On the nonlinearity profile of the Dillon function

Claude Carlet *

Abstract

The nonlinearity profile of a Boolean function is the sequence of its minimum Hamming distances $nl_r(f)$ to all functions of degrees at most r, for $r \geq 1$. The nonlinearity profile of a vectorial function is the sequence of the minimum Hamming distances between its component functions and functions of degrees at most r, for $r \geq 1$.The profile of the multiplicative inverse functions has been lower bounded in a previous paper by the same author. No other example of an infinite class of functions with unbounded algebraic degree has been exhibited since then, whose nonlinearity profile could be efficiently lower bounded. In this preprint, we lower bound the whole nonlinearity profile of the simplest Dillon bent function $(x, y) \mapsto xy^{2^{n/2}-2}$, $x, y \in F_{2^{n/2}}$.

Keywords: Boolean function, Covering radius, higher-order nonlinearity, Reed-Muller code, S-box.

1 Introduction

Boolean functions and more generally vectorial Boolean functions $F : F_2^n \rightarrow F_2^m$ (often called (n, m)-functions) are central objects for the design and the security of symmetric cryptosystems (stream ciphers and block ciphers), see e.g. [5, 6]. In cryptography, the most usual representation of Boolean functions is the *algebraic normal form* (ANF):

$$f(x_1, \dots, x_n) = \sum_{I \subseteq \{1,\dots,n\}} a_I \prod_{i \in I} x_i,$$

where the a_I's are in F_2. The terms $\prod_{i \in I} x_i$ are called *monomials*. The *algebraic degree* $d^\circ f$ of a Boolean function f equals the global degree of its (unique) ANF, that is, the maximum degree of those monomials whose coefficients are nonzero. *Affine functions* are those Boolean functions of algebraic degrees at most 1. The Boolean functions used in stream or block ciphers must have high degrees to avoid the Berlekamp-Massey attack on stream ciphers and the higher order differential cryptanalysis on block ciphers.

*LAGA, University of Paris 8, 2 rue de la liberté, 93526 Saint-Denis, Cedex France; Email: claude.carlet@inria.fr.

Another possible representation of Boolean functions uses the identification between the vector-space F_2^n and the field F_{2^n}. It represents any Boolean function (and more generally any function from F_{2^n} to a subfield of F_{2^n}) as a polynomial in one variable $x \in F_{2^n}$ of the form $f(x) = \sum_{i=0}^{2^n-1} f_i\, x^i$, where the f_i's are elements of the field. This representation exists for every function from F_{2^n} to F_{2^n} (this is easy to prove; note that the polynomial $\sum_{i=0}^{2^n-1} f_i\, x^i$ can be obtained by using the so-called Mattson-Solomon polynomial [43, 5]) and such function f is Boolean if and only if f_0 and f_{2^n-1} belong to F_2 and $f_{2i} = f_i^2$ for every $i \neq 0,\ 2^n-1$, where $2i$ is taken mod 2^n-1. This allows representing $f(x)$ in the form $\sum_{k\in\Gamma(n)} tr_{n_k}(f_k x^k) + f_{2^n-1}x^{2^n-1}$, where $\Gamma(n)$ is the set obtained by choosing one element in each cyclotomic class of 2 modulo 2^n-1 (the most usual choice for k is the smallest element in its cyclotomic class, called the coset leader of the class), where n_k is the size of the cyclotomic class containing k and where tr_{n_k} is the trace function from $F_{2^{n_k}}$ to F_2: $tr_{n_k}(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n_k-1}}$. This representation is called the *trace representation*. Note that, for every $k \in \Gamma(n)$ and every $x \in \mathbb{F}_{2^n}$, we have $f_k \in F_{2^{n_k}}$ (since $f_k^{2^{n_k}} = f_k$) and $x^k \in F_{2^{n_k}}$ as well. A slightly different representation, often called also the trace representation, has the form $f(x) = tr(\sum_{i=0}^{2^n-1} u_i x^i)$, where $tr = tr_n$ and where the $u_i's$ are elements of the field F_{2^n} (it can be easily obtained from $f(x) = \sum_{i=0}^{2^n-1} f_i\, x^i$ since $f(x) = tr(\lambda f(x))$, when $tr(\lambda) = 1$). The former representation is unique for every Boolean function and the latter is not (see more e.g. in [5]). Recall that the 2-weight $w_2(i)$ of an integer i equals by definition the number of 1's in its binary expansion. The algebraic degree of the function is then equal to the maximum 2-weight of the exponents i with nonzero coefficients f_i in the former representation and is upper bounded by the maximum 2-weight of the exponents i with nonzero coefficients u_i in the latter.
A third representation is possible when n is even and m divides $n/2$, as a bivariate polynomial of the form $f(x,y) = \sum_{0\le i,j\le 2^{n/2}-1} f_{i,j}\, x^i y^j$, where the $f_{i,j}$'s are elements of the field $F_{2^{n/2}}$ (this representation is somehow intermediate between the n-variable ANF and the univariate representation). The algebraic degree equals then $\max_{i,j} w_2(i) + w_2(j)$.

A characteristic of Boolean functions, called their nonlinearity profile, plays an important role with respect to the security of the cryptosystems in which they are involved. For every non-negative integer $r \le n$, we denote by $nl_r(f)$ the minimum Hamming distance between f and all functions of algebraic degrees at most r (in the case of $r = 1$, we shall simply write $nl(f)$). In other words, $nl_r(f)$ equals the distance from f to the Reed-Muller code $RM(r,n)$ of length 2^n and of order r, that is, the minimal number of bits to change in the truth table of f to get a Boolean function of algebraic degree at most r). This parameter is called the *r-th order nonlinearity* of f (simply the nonlinearity in the case $r = 1$). The maximum r-th order nonlinearity of all Boolean functions in n variables equals by definition the covering radius of $RM(r,n)$ [19]. The *nonlinearity profile* of a function f is the sequence of those values $nl_r(f)$ for r ranging from 1 to $n-1$.

The same notion can be defined for S-boxes in stream or block ciphers as well, that is, for (n,m)-functions. Such functions are used in stream ciphers in the place of Boolean functions to speed up the enciphering and deciphering processes (since they output m bits instead of one at each clock cycle). They are used as well (and more systematically) in block ciphers to bring *confusion* [49] into the system. The algebraic degree of an S-box is the maximum algebraic degree of its coordinate functions. We shall denote by $nl_r(F)$ the minimum r-th order nonlinearity of all the *component functions* $\ell \circ F$, where ℓ ranges over the set of all the nonzero linear forms over F_2^m (hence, the component functions are those linear combinations of coordinate functions whose coefficients are not all-zero). Equivalently, $nl_r(F)$ is the minimum r-th order nonlinearity of all the functions $v \cdot F$, $v \in F_2^m \setminus \{0\}$, where "$\cdot$" denotes the usual inner product in F_2^m (or any other inner product). If F_2^m is endowed with the structure of the field F_{2^m}, then $nl_r(F)$ is the minimum r-th order nonlinearity of all the functions $tr(vF(x))$, $v \in F_{2^m}^*$. The algebraic degree of an S-box is also the maximum degree of its component functions.

The cryptographic relevance of the higher order nonlinearity has been illustrated by several papers [20, 33, 34, 40, 44, 47, 50]. T. Shimoyama and T. Kaneko have exhibited in [50] several quadratic functions h and sub-S-boxes F of the DES such that $nl_2(h \circ F) = 0$ (and therefore that the global S-box of the DES has the same property). They deduced a "higher-order non-linear" attack (an attack using the principle of the linear attack by Matsui but with non-linear approximations, as introduced by Knudsen and Robshaw in [40]) which needs 26% less data than Matsui's attack. This improvement is not very significant, practically, but some recent studies [32] seem to show that the notion of higher order nonlinearity can be related to potentially more powerful attacks.
Computing the r-th order nonlinearity of a given Boolean function with algebraic degree strictly greater than r is a hard task for $r > 1$. In the case of the first order, much is known in theory and also algorithmically since the nonlinearity is related to the Walsh transform, which can be computed by the algorithm of the Fast Fourier Transform (FFT). Recall that the Walsh transform of f is the Fourier transform of the "sign" function $(-1)^f$, and is defined at any vector $a \in F_2^n$ as $W_f(a) = \sum_{x \in F_2^n} (-1)^{f(x)+x \cdot a}$ (where $x \cdot a$ is an inner product in F_2^n - when the vector space F_2^n is identified to the field F_{2^n}, we can take $x \cdot a = tr(xa)$). The relation between the nonlinearity and the Walsh transform is well-known: $nl(f) = 2^{n-1} - \frac{1}{2} \max_{a \in F_2^n} |W_f(a)|$. But for $r > 1$, very little is known. Even the second order nonlinearity is known only for a few peculiar functions and for functions in small numbers of variables. A nice algorithm due to G. Kabatiansky and C. Tavernier and improved and implemented by Fourquet et al. [29, 30, 31, 35, 28] works well for $r = 2$ and $n \leq 11$ (in some cases, $n \leq 13$). But for $r \geq 3$, it is inefficient, even for $n = 8$ (the number of variables in the sub-S-boxes of the AES). No better algorithm is known.

The best known general upper bound on the first order nonlinearity of any Boolean function is:

$$nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

It can be directly deduced from the Parseval relation $\sum_{a \in F_2^n} W_f^2(a) = 2^{2n}$. It is tight for n even and untight for n odd (some lower bounds on the covering radius

exist then, see e.g. [5]). This bound is obviously valid for (n,m)-functions as well and it is then the best known bound when $m<n$. But, as proved by K. Nyberg, it is tight (achieved with equality by the so-called bent functions) only when n is even and $m\leq n/2$ (see e.g. [6]). The simplest known example of bent $(n,n/2)$-function is the Dillon function of the form $tr(xy^{2^{n/2}-2})$, where x,y live in the field $F_{2^{n/2}}$ and tr is the trace from this field to F_2. It has algebraic degree $n/2$ (which is the maximum for a bent function, see e.g. [5]).
When $m=n$, we have the better bound [16]:

$$nl(F)\leq 2^{n-1}-2^{\frac{n-1}{2}},$$

which is achieved with equality (by the so-called almost bent functions) for every odd n. For $m>n$ further (better) bounds are given in [12] but no such bound is tight. Improving upon all these bounds when they are not tight is a series of difficult open problems.

The best known upper bound on the r-th order nonlinearity of any Boolean function for $r\geq 2$ is given in [14] and has asymptotic version:

$$nl_r(f)=2^{n-1}-\frac{\sqrt{15}}{2}\cdot(1+\sqrt{2})^{r-2}\cdot 2^{n/2}+O(n^{r-2}).$$

This bound is obviously also valid for vectorial functions. It would be nice to improve it, for S-boxes, as the bound has been improved in the case $r=1$. We leave this as an open problem.

It can be proved [19, 7] that, for every positive real c such that $c^2\log_2(e)>1$, where e is the base of the natural logarithm, (e.g. for $c=1$), almost all Boolean functions satisfy

$$nl_r(f)\geq 2^{n-1}-c\sqrt{\sum_{i=0}^{r}\binom{n}{i}}\;\;2^{\frac{n-1}{2}}\approx 2^{n-1}-\frac{c\,n^{r/2}\,2^{n/2}}{\pi^{1/4}\,r^{(2r+1)/4}\,2^{3/4}},\qquad(1)$$

and that the probability that $nl_r(f)$ is smaller than this expression is asymptotically at most $O(2^{(1-\log_2 e)\sum_{i=0}^{r}\binom{n}{i}})$ when n tends to ∞.
This proves that the best possible r-th order nonlinearity of n-variable Boolean functions is asymptotically equivalent to 2^{n-1}, and that its difference with 2^{n-1} is polynomially (in n, for every fixed r) proportional to $2^{n/2}$. The proof of this fact is obtained by counting the number of functions having upper bounded r-th order nonlinearity (or more precisely by upper bounding this number) and it does not help obtaining explicit functions with non-weak r-th order nonlinearity.

In [9] has been proved a lower bound on the r-th order nonlinearity of a given function f, knowing a lower bound on the $(r-1)$-th order nonlinearity of the derivatives of f, and deduced lower bounds on the whole nonlinearity profile of the multiplicative inverse function. We denote by D_af the so-called derivative of any Boolean function f in the direction of $a\in F_2^n$:

$$D_af(x)=f(x)+f(x+a).$$

The addition is performed mod 2 (i.e. $D_a f$ is a Boolean function too). Let f be any n-variable function and r a positive integer smaller than n. We have:

$$nl_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a \in F_2^n} nl_{r-1}(D_a f)}. \tag{2}$$

This bound is tight.

In this same paper has been observed that the r-th order nonlinearity of the restriction f_0 of a function f to a hyperplane H is lower bounded by means of the r-th order nonlinearity of f:

$$nl_r(f_0) \geq nl_r(f) - 2^{n-2}. \tag{3}$$

Moreover, if the restrictions of f to H and to H^c are equal, then $nl_r(f) = 2\, nl_r(f_0)$. Note that applying iteratively this last result shows that if $f(x) = g(x_1, \cdots, x_k)$ for some k and for some k-variable function g, then we have $nl_r(f) = 2^{n-k} nl_r(g)$.

From these results was deduced an efficient lower bound on the profile of the multiplicative inverse function $F_{inv}(x) = x^{2^n-2}$, where n is any positive integer and x ranges over the field F_{2^n}. Denoting $f_{inv}(x) = tr(x^{2^n-2})$, were proved:

$$\begin{aligned} nl_2(F_{inv}) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)2^{n/2+2} + 3 \cdot 2^n} \\ &\approx 2^{n-1} - 2^{3n/4}, \end{aligned}$$

$$\begin{aligned} nl_3(F_{inv}) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n-1)\sqrt{2^{3n/2+3} + 3 \cdot 2^{n+1} - 2^{n/2+3} + 16}} \\ &\approx 2^{n-1} - 2^{7n/8-1/4}, \end{aligned}$$

and more generally:

$$nl_r(F_{inv}) \geq 2^{n-1} - l_r,$$

where the sequence l_r is defined by $l_1 = 2^{n/2}$ and $l_r = \sqrt{(2^n-1)(l_{r-1}+1) + 2^{n-2}}$. The value of l_r approximately equals $2^{n-1} - 2^{(1-2^{-r})\,n}$ and is asymptotically equivalent to 2^{n-1}, whatever is r.

In this paper we exhibit similar bounds on the simplest bent Dillon function, the bivariate function $F(x, y) = x\, y^{2^{n/2}-2}$; $x, y \in F_{2^{n/2}}$ (n even).

2 A bound for the whole nonlinearity profile of the Dillon function

We denote $f_\lambda(x, y) = tr(\lambda x\, y^{2^n-2})$, where λ is any element of $F^*_{2^{n/2}}$. All the Boolean functions f_λ, $\lambda \neq 0$, are affinely equivalent to each others. We shall write f_{dill} for f_1. But we shall need however the notation f_λ in the calculations below. We have $f_\lambda(x, y) = tr\left(\frac{\lambda x}{y}\right)$, with the convention that $\frac{\lambda x}{0} = 0$ (we shall always assume this kind of convention in the sequel).

2.1 First order nonlinearity

The first order nonlinearity of the Dillon function equals $2^{n-1} - 2^{n/2-1}$ since this function is bent.

2.2 Second order nonlinearity

Since the expression of f_λ is bivariate, we must consider its derivatives in the form $(D_{a,b})f_\lambda(x,y) = f_\lambda(x,y) + f_\lambda(x+a, y+b)$. For every $a, b \in F^*_{2^{n/2}}$, we have $(D_{a,b}f_\lambda)(ax, by) = tr\left(\frac{\lambda ax}{by} + \frac{\lambda(ax+a)}{by+b}\right) = tr\left(\frac{\lambda a(x+y)}{b(y^2+y)}\right) = f_{\lambda a/b}(x+y, y^2+y)$ if $y \notin F_2$, $(D_{a,b}f_\lambda)(ax, by) = tr(\lambda a(x+1)/b)$ if $y = 0$ and $(D_{a,b}f_\lambda)(ax, by) = tr(\lambda ax/b)$ if $y = 1$. Denoting $h(x) = tr(x)$, $g_\lambda(x,y) = f_\lambda(x, y^2+y)$ and $\delta_u(y) = 1$ if $y = u$; 0 if $y \neq u$, we deduce that, for every r, we have $nl_r(D_{a,b}f_\lambda(ax, by)) = nl_r[g_{\lambda a/b}(x+y, y) + \delta_1(y)h(\lambda ax/b)) + \delta_0(y)h(\lambda a(x+1)/b] \geq nl_r(g_{\lambda a/b}) - 2w_H(h) = nl_r(g_{\lambda a/b}) - 2^{n/2}$. Note that $nl_r(g_{\lambda a/b})$ equals twice the r-th order nonlinearity of the restriction of $f_{\lambda a/b}$ to the hyperplane H of equation $tr(y) = 0$. Applying then Relation (3), we deduce that

$$\forall a, b \in F^*_{2^{n/2}},\ nl_r(D_{a,b}f_\lambda) \geq 2\, nl_r(f_{\lambda a/b}) - 2^{n-1} - 2^{n/2}. \tag{4}$$

For every $a \in F^*_{2^{n/2}}$, we have $(D_{a,0}f_\lambda)(ax, y) = tr\left(\frac{\lambda ax}{y} + \frac{\lambda(ax+a)}{y}\right) = tr\left(\frac{\lambda a}{y}\right)$ if $y \neq 0$, $(D_{a,0}f_\lambda)(ax, y) = 0$ if $y = 0$.
Hence, according to the results of [9] recalled in the introduction of the present paper, we have the inequalities $nl(D_{a,0}f_\lambda) \geq 2^{n/2}\left(2^{n/2-1} - 2^{n/4} - 1\right) = 2^{n-1} - 2^{3n/4} - 2^{n/2}$, $nl_2(D_{a,0}f_\lambda) \geq 2^{n/2}\left(2^{n/2-1} - \frac{1}{2}\sqrt{(2^{n/2}-1)2^{n/4+2} + 3\cdot 2^{n/2}} - 1\right) = 2^{n-1} - 2^{n/2-1}\sqrt{(2^{n/2}-1)2^{n/4+2} + 3\cdot 2^{n/2}} - 2^{n/2} \approx 2^{n-1} - 2^{7n/8}$, $nl_3(D_{a,0}f_\lambda) \geq 2^{n/2}\left(2^{n/2-1} - \frac{1}{2}\sqrt{(2^{n/2}-1)\sqrt{2^{3n/4+3} + 3\cdot 2^{n/2+1} - 2^{n/4+3} + 16}} - 1\right)$, that is, $nl_3(D_{a,0}f_\lambda) \geq 2^{n-1} - 2^{n/2-1}\sqrt{(2^{n/2}-1)\sqrt{2^{3n/4+3} + 3\cdot 2^{n/2+1} - 2^{n/4+3} + 16}} - 2^{n/2} \approx 2^{n-1} - 2^{15n/16-1/4}$ and $nl_r(D_{a,0}f_\lambda) \geq 2^{n/2}(2^{n/2-1} - h_r) = 2^{n-1} - 2^{n/2}h_r$, where h_r is defined by $h_1 = 2^{n/4}$ and $h_r = \sqrt{(2^{n/2}-1)(h_{r-1}+1) + 2^{n/2-2}}$ and $nl_r(D_{a,0}f_\lambda)$ is lower bounded by approximately $2^{n-1} - 2^{(1-2^{-r-1})\,n}$.
For every $b \in F^*_{2^{n/2}}$, we have $(D_{0,b}f_\lambda)(x, by) = tr\left(\frac{\lambda x}{by} + \frac{\lambda x}{by+b}\right) = tr\left(\frac{\lambda x/b}{y^2+y}\right) = f_{\lambda/b}(x, y^2+y)$ if $y \notin F_2$ and $(D_{a,b}f_\lambda)(x, by) = tr(\lambda x/b)$ if $y \in F_2$. Hence, similarly to the case $a, b \in F^*_{2^{n/2}}$:

$$\forall b \in F^*_{2^{n/2}},\ nl_r(D_{0,b}f_\lambda) \geq 2\, nl_r(f_{\lambda a/b}) - 2^{n-1} - 2^{n/2}, \tag{5}$$

We deduce:

Lemma 1 *Every derivative $(D_{a,b}f_\lambda)$, $a \in F_{2^{n/2}}$, $b \in F^*_{2^{n/2}}$, of the Dillon function has first-order nonlinearity at least $2^{n-1} - 2^{n/2+1}$. Every derivative $(D_{a,0}f_\lambda)$, $a \in F^*_{2^{n/2}}$ has first-order nonlinearity at least $2^{n-1} - 2^{3n/4} - 2^{n/2}$.*

Applying Relation (2) and this lemma, we deduce that $nl_2(f_{dill}) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2(2^n - 2^{n/2})(2^{n-1} - 2^{n/2+1}) - 2(2^{n/2}-1)(2^{n-1} - 2^{3n/4} - 2^{n/2})}$. Hence:

Proposition 1 *Let $F_{dill}(x,y) = xy^{2^n-2}$ and $f_{dill}(x) = tr(xy^{2^n-2})$, $x, y \in F_{2^{n/2}}$. We have:*

$$\begin{aligned} nl_2(f_{dill}) &\geq 2^{n-1} - \frac{1}{2}\sqrt{2^n + (2^{n+2} + 2^{3n/4+1} + 2^{n/2+1})(2^{n/2}-1)} \\ &\approx 2^{n-1} - 2^{3n/4}. \end{aligned}$$

Hence, $nl_2(F_{dill})$ satisfies this same inequality.

2.3 Third order nonlinearity

Thanks to Proposition 1 and to Relations (4) and (5), we deduce from Relation (2) that we have $nl_3(f_{dill}) \geq 2^{n-1} - \frac{1}{2}\sqrt{A}$, where

$$\begin{aligned} A &= 2^{2n} - 2\left[(2^n - 2^{n/2})\left(2^{n-1} - \sqrt{2^n + (2^{n+2} + 2^{3n/4+1} + 2^{n/2+1})(2^{n/2}-1)} - 2^{n/2}\right)\right. \\ &\quad \left. + (2^{n/2}-1)\left(2^{n-1} - 2^{n/2-1}\sqrt{(2^{n/2}-1)2^{n/4+2} + 3\cdot 2^{n/2}} - 2^{n/2}\right)\right] \\ &= 2^n + (2^{n/2}-1)\left(2\sqrt{2^{2n} + (2^{2n+2} + 2^{7n/4+1} + 2^{3n/2+1})(2^{n/2}-1)}\right. \\ &\quad \left. + \sqrt{(2^{n/2}-1)2^{5n/4+2} + 3\cdot 2^{3n/2}}\right) + (2^n - 1)\, 2^{n/2}. \end{aligned}$$

Hence:

Proposition 2 *$nl_3(f_{dill})$ and $nl_3(F_{dill})$ are lower bounded by approximately $2^{n-1} - 2^{7n/8}$.*

2.4 Whole nonlinearity profile

The process leading to Proposition 2 can be iteratively applied, giving a lower bound on the r-th order nonlinearity of the Dillon functions for every r. The expression of this lower bound is:

$$nl_r(f_{dill}) \geq 2^{n-1} - l_r,$$

where, according to Relations (4) and (5), the sequence l_r satisfies $l_1 = 2^{n/2-1}, l_2 = 2^{3n/4}$ and $l_r \approx 2^{n/2}\sqrt{l_{r-1}} \approx 2^{(1-2^{-r})\,n}$ for $r \geq 3$. Hence, $nl_r(f_{dill})$ is asymptotically equivalent to 2^{n-1}. We can see that the lower bound we are able to prove for this profile is similar to what we could prove for the inverse function.

Remark. The approximations above are valid asymptotically when n tends to infinity. Obviously, for $r \geq d^\circ f_\lambda = n/2$ we have $nl_r(f_\lambda) = 0$.

References

[1] F. Armknecht, C. Carlet, P. Gaborit, S. Künzli, W. Meier and O. Ruatta. Efficient computation of algebraic immunity for algebraic and fast algebraic attacks. Advances in Cryptology, EUROCRYPT 2006, Lecture Notes in Computer Science 4004 , pp. 147-164, 2006.

[2] F. Armknecht and M. Krause. Constructing single- and multi-output boolean functions with maximal immunity. Proceedings of *ICALP 2006*, Lecture Notes of Computer Science 4052, Springer, pp. 180-191, 2006.

[3] T. Baignères, P. Junod and S. Vaudenay. How far can we go beyond linear cryptanalysis? *Proceedings of ASIACRYPT 2004*, Advances in Cryptology, LNCS 3329, pp. 432-450, 2004.

[4] A. Braeken and B. Preneel. On the Algebraic Immunity of Symmetric Boolean Functions. Indocrypt 2005, LNCS 3797, pp. 35–48, 2005. Some false results of this reference have been corrected in Braeken's PhD thesis entitled "Cryptographic properties of Boolean functions and S-boxes" and available at URL http://homes.esat.kuleuven.be/ abraeken/thesisAn.pdf.

[5] C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the monography *Boolean Methods and Models*, Y. Crama and P. Hammer eds, Cambridge University Press, to appear. Preliminary version available at http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html

[6] C. Carlet. Vectorial Boolean Functions for Cryptography. Chapter of the monography *Boolean Methods and Models*, Y. Crama and P. Hammer eds, Cambridge University Press, to appear. Preliminary version available at http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html

[7] C. Carlet. The complexity of Boolean functions from cryptographic viewpoint. Dagstuhl Seminar "Complexity of Boolean Functions", 2006. Paper available at URL http://drops.dagstuhl.de/portals/06111/

[8] C. Carlet. On the higher order nonlinearities of algebraic immune functions. CRYPTO 2006. Lecture Notes in Computer Science 4117, pp. 584-601, 2006.

[9] C. Carlet. Recursive Lower Bounds on the Nonlinearity Profile of Boolean Functions and Their Applications *IEEE Transactions on Information Theory* Volume 54, Issue 3, pp. 1262 - 1272, 2008.

[10] C. Carlet. A method of construction of balanced functions with optimum algebraic immunity. To appear in the Proceedings of the International Workshop on Coding and Cryptography, The Wuyi Mountain, Fujiang, China, June 11-15, 2007, published by World Scientific Publishing Co. in its series of Coding and Cryptology, Vol. 4, 2008.

[11] C. Carlet, D. Dalai, K. Gupta and S. Maitra. Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction. IEEE Transactions on Information Theory, vol. 52, no. 7, pp. 3105-3121, July 2006.

[12] C. Carlet and C. Ding. Nonlinearities of S-boxes. *Finite Fields and its Applications* Vol. 13 Issue 1, pp. 121-135, January 2007.

[13] C. Carlet and K. Feng. New balanced Boolean functions satisfying all the main cryptographic criteria. IACR cryptology e-print archive 2008/244.

[14] C. Carlet and S. Mesnager. Improving the upper bounds on the covering radii of binary Reed-Muller codes. *IEEE Transactions on Information Theory* 53, pp. 162-173, 2007.

[15] L. Carlitz and S. Uchiyama. Bounds for exponential sums. Duke Math. Journal 1, pp. 37-41, 1957.

[16] F. Chabaud and S. Vaudenay. Links between Differential and Linear Cryptanalysis. *EUROCRYPT'94, Advances in Cryptology, Lecture Notes in Computer Science* 950, Springer Verlag, pp. 356-365, 1995.

[17] P. Charpin, T. Helleseth and V. Zinoviev. Propagation characteristics of $x \to x^{-1}$ and Kloosterman sums. Finite Fields and their Applications 13, Issue 2, pp. 366-381, 2007.

[18] J. H. Cheon and D. H. Lee. Resistance of S-Boxes against Algebraic Attacks. Proceedings of FSE 2004. Lecture Notes in Computer Science 3017, pp. 83-94, 2004.

[19] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein. *Covering codes.* North-Holland, 1997.

[20] N. Courtois. Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt. Proceedings of ICISC 2002, LNCS 2587, pp. 182-199.

[21] N. Courtois, B. Debraize and E. Garrido. On exact algebraic [non-]immunity of S-boxes based on power functions. IACR e-print archive 2005/203.

[22] N. Courtois and W. Meier. Algebraic attacks on stream ciphers with linear feedback. Advances in Cryptology - EUROCRYPT 2003, number 2656 in Lecture Notes in Computer Science, pp. 345–359. Springer Verlag, 2003.

[23] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. *Advances in cryptology–ASIACRYPT 2002, Lecture Notes in Computer Science* 2501, pp. 267-287, Springer, 2003.

[24] J. Daemen and V. Rijmen. AES proposal: Rijndael. http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf, 1999.

[25] D. K. Dalai, S. Maitra and S. Sarkar. Basic Theory in Construction of Boolean Functions with Maximum Possible Annihilator Immunity. Designs, Codes and Cryptography, Volume 40, Number 1, Pages 41–58, July 2006. Cryptology ePrint Archive, http://eprint.iacr.org/, No. 2005/229, 15 July, 2005.

[26] D. K. Dalai, K. C. Gupta and S. Maitra. Cryptographically Significant Boolean functions: Construction and Analysis in terms of Algebraic Immunity. Workshop on Fast Software Encryption, FSE 2005, pages 98–111, number 3557, Lecture Notes in Computer Science, Springer-Verlag.

[27] F. Didier. A new upper bound on the block error probability after decoding over the erasure channel. *IEEE Transactions on Information Theory* 52, pp. 4496- 4503, 2006.

[28] I. Dumer, G. Kabatiansky and C. Tavernier. List decoding of Reed-Muller codes up to the Johnson bound with almost linear complexity. Proceedings of ISIT 2006. Seattle, USA.

[29] R. Fourquet. Une FFT adaptée au décodage par liste dans les codes de Reed-Muller d'ordres 1 et 2. Master-thesis of the University of Paris VIII, Thales communication, Bois Colombes, 2006.

[30] R. Fourquet. Private communication. 2007.

[31] R. Fourquet and C. Tavernier. An improved list decoding algorithm for the second order ReedMuller codes and its applications. *Designs, Codes and Cryptography*, to appear, 2008.

[32] R. Fourquet and C. Tavernier. Private communication. 2008.

[33] J. Golic. Fast low order approximation of cryptographic functions. Proceedings of EUROCRYPT'96, LNCS 1070, pp. 268-282, 1996.

[34] T. Iwata and K. Kurosawa. Probabilistic higher order differential attack and higher order bent functions. Proceedings of ASIACRYPT'99, LNCS 1716, pp. 62-74, 1999.

[35] G. Kabatiansky and C. Tavernier. List decoding of second order Reed-Muller codes. In Proc. 8^{th} Intern. Simp. Comm. Theory and Applications. Ambelside, UK, july 2005.

[36] B. Kaliski and M. Robshaw. Linear cryptanalysis using multiple approximations. Proceedings of CRTPTO 94. Lecture Notes in Computer Science 839, pp. 26-38, 1994.

[37] T. Kasami and N. Tokura. On the weight structure of Reed-Muller codes. *IEEE Transactions on Information Theory*, Vol. IT-16, N.6, Novembre 1970, pp. 752-825.

[38] T. Kasami, N. Tokura and S.Azumi. On the weight enumeration of weights less than 2.5d of Reed-Muller codes. *Information and Control* 30, 380-95 (1976).

[39] T. Kasami, N. Tokura and S.Azumi. On the weight enumeration of weights less than 2.5d of Reed-Muller codes. Report of faculty of Eng. Sci, Osaka Univ., Japan.

[40] L.R. Knudsen and M. J. B. Robshaw. Non-linear approximations in linear cryptanalysis. Proceedings of EUROCRYPT'96, Lecture Notes in Computer Science 1070, pp. 224-236, 1996.

[41] G. Lachaud and J. Wolfmann. The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes. *IEEE Trans. Inform. Theory*, vol. 36, pp. 686-692, 1990.

[42] M. Lobanov. Tight bound between nonlinearity and algebraic immunity. Paper 2005/441 in http://eprint.iacr.org/

[43] F. J. MacWilliams and N. J. Sloane. *The theory of error-correcting codes*, Amsterdam, North Holland. 1977.

[44] U. M. Maurer. New approaches to the design of self-synchronizing stream ciphers. Proceedings of EUROCRYPT'91. Lecture Notes in Computer Science 547, pp. 458-471, 1991.

[45] W. Meier, E. Pasalic and C. Carlet. Algebraic attacks and decomposition of Boolean functions. EUROCRYPT 2004, number 3027 in Lecture Notes in Computer Science, pp. 474–491. Springer Verlag, 2004.

[46] S. Mesnager. Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity. *IEEE Trans. Inform. Theory*, VOL.54, No.8, August 2008. Preliminary version available at Cryptology ePrint Archive, no. 2007/117.

[47] W. Millan. Low order approximation of cipher functions. Cryptographic Policy and Algorithms. Lecture Notes in Computer Science 1029, pp. 144-155, 1996.

[48] A. Shanbhag, V. Kumar and T. Helleseth. An upper bound for the extended Kloosterman sums over Galois rings. *Finite Fields and their Applications* 4, pp. 218-238, 1998.

[49] C.E. Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28, pp. 656-715, 1949.

[50] T. Shimoyama and T. Kaneko. Quadratic Relation of S-box and Its Application to the Linear Attack of Full Round DES. Proceedings of CRYPTO 98. Lecture Notes In Computer Science; Vol. 1462, pp. 200-211, 1998.