On a New Notion of Nonlinearity Relevant to Multi-output Pseudo-random Generators

Claude Carlet[1]* and Emmanuel Prouff[2]

[1] Claude Carlet, INRIA Projet CODES
BP 105 - 78153, Le Chesnay Cedex, France
claude.carlet@inria.fr
[2] INRIA Projet CODES and University of Paris 11
Laboratoire de Recherche en Informatique
15 rue Georges Clemenceau, 91405 Orsay Cedex, France
prouff@info.unicaen.fr

Abstract. Vectorial functions (i.e. mappings from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$, also called S-boxes) can be used in pseudo-random generators with multiple outputs. The notion of maximum correlation of these S-boxes to linear functions, introduced by Zhang and Chan, plays a central role in the resistance of the resulting stream ciphers to correlation attacks. It can be related to a notion of "unrestricted nonlinearity". We obtain a new lower bound on the overall maximum correlation to linear functions of vectorial functions which results in an upper bound on the unrestricted nonlinearity. We compare it with the known upper bounds on the nonlinearity (which are also valid for the unrestricted nonlinearity of balanced functions). We study its tightness and we exhibit a class of balanced functions whose nonlinearity and unrestricted nonlinearity are high relatively to the upper-bounds.

1 Introduction

Let n and m be two positive integers. We focus in this paper on the mappings from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, called (n, m)-functions or S-boxes. These mappings play a central role in block ciphers. In stream ciphers as well, it would be natural to use S-boxes in order to combine the outputs of n linear feedback shift registers (LFSR) or to filter the contents of a single LFSR, and then to generate m bits at each clock-cycle instead of a single one. This would result in a speed up of the encryption and of the decryption. But the robustness of such pseudo-random generators has to be studied and compared with the single-output ones.

A fundamental principle introduced by Shannon [23] for the design of conventional cryptographic systems is *confusion*, which aims at concealing any algebraic structure. Concerning S-boxes involved in the system, their adequacy with this principle must be quantified, so that we have a precise criterion for choosing

* Also member of GREYC-Caen and of the University of Paris 8

M. Matsui and R. Zuccherato (Eds.): SAC 2003, LNCS 3006, pp. 291–305, 2004.

these S-boxes. In the case of a Boolean function ($m = 1$), the main characteristic quantifying some kind of confusion induced into the system by the function is the *nonlinearity*. As shown in [3, 4, 18], this characteristic is related to the resistance to the *fast correlation attacks* on single-output stream ciphers introduced by Meier and Staffelbach [17].

In [7, 21] is studied a generalization of the nonlinearity of Boolean functions to S-boxes. This generalization is closely related to the *linear attack* of block ciphers introduced by Matsui [16]. A second generalization of the nonlinearity of Boolean functions to S-boxes, called *unrestricted nonlinearity*, can be related to their *maximum correlation* coefficients introduced by Zhang and Chan in [26], which quantify a certain type of correlation between an S-box and linear functions. Given a multi-output combining function in a combination generator or a multi-output filtering function in a nonlinear filtering generator, these coefficients must be as low as possible to make difficult correlation attacks (see [26]). So, we are interested in the maximum possible value of the maximum correlation coefficients (let us call it the *overall maximum correlation to linear functions*) which leads to the notion of unrestricted nonlinearity. Having low overall maximum correlation to linear functions is equivalent, for an S-box, to have high unrestricted nonlinearity. Zhang and Chan give only an upper bound on the maximum correlations of any S-box to linear functions (this upper-bound has been improved by the authors for perfect nonlinear S-boxes and, more recently, by Gong and Khoo [15] for some balanced S-boxes), which results in a lower bound on their unrestricted nonlinearity. This bound does not permit to know what is a reasonably high unrestricted nonlinearity. In this paper we study upper-bounds on the unrestricted nonlinearity and we exhibit S-boxes approaching them.

The paper is organized as follows. In Section 2, we recall the basic facts about the nonlinearity of functions (Boolean or vectorial). In Section 3, we recall how the notion of nonlinearity is relevant to fast correlation attacks on nonlinear filtering generators or on combination generators, and we recall the background on the maximum correlation to linear functions. We conclude this section by introducing the new notion of unrestricted nonlinearity. When the S-box $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is *balanced*, i.e. when it takes every value in $\mathbb{F}_2^m$ the same number 2^{n-m} of times, then its unrestricted nonlinearity is always lower than or equal to its nonlinearity and when $n = m$, it is null. In section 4, we exhibit a new general upper bound on the unrestricted nonlinearity of balanced S-boxes (equivalent to a lower bound on the overall maximum correlation to linear functions). We show that this bound is more precise than the upper bound $2^{n-1} - 2^{n/2-1}$ if and only if $n/2 < m$. To settle the remaining case $m \leq n/2$, we exhibit a class of balanced (n, m)-functions whose nonlinearity and unrestricted nonlinearity equal $2^{n-1} - 2^{n/2}$, which can be considered as high with respect to the introduced upper-bounds.

Length constraints do not permit us to give all proofs in details. They can be found in [6].

2 Preliminaries

2.1 Nonlinearity of Vectorial Functions

For every Boolean function f on $\mathbb{F}_2^n$, the set $\{x \in \mathbb{F}_2^n;\ f(x) = 1\}$, denoted by *Supp* f, is called the *support* of f. The cardinality of *Supp* f is called the *Hamming weight* of f and is denoted by $\omega_H(f)$. The *Hamming distance* between f and another function g, denoted by $d_H(f, g)$, being defined as the size of the set $\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}$, the nonlinearity N_f of f is the minimum Hamming distance between f and all affine functions $\ell(x) = a_1x_1 + \cdots + a_nx_n + a_0 = a \cdot x + a_0$ (where $a = (a_1, \cdots, a_n)$ ranges over $\mathbb{F}_2^n$ and a_0 ranges over $\mathbb{F}_2$). The value $a \cdot x$ in $\mathbb{F}_2$ is the usual inner product between a and x. Since the Hamming distance between two Boolean functions f_1 and f_2 equals $2^{n-1} - \frac{1}{2}\sum_{x\in\mathbb{F}_2^n}(-1)^{f_1(x)+f_2(x)}$, the nonlinearity N_f equals $2^{n-1} - \frac{1}{2}\max_{\ell\in R(1,n)}\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+\ell(x)}$, where $R(1, n)$ denotes the set of all affine functions. Equivalently, we have

$$N_f = 2^{n-1} - \frac{1}{2}\max_{u\in\mathbb{F}_2^n}\left|\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+u\cdot x}\right|. \tag{1}$$

The set of (n, m)-functions shall be denoted by $\mathcal{B}_{n,m}$ (if $m = 1$, we will denote it by $\mathcal{B}_n$, instead of $\mathcal{B}_{n,1}$). To every (n, m)-function F, we associate the m-tuple $(f_1, \cdots, f_m)$ of its coordinate Boolean functions such that $F(x) = (f_1(x), \cdots, f_m(x))$. In [7, 21] is studied a generalization of the nonlinearity of Boolean functions to S-boxes: the nonlinearity of an (n, m)-function F, denoted by N_F, is the minimum nonlinearity of all the Boolean functions $x \mapsto v \cdot F(x)$, $v \in \mathbb{F}_2^m$, $v \neq 0$, which implies

$$N_F = 2^{n-1} - \frac{1}{2}\max_{v\in\mathbb{F}_2^{m*},\ u\in\mathbb{F}_2^n}\left|\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)+u\cdot x}\right|. \tag{2}$$

In other words, N_F equals $\min_{\ell\in R(1,m)^*}\min_{u\in\mathbb{F}_2^n} d_H(\ell \circ F, \ell_u)$, where ℓ_u denotes the linear Boolean function $x \in \mathbb{F}_2^n \mapsto u \cdot x$ and where $R(1, m)^*$ denotes the set of non-constant affine Boolean functions on $\mathbb{F}_2^m$. Notice that the nonlinearity, N_F, can be rewritten $2^{n-1} - 2^{n-1}\max_{u\in\mathbb{F}_2^n} c_F(u)$, where $c_F(u)$ is called the *linear correlation to the linear function* ℓ_u and is defined by

$$c_F(u) = \frac{1}{2^n}\max_{\ell\in R(1,m)^*}\sum_{x\in\mathbb{F}_2^n}(-1)^{\ell\circ F(x)+u\cdot x} = \frac{1}{2^n}\max_{v\in\mathbb{F}_2^{m*}}\left|\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)+u\cdot x}\right|.$$

Relation (2) relates the nonlinearity of F to the Fourier transform of the so-called *sign* function, $\chi_F(x, v) = (-1)^{v\cdot F(x)}$, of F. This transform, that we shall call *Walsh transform*, is defined by the formula

$$\widehat{\chi_F}(u, v) = \sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot F(x)+u\cdot x}.$$

More generally, the Fourier transform of an integer-valued function φ on $\mathbb{F}_2^n$ is defined by $\widehat{\varphi}(u) = \sum_{x\in\mathbb{F}_2^n} \varphi(x)(-1)^{u\cdot x}$, $u \in \mathbb{F}_2^n$.

Using the Walsh transform, one can rewrite Relations (1) and (2) respecively as $N_f = 2^{n-1} - \frac{1}{2}\max_{u\in\mathbb{F}_2^n} |\widehat{\chi_f}(u)|$ and

$$N_F = 2^{n-1} - \frac{1}{2}\max_{v\in\mathbb{F}_2^{m*},u\in\mathbb{F}_2^n} |\widehat{\chi_F}(u,v)|. \tag{3}$$

For any (n,m)-function F, let φ_z denote the indicator function of the set $F^{-1}(z)$ (φ_z is defined by $\varphi_z(x) = 1$ if $F(x) = z$ and $\varphi_z(x) = 0$ otherwise), then we have

$$\widehat{\chi_F}(u,v) = \sum_{z\in\mathbb{F}_2^m} \widehat{\varphi_z}(u)(-1)^{v\cdot z} \tag{4}$$

(note that, $c_F(u)$, $u \in \mathbb{F}_2^n$, equals $1/2^n \max_{v\in\mathbb{F}_2^{m*}} |\sum_{z\in\mathbb{F}_2^m} \widehat{\varphi_z}(u)(-1)^{v\cdot z}|$).

We recall that every numerical function φ defined on $\mathbb{F}_2^n$ satisfies Parseval's relation,

$$\sum_{u\in\mathbb{F}_2^n} \widehat{\varphi}^2(u) = 2^n \sum_{x\in\mathbb{F}_2^n} \varphi^2(x), \tag{5}$$

and the inverse Fourier formula

$$\widehat{\widehat{\varphi}} = 2^n\varphi. \tag{6}$$

In the case of the Walsh transform of an (n,m)-function F, Relation (5) shows that $\sum_{u\in\mathbb{F}_2^n} \widehat{\chi_F}^2(u,v) = 2^{2n}$, for every $v \in \mathbb{F}_2^m$, which implies that N_F is upper bounded by $2^{n-1} - 2^{n/2-1}$ for every (n,m)-function F. If n is even and $m \leq \frac{n}{2}$, then this bound is tight [20]. The functions achieving it are called *bent*. Chabaud and Vaudenay proved in [7] that the nonlinearity N_F also satisfies $N_F \leq 2^{n-1} - \frac{1}{2}\sqrt{3\times 2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}}$. This bound equals $2^{n-1} - 2^{n/2-1}$ if and only if $m = n-1$ and it is better than $2^{n-1} - 2^{n/2-1}$ if and only if $m \geq n$. When $m = n$, then Chabaud-Vaudenay's bound implies that the maximum possible nonlinearity of any (n,n)-function is upper bounded by $2^{n-1} - 2^{\frac{n-1}{2}}$. The functions achieving this nonlinearity are called *almost bent* [7] and exist only when n is odd. In the other cases (when $m = n$ and n is even or when $m < n < 2m$), the maximum values achieved by the nonlinearity are unknown.

2.2 Resilient Functions

A *combination generator* consists of several linear feedback shift registers whose output sequences are combined by a nonlinear Boolean - or vectorial - function (called a *nonlinear combining function* or a *combining function*). Let F be an (n,m)-function, used as combining function, and let t be a positive integer smaller than n. We know (see [2, 24]) that a stream cipher using F as combining function opposes a maximum resistance to correlation attacks involving

at most t LFSRs, if and only if F is *t-th order correlation immune* i.e. if and only if its output distribution probability is unchanged when t - or at most t - of its input bits are kept constant. A function F is *t-resilient* if it is balanced and t-th order correlation immune. Clearly, an (n,m)-function F is t-th order correlation immune if and only if all the Boolean functions φ_z ($z \in \mathbb{F}_2^m$) defined before Equation (4) are t-th order correlation immune and it is t-resilient if and only if all the Boolean functions φ_z ($z \in \mathbb{F}_2^m$) have Hamming weight 2^{n-m} and are t-th order correlation immune. The property of t-th order correlation immunity (resp. the property of t-resiliency) can also be characterized (see [25, 2]) by the fact that $\widehat{\chi_F}(u,v)$ is null for every nonzero vector $v \in \mathbb{F}_2^m$ and for every vector $u \in \mathbb{F}_2^n$ such that $1 \leq w_H(u) \leq t$ (resp. such that $0 \leq w_H(u) \leq t$). Thus, an S-box F is t-th order correlation immune if and only if all the functions $v \cdot F$ ($v \in \mathbb{F}_2^{m*}$) are t-th order correlation immune and it is t-resilient if and only if all the functions $v \cdot F$ ($v \in \mathbb{F}_2^{m*}$) are t-resilient. Equivalently, an (n,m)-function F is t-th order correlation immune if and only if all the functions $g \circ F$ are t-th order correlation immune when g ranges over the set, $\mathcal{B}_m$, of m-variables Boolean functions (see [24]) and F is t-resilient if and only if all the functions $g \circ F$ are t-resilient when g ranges over the set of m-variables balanced Boolean functions.

Sarkar and Maitra proved in [22] that the values of the Walsh transforms of t-th order correlation immune (resp. t-resilient) Boolean functions on $\mathbb{F}_2^n$ are all divisible by 2^{t+1} (resp. 2^{t+2}). Obviously, according to the observations above, this property can be extended to S-boxes. This divisibility resulted in upper bounds (partially also obtained by Tarannikov and Zheng and Zhang) on the nonlinearities of t-th order correlation immune Boolean functions and t-resilient Boolean functions (see [22]), which are still valid for vectorial functions (see more in [6]).

3 Maximum Correlation and Unrestricted Nonlinearity

A *nonlinear filtering generator* consists of a single LFSR which is filtered by a nonlinear function. More precisely, the output sequence of a nonlinear filtering generator corresponds to the output, during a number of clock cycles, of a nonlinear function whose input bits are taken from some stages of the LFSR. To make a stream cipher with nonlinear filtering generator resistant against fast correlation attacks (see [1, 12, 13, 14, 17, 19]), the Boolean filtering function must be highly nonlinear. In the case of stream ciphers with a Boolean combining t-resilient functions f as well, Canteaut and Trabbia [4] and Canteaut [3] show that fast correlation attacks are as unefficient as possible if the coefficients $\widehat{\chi_f}(u)$ are small for every vector u of Hamming weight higher than, but close to, t and this condition is satisfied by highly nonlinear Boolean t-resilient functions. Since every known attack on a Boolean combining - or filtering - function can be applied to a Boolean function taking the form $v \cdot F$, where F is an (n,m)-function and v is a nonzero vector in $\mathbb{F}_2^m$, a vectorial combining - or filtering - function must be highly nonlinear (this ensures, by definition of the nonlinearity, that

every nonzero linear combination $v \cdot F$ has also a high nonlinearity) and must also admit, in the case of stream ciphers with combination generator, a high resiliency order (ensuring then, as showed in section 2.2, that all the nonzero linear combinations $v \cdot F$ have also a high resiliency order). But, as observed by Zhang and Chan in [26], a correlation attack on stream ciphers involving a vectorial function F can still be made by considering all the non-constant Boolean combinations, $g \circ F$, instead of only the non-zero linear ones. As we recalled in section 2.2, the high-resiliency of an (n, m)-function F implies the high correlation immunity of the Boolean functions $g \circ F$. However, as mentioned by Zhang and Chan (see [26]) the high nonlinearity of F does not imply the high nonlinearity of the functions $g \circ F$.

3.1 Maximum Correlation of Vectorial Functions

The *maximum correlation* of a vectorial (n, m)-function F to the linear function $x \mapsto u \cdot x$, denoted $\mathcal{C}_F(u)$, has been defined by Zhang and Chan as $\mathcal{C}_F(u) = \frac{1}{2^n} \max_{g \in \mathcal{B}_m} \sum_{x \in \mathbb{F}_2^n} (-1)^{g(F(x))+u \cdot x}$.

We shall exclude henceforth the case $g = cst$ in the definition of the maximum correlation during our study of the coefficients of $\mathcal{C}_F$, since composing F by a constant function g has no cryptographic relevance. Notice that this changes only the value of $\mathcal{C}_F(0)$, since the summation $\sum_{x \in \mathbb{F}_2^n} (-1)^{g \circ F(x)+u \cdot x}$ is null for every constant function g and every nonzero vector $u \in \mathbb{F}_2^n$. So we define

$$\mathcal{C}_F(u) = 2^{-n} \max_{g \in \mathcal{B}_m^*} \sum_{x \in \mathbb{F}_2^n} (-1)^{g(F(x))+u \cdot x}; \ u \in \mathbb{F}_2^n, \tag{7}$$

where $\mathcal{B}_m^*$ denotes the set of all non constant Boolean functions defined on $\mathbb{F}_2^m$. The restriction on g (being not constant) makes $\mathcal{C}_F(0)$ an indicator of the balancedness of F whereas the definition of $\mathcal{C}_F(0)$ by Zhang-Chan (i.e. without this restriction) makes it always equal to 1.

Remark 1. The maximum correlation of the S-box to the null function is not of the same type as its maximum correlation to the nonzero linear functions. Indeed, the value $\mathcal{C}_F(0)$ gives statistic information about the system whereas the other coefficients are directly related to correlation attacks. Recall that an S-box gives no statistic information to the attacker if it is balanced. If F is an (n, m)-function, then we have

$$\mathcal{C}_F(0) \geq 1 - 2^{-m+1}, \tag{8}$$

the bound being tight if and only if F is balanced. Indeed, there always exists $z_0 \in \mathbb{F}_2^m$ such that $\#F^{-1}(z_0) \leq 2^{n-m}$ and choosing g equal to the indicator of the singleton $\{z_0\}$ in (7), shows Relation (8). The case of equality is easy to prove. Relation (8) shows that, for every function F, the coefficient $\mathcal{C}_F(0)$ takes a value near 1 (if m is large enough) whereas we shall see that, for a highly nonlinear (n,m)-function, the other coefficients are close to zero (see Remark 2). ◇

It is shown in [26] that

$$\mathcal{C}_F(u) = \frac{1}{2^n} \sum_{z \in \mathbb{F}_2^m} | \sum_{x \in F^{-1}(z)} (-1)^{u \cdot x}| = \frac{1}{2^n} \sum_{z \in \mathbb{F}_2^m} |\widehat{\varphi_z}(u)| \ . \tag{9}$$

This implies, as shown in [26], the following relation between the maximum correlation to non-zero linear functions and the Walsh transform:

$$\forall u \in \mathbb{F}_2^{n*}, \ \mathcal{C}_F(u) = \frac{1}{2^{m+n}} \sum_{z \in \mathbb{F}_2^m} | \sum_{v \in \mathbb{F}_2^m} \widehat{\chi_F}(u,v)(-1)^{v \cdot z}|. \tag{10}$$

Relation (9) and the facts recalled at Subsection 2.2 imply:

Proposition 1. *A balanced (n,m)-function F is t-resilient if and only if, for every vector $u \in \mathbb{F}_2^n$ such that $1 \leq w_H(u) \leq t$, one of the two following conditions is satisfied :*
1. $c_F(u) = 0$,
2. $\mathcal{C}_F(u) = 0$,
that is, if and only if, for every vector $z \in \mathbb{F}_2^m$,
3. the Boolean function φ_z is t-th order correlation immune.

We recall now the following theorem giving an upper bound on the maximum correlation coefficients and which can be deduced straightforwardly from Relation (10).

Theorem 1. *[26] Let F be an (n,m)-function. For any nonzero vector $u \in \mathbb{F}_2^n$, we have*

$$\mathcal{C}_F(u) \leq 2^{m/2}(1 - 2^{-n+1}N_F). \tag{11}$$

Remark 2. If an (n,m)-function F (m small compared to n) has a high nonlinearity, say $N_F \geq 2^{n-1} - c \times 2^{n/2-1}$, where c is any constant value close to 1, then a first consequence of this theorem, is that, for $u \in \mathbb{F}_2^{n*}$, the maximum correlation coefficients to linear functions, $\mathcal{C}_F(u)$, are close to zero since according to Relation (11), we have $\mathcal{C}_F(u) \leq c \times 2^{m/2-n/2}$. ◇

3.2 A New Notion of Nonlinearity of Vectorial Functions: The Unrestricted Nonlinearity

We introduce, now, a generalization of the nonlinearity of Boolean functions to S-boxes, which is directly related to the maximum correlation coefficients to linear functions.

Definition 1. *Let F be an (n,m)-function. We call* unrestricted nonlinearity *of F and we denote by UN_F the minimum Hamming distance between all Boolean functions $g \circ F$ ($g \in \mathcal{B}_m{}^*$) and all* non-constant *affine functions ℓ on $\mathbb{F}_2^n$, that is, the minimum distance of the functions $g \circ F$ to $R(1,n)^*$.*

According to Relations (1) and (7), we have

$$UN_F = 2^{n-1} - 2^{n-1} \max_{u \in \mathbb{F}_2^{n*}} \mathcal{C}_F(u). \tag{12}$$

For $m > 1$, we are obliged to exclude the case ℓ constant in Definition 1 (that is to exclude $u = 0$ in Relation (12)). If we did not, then, according to Remark 2, for all S-boxes F with reasonably high nonlinearities, we would have $UN_F = 2^{n-1} - 2^{n-1}\mathcal{C}_F(0)$ and UN_F would only quantify the balancedness of F. Note that $g \in \mathcal{B}_m{}^*$ can then be replaced by $g \in \mathcal{B}_m$ in Definition 1.

We shall call *overall maximum correlation* of an (n,m)-function F to non-zero linear functions, the value $\max_{u \in \mathbb{F}_2^{n*}} \mathcal{C}_F(u)$.

Relation (12) and Relation (9), for every $u \in \mathbb{F}_2^{n*}$, imply

$$UN_F = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^{n*}} \sum_{z \in \mathbb{F}_2^m} |\widehat{\varphi_z}(u)|. \tag{13}$$

According to Theorem 1 and to Relations (11) and (12), the unrestricted nonlinearity, UN_F, of any (n,m)-function F satisfies

$$2^{n-1} - 2^{m/2}(2^{n-1} - N_F) \leq UN_F. \tag{14}$$

Remark 3. If F is balanced, then $\widehat{\chi_F}(0,v) = 0$, for every $v \in \mathbb{F}_2^{m*}$, and we have then $N_F = 2^{n-1} - \frac{1}{2}\max_{u \neq 0, v \neq 0} |\widehat{\chi_F}(u,v)|$ that is $N_F = \min_{\ell \in R(1,m)^*} \min_{u \in \mathbb{F}_2^{n*}} d_H(\ell \circ F, \ell_u)$, which implies:

$$UN_F \leq N_F \leq 2^{n-1} - 2^{n/2-1}. \tag{15}$$

$\diamond$

This implies that the unrestricted nonlinearity of a surjective linear mapping L is null, since the inequality $0 \leq UN_L \leq N_L \leq 0$ holds.

The nonlinearity UN_F is actually "unrestricted" only for balanced functions F; for these functions, the condition $\ell \neq cst$ (that is, $u \neq 0$) does not make UN_F greater than N_F.

Since $R(1,n)^*$ is invariant under the right action of an affine invertible mapping, we deduce that, for any balanced (n,m)-function F, the unrestricted nonlinearity of F is unchanged when F is right-composed with such a mapping. Moreover, if A is a surjective linear (or affine) function from $\mathbb{F}_2^p$ into $\mathbb{F}_2^n$, then we have $UN_{F \circ A} = 2^{p-n} UN_F$.

Proposition 2. *Let F be an (n,m)-function and let p be any integer, then, for every (m,p)-function ϕ, we have $UN_{\phi\circ F} \geq UN_F$. If ϕ is a permutation on $\mathbb{F}_2^m$, then we have $UN_{\phi\circ F} = UN_F$.*

Remark 4. If F is a surjective (that is, balanced) affine function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^m$, then we showed that $UN_F = 0$. Thus, the relation $UN_{\phi\circ F} = UN_F$, valid for every permutation ϕ, implies that, for every surjective affine (n,m)-function A and for every permutation ϕ on $\mathbb{F}_2^m$, the unrestricted nonlinearity of the (n,m)-function $\phi \circ A$ is null. ◇

The classical nonlinearity N_F corresponds, for balanced functions, to a version of UN_F in which g is chosen in the set of non-constant affine functions and not in the whole set $\mathcal{B}_m^*$ (cf. Remark 3). It is well known that the low nonlinearity of a function F permits a linear attack on block ciphers using this function as S-box. This attack is based on the fact that there exists at least one linear combination of the outputs of an S-box whose Hamming distance to the set of affine functions is small. Due to the iterative structure of a block cipher, the knowledge of a combination of the outputs of F with a low nonlinearity does not make more efficient the linear attack if the combination is not a linear one. But the knowledge of a nonlinear combination of the outputs of F with a low nonlinearity does make more efficient the correlation attacks in the case of stream ciphers. Indeed, as explained in [26], the maximum correlation to linear functions is relevant to stream ciphers because, when an S-box is used to combine n LFSR's or a single one (as filtering function), all of the m binary sequences it produces can be combined by a linear, or nonlinear, function g to perform correlation attacks. From this point of view, the unrestricted nonlinearity of an S-box used as combining - or filtering - function plays the same role with respect to correlation attacks on stream ciphers as nonlinearity with respect to linear attacks on block ciphers.

4 Analysis of the Unrestricted Nonlinearity

We recalled that the nonlinearity of any (n,m)-function is upper bounded by $2^{n-1} - 2^{n/2-1}$ and by $2^{n-1} - 2^{\frac{n-1}{2}}$ if $m = n$. Since we considered not only the non-constant affine functions but all the Boolean functions in ${\mathcal{B}_m}^*$ to define the unrestricted nonlinearity, there may exist a better upper bound on UN_F than $2^{n-1} - 2^{n/2-1}$. We study now such a bound.

4.1 An Upper Bound on The Unrestricted Nonlinearity of S-Boxes

We shall derive for any balanced (n,m)-function F such that $m < n$, a lower bound on the overall maximum correlation to non-zero linear functions, that is, an upper bound on UN_F.

Theorem 2. *Let F be a balanced (n,m)-function, then its overall maximum correlation to non-zero linear functions satisfies $\max_{u\in\mathbb{F}_2^{n*}} \mathcal{C}_F(u) \geq C_{n,m}$, where $C_{n,m}$ is defined for every pair (n,m) by*

$$C_{n,m} = \frac{1}{2^n}\left(\frac{2^{2m}-2^m}{2^n-1} + \sqrt{\frac{2^{2n}-2^{2n-m}}{2^n-1} + \left(\frac{2^{2m}-2^m}{2^n-1}-1\right)^2} - 1\right),$$

and its unrestricted nonlinearity is upper bounded by

$$\min\left(2^{n-1} - 2^{n/2-1}, 2^{n-1} - 2^{n-1}C_{n,m}\right) .$$

To prove this Theorem, we need the following lemma:

Lemma 1. *Let S be a set and let $\lambda = \sum_{z\in S}\lambda_z$ be a sum of $\#S$ non-negative integers indexed by the elements of S. Let M and k be two integers such that $\sum_{z\in S}\lambda_z^2 \geq M$ and $0 \leq \lambda_z \leq k$, for $z \in S$. Then we have*

$$\lambda \geq \frac{M}{2k^2} + \frac{1}{2}\sqrt{4M + \left(\frac{M}{k^2}-1\right)^2} - \frac{1}{2}. \tag{16}$$

Proof. Since, for every vector $z \in S$ such that $\lambda_z \neq 0$, the value of λ_z is lower than or equal to k, we deduce that $M \leq \sum_{z\in S}\lambda_z^2 \leq \#\{z \in S;\ \lambda_z \neq 0\} \times k^2$ i.e.

$$\#\{z \in S;\ \lambda_z \neq 0\} \geq \frac{M}{k^2}. \tag{17}$$

On the other hand, we have

$$\left(\sum_{z\in S}\lambda_z\right)^2 = \sum_{z\in S}\lambda_z^2 + \sum_{z,z'\in S, z\neq z'}\lambda_z\lambda_{z'} = \sum_{z\in S}\lambda_z^2 + \sum_{z\in S}\lambda_z[\sum_{z'\in S, z'\neq z}\lambda_{z'}].$$

According to Inequality (17), the summation $\sum_{z'\in S, z\neq z'}\lambda_{z'}$ contains at least $\frac{M}{k^2}-1$ nonzero terms (upper than or equal to 1). We deduce that

$$\lambda^2 \geq \sum_{z\in S}\lambda_z^2 + \left(\frac{M}{k^2}-1\right)\sum_{z\in S}\lambda_z \geq M + \lambda\left(\frac{M}{k^2}-1\right),$$

that is $\lambda^2 - \lambda\left(\frac{M}{k^2}-1\right) - M \geq 0$ and therefore $\lambda \geq \frac{1}{2}\left(\frac{M}{k^2}-1+\sqrt{\Delta}\right)$, where Δ equals $\left(\frac{M}{k^2}-1\right)^2 + 4M$ (since $\frac{M}{k^2}-1-\sqrt{\Delta}$ is negative).

Proof of Theorem 2.
Due to Parseval's Relation (5), for every $z \in \mathbb{F}_2^m$, we have $\sum_{u\in\mathbb{F}_2^n}\widehat{\varphi_z}^2(u) = 2^n\sum_{u\in\mathbb{F}_2^n}\varphi_z^2(u)$, which becomes $\sum_{u\in\mathbb{F}_2^n}\widehat{\varphi_z}^2(u) = 2^n\omega_H(\varphi_z)$ since φ_z is a Boolean function. Thus, for every $z \in \mathbb{F}_2^m$, we have

$$\sum_{u\in\mathbb{F}_2^{n*}}\widehat{\varphi_z}^2(u) = 2^n\omega_H(\varphi_z) - \widehat{\varphi_z}^2(0) = 2^n\omega_H(\varphi_z) - \omega_H^2(\varphi_z),$$

that is $\sum_{u\in\mathbb{F}_2^{n*}} \widehat{\varphi_z}^2(u) = 2^n(2^{n-m}) - 2^{2(n-m)}$, since F is assumed to be balanced. After summing up over $z \in \mathbb{F}_2^m$, we get

$$\sum_{u\in\mathbb{F}_2^{n*}} \sum_{z\in\mathbb{F}_2^m} \widehat{\varphi_z}^2(u) = 2^{2n} - 2^{2n-m}, \tag{18}$$

which implies

$$\max_{u\in\mathbb{F}_2^{n*}} \sum_{z\in\mathbb{F}_2^m} \widehat{\varphi_z}^2(u) \geq \frac{2^{2n} - 2^{2n-m}}{2^n - 1}. \tag{19}$$

On the other hand, for every $z \in \mathbb{F}_2^m$ and for every $u \in \mathbb{F}_2^{n*}$, the value of $|\widehat{\varphi_z}(u)|$ is upper bounded by $\omega_H(\varphi_z) = 2^{n-m}$, since we have $|\widehat{\varphi_z}(u)| = |\sum_{x\in\mathbb{F}_2^n} \varphi_z(x)(-1)^{u\cdot x}| \leq \sum_{x\in\mathbb{F}_2^n} |\varphi_z(x)| = \omega_H(\varphi_z)$ and since F is balanced. Moreover, F being balanced and m being strictly lower than n, the number $\widehat{\varphi_z}(u) = \sum_{x\in\mathbb{F}_2^n} \varphi_z(x)(-1)^{u\cdot x}$ is a summation of an even number of ± 1's and thus, $\widehat{\varphi_z}(u)$ is even. Then, due to Equations (18) and (19), one can apply Lemma 1 to

$$(S, \lambda, M, k) = (\mathbb{F}_2^m, \max_{u\in\mathbb{F}_2^{n*}} \sum_{z\in\mathbb{F}_2^m} \frac{|\widehat{\varphi_z}(u)|}{2}, \frac{2^{2n} - 2^{2n-m}}{4(2^n - 1)}, 2^{n-m-1}),$$

and Relation (13) easily completes the proof. ◇

When the resiliency order t of a balanced (n, m)-function is strictly positive, then it is possible to improve the upper bound given in Theorem 2 by applying the divisibility property of Sarkar and Maitra and Relations (15), (12) and (7).

Proposition 3. *Let F be a t-resilient (n, m)-function. Then its unrestricted nonlinearity UN_F is upper bounded by the highest multiple of 2^{t+1} which is smaller than or equal to $2^{n-1} - 2^{n/2-1}$, and to the highest multiple of 2^t which is smaller than or equal to*

$$2^{n-1} + \frac{1}{2} - \frac{2^{2m} - 2^m}{2(2^n - 1)} - \frac{1}{2}\sqrt{\frac{2^{2n} - 2^{2n-m}}{2^n - 1} + \left(\frac{2^{2m} - 2^m}{2^n - 1} - 1\right)^2}.$$

Remark 5. If the degrees of the functions φ_z are all upper bounded by some integer $d < n - t - 1$, then the bounds above can be slightly improved if $n - m \geq t + 1 + \lfloor \frac{n-t-1}{d} \rfloor$: according to the proof of [5, Theorem 6] and since all the functions φ_z have weight 2^{n-m}, the values of the Fourier transforms of the functions φ_z are then divisible by $2^{t+1+\lfloor \frac{n-t-1}{d} \rfloor}$ and UN_F is then upper bounded by the highest multiple of $2^{t+\lfloor \frac{n-t-1}{d} \rfloor}$ which is smaller than or equal to $2^{n-1} + \frac{1}{2} - \frac{2^{2m}-2^m}{2(2^n-1)} - \frac{1}{2}\sqrt{\frac{2^{2n}-2^{2n-m}}{2^n-1} + \left(\frac{2^{2m}-2^m}{2^n-1} - 1\right)^2}$. ◇

We checked that Theorem 2 gives better information than the general upper bound $2^{n-1} - 2^{n/2-1}$ if and only if $m \geq n/2 + 1$.

4.2 Construction of Balanced Vectorial Functions with High Nonlinearity and High Unrestricted Nonlinearity

Since the upper bound on the unrestricted nonlinearity of balanced (n, m)-functions given in Theorem 2 does not improve the general bound $2^{n-1} - 2^{n/2-1}$, when m is lower than or equal to $n/2$, we can try to find $(n, n/2)$-functions whose unrestricted nonlinearities approach $2^{n-1} - 2^{n/2-1}$. This will give a lower bound on the maximal possible value achieved by the unrestricted nonlinearity of the (n, m)-functions such that $m \leq n/2$.

In his Phd Thesis [9], Dillon introduces and studies a function, that we shall call *Dillon's function*, defined on the product of two finite fields of order $2^{n/2}$ by $F(x, y) = xy^{2^{n/2}-2}$, $(x, y) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$, or equivalently:

$$F(x, y) = \begin{cases} \frac{x}{y} & \text{if } y \neq 0 \\ 0 & \text{if } y = 0 \end{cases} \tag{20}$$

One can check that, for a given even integer n, this Dillon's function admits an unrestricted nonlinearity equal to $2^{n-1} - 2^{n/2} + 1$. However, being bent, this function cannot be balanced and hence, does not satisfy an essential cryptographic criterion. One can modify the definition of Dillon to obtain balanced functions which still have high unrestricted nonlinearities (recall that the idea of modifying bent functions was that of Dobbertin in [10] to design highly nonlinear balanced Boolean functions). For a given even integer n, we shall call *modified Dillon's function* the function F defined on the product of two finite fields of order $2^{n/2}$ as:

$$F(x, y) = \begin{cases} \frac{x}{y} & \text{if } y \neq 0 \\ x & \text{if } y = 0 \end{cases} \tag{21}$$

One can easily check that this kind of function is balanced.

Proposition 4. *Let F be the modified Dillon's function defined on $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$, then its unrestricted nonlinearity equals $2^{n-1} - 2^{n/2}$.*

Proof. For every pair $(x, y) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$ and for every $z \in \mathbb{F}_{2^{n/2}}$, we have

$$\varphi_z(x, y) = 1 \Longleftrightarrow \begin{cases} x = 0 & \text{, if } z = 0 \\ (x = yz \text{ and } y \neq 0) \text{ or } (x = z \text{ and } y = 0) & \text{, if } z \neq 0 \end{cases}$$

We deduce that

$$\varphi_z = \begin{cases} \mathbb{1}_{\{0\} \times \mathbb{F}_{2^{n/2}}} & \text{, if } z = 0 \\ \mathbb{1}_{\mathbb{F}_{2^{n/2}} \times (z,1)} - \delta_{(0,0)} + \delta_{(z,0)} & \text{, if } z \neq 0 \end{cases}$$

where $\mathbb{F}_{2^{n/2}} \times (z, 1)$ denotes the set $\{(uz, u);\ u \in \mathbb{F}_{2^{n/2}}\}$. So we have $\varphi_z = \mathbb{1}_{\mathbb{F}_{2^{n/2}} \times (z,1)} - \delta_{(0,0)} + \delta_{(z,0)}$ for every z. Then, for every element $z \in \mathbb{F}_{2^{n/2}}$ and

every nonzero pair $(u,u') \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$, the value of $\widehat{\varphi_z}(u,u')$ equals:

$$\sum_{(x,y)\in \mathbb{F}_{2^{n/2}}\times \mathbb{F}_{2^{n/2}}} [\mathbb{1}_{\mathbb{F}_{2^{n/2}}\times(z,1)} - \delta_{(0,0)} + \delta_{(z,0)}](x,y)(-1)^{tr(ux)+tr(u'y)}$$
$$= \sum_{(x,y)\in \mathbb{F}_{2^{n/2}}\times(z,1)} (-1)^{tr(ux)+tr(u'y)} - 1 + (-1)^{tr(uz)}.$$

The summation $\sum_{(x,y)\in \mathbb{F}_{2^{n/2}}\times(z,1)}(-1)^{tr(ux)+tr(u'y)}$ equals

$$\sum_{y\in \mathbb{F}_{2^{n/2}}} (-1)^{tr(uyz)+tr(u'y)} = \sum_{y\in \mathbb{F}_{2^{n/2}}} (-1)^{tr(y(uz+u'))}.$$

The right-hand side equals $2^{n/2}$ if $uz = u'$ i.e. if (u,u') belongs to $\mathbb{F}_{2^{n/2}} \times (1,z)$ and equals 0 otherwise. Thus, we have

$$\widehat{\varphi_z}(u,u') = 2^{n/2}\mathbb{1}_{\mathbb{F}_{2^{n/2}}\times(1,z)}(u,u') - 1 + (-1)^{tr(uz)}, \tag{22}$$

and the result follows from Relation (13).

Remark 6. When the parameters m and n satisfy $m \leq n/2$, then one can apply Proposition 2 to modified Dillon's functions to establish that every (n,m)-function $\phi \circ F$, where ϕ is an $(m, n/2)$-function and where F is a modified Dillon's $(n, n/2)$-function, has an unrestricted nonlinearity greater than or equal to $2^{n-1} - 2^{n/2}$. If ϕ is balanced, then $\phi \circ F$ is balanced. ◇

According to Proposition 4, modified Dillon's function is an example of balanced function having a high unrestricted nonlinearity. Thus, for $m \leq n/2$, an upper bound on the unrestricted nonlinearity of the (n,m)-functions cannot lie below $2^{n-1} - 2^{n/2}$.

Note that the nonlinearity of modified Dillon's $(n, n/2)$-function equals $2^{n-1} - 2^{n/2}$. Indeed, due to Equation (4), for every pair $(u,u') \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$ and every element $v \in \mathbb{F}^*_{2^{n/2}}$, the number $\widehat{\chi_F}((u,u'),v)$ equals $\sum_{z\in \mathbb{F}_{2^{n/2}}} \widehat{\varphi_z}(u,u')(-1)^{tr(vz)}$ and the result can thus easily be deduced from Relation (22).

Modified Dillon's functions seem to satisfy all the criteria needed to be used as a filtering function in a nonlinear filtering registor. However, a new kind of attacks, called *algebraic attacks*, has been introduced against cryptosystems involving S-boxes as cryptographic primitives. The best such attacks have been led by Faugere and Ars or Courtois (see [8, 11]) against stream ciphers. Also, further work has to be done to define criteria, others than the algebraic degree, on Boolean or vectorial functions related to algebraic attacks (the algebraic degree has been pointed out as a relevant criterion but other criteria are needed; the classical criteria as resiliency and nonlinearity seem to be irrelevant to quantify the resistance of an S-box against this kind of cryptanalysis).

As it can be easily check, the resiliency of modified Dillon's functions cannot be greater than 0 and, thus, it is still an open problem to define resilient vectorial functions having a high unrestricted nonlinearity and being, then, good combining functions for a multi-output stream cipher with combination generator.

References

[1] R. Anderson. Searching of the optimum correlation attack. In *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, volume 1008 of *Lecture Notes in Computer Science*. Springer, 1995. 295

[2] P. Camion and A. Canteaut. Generalization of Siegenthaler inequality and Schnorr-Vaudenay multipermutations. In *Advances in cryptology—CRYPTO '96 (Santa Barbara, CA)*, volume 1109 of *Lecture Notes in Comput. Sci.*, pages 372–386. Springer, Berlin, 1996. 294, 295

[3] A. Canteaut. On the correlations between a combining function and functions of fewer variables. In *IEEE Information Theory Workshop 2002*, 2002. 292, 295

[4] A. Canteaut and M. Trabbia. Improved fast correlation attacks using parity-check equations of weight 4 and 5. In B. Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 573–588. Springer, 2000. 292, 295

[5] C. Carlet. On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions. In *Sequences and their applications (Bergen, 2001)*, Discrete Math. Theor. Comput. Sci. (Lond.), pages 131–144. Springer, London, 2002. 301

[6] C. Carlet and E. Prouff. On the unrestricted nonlinearity. Rapport de recherche, INRIA, 2003. To appear, available at http:\\www-rocq.inria.fr/codes/Claude.Carlet/Conf/UNFSAC2003.ps. 292, 295

[7] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis. In *Advances in cryptology—EUROCRYPT '94 (Perugia)*, volume 950 of *Lecture Notes in Comput. Sci.*, pages 356–365. Springer, Berlin, 1995. 292, 293, 294

[8] N. Courtois. Fast algebraic attacks on stream ciphers with linear feedback. In *Advances in cryptology—CRYPTO 2003 (Santa Barbara, CA)*, volume 2729 of *Lecture Notes in Computer Science*, pages 177–194. Springer, Berlin, 2003. 303

[9] J. F. Dillon. *Elementary Hadamard Difference sets*. PhD thesis, University of Maryland, 1974. 302

[10] H. Dobbertin. Construction of bent functions and balanced boolean functions with high nonlinearity. In *Fast Software Encryption*, volume 1008 of *Lecture Notes in Computer Science*, pages 61–74. Springer-Verlag, 1994. 302

[11] J.-C. Faugère and G. Ars. An algebraic cryptanalysis of nonlinear filter generators using gröbner bases. Rapport de Recherche 4739, INRIA, february 2003. 303

[12] R. Forré. A fast correlation attack on nonlinearly feedforward filtered shift register sequences. In *Advances in cryptology—EUROCRYPT '89 (Brighton, 1991)*, volume 434 of *Lecture Notes in Comput. Sci.*, pages 586–595. Springer, Berlin, 1990. 295

[13] J. D. Golić, M. Salmasizadeh, L. Simpson, and E. Dawson. Fast correlation attacks on nonlinear filter generators. *Inform. Process. Lett.*, 64(1):37–42, 1997. 295

[14] T. Johansson and F. Jönsson. Improved fast correlation attacks on stream ciphers via convolutional codes. In M. Wiener, editor, *Advances in Cryptology — CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 181–197. Springer-Verlag, 1999. 295

[15] K. Khoo and G. Gong. Highly nonlinear sboxes with reduced bound on maximum correlation. In *Proceedings of IEEE International Symposium on Information Theory*, page 254, 2003. 292

[16] M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology - EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer-Verlag, 1994. 292

[17] W. Meier and O. Staffelbach. Fast correlation attacks on certain stream ciphers. *J. Cryptology*, 1(3):159–176, 1989. 292, 295

[18] W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in cryptology—EUROCRYPT '89 (Houthalen, 1989)*, volume 434 of *Lecture Notes in Comput. Sci.*, pages 549–562. Springer, Berlin, 1990. 292

[19] M. J. Mihaljević and J. D. Golić. Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence. In *Advances in cryptology—EUROCRYPT '92 (Balatonfüred, 1992)*, volume 658 of *Lecture Notes in Comput. Sci.*, pages 124–137. Springer, Berlin, 1993. 295

[20] K. Nyberg. Perfect nonlinear S-boxes. In *Advances in cryptology—EUROCRYPT '91 (Brighton, 1991)*, volume 547 of *Lecture Notes in Comput. Sci.*, pages 378–386. Springer, Berlin, 1991. 294

[21] K. Nyberg. On the construction of highly nonlinear permutations. In *Advances in cryptology—EUROCRYPT '92 (Balatonfüred, 1992)*, volume 658 of *Lecture Notes in Comput. Sci.*, pages 92–98. Springer, Berlin, 1993. 292, 293

[22] P. Sarkar and S. Maitra. Nonlinearity bounds and constructions of resilient Boolean functions. In *Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA)*, volume 1880 of *Lecture Notes in Comput. Sci.*, pages 515–532. Springer, Berlin, 2000. 295

[23] C. E. Shannon. Communication theory of secrecy systems. *Bell System Tech. J.*, 28:656–715, 1949. 291

[24] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. Inform. Theory*, 30(5):776–780, 1984. 294, 295

[25] G.-Z. Xiao and J. Massey. A spectral characterization of correlation-immune combining functions. In *IEEE Transactions on Information Theory*, volume IT 34, pages 569–571, May 1988. 295

[26] M. Zhang and A. Chan. Maximum correlation analysis of nonlinear S-boxes in stream ciphers. In *Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA)*, volume 1880 of *Lecture Notes in Comput. Sci.*, pages 501–514. Springer, Berlin, 2000. 292, 296, 297, 299