation characteristics, resiliency, linear structure, linear space.

A short version of this paper will be published in the proceedings of *Selected Areas in Cryptography*, SAC 2002, Lecture Notes in Computer Sciences.

* INRIA, projet CODES, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France. e-mail: Pascale.Charpin@inria.fr.
† Department of Information Technology, Lund University, P. O. Box 118, 221 00 Lund, Sweden. e-mail: enes@it.lth.se

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex (France)
Téléphone : +33 1 39 63 55 11 — Télécopie : +33 1 39 63 53 30

Propriétés de propagation des fonctions résilientes

Résumé : L'objet de ce travail est d'abord une meilleure compréhension des propriétés de propagation des fonctions booléennes résilientes.

D'un point de vue cryptographique, un critère de propagation évalue l'impact en *sortie* d'une perturbation de l'*entrée*. Pour une fonction booléenne, l'étude des propriétés de propagation est en fait l'étude de sa fonction d'autocorrélation qui à chaque direction associe la dérivée de la fonction dans cette direcion. On dispose de plusieurs indicateurs qui, schématiquement, doivent être *petits* pour que la fonction soit *cryptographiquement bonne*. Le fait d'avoir des dérivées constantes représente une faiblesse, l'un des indicateurs étant à son maximum. Dans ce cas, les directions des dérivées constantes sont appelées *structures linéaires* de la fonction.

Un fonction résiliente est équilibrée – son image binaire contient autant de 0 que de 1. L'ordre de résilience d'une fonction booléenne mesure la stabilité de cette propriété lorsque l'on approxime la fonction avec une fonction linéaire. Le critére de résilience répond à une famille d'attaques *par corrélation* sur certains systèmes de chiffrement. Ce critère est fortement lié à la distance (mesurée en poids de Hamming) de la fonction aux fonctions linéaires, la *nonlinéarité* de la fonction.

Nous introduisons d'abord une nouvelle borne concernant la nonlinéarité des fonctions résilientes, borne qui prend en compte le degré de la fonction et certains critères de propagation. D'autre part, nous montrons que l'ordre de résilience induit des propriétés de divisibilité pour les dérivées, celles-ci pouvant être renforcées par le degré de propagation. Ainsi nous caractérisons une large famille de fonctions hautement résilientes ayant des structures linéaires. Nous montrons aussi, par ces bornes, l'influence du degré de la fonction dans l'établissement de bons compromis.

Nous étudions enfin plusieurs constructions de fonctions résilientes qui nous paraissent matérialiser les principales méthodes (par concaténation et récursives). Notre but est ici de fournir des outils pour éviter les structures linéaires.

Mots-clés : fonctions booléennes, nonlinéarité, critères de propagations, résilience, structure linéaire, espace linéaire.

1 Introduction

The security of most conventional cryptographic systems is based on some properties of Boolean functions – currently called *cryptographic criteria*. This paper deals with well-known such criteria. The *nonlinearity*, the distance from a Boolean function to the set of all affine functions, prevents linear attacks in block ciphers [11]. *Correlation-immune* functions were first introduced by Siegenthaler [16] in order to construct running-key generators for stream ciphers which resist to correlation attack. A balanced such function is said to be *resilient*; resiliency appears as the main criterion in several systems (see, for instance, [2]). The *propagation criterion* (PC) was introduced by Preneel [14], generalizing the *strict avalanche criterion* [19]. More generally, the *propagation characteristics* of any Boolean function refer to certain properties of its derivatives [21]. A function which has constant derivatives is said to have a nontrivial *linear space*, the space of its *linear structures*. The distance from a Boolean function to the set of functions with linear structures was explained by Meier and Staffelbach in [12].

Recently, the relationships between propagation characteristics, nonlinearity, and correlation-immunity were investigated (see notably [3], [15], [17],[22], [5]). Generally, in all recent works, it appears that good cryptographic properties imply that the given function belongs to some well-structured class. It is especially true for resilient functions; a few effective constructions are known and the main of these are based on concatenations [8, 18]. Our main purpose is the study of the consequences of high resiliency for other cryptographic criteria. How high resiliency could lead to some weakness ? In accordance with [12], such weakness has to be considered up to any simple transformation (for instance, any affine transformation).

In Section 2, we present the main tools for the study of Boolean functions on $\mathbb{F}_2^n$, the basic definitions and some recent results concerning the cryptographic criteria. In Section 3 we consider resilient functions which satisfy a certain propagation criterion. We introduce a new nontrivial upper bound on the nonlinearity of t-resilient functions satisfying PC with respect to some subspace of dimension p (Theorem 3). We then emphasize that for a fixed order of resiliency, the upper bound on nonlinearity of f, is smaller for larger p. Section 4 is devoted to the characterization of the linear space of functions. Different criteria regarding the functions with linear structures are addressed here. We then deduce that high resiliency leads to the existence of linear structures (Corollary 2). In Section 5, we study the weights of the derivatives of resilient functions which satisfy (or not) some propagation criterion. Our results reinforce those of the previous section. Namely, high resiliency leads to high divisibility for the weights of derivatives; moreover, taking into account the degree of propagation and the degree of the function, this divisibility increases (Theorem 5). In Section 6 we discuss the main known constructions of resilient functions. We first characterize resilient functions, obtained by linear concatenation, which have no linear structure (Proposition 6). We later study two recursive constructions [18] [13]. We prove that the first one provides resilient functions which have a linear space not reduced to 0, while the second one preserves the lack of linear structure (Proposition 10).

2 Definitions and basic properties

2.1 Boolean functions

We denote by $\mathcal{B}_n$ the set of Boolean functions of n variables. Thus $f \in \mathcal{B}_n$ is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$; it is generally represented by its *algebraic normal form*:

$$f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}_2^n} \lambda_u \left(\prod_{i=1}^{n} x_i^{u_i} \right) , \quad \lambda_u \in \mathbb{F}_2 \ .$$

The *degree* of f is the maximal value of the Hamming weight of u such that $\lambda_u \neq 0$. The linear functions will be represented by means of the scalar product, with respect to the standard basis. They will be denoted as follows: for any $\alpha \in \mathbb{F}_2^n$, $\varphi_\alpha : x \in \mathbb{F}_2^n \longmapsto \alpha \cdot x = \sum_{i=1}^{n} \alpha_i x_i$.

The *Walsh transform* of $f \in \mathcal{B}_n$ in point α is denoted $\mathcal{F}(f + \varphi_\alpha)$ and calculated as,

$$\alpha \in \mathbb{F}_2^n \longmapsto \mathcal{F}(f + \varphi_\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \varphi_\alpha(x)} \ .$$

The values of these coefficients form the *Walsh-spectrum* of f. The *nonlinearity* $\mathcal{N}_f$ of $f \in \mathcal{B}_n$ is related to the Walsh transform via following expression:

$$\mathcal{N}_f = 2^{n-1} - \frac{\mathcal{L}(f)}{2} \quad \text{where} \quad \mathcal{L}(f) = \max_{\alpha \in \mathbb{F}_2^n} \mid \mathcal{F}(f + \varphi_\alpha) \mid .$$

The *propagation characteristics* of f are described by the behaviour of its derivatives. The *derivative* of $f \in \mathcal{B}_n$ with respect to any direction $a \in \mathbb{F}_2^n$, is the mapping $D_a f : x \longmapsto f(x) + f(a+x)$. Thus, the *auto-correlation function* of f refers to the function $a \mapsto \mathcal{F}(D_a f)$. The main indicators of propagation characteristics are the *absolute indicator* and the *sum-of-square indicator* [21]:

$$\mathcal{M}(f) = \max_{a \in \mathbf{F}_2^n, \ a \neq 0} \mid \mathcal{F}(D_a f) \mid \quad \text{and} \quad \mathcal{V}(f) = \sum_{a \in \mathbf{F}_2^n} \mathcal{F}^2(D_a f) \ .$$

For any linear subspace V of $\mathbb{F}_2^n$, its dual $V^\perp$ will be the subspace of elements $x \in \mathbb{F}_2^n$ such that $x \cdot y = 0$ for all $y \in V$. The next formula provides a link between the Walsh and autocorrelation spectra of f. The proof can be found in [4, Lemma V.2].

Lemma 1 *Let V be a linear subspace of $\mathbb{F}_2^n$ of dimension k. Then for any function f in $\mathcal{B}_n$ we have for any $\beta \in \mathbb{F}_2^n$,*

$$\sum_{v \in V} \mathcal{F}^2(f + \varphi_{\beta + v}) = 2^k \sum_{u \in V^\perp} (-1)^{\beta \cdot u} \mathcal{F}(D_u f). \tag{1}$$

For $V = \{0\}$, (1) becomes the well-known relation:

$$\mathcal{F}^2(f + \varphi_\beta) = \sum_{u \in \mathbb{F}_2^n} (-1)^{\beta \cdot u} \mathcal{F}(D_u f) \ .$$

2.2 Resiliency and propagation characteristics

The next definitions are now classical. They were introduced in [12, 14] (for the propagation characteristics) and in [16, 20] (for the resiliency). Recall that the Hamming weight of any binary vector y is

$$wt(y) = \#\{i \mid y_i = 1\},$$

where $\#A$ denotes the cardinality of any set A. By convention, the weight of $f \in \mathcal{B}_n$ is the Hamming weight of its corresponding codeword, *i.e.,* the sequence of values $f(x)$, when x runs through $\mathbb{F}_2^n$. Any function $f \in \mathcal{B}_n$ is *balanced* when $wt(f) = 2^{n-1}$ or, equivalently, $\mathcal{F}(f) = 0$. A function exhibits *good propagation characteristics* when its autocorrelation function takes "small" (absolute) values; therefore the related indicators have to be "small" [21].

Definition 1 *The* linear space *of any Boolean function f is the linear subspace of those elements a such that the function $D_a f$ is constant. Such nonzero a is called a linear structure of f.*

The function $f \in \mathcal{B}_n$ has a linear structure if and only if $\mathcal{M}(f)$ takes its maximal value 2^n. On the other hand the sum-of-square indicator provides a bound for the nonlinearity.

Theorem 1 [3] *Let $f \in \mathcal{B}_n$. Then we have $\mathcal{V}(f) \leq 2^n \mathcal{L}^2(f)$ with equality if and only if the Walsh spectrum of f takes at most three values, which are 0, $\mathcal{L}(f)$ and $-\mathcal{L}(f)$.*

The propagation criterion of f concerns the set of balanced derivatives.

Definition 2 *Let $E \subset \mathbb{F}_2^n$. The function $f \in \mathcal{B}_n$ satisfies* the propagation criterion (PC) with respect to *E if for all $e \in E$ the function $D_e f$ is balanced. The function f satisfies* PC *of degree p (PC(p)) for some positive integer p when $D_a f$ is balanced for any $a \in \mathbb{F}_2^n$ such that $1 \leq wt(a) \leq p$.*

The correlation-immunity is characterized by the set of zero values in the Walsh spectrum.

Definition 3 *Let $f \in \mathcal{B}_n$ and let t be some positive integer. The function f is said to be* correlation-immune of order *t if and only if $\mathcal{F}(f + \varphi_\alpha) = 0$ for any $\alpha \in \mathbb{F}_2^n$ such that $1 \leq wt(\alpha) \leq t$. Moreover, when f is balanced, it is said to be t-resilient. A balanced function is said to be 0-resilient.*

Besides its maximum value, the whole Walsh spectrum of a Boolean function has a great cryptographic significance. Several recent works are devoted to the divisibility of the Walsh coefficients of resilient functions. Sarkar and Maitra proved in [15] that any t-resilient function $f \in \mathcal{B}_n$ satisfies for all α: $\mathcal{F}(f + \varphi_\alpha) \equiv 0 \pmod{2^{t+2}}$. This result was improved by Carlet in [5] by including the algebraic degree d of the function:

$$\mathcal{F}(f + \varphi_\alpha) \equiv 0 \pmod{2^{t+2+\lfloor \frac{n-t-2}{d} \rfloor}}, \ \forall\, \alpha \in \mathbb{F}_2^n \tag{2}$$

(where $\lfloor r \rfloor$ denotes the integer part of r). Carlet then derived a *new upper bound on the nonlinearity $\mathcal{N}_f$ of any t-resilient function f of degree d* :

$$\mathcal{N}_f \leq 2^{n-1} - 2^{t+1+\lfloor \frac{n-t-2}{d} \rfloor}. \tag{3}$$

This bound is lose for small t, since there is a tighter upper bound derived from the nonlinearity of bent functions. However, for $t > \frac{n}{2} - 2$ the bound above is tighter for any n.

3 On resilient Boolean functions satisfying PC

In this section, we focus on an improvment of the bound (3) when considering any t-resilient function which moreover satisfies some propagation criterion.

3.1 Preliminary

In a recent paper, Zhang and Zheng introduced several properties regarding the relationship between the correlation-immunity and propagation criteria [22]. They begin by giving a lower bound for the nonlinearity of functions satisfying PC(p). The following result is given in [22, Theorem 1].

Theorem 2 *Let f be a non-bent function in $\mathcal{B}_n$ satisfying* PC(p). *Then the nonlinearity of f satisfies*

$$\mathcal{N}_f \geq 2^{n-1} - 2^{n-\frac{p}{2}-1} \quad \textit{or, equivalently,} \quad \mathcal{L}(f) \leq 2^{n-\frac{p}{2}} \ . \tag{4}$$

Moreover, if $\mathcal{L}(f) = 2^{n-\frac{p}{2}}$, then $p = n-1$ and n is odd.

Actually this lower bound can be established more generally.

Proposition 1 *Let f be a non-bent function in $\mathcal{B}_n$. Assume that f satisfies PC with respect to $U \setminus \{0\}$, where U is a subspace of $\mathbb{F}_2^n$ of dimension p. Then the nonlinearity of f satisfies (4). This especially holds when f satisfies PC(p). When $p = n-1$, for odd n, or $p = n-2$, for even n, then $\mathcal{L}(f) = 2^{n-\frac{p}{2}}$.*

Proof: We apply (1) with $k = n - p$ and $V = U^\perp$. Then for any β,

$$\sum_{v \in U^\perp} \mathcal{F}^2(f + \varphi_{\beta+v}) = 2^{n-p}\mathcal{F}(D_0 f) = 2^{2n-p} \ ,$$

since $\mathcal{F}(D_u f) = 0$ for $u \in U \setminus \{0\}$. This implies that $\mathcal{L}^2(f) \leq 2^{2n-p}$ or, equivalently, that $\mathcal{N}_f \geq 2^{n-1} - 2^{\frac{2n-p}{2}-1}$. When the function f satisfies PC(p), it satisfies PC with respect to $U_a \setminus \{0\}$ for any a where

$$U_a = \{\ u \in \mathbb{F}_2^n \mid \preccurlyeq a\ \} \ \text{ with } \ wt(a) = p \ . \tag{5}$$

Note that $u \preccurlyeq a$ means that a *covers* u, i.e.,

$$u_i \leq a_i \quad \text{for all } i \text{ in the range } [1, n].$$

The cases $p = n-1$ and $p = n-2$ were explained in [4, § V.C]. Note that, according to the previous theorem, it is impossible to have: f satisfies PC$(n-2)$ and $\mathcal{L}(f) = 2^{n-\frac{p}{2}}$.

■

With the hypothesis of Theorem 2, $\mathcal{L}(f) = 2^{n-\frac{p}{2}}$ implies that $p = n-1$ for odd n (and that f is bent for even n). The functions satisfying PC$(n-1)$ were fully-characterized in [3]. Such a function f admits one and only one linear structure, say e, and is such that $D_a f$ is balanced unless $a \in \{0, e\}$. Moreover it cannot be 1-resilient, with respect to any basis. In the case of Proposition 1, it is possible to have $\mathcal{L}(f) = 2^{n-\frac{p}{2}}$ for any even p. Furthermore for $p = n-1$, when f is balanced it is generally 1-resilient, with respect to some basis (see [3], Corollary 2, Theorems 4 and 7).

In the sequel of this section, we will consider functions which are t-resilient with respect to the standard basis. We will fix the basis for the definitions of the t-resiliency; for the PC property we consider particular subspaces which are defined by means of this standard basis. We first indicate some restriction on the sum $p + t$.

Lemma 2 *Let f be a t-resilient function satisfying PC with respect to the nonzero elements of U_a, $wt(a) = p$, defined as in (5). Denote by $\overline{a}$ the vector $(1 + a_1, \ldots, 1 + a_n)$.*

Then $p + t \leq n - 1$. If $p + t = n - 1$ and $\mathcal{F}(f + \varphi_{\overline{a}}) \neq 0$ then

$$\mathcal{L}^2(f) = \mathcal{F}^2(f + \varphi_{\overline{a}}) = 2^{2n-p}.$$

When $p + t = n - 1$ and f satisfies PC(p) then $p = n - 1$, n is odd and $t = 0$.

Proof: We apply (1) with $k = n - p$, $V = U_a^{\perp}$ and $\beta = 0$:

$$\sum_{v \preccurlyeq \overline{a}} \mathcal{F}^2(f + \varphi_v) = 2^{2n-p} .$$

Since $wt(\overline{a}) = n - p$ and f is t-resilient, $t \geq n - p$ would imply that each term in the sum above is zero, a contradiction. Now, assuming that $t = n - p - 1$, there is only one possible non-zero term in this sum (for $v = \overline{a}$). According to Proposition 1, $\mathcal{F}^2(f + \varphi_{\overline{a}}) = 2^{2n-p}$ provides $\mathcal{L}^2(f) = 2^{2n-p}$. The proof is completed by means of Theorem 2.

■

To conclude this section we want to show that a large class of resilient functions satisfy the hypothesis of Proposition 1. These functions are the so-called Maiorana-McFarland functions. A method for constructing such resilient functions was first proposed in [1, Proposition 4.2] :

Proposition 2 *Let $s \in [1, n[$, $g \in \mathcal{B}_{m-r}$ and ϕ a mapping from $\mathbb{F}_2^{n-s}$ to $\mathbb{F}_2^s$ such that $\phi(y) \neq 0$ for all y. Let us denote by ϕ_i, $1 \leq i \leq s$, the coordinate functions of ϕ. Let f be*

the Boolean function defined for all $(x,y) \in \mathbb{F}_2^s \times \mathbb{F}_2^{n-s}$ *by*

$$f(x,y) = \sum_{i=1}^{s} x_i \phi_i(y) \ + \ g(y) \ .$$

Then f *is* t*-resilient where* $t \geq \min_y\{wt(\phi(y)) - 1\}$.

We will study a subclass of these functions in Section 6. Here we only want to define a class of such a function satisfying PC with respect to $U \setminus \{0\}$, where U is a subspace of dimension $n-s$.

Proposition 3 *Let* f *be a function defined by Proposition 2. Assume that* ϕ *is such that for all* $u \in \mathbb{F}_2^{n-s}$, $u \neq 0$, *and for all* y *there is* i *such that* $D_u\phi_i(y) \neq 0$.

Then f *satisfies PC with respect to* $V = \{(0,u) \mid u \in \mathbb{F}_2^{n-s} \setminus \{0\}\}$. *Moreover* $\mathcal{L}(f) \leq 2^{\frac{n+s}{2}}$.

Proof: We compute the derivative of f with respect to any $(0,u)$:

$$D_{(0,u)}f(x,y) = \sum_{i=1}^{s} x_i (D_u\phi_i(y)) \ + \ D_u g(y) \ .$$

For any fixed y, the function $x \mapsto D_{(0,u)}f(x,y)$ is affine or constant. It cannot be constant since the hypothesis on the ϕ_i. Thus $D_{(0,u)}f$ is balanced for any non zero u. Therefore f satisfies PC with respect to V which implies, from Proposition 1, that $\mathcal{L}(f) \leq 2^{n-(n-s)/2}$. ■

3.2 A new upper bound

We will show that there exists a nontrivial upper bound on the nonlinearity of t-resilient functions satisfying PC with respect to the nonzero elements of some subspace of dimension p. According to the previous discussion we will assume that $p+t = n-k$ with $k \geq 2$. Recall that the degree d of any t-resilient function in $\mathcal{B}_n$ satisfies $d \leq n-t-1$ [16].

Theorem 3 *Let* $f \in \mathcal{B}_n$ *be a* t*-resilient function of degree* d *with* $d \geq 2$. *Assume that* f *satisfies PC with respect to* $U_a \setminus \{0\}$ *where*

$$U_a = \{u \in \mathbb{F}_2^n \,|\, u \preccurlyeq a\} \quad \textit{with } wt(a) = p \ .$$

Let $p + t = n - k$ *with* $2 \leq k \leq n-2$. *Then the upper bound on nonlinearity of* f *is given by,*

$$\mathcal{N}_f \leq 2^{n-1} - \ell \ 2^{t+1+\lfloor \frac{n-t-2}{d} \rfloor}, \tag{6}$$

where ℓ *is the minimum integer among all positive integers* i *satisfying*

$$i^2 \sum_{j=1}^{k} \binom{t+k}{t+j} \geq 2^{p+2k-4-2\lfloor \frac{n-t-2}{d} \rfloor}. \tag{7}$$

This is especially true when f *satisfies PC(p).*

Proof: From Lemma 1, since $\mathcal{F}(D_u f) = 0$ for any nonzero $u \in U_a$, we have:

$$\sum_{v \in U_a^\perp} \mathcal{F}^2(f + \varphi_v) = 2^{n-p}\mathcal{F}(D_0 f) = 2^{2n-p}, \tag{8}$$

On the other hand we know that, as any t-resilient function, f satisfies for all α: $\mathcal{F}(f + \varphi_\alpha) \equiv 0 \pmod{2^{t+2+\epsilon}}$, where $\epsilon = \lfloor \frac{n-t-2}{d} \rfloor$ (see (2)). Combining this result with (8), we conclude that for any $v \in U_a^\perp$ there is an integer i such that $0 \leq i^2 \leq 2^{p+2k-4-2\epsilon}$ and $\mathcal{F}^2(f + \varphi_v) = i^2 2^{2(t+2+\epsilon)}$.

Remark that $2n - p - 2(t + 2 + \epsilon) = p + 2k - 4 - 2\epsilon$, since $p + t = n - k$, providing the upper bound on i^2. Moreover, the equality (8) implies $p + 2k - 4 - 2\epsilon \geq 0$. Now we set for any i:

$$\lambda_i = \text{card } \{v \in U_a^\perp : |\mathcal{F}(f + \varphi_v)| = i 2^{t+2+\epsilon}\} .$$

Then we may rewrite (8) in terms of λ_i. We obtain (where $c = 2^{p+2k-4-2\epsilon}$):

$$\sum_{i=1}^{c} \lambda_i i^2 2^{2t+4+2\epsilon} = 2^{2n-p} , \quad i.e., \quad \sum_{i=1}^{c} \lambda_i i^2 = 2^{p+2k-4-2\epsilon},$$

On the other hand, we consider the number Λ of nonzero coefficients $\mathcal{F}(f + \varphi_v)$ when v describes $U_a^\perp$. Since f is t-resilient, then $\Lambda \leq \sum_{j=1}^{k} \binom{t+k}{t+j}$. Thus we claim that from a certain positive value of i, say for all $i \geq i_0$, we have :

$$\sum_{j=1}^{c} \lambda_j j^2 \leq \Lambda i^2 \leq i^2 \sum_{j=1}^{k} \binom{t+k}{t+j} . \tag{9}$$

Therefore, we can define ℓ as the smallest integer such that $2^{p+2k-4-2\epsilon} \leq \ell^2 \sum_{j=1}^{k} \binom{t+k}{t+j}$. Moreover we are sure that there is some $v \in U_a^\perp$ such that $|\mathcal{F}(f + \varphi_v)| \geq \ell\, 2^{t+2+\epsilon}$, because if this is not true then we can define $i < \ell$ such that $|\mathcal{F}(f + \varphi_v)| \leq i 2^{t+2+\epsilon}$ for all v ; such i satisfies (9) contradicting the assumption. Thus we have proved that the maximal absolute value of the coefficients $\mathcal{F}(f + \varphi_v)$ is at least $\ell\, 2^{t+2+\epsilon}$ or, equivalently, that $\mathcal{N}_f$ satisfies (6). ■

According to the previous theorem, it is easy to see that for a fixed order of resiliency the upper bound on nonlinearity becomes smaller as p increases. Note that the lower bound (4), which has concern with propagation criterion only, increases with p. The next example clearly indicates the trade-off between the nonlinearity and propagation. Another illustration is the following corollary, directly deduced from Theorem 3 (for $k = 2$).

Corollary 1 *Let f be a Boolean function in $\mathcal{B}_n$ of degree d satisfying the hypothesis of Theorem 3. Furthermore, let $p + t = n - 2$, $p > 0$. Then the upper bound on nonlinearity is given by, $\mathcal{N}_f \leq 2^{n-1} - \ell\, 2^{t+1+\lfloor \frac{p}{d} \rfloor}$, where ℓ is the minimum integer among all positive integers i satisfying*

$$i^2(t + 3) \geq 2^{p-2\lfloor \frac{p}{d} \rfloor}. \tag{10}$$

Example 1 Let f be a 4-resilient function in $\mathcal{B}_{10}$. Assume there is $a \in \mathbb{F}_2^{10}$ of weight $wt(a) = 3$ such that $D_u f$ is balanced for any nonzero $u \preccurlyeq a$, i.e., $t = 4$ and $p = 3$ in Theorem 3. We suppose that the degree d of f is such that $\epsilon = 0$; for instance $d = 5$.

We have $p+t = 7$ and $k = 3$. Thus ℓ is the smallest integer i satisfying $i^2 \sum_{j=1}^{3} \binom{7}{4+j} \geq 32$; so $\ell = 2$. Then the nonlinearity of f is less than or equal to $2^{n-1} - 2 \cdot 2^{t+1} = 448$, for $n = 10, t = 4, p = 3$. We conclude that $\mathcal{N}_f \leq 448$, while the upper bound (3) gives $\mathcal{N}_f \leq 480$. Such a function, with these parameters, was firstly constructed in [13].

Remark 1 The class of resilient functions defined by Proposition 2 could provide a lot of examples where our bound is efficient. Consider such a function f with degree d satisfying the hypothesis of Proposition 3. Then we have, according to Proposition 3 and Theorem 3 :

$$\ell \; 2^{t+2+\lfloor \frac{n-t-2}{d} \rfloor} \leq \mathcal{L}(f) \leq 2^{\frac{n+s}{2}} \tag{11}$$

where $t \geq \min_y\{wt(\phi(y)) - 1\}$ and ℓ is the minimum integer among all positive integers i satisfying (see (7): with $k = s - t$)

$$i^2 \sum_{j=1}^{s-t} \binom{s}{t+j} \geq 2^{n+s-2t-4-2\lfloor \frac{n-t-2}{d} \rfloor}.$$

In the next example, we consider $t > \frac{n}{2} - 2$, since in this case the upper bound (3) on $\mathcal{N}_f$ is efficient. In the two examples below we assume that the functions have maximum degree $d = n - t - 1$, which implies that $\lfloor \frac{n-t-2}{d} \rfloor = 0$.

Example 2 Let $f \in \mathcal{B}_{12}$ with $t = 5$ and $p = 5$. Thus, $p + t = 10$. From Corollary 1, ℓ is the smallest integer i satisfying $8i^2 \geq 32$; so $\ell = 2$. This yields the upper bound on the nonlinearity $\mathcal{N}_f \leq 2^{n-1} - 2 \cdot 2^{t+1} = 1920$, for $n = 12, t = 5, p = 5$. The upper bound given by (3) is $\mathcal{N}_f \leq 1984$.

Consider now $f \in \mathcal{B}_{12}$ with $t = 5$ but $p = 1$. In this case $k = n - p - t = 6$, $\sum_{j=1}^{k} \binom{t+k}{t+j} = 1024$ and $2^{p+2k-4} = 512$. Clearly $1024 \times \ell^2 \geq 512$ is satisfied for $\ell = 1$. Thus the upper bound is given by the weight divisibility result, i.e., $\mathcal{N}_f \leq 2^{n-1} - 2^{t+1} = 1984$.

We now fix $p + t = n - 2$ and investigate the upper bound on nonlinearity for different choices of p and t – according to Corollary 1.

Example 3 Let $f \in \mathcal{B}_{12}$ with $t = 1$ and $p = 9$. The minimum positive integer ℓ among all i satisfying $i^2(t + 3) \geq 2^p$ is $\ell = 2$. This yields the upper bound on the nonlinearity $\mathcal{N}_f \leq 2^{11} - 12 \cdot 2^2 = 2000$, for $n = 12, t = 5, p = 5$. The upper bound, derived from the nonlinearity of bent functions, is equal to 2012.

Now, take $t = 4$ and $p = 6$. In the same manner as above it is verified that $i^2(t+3) \geq 2^p$ is first satisfied for $i = 4$. Thus the upper bound, given by Corollary 1 is $\mathcal{N}_f \leq 2^{11} - 4 \cdot 2^5 = 1920$. The upper bound, derived combining the weight divisibility results and the upper bound stemming from bent functions, is $\mathcal{N}_f \leq 1984$.

The consequences of the results above are that we have implicitly proved that for a fixed q, an increase of p will cause the upper bound given by Theorem 3 to decrease, and at the same time the lower bound (4) will increase. A natural question that arises here is as follows: *For which values of parameters p, q, d (if there exists any) two bounds meet each other ?* More precisely, considering functions which are PC(p), since the lower bound is achieved for $p = n - 1$ only, proving the fact that two bounds meet each other is equivalent to proving that the class of functions with such parameters does not exist.

Proposition 4 *There does not exist a t-resilient Boolean function f of degree $d = 2$, $t \geq 0$, satisfying PC(p) with $p + t = n - 2$, p even.*

Proof: We consider a general case for the $p + t$ sum assuming only that p is even. Since $p + t \leq n - 2$ we write $p + t = n - k$ for $2 \leq k \leq n - 2$. From the lower and upper bound we know,

$$\ell \, 2^{t+2+\epsilon} \leq \mathcal{L}(f) \leq 2^{n-\frac{p}{2}}, \tag{12}$$

where $\epsilon = \lfloor \frac{n-t-2}{d} \rfloor$ and ℓ is the smallest positive integer satisfying (7) in Theorem 3, i.e.,

$$i^2 \sum_{j=1}^{k} \binom{t+k}{t+j} \geq 2^{p+2k-4-2\epsilon}. \tag{13}$$

Clearly (12) is contradicted when p, t, k and d are such that

$$2^{n-\frac{p}{2}} \leq \ell \, 2^{t+2+\epsilon}, \text{i.e.,} \quad \ell \geq 2^{k+\frac{p}{2}-2-\epsilon}, \tag{14}$$

where in the right-hand inequality $n - p - t = k$ was used. Considering (13) and (14) we deduce that both equations are satisfied only if,

$$\ell = 1 \text{ and } \quad k + \frac{p}{2} - 2 - \epsilon \leq 0.$$

Denote by $I = k + \frac{p}{2} - 2 - \epsilon$. Then, since $k \geq 2$ we have,

$$2 + \frac{p}{2} \leq k + \frac{p}{2} \leq 2 + \epsilon. \tag{15}$$

On the other hand since $\epsilon = \lfloor \frac{n-t-2}{d} \rfloor$, we have $\epsilon d \leq n - t - 2$. By noting that $I = (n - t - 2) - \frac{p}{2} - \epsilon \leq 0$ we obtain,

$$\epsilon d \leq n - t - 2 \leq \epsilon + \frac{p}{2}. \tag{16}$$

From (15) we conclude that $p \leq 2\epsilon$ with equality if and only if $k = 2$. Also, considering (16) we deduce that $p \geq 2\epsilon(d - 1)$. These two conditions implies that we must have $d = 2$, and then $p = 2\epsilon$; so $k = 2$.

Thus, we have proved that for $d = 2$, and $p + t = n - 2$ both the upper and lower bound are achieved by equality. Since the lower bound is attained only for $p = n - 1$ we conclude that there do not exist quadratic functions satisfying $p + t = n - 2$, for $t \geq 0$ and p even. ■

4 On functions with(out) linear structure

To construct effectively functions with high resiliency remains an important open problem. However, high resiliency could implies some property which leads to some cryptographic weakness. This section is devoted to the existence of linear structures. We propose some general tools characterizing linear structures; then we can show that high resiliency provides linear structures. Recall that an attack on block ciphers, based on the existence of linear stuctures, was proposed by Evertse [10].

4.1 On distance to linear structures

In [12], the propagation criterion was defined as the *nonlinearity* of f with respect to a linear structure. Since this criterion is invariant under the general affine group, it was considered as a *useful criterion.* It allows to quantify the distance of f to any linear structure as we explain briefly.

Definition 4 *Let $LS(n)$ denote the subset of Boolean functions having linear structures:*

$$LS(n) = \{\ g \in \mathcal{B}_n \mid \exists\ a \text{ such that } D_a g \in \{0,1\}\ \}.$$

The nonlinearity *of f with respect to the functions with linear structures is defined as,*

$$\sigma(f) = \min_{g \in LS(n)} wt(f+g)\ .$$

Note that $LS(n)$ properly contains the set of all affine functions. Moreover, it contains quadratic functions which are not bent. Thus, this kind of nonlinearity is much stronger than the usual nonlinearity. In [12], it was also proved that $\sigma(f) \leq 2^{n-2}$ for $f \in \mathcal{B}_n$ with equality if and only if f is bent. More precisely, *the minimum distance of f to the set of the functions which have a linear structure a is less than or equal to 2^{n-2} with equality if and only if $D_a f$ is balanced.*

4.2 Criteria for linear structure

A priori, there is no criteria to decide upon whether a Boolean function has a linear structure except of checking for all possible linear structures. However, as we will show, this problem for any function f, is strongly related with some properties of its Walsh-spectrum. Note that the problem of the existence of linear structures was studied in [9] (concerning functions from $\mathbb{F}_2^r$ to $\mathbb{F}_2^s$). Lemma 3 and Theorem 4 are directly obtained from the results of this paper. We give the full proofs for clarity.

Lemma 3 *Let f be a Boolean function in $\mathcal{B}_n$. Then f has a linear structure, say a, if and only if either the hyperplane $\{0,a\}^\perp$ (if $D_a f = 1$) or its complement (if $D_a f = 0$) is contained in the set*

$$Z_f = \{\alpha \mid \mathcal{F}(f+\varphi_\alpha) = 0\}\ . \tag{17}$$

In particular, if the cardinality of Z_f does not exceed $2^{n-1}-1$ then f has no linear structure.

Proof: For any $a \neq 0$ we consider the hyperplane $H = \{0, a\}^{\perp}$; then we can write (1) as follows:

$$\sum_{u \in H} \mathcal{F}^2(f + \varphi_u) = 2^{n-1}(\mathcal{F}(D_0 f) + \mathcal{F}(D_a f)) = 2^{2n-1} + 2^{n-1}\mathcal{F}(D_a f) \ . \qquad (18)$$

Note that a is a linear structure of f if and only if either $\mathcal{F}(D_a f)) = 2^n$ (when $D_a f = 0$) or $\mathcal{F}(D_a f)) = -2^n$ (when $D_a f = 1$). We deduce from (18) that $D_a f = 1$ if and only if $\mathcal{F}(f+\varphi_u) = 0$ for all u in H ; on the other hand, $D_a f = 0$ if and only if $\sum_{u \in H} \mathcal{F}^2(f+\varphi_u) = 2^{2n}$. But this last property means $\sum_{u \in \mathbb{F}_2^n \setminus H} \mathcal{F}^2(f + \varphi_u) = 0$, because of Parseval's relation. So we have proved that $D_a f$ is constant if and only if the set Z_f contains either H or $\mathbb{F}_2^n \setminus H$. Therefore, the cardinality of Z_f must be at least 2^{n-1} when f has a linear structure, completing the proof.

■

Remark 2 Let $f \in \mathcal{B}_n$ be such that $\mathcal{F}(f + \varphi_\alpha) \neq 0$ implies $wt(\alpha)$ even. Then f has a linear structure and we have the same result by replacing "even" by "odd". Indeed the set $\{\alpha | wt(\alpha)\ is\ even\}$ is an hyperplane of $\mathbb{F}_2^n$, say H. The coset of this hyperplane, $\overline{H}$, is the set $\{\alpha | wt(\alpha)\ is\ odd\}$. So we are looking at f which is such that Z_f contains $\overline{H}$ — respectively Z_f contains H. We can then apply Lemma 3. More precisely $D_\beta f = 0$ where $\beta = (1, \ldots, 1)$ (even case) — respectively $D_\beta f = 1$ (odd case).

In [7], Carlet and Taranikov introduce a class of resilient functions which are called ρ-*regular* functions. Such a function f satisfies: $\mathcal{F}(f+\varphi_\alpha) \neq 0$ implies $wt(\alpha) = \rho$, for a fixed ρ. These functions have resiliency of degree $\rho - 1$. Thanks to Lemma 3 these resilient functions always have linear structure.

Note that any t-resilient function $f \in \mathcal{B}_n$, with $t \geq \lfloor \frac{n}{2} \rfloor$, is such that the number of zero values in its Walsh spectrum is greater than or equal to 2^{n-1}. Thus, for such a function, we cannot apply the previous lemma. An important consequence is that the design rule for $t < \frac{n}{2}$ may be formulated as: *Construct a Boolean function $f \in \mathcal{B}_n$ by selecting an optimum choice of the design parameters of concern (nonlinearity, order of resiliency, PC degree) such that its Walsh spectrum contains less than 2^{n-1} zeros.* Now the previous lemma yields a more practical condition.

Theorem 4 *Let $f \in \mathcal{B}_n$. Then $D_a f \neq 0$ for any nonzero a if and only if f satisfies $S(f)$: there exists a basis $(e_1, \ldots, e_n)$ of $\mathbb{F}_2^n$ such that*

$$\mathcal{F}(f + \varphi_{e_i}) \neq 0 \ , \ 1 \leq i \leq n \ .$$

Moreover

(i) *when f is not balanced, f has no linear structure if and only if the condition $S(f)$ is satisfied;*

(ii) *when f is balanced, f has no linear structure if and only if there is $e \neq 0$ in $\mathbb{F}_2^n$ such that the function $g = f + \varphi_e$ is not balanced and the condition $S(g)$ is satisfied.*

Proof: We assume that f is neither affine nor constant. In accordance with Lemma 3, $D_a f = 0$ for some nonzero a if and only if Z_f contains the complement of the hyperplane $\{0, a\}^\perp$. Let

$$N_f = \{ \alpha \mid \mathcal{F}(f + \varphi_\alpha) \neq 0 \} \tag{19}$$

be the complement of Z_f in $\mathbb{F}_2^n$. Denote by $\overline{H}$ the complement of some hyperplane H. Clearly, Z_f contains $\overline{H}$ if and only if N_f is contained in H. More generally, Z_f contains the complement of some hyperplane if and only if the rank of the set N_f is at most $n-1$ (*i.e.*, $S(f)$ cannot be satisfied), completing the first part of the proof.

Now, when f is not balanced then $D_a f$ cannot be equal to 1 for some a. So *"f not balanced and $D_a f \neq 0$ for any nonzero a"* is equivalent to *"f has no linear structure"*, completing the proof of **(i)**. When f is balanced, there exists some function in the spectrum of f which is not balanced. Moreover to prove that f has no linear structure is equivalent to prove that $f + \varphi_e$ has no linear structure, for some e. When e is such that $g = f + \varphi_e$ is not balanced, g has no linear structure if and only if $S(g)$ is satisfied, as remarked above.

■

Corollary 2 *Let $f \in \mathcal{B}_n$ be a t-resilient function of degree d. Then $\# N_f \leq 2^{2(n-t-\epsilon-2)}$, where N_f is defined by (19) and $\epsilon = \lfloor \frac{n-t-2}{d} \rfloor$. Moreover, for $n \geq 2^{2(n-t-\epsilon-2)}$, f admits a linear structure.*

Proof: By Parseval's equality and according to (2), we have:

$$2^{2n} = \sum_{v \in \mathbb{F}_2^n} \mathcal{F}^2(f + \varphi_v) = 2^{2(t+2+\epsilon)} \Lambda \ ,$$

where clearly $\Lambda \geq \# N_f$. This implies $\# N_f \ 2^{2(t+2+\epsilon)} \leq 2^{2n}$ or, equivalently, $\# N_f \leq 2^{2(n-t-\epsilon-2)}$. This proves the first part of the corollary.

To prove the second part we notice that f is balanced but there always exists some $\alpha \neq 0$ such that $\mathcal{F}(f + \varphi_\alpha) \neq 0$. In accordance with Theorem 4, we need at least n other nonzero elements, say $(e_1, \ldots, e_n)$, such that $\mathcal{F}(f + \varphi_{\alpha + e_i}) \neq 0$, for any i. But this is impossible when $n + 1 > \# N_f$, completing the proof.

■

The previous corollary implies that for certain fixed values of the parameters n, d and t, it is impossible to construct a resilient function without linear structure. As an illustration, set $t = n - 5$ and $d = 3$ in Corollary 2. Then $\epsilon = 1$ and $2^{2(n-t-\epsilon-2)} = 2^4 = 16$. We can conclude as follows.

Corollary 3 *For $n \geq 16$, any $(n-5)$-resilient function $f \in \mathcal{B}_n$ which is of degree 3 has a linear structure.*

We conclude this section by giving a simple algorithm for checking that a function has no derivative equal to the constant function 1.

Proposition 5 *Let $f \in \mathcal{B}_n$. Suppose that there are u and v in $\mathbb{F}_2^n$ such that $u \neq v \neq 0$ and the four coefficients $\mathcal{F}(f)$, $\mathcal{F}(f+\varphi_u)$, $\mathcal{F}(f+\varphi_v)$ and $\mathcal{F}(f+\varphi_{u+v})$ are such that only one of them is zero. Then f has no linear structure a such that $D_a f = 1$.*

Proof: The sets Z_f and N_f are respectively defined by (17) and (19). We proved that $D_a f \neq 1$ for all a if and only if Z_f does not contain any hyperplane (see Lemma 3). Let H be any hyperplane and let $\overline{H}$ its coset. The intersection of H with any subspace $< u, v >$, $u \neq v \neq 0$, is either of dimension 2 or of dimension 1.

If $H \subset Z_f$ for some H, then $\mathcal{F}(f) = 0$ and $N_f \subset \overline{H}$. Thus, for any $u, v \in N_f$, $u+v \in Z_f$. We conclude that if a pair (u, v) satisfies the hypothesis, it is impossible to have $H \subset Z_f$ for any H.

■

5 Resilient functions and their derivatives

In this section, we focus on the values of the auto-correlation function of $f \in \mathcal{B}_n$ when f is t-resilient. Actually we want to obtain some bounds for the absolute indicator $\mathcal{M}(f)$ (defined in § 2.1) of such a function. We begin by giving a general property concerning the weights of the derivatives of Boolean functions.

Lemma 4 *Let $f \in \mathcal{B}_n$, $n \geq 3$. Assume that the weight of f is even. Then*

$$\mathcal{F}(D_a f) \equiv 0 \pmod 8 \quad \textit{for any } a \in \mathbb{F}_2^n. \tag{20}$$

Proof: Let a be any nonzero word in $\mathbb{F}_2^n$, and $D_a f(x) = f(x) + f(x+a)$. The Boolean functions $D_a f(x), f(x), f(x+a)$ can be associated to codewords of length 2^n denoted respectively $D_a f, f, f_a$. Then we have,

$$wt(D_a f) = wt(f) + wt(f_a) - 2wt(f f_a).$$

We note that $wt(f) = wt(f_a)$ for any a since f_a can be seen as a permutation of f. Thus the equation above may be rewritten to yield $wt(D_a f) = 2wt(f) - 2wt(f f_a)$. Since by assumption f is of even weight it remains to prove that $wt(f f_a)$ is even. We note that $\alpha \in \mathbb{F}_2^n$ satisfies $f(x)f(x+a) = 1$ if and only if $\alpha + a$ satisfies it too. Thus we conclude that $wt(f f_a) \equiv 0 \pmod 2$ and consequently $wt(D_a f) \equiv 0 \pmod 4$. This completes the proof.

■

Remark 3 One might expect that an arbitrary t-resilient function satisfies the following congruence, $\mathcal{F}(D_a f) \equiv 0 \pmod{2^{t+3}}$. This congruence holds for $t = 0$, but we easily found a 1-resilient function f such that $\mathcal{F}(D_a f) \equiv 0 \pmod{16}$ is not true for some a (by computer).

Next we investigate how the divisibility of derivatives is related to the resiliency order, PC degree, and algebraic degree.

Theorem 5 *Let $f \in \mathcal{B}_n$ be a t-resilient function of degree d satisfying PC(p). Set $\epsilon = \lfloor \frac{n-t-2}{d} \rfloor$. Then for $p, t \geq 0$ and for any $a \in \mathbb{F}_2^n$ we have:*

$$\mathcal{F}(D_a f) \equiv 0 \pmod{2^{2t+p+2\epsilon+5-n}} . \tag{21}$$

This property is significant for $2t + p + 2\epsilon + 2 > n$ only.

Proof: Let $a \in \mathbb{F}_2^n$ such that $wt(a) = p + 1$. Let $U_a = \{v \in \mathbb{F}_2^n \mid v \preccurlyeq a\}$ and $\overline{a} = (1 + a_1, \ldots, 1 + a_n)$. Then, since f satisfies PC(p), we can write (1) (setting $\beta = 0$ and $V^\perp = U_a$) in the following form:

$$\sum_{\alpha \preccurlyeq \overline{a}} \mathcal{F}^2(f + \varphi_\alpha) = 2^{n-(p+1)}(2^n + \mathcal{F}(D_a f)),$$

where $\mathcal{F}^2(f + \varphi_\alpha) \equiv 0 \pmod{2^{2(t+2+\epsilon)}}$ because f is t-resilient (see (2)). Since $|\mathcal{F}(D_a f)| \leq 2^n$, it is easy to see that $\mathcal{F}(D_a f)$ is congruent to 0 modulo $2^{2t+p+2\epsilon+5-n}$. Thus, we have proved that (21) holds for any a such that $wt(a) = p+1$. Now, we proceed by induction on the weight of a. Assuming that (21) holds for $wt(a) \leq p + s - 1$, $s \geq 2$ we rewrite (1) for $wt(a) = p + s$:

$$\sum_{\alpha \preccurlyeq \overline{a}} \mathcal{F}^2(f + \varphi_\alpha) = 2^{n-(p+s)}(2^n + \sum_{u \preccurlyeq a,\ wt(u) \geq p+1} \mathcal{F}(D_u f)) . \tag{22}$$

For convenience, let $\rho = 2t + p + 2\epsilon + 5 - n$. The sum on the left is congruent to 0 modulo $2^{2(t+2+\epsilon)}$. In the sum on the right, all $\mathcal{F}(D_u f)$ are known to be congruent to 0 modulo 2^ρ (by induction hypothesis) unless $u = a$. Hence the formula (22) has the following form: $2^{2(t+2+\epsilon)}\lambda = 2^{n-(p+s)}(2^\rho \lambda' + \mathcal{F}(D_a f))$, for some integers λ and λ'. This leads to:

$$\mathcal{F}(D_a f) = 2^{2(t+2+\epsilon)-n+p+s}\lambda - 2^\rho \lambda' = 2^{\rho+s-1}\lambda - 2^\rho \lambda' ,$$

since $\rho = 2(t + 2 + \epsilon) - n + p + 1$. Then we deduce that $\mathcal{F}(D_a f)$ is congruent to 0 modulo 2^ρ and conclude that this property holds for any a. Thus $\mathcal{F}(D_a f)$ is of the form $\pm 2^\rho \lambda$, for some integer $\lambda \geq 0$. Due to Lemma 4, this property is significant for $2t + p + 2\epsilon + 5 - n > 3$, completing the proof.

■

Remark 4 The first consequence of Theorem 5 is that for high order of resiliency the autocorrelation properties becomes rather poor. We proved actually that the indicators related with the propagation criterion satisfy here: $\mathcal{M}(f) \geq 2^\rho$ and $\mathcal{V}(f) \geq 2^{2n} + 2^{2\rho} \times \mu$, where $\rho = 2t + p + 2\epsilon + 5 - n$ and μ denotes the number of $a \neq 0$ such that $\mathcal{F}(D_a f) \neq 0$.

Note that for fixed p and t the divisibility of derivatives depends entirely on algebraic degree d via $\epsilon = \lfloor \frac{n-t-2}{d} \rfloor$. Hence the overall good cryptographic properties are exhibited only by functions of high algebraic degree. Furthermore, the congruence relation above clearly indicates that the size of derivatives is more sensitive to the changes of resiliency order t, than to the changes of p.

Now, we want to illustrate that *due to the previous result a large class of resilient functions cannot be used in the design of Boolean functions having good propagation properties.*

Example 4 With notation of Theorem 5, take $n = 11$ and $t = 3$. Then $d \leq 7$ and $\epsilon = \lfloor \frac{6}{d} \rfloor$. Applying Theorem 5, we get for any $a \in \mathbb{F}_2^{11}$,

$$\mathcal{F}(D_a f) \equiv 0 \pmod{2^\rho} \text{ with } \rho = p + 2\epsilon \ .$$

If $d = 3$ then $\epsilon = 2$, we obtain respectively for $p = 0, 1, \ldots, 6$ the values $\rho = 4, 5, \ldots, 10$.
If $3 < d \leq 6$ then $\epsilon = 1$. We obtain respectively for $p = 0, 1, \ldots, 6$ the values $\rho = 2, 3, \ldots, 8$.
Note that by Lemma 4 the results for $p = 0, 1$, are not significant.

Corollary 4 *Let $f \in \mathcal{B}_n$ be a t-resilient function of degree 3. Assume that $t = n - 4$. Then the derivatives of f satisfy:*

$$\mathcal{F}(D_a f) \equiv 0 \pmod{2^{n-3}} \quad \textit{for any } a \in \mathbb{F}_2^n \ .$$

Moreover, if f satisfies PC(1), then $\mathcal{F}(D_a f) \equiv 0 \pmod{2^{n-2}}$ for any a.

Proof: Due to the Siegenthaler's upper bound, $d \leq 3$ for $t = n - 4$. By setting $t = n - 4$, $p = 0$ and $d = 3$ in Theorem 5, we have $\epsilon = 0$ and then $2t + p + 2\epsilon + 5 - n = n - 3$.

If f satisfies PC(1) then $2t + p + 2\epsilon + 5 - n = n - 2$.

■

Open problem 1 Consider the set of $(n-4)$-resilient functions of degree 3 (with n variables). According to (2) and to Theorem 5, such a function presents strong divisibility properties. We can conjecture, for instance, that it has a specific ANF. Is it possible to characterize effectively this set of functions ?

Note that for $p + t = n - 2$, the result of Theorem 5 is significant for any $t \geq 0$. Taking a such that $wt(a) = p + 1$, we have $wt(\overline{a}) = t + 1$. So (1) gives here:

$$\sum_{\alpha \preccurlyeq \overline{a}} \mathcal{F}^2(f + \varphi_\alpha) = \mathcal{F}^2(f + \varphi_{\overline{a}}) = 2^{n-(p+1)}(2^n + \mathcal{F}(D_a f)) \ .$$

Hence $\mathcal{F}^2(f + \varphi_{\overline{a}}) = 0$ if and only if $\mathcal{F}(D_a f) = -2^n$, *i.e.,* a is a linear structure of f with $D_a f = 1$. We deduce the following corollary:

Corollary 5 *Let $f \in \mathcal{B}_n$ satisfying the hypothesis of Theorem 5, with $p + t = n - 2$. Then*

- *for any a: $\mathcal{F}(D_a f) \equiv 0 \pmod{2^{t+3+2\lfloor \frac{p}{d} \rfloor}}$;*
- *for any a such that $wt(a) = p + 1$: $\mathcal{F}^2(f + \varphi_{\overline{a}}) = 0$ if and only if $D_a f = 1$.*

Every Boolean function f in $\mathcal{B}_n$ can be viewed as a concatenation of two functions from $\mathcal{B}_{n-1}$, called *subfunctions of f of dimension $n - 1$*. More precisely, f can be written as,

$$f(x_1, \ldots, x_n) = (1 + x_n) f_1(x_1, \ldots, x_{n-1}) + x_n f_2(x_1, \ldots, x_{n-1}),$$

for some f_1, f_2 in $\mathcal{B}_{n-1}$.

Corollary 6 *Let $f \in \mathcal{B}_n$ and f_1, f_2 its subfunctions in $\mathcal{B}_{n-1}$. Assume that f is t-resilient and satisfies PC(p) with $p = n - t - 2$.*

Then for any $\beta \in \mathbb{F}_2^{n-1}$ such that $wt(\beta) = t$ and $\mathcal{F}(f_1 + \varphi_\beta) = \mathcal{F}(f_2 + \varphi_\beta)$, $(\beta, 1)$ is a linear structure of f. Furthermore, if both f_1 and f_2 are t-resilient, then f is affine or constant.

Proof: Note that if f is t-resilient then either both f_1 and f_2 are $(t-1)$-resilient or both f_1 and f_2 are t-resilient.

Let β be a vector satisfying the hypothesis. The Walsh transform of f in the point $(1, \beta) \in \mathbb{F}_2^n$ is calculated as,

$$\mathcal{F}(f + \varphi_{(1,\beta)}) = \mathcal{F}(f_1 + \varphi_\beta) - \mathcal{F}(f_2 + \varphi_\beta). \tag{23}$$

Then, $\mathcal{F}(f + \varphi_{(1,\beta)}) = 0$ due to the assumption. Since the weight of $(1, \beta)$ is $t + 1$, by Corollary 5 f has a linear structure.

Assume now that f_1 and f_2 are t-resilient. Then for any $\beta \in \mathbb{F}_2^{n-1}$ such that $wt(\beta) = t$ we have $\mathcal{F}(f_1 + \varphi_\beta) = \mathcal{F}(f_2 + \varphi_\beta) = 0$. Applying Corollary 5, we conclude that, for all such β, $(1, \beta)$ belongs to the linear space of f. Then the subspace V, generated by all these elements in contained in the linear space of f. Since $0 \leq t \leq n - 2$ the dimension of V is at least $n - 1$, completing the proof.

■

Open problem 2 Find other properties concerning the t-resilient functions of n variables satisfying PC(p) with $p + t = n - 2$.

6 The main classes of resilient functions

6.1 Linear concatenation

The class of t-resilient functions, described by the next theorem, is actually a subclass of the Maiorana-McFarland class (see Proposition 2). It provides one of a few designs that guarantees a moderate value of nonlinearity for a given order of resiliency. We first need to introduce some notation. Let us denote by L_k the set of all linear functions on $\mathbb{F}_2^k$; note that $\#L_k = 2^k$. We define for any $0 \leq t < k$:

$$L_k^t = \{ \varphi_c(x) = c \cdot x \mid c \in \mathbb{F}_2^k, wt(c) > t \} . \tag{24}$$

The cardinality of L_k^t is equal to $\sum_{i=0}^{k-(t+1)} \binom{k}{t+1+i}$. For fixed integers t and n, $0 \leq t < n$, we define

$$\mathbf{k} = \min_{t<k} \left\{ k \mid \sum_{i=0}^{k-(t+1)} \binom{k}{t+1+i} \geq 2^{n-k} \right\} . \tag{25}$$

Theorem 6 [8] *For any $0 \leq t < n$, let $\mathbf{k}$ be defined by (25) and $L^t_{\mathbf{k}}$ by (24). Let us choose $2^{n-\mathbf{k}}$ linear functions in $L^t_{\mathbf{k}}$, each being labeled by an element of $\mathbb{F}_2^{n-\mathbf{k}}$ as follows:*

$$\tau \in \mathbb{F}_2^{n-\mathbf{k}} \quad \longleftrightarrow \quad \ell_{[\tau]} \in L^t_{\mathbf{k}}, \text{ where } [\tau] = \sum_{i=0}^{n-\mathbf{k}-1} \tau_i 2^i \ .$$

Then the Boolean function defined for all $(y,x) \in \mathbb{F}_2^{n-\mathbf{k}} \times \mathbb{F}_2^{\mathbf{k}}$ by

$$f(y,x) = \sum_{\tau \in \mathbb{F}_2^{n-\mathbf{k}}} (y_1 + \tau_1 + 1) \cdots (y_{n-\mathbf{k}} + \tau_{n-\mathbf{k}} + 1) \ell_{[\tau]}(x), \tag{26}$$

is a t-resilient function with nonlinearity $\mathcal{N}_f = 2^{n-1} - 2^{\mathbf{k}-1}$. In general $deg(f) \leq n - \mathbf{k} + 1$ with equality if there exists a variable x_i, $i = 1, \ldots, \mathbf{k}$, which occurs an odd number of times in $\ell_{[\tau]}(x)$ when τ runs through $\mathbb{F}_2^{n-\mathbf{k}}$.

The proof of this theorem is due to Chee et al. [8]. Note that the linear functions $\ell_{[\tau]}$ in (26) are two-by-two distinct, and that, obviously, $\mathbf{k} > n/2$. Any resilient function defined above has a simple algebraic structure, since it can be viewed as a concatenation of the linear functions $\ell_{[\tau]}$: for any fixed value of y, we get $f(y,x) = \ell_{[\tau]}(x)$, where $\tau = y$. Moreover it is easy to characterize the zeros of its Walsh-spectrum and its propagation characteristics (see the next Lemma). On the one hand, these properties can be considered as a weakness. However it allows us to define precisely the cryptographic properties. We will show that a well-chosen set of functions $\ell_{[\tau]}$ insures that such a function has no linear structure.

Lemma 5 *Let f be a function in $\mathcal{B}_n$ constructed by means of Theorem 6; let (α, β) be any element in $\mathbb{F}_2^{n-\mathbf{k}} \times \mathbb{F}_2^{\mathbf{k}}$. Then f satisfies:*

(i) *$\mathcal{F}(f + \varphi_{(\alpha,\beta)}) = \pm 2^{\mathbf{k}}$ if and only if $\varphi_{(\alpha,\beta)} = \sum_{i=1}^{n-\mathbf{k}} \alpha_i y_i + \ell_{[\tau]}(x)$ for some τ. Otherwise $f + \varphi_{(\alpha,\beta)}$ is balanced.*

(ii) *$D_{(\alpha,\beta)} f$ is balanced if and only if $\alpha \neq 0$ or $\alpha = 0$ and $D_\beta \ell_{[\tau]} = 0$ for $2^{n-\mathbf{k}-1}$ values of τ exactly. Moreover $\mathcal{F}(D_{(0,\beta)}) \equiv 0 \pmod{2^{\mathbf{k}}}$.*

(iii) *(α, β) is a linear structure of f if and only if $\alpha = 0$ and $\ell_{[\tau]}(\beta) = c$ for all τ, where $c \in \mathbb{F}_2$.*

Proof: **(i)** For every fixed value of y, we get

$$f(y,x) + \varphi_{(\alpha,\beta)}(y,x) = \ell_{[y]}(x) + \sum_{i=1}^{n-\mathbf{k}} \alpha_i y_i + \sum_{i=1}^{\mathbf{k}} \beta_i x_i \ .$$

This function is balanced unless $\beta \cdot x = \ell_{[y]}(x)$. When it is not balanced, it is constant and this happens for this value of y only. Indeed, assuming that it is constant for y, we know that $\ell_{[y']}(x) \neq \ell_{[y]}(x)$, for all $y' \neq y$, providing $\mathcal{F}(f + \varphi_{(\alpha,\beta)}) = \pm 2^{\mathbf{k}}$.

(ii) We compute the derivative of f with respect to (α, β):

$$\begin{aligned} D_{(\alpha,\beta)}f &= f(y,x) + f(y+\alpha, x+\beta) \\ &= \sum_{\tau \in \mathbb{F}_2^{n-\mathbf{k}}} (y_1+\tau_1+1)\cdots(y_{n-\mathbf{k}}+\tau_{n-\mathbf{k}}+1)\ell_{[\tau]}(x) \\ &\quad + \sum_{\tau \in \mathbb{F}_2^{n-\mathbf{k}}} (y_1+\tau_1+\alpha_1+1)\cdots(y_{n-\mathbf{k}}+\tau_{n-\mathbf{k}}+\alpha_{n-\mathbf{k}}+1)\ell_{[\tau]}(x+\beta) \\ &= \sum_{\tau \in \mathbb{F}_2^{n-\mathbf{k}}} (y_1+\tau_1+1)\cdots(y_{n-\mathbf{k}}+\tau_{n-\mathbf{k}}+1)(\ell_{[\tau]}(x)+\ell_{[\tau+\alpha]}(x+\beta)). \end{aligned}$$

For any nonzero α, each sum $\ell_{[\tau]}(x)+\ell_{[\tau+\alpha]}(x+\beta)$ is a linear (affine) function for any β in $\mathbb{F}_2^{\mathbf{k}}$ – since it is not constant by construction. So $D_{(\alpha,\beta)}f$ is balanced for any nonzero α. When $\alpha = 0$, the expression above gives:

$$D_{(0,\beta)}f(y,x) = \sum_{\tau \in \mathbb{F}_2^{n-\mathbf{k}}} (y_1+\tau_1+1)\cdots(y_{n-\mathbf{k}}+\tau_{n-\mathbf{k}}+1)\ell_{[\tau]}(\beta),$$

since $\ell_{[\tau]}(x+\beta) = \ell_{[\tau]}(x)+\ell_{[\tau]}(\beta)$. Thus $D_{(0,\beta)}f(y,x)$ is constant for any fixed y. We deduce: $\mathcal{F}(D_{(0,\beta)}f) = 2^{\mathbf{k}} \times \sum_\tau (-1)^{\ell_{[\tau]}(\beta)}$.

We directly obtain **(iii)** from this last equality, since we have proved that (α, β) can be a linear structure when $\alpha = 0$ only.

■

Remark 5 The functions defined by means of Theorem 6 are said to be three-valued, since their Fourier-spectrum has three values only, i.e., 0 and $\pm 2^{\mathbf{k}}$. They are also called three-valued almost optimal when $\mathbf{k} = (n+1)/2$ for odd n or $\mathbf{k} = (n+2)/2$ for even n; in this case, the nonlinearity is maximal (for three-valued functions). Concerning the propagation characteristics, the value of the sum-of-squares indicator is known: $\mathcal{V}(f) = 2^n\mathcal{L}^2(f) = 2^{n+2\mathbf{k}}$. The value of the absolute indicator depends on the choice of the functions $\ell_{[\tau]}$. More about this kind of functions can be found in [3, 4].

So, it turns out that the choice of the set $\{\ell_0, \ldots, \ell_{2^{n-\mathbf{k}}-1}\}$ is crucial for propagation characteristics, especially if we want to construct resilient functions without linear structure. For clarity, we begin by giving a small example. By the next proposition, we indicate how this set can be chosen.

Example 5 Let $n = 5$ and $t = 0$. Thus $\sum_{i=0}^{k-1} \binom{k}{1+i} = 2^k - 1$ and we have to choose the smallest k such that $2^k - 1 \geq 2^{5-k}$. Clearly $\mathbf{k} = 3$ and we have to select $S = \{\ell_0, \ldots, \ell_3\}$, four linear functions from the set L_3^0. Note that $\#L_3^0 = 7$.

We first choose $S = \{x_1, x_2, x_3, x_1+x_2+x_3\}$. Then the function

$$f(y,x) = \sum_{\tau \in \mathbb{F}_2^2} (y_1+\tau_1+1)(y_2+\tau_2+1)\ell_{[\tau]}(x)$$

is a balanced function with $\mathcal{N}_f = 12$ – according to Theorem 6. But $(0,0,1,1,1)$ is a linear structure of f, since $\ell_i(1,1,1) = 1$ for all i, $i = 0, \ldots, 3$.

Now we take $S = \{x_1 + x_2, x_1 + x_3, x_2 + x_3, x_1 + x_2 + x_3\}$. It is easy to check that in this case we cannot have: $\ell_i(\beta) = c$ for all i, $0 \leq i \leq 3$, and for any $\beta \in \mathbb{F}_2^3$ (where c is a binary constant). Thus, f has no linear structure. Furthermore, since the linear functions ℓ_i are of weight greater than one, f is 1-resilient with $\mathcal{N}_f = 12$.

Notice that the set L_k^t defined by (24) has always rank k. Indeed, since $k > t+1$, at least the all-one vector and the k vectors of weight $(k-1)$ are in L_k^t. By adding the all-one vector to each vector of weight $(k-1)$ we obtain the standard basis.

Proposition 6 *Let f be a function in $\mathcal{B}_n$ constructed by means of Theorem 6; so $\mathbf{k}$ and t are fixed (and $\mathbf{k} > t+1$). Let us denote by S the set of the $2^{n-\mathbf{k}}$ linear functions $\ell_{[\tau]}$ which have to be chosen in $L_{\mathbf{k}}^t$. Then, there is at least one choice S such that f has no linear structure if and only if $\mathbf{k} < 2^{n-\mathbf{k}}$. In this case, S can be chosen as follows:*
— $\ell_0(x) = \lambda \cdot x$, where λ is the all-one vector;
— for every i, $1 \leq i \leq \mathbf{k}$, $\ell_i(x) = (\lambda + e_i) \cdot x$ where $e_i = (0, \ldots, 0, \overset{i}{1}, 0, \ldots, 0)$, i.e., $(e_1, \ldots, e_{\mathbf{k}})$ is the standard basis;
— $(\ell_{\mathbf{k}+1}, \ldots, \ell_{2^{n-\mathbf{k}}-1})$ are some other elements of $L_{\mathbf{k}}^t$.

Proof: It is a direct application of Theorem 4, **(ii)**. Indeed f is balanced and here we know exactly the nonzero coefficients of the Fourier-spectrum of f. So f has no linear structure if and only if we can construct one S such that the corresponding function f satisfies the hypothesis of this theorem. From Lemma 5, we know that $f + \varphi_{(\alpha,\beta)}$ is not balanced if and only if the function $\beta \cdot x$ is in S. Now we proceed as it is indicated in the proposition, and we have:

- $\ell_0 = \lambda \cdot x$ with $wt(\lambda) = \mathbf{k}$;
- so for any basis of $\mathbb{F}_2^{n-\mathbf{k}}$, say $(\alpha_1, \ldots, \alpha_{n-\mathbf{k}})$, the functions $f + \varphi_{(\alpha_j,\lambda)}$ are not balanced;
- set $\ell_i(x) = \lambda \cdot x + e_i \cdot x$, $1 \leq i \leq \mathbf{k}$ (note that $wt(\lambda + e_i) = \mathbf{k} - 1$); complete the set S with any other functions in $L_{\mathbf{k}}^t$.

Now f is fully defined and we can check that, according to Theorem 4, it has no linear structure. Set $g = f + \varphi_{(0,\lambda)}$; so g is not balanced. Our construction is such that there is a basis of $\mathbb{F}_2^{n-\mathbf{k}} \times \mathbb{F}_2^{\mathbf{k}}$,

$$(\alpha_1, 0), \ldots, (\alpha_{n-\mathbf{k}}, 0), (0, e_1), \ldots, (0, e_{\mathbf{k}})$$

such that the functions $g + \varphi_{(\alpha_j,0)}$ and $g + \varphi_{(0,e_i)}$, which are respectively the functions $f + \varphi_{(\alpha_j,\lambda)}$ and $f + \varphi_{(0,\lambda+e_i)}$, are not balanced. Applying Theorem 4, f has no linear structure.

Since the rank of $L_{\mathbf{k}}^t$ is always equal to $\mathbf{k}$, such a construction is possible if and only if the cardinality of S is strictly greater than $\mathbf{k}$, *i.e.*, $\mathbf{k} < 2^{n-\mathbf{k}}$.

■

Example 6 Let $n = 9$. For $t = 4$, we obtain $\mathbf{k} = 7$ (see (25)). But, in this case, $2^{n-\mathbf{k}} = 4$, implying that f has always a linear structure.

Now for $t = 3$, we obtain $\mathbf{k} = 6$ with $2^{n-\mathbf{k}} = 8$. So we can choose $S = \{\ell_0, \ldots, \ell_8\}$ in L_6^3, the set of linear functions $x \mapsto \beta \cdot x$ such that $\beta \in \mathbb{F}_2^6$ and $wt(\beta) \geq 4$, in such a manner that f has no linear structure. According to the previous proposition, $\ell_0(x) = x_1 + x_2 + x_3 + x_4 + x_5 + x_6$, and $\ell_i(x) = \ell_0(x) + x_i$, $1 \leq i \leq 6$. We can choose ℓ_7 to be any other function from L_6^3.

Corollary 7 *For any odd* $\mathbf{k} \geq 3$ *it is possible to construct a* $\lfloor \mathbf{k}/2 \rfloor$*-resilient Boolean function* f *of* $n = 2\mathbf{k} - 1$ *variables of degree* $\mathbf{k}$ *without linear structure and with nonlinearity* $\mathcal{N}_f = 2^{n-1} - 2^{\frac{n-1}{2}}$.

Proof: Since $\mathbf{k}$ is odd it is well-known that $\sum_{i=\lfloor \mathbf{k}/2 \rfloor + 1}^{\mathbf{k}} \binom{\mathbf{k}}{i} = 2^{\mathbf{k}-1}$. Thus, by choosing $t = \lfloor \mathbf{k}/2 \rfloor$ the cardinality of $L_{\mathbf{k}}^t$ is $2^{\mathbf{k}-1}$. Thus, we can construct a t-resilient function f in $n = 2\mathbf{k} - 1$ variables, with $\mathcal{N}_f = 2^{n-1} - 2^{\frac{n-1}{2}}$. Also, $deg(f) = n - \mathbf{k} + 1 = \mathbf{k}$ since each variable x_i, $i = 1, \ldots, \mathbf{k}$ occurs an odd number of times in $L_{\mathbf{k}}^t$. By Proposition 6, f is without linear structure.

■

Example 7 Let us construct f by means of Corollary 7 for $\mathbf{k} = 5$. So we take $t = \lfloor \mathbf{k}/2 \rfloor = 2$. Since $\sum_{i=0}^{2} \binom{5}{3+i} = 2^4$, $\#L_5^2 = 2^4$, and we must take all sixteen linear functions from L_5^2 to construct f. By Corollary 7, f is a 2-resilient function with nonlinearity $N_f = 2^{n-1} - 2^{\mathbf{k}-1} = 240$, and without linear structure. Furthermore, the degree of f is 5.

6.2 Linear structures in recursive constructions of optimal resilient functions

We are going to discuss two recursive constructions of resilient functions given respectively in [18] and [13]. The main interest of these constructions is that they provide *optimal* functions, in the sense that they have the best nonlinearity with respect to the upper bound (3). Both constructions are based on a concatenation of resilient functions with high nonlinearity. We will prove that the first construction leads to functions with linear structure while the second construction allows to avoid linear structures.

In this section, we assume that for any t-resilient function in $\mathcal{B}_n$, t satisfies $t \geq \frac{n}{2} - 2$. For this range of t the upper bound on nonlinearity is $\mathcal{N}_f \leq 2^{n-1} - 2^{t+1}$. This bound is achieved by the functions meeting the Siegenthaler's bound. Since we focus here on the existence of linear structure, we give the iterative formula proposed in [18] and indicate the nonlinearity without more explanations. By Proposition 8, we claim that such a construction in which each f_i appears several times in the concatenation, provides functions with linear space.

Proposition 7 [18] *Assume that $f_0(x), \ldots, f_{2^k-1}(x)$ are all t-resilient functions in $\mathcal{B}_m$. Let (y,z) in $\mathbb{F}_2^k \times \mathbb{F}_2^s$, where $k \geq s$. Then the function f defined by*

$$f(x,y,z) = \Big(\sum_{\tau \in \mathbb{F}_2^k} \big(\prod_{i=1}^{s} (y_i + z_i + \tau_i) \big) \big(\prod_{i=s+1}^{k} (y_i + \tau_i) \big) f_{[\tau]}(x) \Big) + \sum_{i=1}^{s} z_i, \qquad (27)$$

is an $(t+s)$-resilient function on $\mathbb{F}_2^{m+k+s}$ (where the label $[\tau]$ is computed as in Theorem 6). Furthermore, if the nonlinearity of $f_0, \ldots, f_{2^k-1}$ is at least ν_0 and the functions $f_{[\tau]}$ satisfy certain properties (see [18]) then $\mathcal{N}_f \geq 2^s(2^{n-1}(2^k-1) + \nu_0)$.

Proposition 8 *Let $f \in \mathcal{B}_{m+k+s}$ be a function constructed by means of Proposition 7. Then the subspace*

$$\{ \ (\alpha, \beta, \gamma) \in \mathbb{F}_2^m \times \mathbb{F}_2^k \times \mathbb{F}_2^s \mid \alpha = 0, \ \beta = (\gamma_1, \ldots, \gamma_s, 0, \ldots, 0) \ \}$$

is contained in the linear space of f. The linear space of f has dimension at least s.

Proof: The derivative of f with respect to any direction $(0, \beta, \gamma)$, where β is of the form $(\gamma_1, \ldots, \gamma_s, 0, \ldots, 0)$, is as follows :

$$\begin{aligned} D_{(0,\beta,\gamma)} f &= f(x,y,z) + f(x, y+\beta, z+\gamma) \\ &= \Big(\sum_{\tau \in \mathbb{F}_2^k} \big(\prod_{i=1}^{s} (y_i + z_i + \tau_i) \big) \big(\prod_{i=s+1}^{k} (y_i + \tau_i) \big) f_{[\tau]}(x) \Big) + \sum_{i=1}^{s} z_i \\ &+ \Big(\sum_{\tau \in \mathbb{F}_2^k} \big(\prod_{i=1}^{s} (y_i + \gamma_i + z_i + \gamma_i + \tau_i) \big) \big(\prod_{i=s+1}^{k} (y_i + \tau_i) \big) f_{[\tau]}(x) \Big) \\ &+ \sum_{i=1}^{s} (z_i + \gamma_i) = \sum_{i=1}^{s} z_i + \sum_{i=1}^{s} (z_i + \gamma_i) = \sum_{i=1}^{s} \gamma_i \ . \end{aligned}$$

Thus each such derivative is constant implying that the space of linear structures of f has dimension at least s.

■

By an $(n,t,d,\mathcal{N}_f)$ function we mean an n-variable, t-resilient function f with degree d and nonlinearity $\mathcal{N}_f$. The construction introduced in [13] is a recursive one and starts with a suitable input function f^0 of type $(n,t,d,\mathcal{N}_f)$, which is said to be in *desired form.*

Definition 5 *An $(n,t,d,-)$ function f is in* desired form *if it is of the form $f = (1 + x_n)f_1 + x_n f_2$, where f_1, f_2 are $(n-1,t,d-1,-)$ functions.*

An infinite sequence f^i of

$$(n+3i, \ t+2i, \ d+i, \ \mathcal{N}_{f^i} = 2^{n+3(i-1)+1} + 4\mathcal{N}_{f^{i-1}})$$

functions is then obtained for $i \geq 1$. Furthermore, if $t \geq \frac{n}{2} - 2$ and $\mathcal{N}_{f^0} = 2^{n-1} - 2^{t+1}$ then any function in this sequence will be optimal in the sense that its nonlinearity attains the upper bound on nonlinearity (see [13] for more details). We next describe one step of the algorithm.

Proposition 9 [13] *Let $f = (1 + x_n)f_1 + x_n f_2$ be an $(n, t, d, \mathcal{N}_f)$ function in desired form,where f_1, f_2 are both $(n-1, t, d-1, -)$ functions. Let the functions F and G on $\mathbb{F}_2^{n+2}$ be defined by,*

$$\begin{aligned} F &= x_{n+2} + x_{n+1} + f \quad \textit{and} \\ G &= (1 + x_{n+2} + x_{n+1})f_1 + (x_{n+2} + x_{n+1})f_2 + x_{n+2} + x_n. \end{aligned} \tag{28}$$

Then the function $H \in \mathcal{B}_{n+3}$, $H = (1 + x_{n+3})F + x_{n+3}G$ is an

$$(n+3,\ t+2,\ d+1,\ 2^{n+1} + 4\mathcal{N}_f)$$

function in desired form.

Proposition 10 *Let $f = (1 + x_n)f_1 + x_n f_2$ be an $(n, t, d, \mathcal{N}_f)$ function in desired form. Assume that f has no linear structure. Then, the function H constructed by means of Proposition 9 has no linear structure.*

Proof: Considering the restrictions of H to the hyperplane defined by $x_{n+3} = 0$ and to its coset, we note $H = (F, G)$. We will consider the restrictions of $D_\beta H$ to the same hyperplane and to its coset. When $\beta_{n+3} = 0$, then we look at $D_\beta H$ with $\beta = (a, 0)$, where $a = (\beta_1, \ldots, \beta_{n+2})$. But in this case $D_\beta H = (D_a F,\ D_a G)$. Thus $D_\beta H = c$, $c \in \{0, 1\}$, if and only if $D_a F = D_a G = c$.

The derivative of F is as follows, where $\beta' = (\beta_1, \ldots, \beta_n)$:

$$D_{(\beta', \beta_{n+1}, \beta_{n+2})} F = \beta_{n+1} + \beta_{n+2} + D_{\beta'} f\ .$$

Since f has no linear structure, the linear structures of F are of the form $(0, \ldots, 0, \beta_{n+1}, \beta_{n+2})$. So we have to compute the derivatives of G with respect to $a = (0, \ldots, 0, \beta_{n+1}, \beta_{n+2})$:

$$D_a G = (\beta_{n+2} + \beta_{n+1})(f_1 + f_2) + \beta_{n+2}\ .$$

Since f has no linear structure, then $f_1 + f_2$ cannot be constant because $D_{(0,\ldots,0,1)} f = f_1 + f_2$. Therefore $D_a G = c$ if and only if $\beta_{n+2} = \beta_{n+1} = 1$ (since $a \neq 0$). But, in this case, $D_a G = 1$ and $D_a F = 0$; we conclude that $(a, 0)$ cannot be a linear structure of H.

When $\beta_{n+3} = 1$, we use the general formula

$$D_{(a,1)} H = D_{(a,0)} H + D_{(0,\ldots,0,1)} H + D_{(a,0)} D_{(0,\ldots,0,1)} H\ .$$

We obtain: $D_{(a,1)} H = (\ D_a F + G(x + a),\ D_a G + F(x + a)\ )$. If $D_a F + G(x + a) = c$ then, by replacing $F(x + a)$ in the term on the right,

$$D_a G + F(x + a) = D_a G + F(x) + G(x + a) + c = G(x) + F(x) + c.$$

But it is easy to check that the function $F + G$ cannot be constant, implying that $D_{(1,a)} H$ cannot be equal to (c, c) where c is a binary constant.

■

References

[1] P. Camion, C. Carlet, P. Charpin and N. Sendrier, On correlation-immune functions, in *Advances in Cryptology - CRYPTO'91*. Lecture Notes in Computer Science, 576, pp. 86-100, Springer-Verlag.

[2] A. Canteaut and M. Trabbia, "Improved fast correlation attacks using parity-check equations of weight 4 and 5," in *Advances in Cryptology - EUROCRYPT 2000*. Lecture Notes in Computer Science, 1807, pp. 573–588, Springer-Verlag.

[3] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions," in *Advances in Cryptology - EUROCRYPT 2000*. Lecture Notes in Computer Science, 1807, pp. 507–522, Springer-Verlag.

[4] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine. On cryptographic properties of the cosets of $R(1,m)$. *IEEE Trans. Inform. Theory*, 47(4):1494–1513, 2001.

[5] C. Carlet, "On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions," in *Sequences and their Applications - SETA '01*, Discrete Mathematics and Theoretical Computer Science, pp. 131–144. Springer-Verlag, 2001.

[6] C. Carlet, "On cryptographic propagation criteria for Boolean functions," *Information and Computation*, no. 151, pp. 32–56, 1999.

[7] C. Carlet and Yu. Tarannikov, "Covering sequences of Boolean functions and their cryptographic significance", *Designs, Codes and Cryptography*, 25, pp. 263-279 (2002).

[8] S. Chee, S. Lee, D. Lee, and S.H. Sung, "On the correlation immune functions and their nonlinearity," in *Advances in Cryptology - ASIACRYPT'96*. Lecture Notes in Computer Science, 1163, pp. 232–243, Springer-Verlag.

[9] S. Dubuc, "Characterization of linear structures," *Designs, Codes and Cryptography*, 22, pp. 33–45, 2001.

[10] J. H. Evertse, "Linear structures in block ciphers," in *Advances in Cryptology - EUROCRYPT' 87*. Lecture Notes in Computer Science, 304, pp. 249–266, Springer Verlag.

[11] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology - EUROCRYPT'93*. Lecture Notes in Computer Science, 765, pp. 386–397, Springer-Verlag.

[12] W. Meier, and O. Staffelbach., "Nonlinearity criteria for cryptographic functions," in *Advances in Cryptology - EUROCRYPT'93*. Lecture Notes in Computer Science, 434, pp. 549–562, Springer-Verlag.

[13] E. Pasalic, T. Johansson, S. Maitra, and P. Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity. *Cryptology ePrint Archive, eprint.iacr.org, No. 2000/048*, September 26, 2000.

[14] B. Preneel, W.V. Leekwijck, L.V. Linden, R. Govaerts, and J. Vandewalle, "Propagation characteristics of Boolean functions," in *Advances in Cryptology - EUROCRYPT'90.* Lecture Notes in Computer Science, 437, pp. 155–165, Springer-Verlag.

[15] P. Sarkar and S. Maitra, "Nonlinearity bounds and constructions of resilient Boolean functions," in *Advances in Cryptology - CRYPTO 2000.* Lecture Notes in Computer Science, 1880, pp. 515-532, Springer-Verlag.

[16] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications", *IEEE Trans. Inform. Theory*, IT-30(5): 776-780, 1984.

[17] Y. Tarannikov, "On resilient Boolean functions with maximal possible nonlinearity," in *Proceedings of Indocrypt 2000.* Lecture Notes in Computer Science, 1977, pp. 19–30 , Springer Verlag.

[18] Y. V. Tarannikov, "New constructions of resilient Boolean functions with maximal nonlinearity," in *Fast Software Encryption - FSE 2001*, to be published in Lecture Notes in Computer Science, pp. 70–81 (in preproceedings). Springer Verlag, 2001.

[19] A.F. Webster and S.E. Tavares, "On the design of S-boxes," in *Advances in Cryptology - CRYPTO'85.* Lecture Notes in Computer Science, 219, pp. 523–534, Springer-Verlag.

[20] G. Xiao and J.L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Trans. Inform. Theory*, IT-34(3):569–571, 1988.

[21] X.-M. Zhang and Y. Zheng, "GAC - the criterion for global avalanche characterics of cryptographic functions," *Journal of Universal Computer Science*, vol. 1, no. 5, pp. 320–337, 1995.

[22] X.-M. Zhang and Y. Zheng, "On relationship among avalanche, nonlinearity, and propagation criteria," *in: Advances in Cryptology - Asiacrypt 2000, Lecture Notes in Computer Science*, 1976, Springer-Verlag, p. 470–483,

Contents

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)

Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot-St-Martin (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399