On Bent and Highly Nonlinear Balanced/Resilient Functions and Their Algebraic Immunities

Claude Carlet*

INRIA, Projet CODES, BP 105 - 78153, Le Chesnay Cedex, France
claude.carlet@inria.fr

Abstract. Since the introduction of the notions of nonlinearity in the mid-70's (the term has been in fact introduced later), of correlation immunity and resiliency in the mid-80's, and of algebraic immunity recently, the problem of efficiently constructing Boolean functions satisfying, at high levels, one or several of these criteria has received much attention. Only few primary constructions are known, and secondary constructions are also necessary to obtain functions achieving or approaching the best possible cryptographic characteristics. After recalling the background on cryptographic criteria and making some general observations, we try to give a survey of all these constructions and their properties. We then show that a nice and simple property of Boolean functions leads to a general secondary construction building an n-variable function from three known n-variable functions. This construction generalizes secondary constructions recently obtained for Boolean bent functions and also leads to secondary constructions of highly nonlinear balanced or resilient functions, with potentially better algebraic immunities than the three functions used as building blocks.

Keywords: stream cipher, Boolean function, algebraic degree, resiliency, nonlinearity, algebraic attack.

1 Introduction

Boolean functions, that is, F_2-valued functions defined on the vector space F_2^n of all binary words of a given length n, are used in the S-boxes of block ciphers and in the pseudo-random generators of stream ciphers. They play a central role in their security. The generation of the keystream consists, in many stream ciphers, of a linear part, producing a sequence with a large period, usually composed of one or several LFSR's, and a nonlinear combining or filtering function f which produces the output, given the state of the linear part. The main classical cryptographic criteria for designing such function f are balancedness (f is balanced if its Hamming weight equals 2^{n-1}) to prevent the system from leaking statistical information on the plaintext when the ciphertext is known, a high algebraic

[*] Also member of the University of Paris 8 (MAATICAH).

M. Fossorier et al. (Eds.): AAECC 2006, LNCS 3857, pp. 1–28, 2006.

degree (that is, a high degree of the algebraic normal form of the function) to prevent the system from Massey's attack by the Berlekamp-Massey algorithm, a high order of correlation immunity (and more precisely, of resiliency, since the functions must be balanced) to counter correlation attacks (at least in the case of combining functions), and a high nonlinearity (that is, a large Hamming distance to affine functions) to withstand correlation attacks (again) and linear attacks.

The recent algebraic attacks have led to further characteristics of Boolean functions. These attacks recover the secret key by solving an overdefined system of multivariate algebraic equations. The scenarios found in [26], under which low degree equations can be deduced from the knowledge of the nonlinear combining or filtering function, have led in [48] to a new parameter, the (basic) algebraic immunity, which must be high. This condition is itself not sufficient, since a function can have sufficiently high algebraic immunity and be weak against fast algebraic attacks [25]. A further criterion strengthening the basic notion of algebraic immunity can be defined accordingly.

The problems of designing numerous bent functions (that is, functions with highest possible nonlinearity) and of efficiently constructing highly nonlinear balanced (or, if necessary, resilient) functions with high algebraic degrees have been receiving much attention for several years. They are relevant to several domains: mainly cryptography, but also combinatorics, design theory, coding theory ... Few primary constructions (in which the functions are designed *ex nihilo*) are known, and secondary constructions (which use already defined functions to design new ones) are also necessary to obtain functions, on a sufficient number of variables, achieving or approaching the best possible cryptographic characteristics. We can say that research has obtained limited but non-negligible success in these matters. However, the problem of meeting all of these characteristics at sufficient levels and, also, achieving high algebraic immunities, with functions whose outputs can be fastly computed (this is also a necessary condition for using them in stream ciphers) shows some resistance. The most efficient primary construction in this matter has been obtained in [29] (the authors present their result as a secondary construction, but as they observe themselves, their construction is just a direct sum of a function taken as a building block, with a function that they design and which corresponds to a primary construction). It leads to functions in any even numbers of variables and with optimal algebraic immunities. And as shown in [19], their algebraic degrees are very high and their output can be very fastly computed. They are not balanced, but any function! can be made balanced by adding one variable. The remaining problem is in their insufficient nonlinearities, which makes them unusable in cryptosystems. Used as a secondary construction, their method does not give full satisfaction either, for the same reason. Hence, this secondary construction represents a very nice but still partial step towards a good tradeoff between nonlinearity, resiliency and algebraic immunity.

Most classical primary or secondary constructions of highly nonlinear functions seem to produce insufficient algebraic immunities. For instance, the

10-variable Boolean function used in the LILI keystream generator (a submission to NESSIE European call for cryptographic primitives) is built following [56] by using classical constructions; see [59]. It has algebraic immunity 4 and is responsible for the lack of resistance of LILI to algebraic attacks, see [26].

As shown in [48], taking random balanced functions on sufficiently large numbers of variables could suffice to withstand algebraic attacks on the stream ciphers using them. It would also withstand fast algebraic attacks (this can be checked with the same methods as in [48]). As shown in [49], it would moreover give reasonable nonlinearities. But such solution would imply using functions on large numbers of variables, whose outputs would be computable in much too long time. This would not allow acceptable efficiency of the corresponding stream ciphers. It would not allow nonzero resiliency orders either.

The present paper tries to present the state of the art on Boolean cryptographic functions and to suggest several directions for further research. At the end of the paper, a construction (first presented in [17]) of functions on F_2^n from functions on F_2^n is presented, which combined with the classical primary and secondary constructions can lead to functions achieving high algebraic degrees, high nonlinearities and high resiliency orders, and which also allows attaining potentially high algebraic immunity. The same principle allows constructing bent functions too.

2 Preliminaries and General Observations

In some parts of this paper, we will deal in the same time with sums modulo 2 and with sums computed in $\mathbb{Z}$. We denote by $\oplus$ the addition in F_2 (but we denote by $+$ the addition in the field F_{2^n} and in the vector space F_2^n, since there will be no ambiguity) and by $+$ the addition in $\mathbb{Z}$. We denote by $\bigoplus_{i\in\dots}$ (resp. $\sum_{i\in\dots}$) the corresponding multiple sums. Let n be any positive integer. Any Boolean function f on n variables admits a unique algebraic normal form (A.N.F.):

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

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 maximum degree of those monomials with nonzero coefficients in its algebraic normal form. *Affine functions* are those Boolean functions of degrees at most 1.

Another representation of Boolean functions is also very useful. The vector space F_2^n can be endowed with the structure of the field F_{2^n}, since this field is an n-dimensional F_2-vector space. The function $(u,v)\mapsto tr(u\,v)$, where $tr(u)=u+u^2+u^{2^2}+\cdots+u^{2^{n-1}}$ is the *trace function*, is an inner product in F_{2^n}. Every Boolean function can be written in the form $f(x)=tr(F(x))$ where F is a mapping from F_{2^n} into F_{2^n}, and this leads to the *trace representation*: $f(x)=tr\left(\sum_{i=0}^{2^n-1}\beta_i\,x^i\right)$, where $\beta_i\in F_{2^n}$. Thanks to the fact that $tr(u^2)=tr(u)$ for every $u\in F_{2^n}$, we can restrict the exponents i with nonzero coefficients β_i so that there is at most one such exponent in each cyclotomic class $\{i \times 2^j\, [\bmod (2^n-1)]\,;\ j \in N\}$.

The *Hamming weight* $w_H(f)$ of a Boolean function f on n variables is the size of its support $\{x \in F_2^n;\ f(x)=1\}$. The *Hamming distance* $d_H(f,g)$ between two Boolean functions f and g is the Hamming weight of their difference $f \oplus g$. The *nonlinearity* of f is its minimum distance to all affine functions. Functions used in stream or block ciphers must have high nonlinearities to resist the attacks on these ciphers (correlation and linear attacks, see [4, 40, 41, 58]). The nonlinearity of f can be expressed by means of the discrete Fourier transform of the "sign" function $\chi_f(x) = (-1)^{f(x)}$, equal to $\widehat{\chi_f}(s) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus x \cdot s}$ (and which is called the *Walsh transform*, or Walsh-Hadamard transform): the distance $d_H(f,l)$ between f and the affine function $l(x) = s \cdot x \oplus \epsilon$ ($s \in F_2^n;\ \epsilon \in F_2$) and the number $\widehat{\chi_f}(s)$ are related by:

$$\widehat{\chi_f}(s) = (-1)^{\epsilon}(2^n - 2d_H(f,l)) \qquad (1)$$

and the nonlinearity N_f of any Boolean function on F_2^n is therefore related to the Walsh spectrum of χ_f via the relation:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{s \in F_2^n} |\widehat{\chi_f}(s)|. \qquad (2)$$

It is upper bounded by $2^{n-1} - 2^{n/2-1}$ because of the so-called Parseval's relation $\sum_{s \in F_2^n} \widehat{\chi_f}^2(s) = 2^{2n}$.

A Boolean function is called *bent* if its nonlinearity equals $2^{n-1} - 2^{n/2-1}$, where n is necessarily even. Then, its distance to every affine function equals $2^{n-1} \pm 2^{n/2-1}$, according to Parseval's relation again and to (1).

A Boolean function f is bent if and only if all of its *derivatives* $D_a f(x) = f(x) \oplus f(x+a)$ are balanced, (see [53]). Hence, f is bent if and only if its support is a *difference set* (cf. [30]).

If f is bent, then the *dual* Boolean function $\widetilde{f}$ defined on F_2^n by $\widehat{\chi_f}(s) = 2^{\frac{n}{2}} \chi_{\widetilde{f}}(s)$ is bent. The dual of $\widetilde{f}$ is f itself. The mapping $f \mapsto \widetilde{f}$ is an isometry (the Hamming distance between two bent functions is equal to that of their duals).

The notion of bent function is invariant under linear equivalence and it is independent of the choice of the inner product in F_2^n (since any other inner product has the form $\langle x, s\rangle = x \cdot L(s)$, where L is an auto-adjoint linear isomorphism).

Rothaus' inequality [53] states that any bent function has algebraic degree at most $n/2$. Algebraic degree being an important complexity parameter, bent functions with high degrees are preferred from cryptographic viewpoint.

The class of bent functions, whose determination or classification is still an open problem, is relevant to cryptography (cf. [47]), to algebraic coding theory (cf. [45]), to sequence theory (cf. [51]) and to design theory (any difference set can be used to construct a symmetric design, cf. [1], pages 274-278). More information on bent functions can be found in the survey paper [10] or in the more recent chapter [18].

The class of bent functions is included in the class of the so-called *plateaued* functions. This notion has been introduced by Zheng and Zhang in [62]. A function is called plateaued if its Walsh transform takes at most three values 0 and $\pm\lambda$ (where λ is some positive integer, that we call the *amplitude* of the plateaued function). Because of Parseval's relation, λ must be of the form 2^r where $r \geq \frac{n}{2}$, and the suppport $\{s \in F_2^n / \widehat{\chi_f}(s) \neq 0\}$ of the Walsh transform of a plateaued function of amplitude 2^r has size 2^{2n-2r}.

Bent functions cannot be *balanced*, i.e. have uniformly distributed output. Hence, they cannot be used without modifications in the pseudo-random generator of a stream cipher, since this would leak statistical information on the plaintext, given the ciphertext[1]. Finding balanced functions with highest known nonlinearities is an important cryptographic task, as well as obtaining the best possible upper bounds on the nonlinearities of balanced functions. A nice way of designing highly nonlinear balanced functions is due to Dobbertin [33]: taking a bent function f which is constant on an $n/2$-dimensional flat A of F_2^n and replacing the values of f on A by the values of a highly nonlinear balanced function on A (identified to a function on $F_2^{n/2}$). The problem of similarly modifying bent functions into resilient functions (see definition below) has been studied in [46].

After the criteria of balancedness, high algebraic degree and high nonlinearity, which are relevant to all stream ciphers, another important cryptographic criterion for Boolean functions is resiliency. It plays a central role in their security, at least in the case of the standard model – the combination generator (cf. [57]). In this model, the vector whose coordinates are the outputs to n linear feedback shift registers is the input to a Boolean function. The output to the function during N clock cycles produces the keystream (of length N, the length of the plaintext), which is then (as in any stream cipher) bitwise xored with the message to produce the cipher. Some divide-and-conquer attacks exist on this method of encryption (cf. [4, 40, 41, 58]). To withstand these *correlation attacks*, the distribution probability of the output to the function must be unaltered when any m of its inputs are fixed [58], with m as large as possible. This property, called *m-th order correlation-immunity* [57], is characterized by the set of zero values in the Walsh spectrum [61]: f is m-th order correlation-immune if and only if $\widehat{\chi_f}(u) = 0$, for all $u \in F_2^n$ such that $1 \leq w_H(u) \leq m$, where $w_H(u)$ denotes the Hamming weight of the n-bit vector u, (the number of its nonzero components). Balanced m-th order correlation-immune functions are called *m-resilient* functions. They are characterized by the fact that $\widehat{\chi_f}(u) = 0$ for all $u \in F_2^n$ such that $0 \leq w_H(u) \leq m$.

The notions of correlation immune and resilient functions are not invariant under linear equivalence; they are invariant under translations $x \mapsto x + a$, since, if $g(x) = f(x + a)$, then $\widehat{\chi_g}(u) = \widehat{\chi_f}(u)(-1)^{a \cdot u}$, under permutations of the input coordinates, and when n is even, under an additional involution (see [38]).

Siegenthaler's inequality [57] states that any m-th order correlation immune function on n variables has degree at most $n - m$, that any m-resilient function

[1] However, as soon as n is large enough (say $n \geq 20$), the bias $\frac{2^{n/2-1}}{2^{n-1}}$ between their weights and the weight of balanced functions is quite small.

$(0 \leq m < n-1)$ has algebraic degree smaller than or equal to $n-m-1$ and that any $(n-1)$-resilient function has algebraic degree 1. We shall call *Siegenthaler's bound* this property.

Sarkar and Maitra have shown that the Hamming distance between any m-resilient function and any affine function is divisible by 2^{m+1} (this divisibility bound is improved in [11, 23] for functions with specified algebraic degrees). This leads to an upper bound on the nonlinearity of m-resilient functions (also partly obtained by Tarannikov and by Zhang and Zheng): the nonlinearity of any m-resilient function is smaller than or equal to $2^{n-1} - 2^{m+1}$ if $\frac{n}{2} - 1 < m + 1$, to $2^{n-1} - 2^{\frac{n}{2}-1} - 2^{m+1}$ if n is even and $\frac{n}{2} - 1 \geq m+1$ and to $2^{n-1} - 2^{m+1} \left\lceil 2^{n/2-m-2} \right\rceil$ if n is odd and $\frac{n}{2} - 1 \geq m + 1$. We shall call this set of upper bounds *Sarkar et al.'s bound.* A similar bound exists for correlation immune functions, but we do not recall it since non-balanced correlation immune functions present little cryptographic interest.

Two kinds of constructions, providing resilient functions with degrees and nonlinearities approaching or achieving the known bounds, can be identified. Some constructions give direct definitions of Boolean functions. There are few such *primary* constructions and new ideas for designing them are currently lacking. Except for small values of the number of variables, the only known primary construction of resilient functions which leads to a wide class of such functions, the Maiorana-McFarland's construction, does not allow designing balanced or resilient functions with high degrees and high nonlinearities (see e.g. [12, 13]), for which the trade-off between these parameters achieve the bounds recalled above. Moreover, the stream ciphers using the constructed functions are subject to the time-memory-data trade-off attack (see [42]). Modifications and generalizations of this construction have been proposed (see e.g. [12, 16, 50, 55]), but these generalizations lead to classes with roughly the same properties as the original class. *Secondary* constructions use previously defined functions (that we shall call "building blocks") to build new ones. Most of them design n-variable functions from m-variable functions with $m < n$ and lead in practice to recursive constructions.

Until recently, these criteria were the only requirements needed for the design of the function f used in a stream cipher as a combining function or as a filtering one (in the filter model, a single LFSR of greater length is used and the input to the n-variable Boolean function is given by a subset of n positions in this LFSR). The recent algebraic attacks [25, 26] have changed this situation by adding new criteria of considerable importance to this list. Algebraic attacks exploit multivariate relations involving key/state bits and output bits of f. If one such relation (or, better, several) is found that is of low degree in the key/state bits, algebraic attacks are very efficient. It is demonstrated in [26] that low degree relations and thus successful algebraic attacks exist for several well known constructions of stream ciphers that are immune to all previously known attacks. These low degree relations are obtained by multiplying the Boolean function f by a well chosen low degree nonzero function g, such that the product function

fg (that is, the function which support equals the intersection of the supports of f and g) has also low degree.

The scenarios found in [26], under which functions $g \neq 0$ and h of degrees at most d exist such that $fg = h$, have been simplified in [48] into two scenarios: (1) there exists a nonzero Boolean function g of degree at most d whose support is disjoint from the support of f, i.e. such that $fg = 0$ (such a function g is called an *annihilator* of f); (2) there exists a nonzero annihilator, of degree at most d, of $f \oplus 1$ (we write then: $g \preceq f$).

The (basic) *algebraic immunity* $AI(f)$ of a Boolean function f is the minimum value of d such that f or $f \oplus 1$ admits a nonzero annihilator of degree d. Obviously, $AI(f)$ is upper bounded by the degree $d^\circ f$. It should be high enough (at least equal to 7).

When the total number $1 + \ldots + \binom{n}{d}$ of monomials of degrees at most d is strictly greater than 2^{n-1}, these monomials and their products with f cannot be linearly independent. This proves, as observed in [26], that the algebraic immunity of any function f satisfies $AI(f) \leq \lceil n/2 \rceil$. This implies that Boolean functions used in stream ciphers must have at least 13 variables. In fact, 13 is very probably insufficient.

Another upper bound on $AI(f)$, which involves the nonlinearity of f, has been proved in [28]: $\sum_{i=0}^{AI(f)-2} \binom{n}{i} \leq N_f$. It is a consequence of the double inequality $\sum_{i=0}^{AI(f)-1} \binom{n}{i} \leq w_H(f) \leq \sum_{i=0}^{n-AI(f)} \binom{n}{i}$, which also implies that a function f such that $AI(f) = \frac{n+1}{2}$ (n odd) must be balanced.

There is more generally a relationship between $AI(f)$ and the minimum distance $N_f^{(r)}$ between f and all Boolean functions of degrees at most r (the so-called Reed-Muller code of order r), that we shall call the r-th order nonlinearity of f. We have $\sum_{i=0}^{AI(f)-r-1} \binom{n}{i} \leq N_f^{(r)}$ (see [19]). Moreover:

Proposition 1. *If $AI(f) \leq r$ and if f is balanced, then we have $N_f^{(r)} \leq 2^{n-1} - 2^{n-r}$.*

Proof. By hypothesis, there exists a nonzero function g of degree at most r such that $g \preceq f$ or $g \preceq f \oplus 1$. Since g is nonzero and belongs to the Reed-Muller code of order r, it has weight at least the minimum distance of this code, that is 2^{n-r}. If $g \preceq f$, then $d_H(f,g) = w_H(f \oplus g) = w_H(f) - w_H(g) \leq 2^{n-1} - 2^{n-r}$. If $g \preceq f \oplus 1$, then $d_H(f, g \oplus 1) = w_H(f \oplus g \oplus 1) = w_H(f \oplus 1) - w_H(g) \leq 2^{n-1} - 2^{n-r}$. This implies in both cases that $N_f^{(r)} \leq 2^{n-1} - 2^{n-r}$. ◇

This observation opens a direction for research: finding balanced functions with r-th order nonlinearity strictly greater than $2^{n-1} - 2^{n-r}$ for some high value of r. A combinatorial argument shows that such functions exist almost surely as soon as $r \leq .17 \times n$. Indeed, the number of n-variable Boolean functions of algebraic degrees at most r equals $2^{1+n+\binom{n}{2}+\cdots+\binom{n}{r}}$. Such a function h being given, the number of those Boolean functions f such that the Hamming distance $d_H(f,h)$ satisfies $d_H(f,h) \leq 2^{n-1} - R$ for some positive number R equals $\displaystyle\sum_{0 \leq i \leq 2^{n-1}-R} \binom{2^n}{i}$.

It is known (see [45], page 310) that, for every integer N and every $\delta < 1/2$, the number $\sum_{0\leq i\leq \delta N}\binom{N}{i}$ is upper bounded by $2^{NH_2(\delta)}$, and it is noticed in [15] that $2^{NH_2(\delta)} < 2^{N-2N(\frac{1}{2}-\delta)^2\,\log_2 e}$. Hence, $\sum_{0\leq i\leq 2^{n-1}-R}\binom{2^n}{i}$ is upper bounded by $2^{2^n-2^{-n+1}R^2\,\log_2 e}$, and the number of those Boolean functions such that $N_f^{(r)} \leq 2^{n-1}-R$ is therefore smaller than $2^{1+n+\binom{n}{2}+\ldots+\binom{n}{r}+2^n-2^{-n+1}R^2\,\log_2 e}$. According to [45] again, we have: $1+n+\binom{n}{2}+\ldots+\binom{n}{r} \leq 2^{nH_2(r/n)}$. The probability that a random n-variable Boolean function f satisfies $N_f^{(r)} \leq 2^{n-1}-2^{n-r}$ is then smaller than $2^{2^{nH_2(r/n)}-2^{n(1-2r/n)+1}\,\log_2 e}$. It is a simple matter to show that, when $r/n \leq .17$, this probability tends to 0 when n tends to infinity.

A high value of $AI(f)$ is not a sufficient property for a resistance to algebraic attacks, because of fast algebraic attacks [25], in which h can have a greater degree than g. Indeed, while the complexity of the standard algebraic attack is roughly $O\left(\binom{n}{AI(f)}^3\right)$, the complexity of the fast algebraic attack, when functions $g \neq 0$ and h have been found such that $fg = h$, is roughly $O\left(\binom{n}{d^\circ g}\binom{n}{d^\circ h}\log_2\left(\binom{n}{d^\circ h}\right)+\binom{n}{d^\circ g}^3+\binom{n}{d^\circ h}{\log_2}^2\left(\binom{n}{d^\circ h}\right)\right)$ [36]. Similarly as above, when the number of monomials of degrees at most e, plus the number of monomials of degrees at most d, is strictly greater than 2^n – that is, when $d^\circ g + d^\circ h \geq n$ – there exist $g \neq 0$ of degree at most e and h of degree at most d such that $fg = h$. An n-variable function f is then optimal with respect to fast! algebraic attacks if there do not exist two functions $g \neq 0$ and h such that $fg = h$ and $d^\circ g + d^\circ h < n$. Very little research in this direction has been done already.

3 The Known Constructions of Bent Functions and of Resilient Functions and the Corresponding Degrees, Nonlinearities and Algebraic Immunities

3.1 Primary Constructions

Maiorana-McFarland Constructions. Maiorana-McFarland class (cf. [31]) is the set of all the (bent) Boolean functions on $F_2^n = \{(x,y), x,y \in F_2^{\frac{n}{2}}\}$ (n even) of the form :

$$f(x,y) = x\cdot\pi(y)\oplus g(y) \tag{3}$$

where π is any permutation on $F_2^{\frac{n}{2}}$ and g is any Boolean function on $F_2^{\frac{n}{2}}$.

The dual of f is then $\widetilde{f}(x,y) = y\cdot\pi^{-1}(x)\oplus g(\pi^{-1}(x))$. Notice that the degree of f can be $n/2$, i.e. be optimal.

In [3] is introduced a generalization leading to balanced and resilient functions: let m and $n = r+s$ be any integers such that $r > m \geq 0$, $s > 0$, g any Boolean function on F_2^s and ϕ a mapping from F_2^s to F_2^r such that every element in $\phi(F_2^s)$ has Hamming weight strictly greater than m, then the function:

$$f(x,y) = x \cdot \phi(y) \oplus g(y), \; x \in F_2^r, \; y \in F_2^s \tag{4}$$

is m-resilient, since we have

$$\widehat{\chi_f}(a,b) = 2^r \sum_{y \in \phi^{-1}(a)} (-1)^{g(y) \oplus b \cdot y}. \tag{5}$$

The degree of f (which is upper bounded by $s+1$) and its nonlinearity have been studied in [12, 13]. The functions of the form (4), for $\frac{n}{2} - 1 < m+1$, can have high nonlinearities. However, optimality or sub-optimality with respect to Siegenthaler's and Sarkar et al's bounds could be obtained with this construction only with functions in which r was large and s was small. These functions having then low degrees, they are not suitable for practical use. In the case $\frac{n}{2} - 1 \geq m+1$, no function belonging to Maiorana-McFarland's class and having nearly optimal nonlinearity could be constructed, except in the limit case $\frac{n}{2} - 1 = m+1$.

It has been shown in [22] that, under an assumption on ϕ which seems highly probable, unless r is much greater than s (case that we must exclude for degree reasons), every highly nonlinear function (4) satisfies $AI(f) \leq s$. This has been also checked by computer experiment. Table 1, from [22], gives the AI of some resilient functions built by the Maiorana-McFarland. The notation 'Const' is for the type of construction used: the classical construction of [3] is denoted by 'a', the case where exactly two elements of F_2^s have the same image of weight at least w but with different values for the function g is denoted by 'b'.

Generalizations of Maiorana-McFarland's functions have been studied in [12, 16]. They have the respective forms $f(x,y) = \bigoplus_{i=1}^{\lfloor r/2 \rfloor} x_{2i-1} x_{2i} \, \psi_i(y) \oplus x \cdot \phi(y) \oplus$

Table 1. Computation of some characteristics for Boolean functions built by the Maiorana-McFarland construction

n	r	s	degree	Const.	w	resiliency	nonlinearity	alg. immunity
8	4	4	5	b	2	2	112	3
9	5	4	5	b	3	3	224	3
9	5	4	5	a	3	2	240	4
10	5	5	6	b	3	3	480	4
10	6	4	5	a	4	3	480	4
11	6	5	6	b	4	4	960	4
11	6	5	6	a	3	2	992	5
12	6	6	7	b	4	4	$2^{11} - 2^6$	5
12	7	5	6	a	4	3	$2^{11} - 2^6$	5
13	7	6	7	a	4	3	$2^{11} - 2^6$	5
13	7	6	7	b	4	4	$2^{12} - 2^7$	5
13	8	5	6	a	5	4	$2^{12} - 2^7$	5
14	7	7	8	b	4	4	$2^{13} - 2^7$	5
14	8	6	7	b	6	6	$2^{13} - 2^8$	5
14	8	6	7	a	5	4	$2^{13} - 2^7$	5
14	8	6	7	a	5	4	$2^{13} - 2^7$	5
14	9	5	6	a	7	6	$2^{13} - 2^8$	5

$g(y)$ and $f(x,y) = \prod_{i=1}^{\varphi(y)} (x \cdot \phi_i(y) \oplus g_i(y) \oplus 1) \oplus x \cdot \phi(y) \oplus g(y)$. The first one has more or less the same behavior with respect to resiliency and nonlinearity as the original construction, but allows achieving some particular tradeoffs that seemed impossible to achieve before. Its degree is upper bounded by $s+2$, and, *under the same reasonable assumption on ψ as the one evoked above for ϕ, we have $AI(f) \leq s+1$. The degree and the algebraic immunity of the second form have potential better behavior. Further work on this subject will have to be made in the future.* Modifications have also been proposed (see e.g. [52], in which some affine functions, at least one, are replaced by suitably chosen nonlinear functions) but it is shown in [48] that the algebraic immunities of these functions are often low.

Effective Partial-Spreads Constructions. In [31] is also introduced the class of bent functions called $\mathcal{PS}_{ap}$ (a subclass of the so-called Partial-Spreads class), whose elements are defined the following way:
$F_2^{\frac{n}{2}}$ is identified to the Galois field $F_{2^{\frac{n}{2}}}$ and F_2^n is identified to $F_{2^{\frac{n}{2}}} \times F_{2^{\frac{n}{2}}}$; $\mathcal{PS}_{ap}$ (or more precisely an extended version of the original one given by Dillon) is the set of all the functions of the form $f(x,y) = g(x\, y^{2^{\frac{n}{2}}-2})$ (i.e. $g(\frac{x}{y})$ with $\frac{x}{y}=0$ if $x=0$ or $y=0$) where g is a balanced Boolean function on $F_2^{\frac{n}{2}}$. We have then $\widetilde{f}(x,y) = g(\frac{y}{x})$. The degree of f is optimal, even if g is affine (see e.g. [21]).

An alternative representation of these functions is as follows. F_{2^n} equals $F_{2^{n/2}} + \omega F_{2^{n/2}}$, where $\omega \in F_{2^n} \setminus F_{2^{n/2}}$. A function f belongs to $\mathcal{PS}_{ap}$ if and only if it has weight $2^{n-1} \pm 2^{n/2-1}$ and satisfies $f(\beta x) = f(x)$, for every $\beta \in F^*_{2^{n/2}}$. This last condition is equivalent to $f(\alpha^{2^{n/2}+1}x) = f(x)$, where α is a primitive element of F_{2^n}. Indeed, $\alpha^{2^{n/2}+1}$ is a primitive element of $F_{2^{n/2}}$.

It is proved in [35] that, almost surely, any function in this class satisfies $AI(f) = d^\circ(f) = n/2$.

The idea of this construction is used in [9] to obtain a construction of correlation-immune functions:
Let s and r be two positive integers and $n = r+s$, g a function from F_{2^r} to F_2, ϕ a linear mapping from F_2^s to F_{2^r} and u an element of F_{2^r} such that $u+\phi(y) \neq 0$, $\forall y \in F_2^s$. Let f be the function from $F_{2^r} \times F_2^s \sim F_2^n$ to F_2 defined by:

$$f(x,y) = g\left(\frac{x}{u+\phi(y)}\right) \oplus v \cdot y, \tag{6}$$

where $v \in F_2^s$. If, for every z in F_{2^r}, $\phi^*(z) \oplus v$ has weight greater than m, where $\phi^* : F_{2^r} \mapsto F_2^s$ is the adjoint of ϕ, then f is m-resilient.

The same observations as for Maiorana-McFarland's construction on the ability of these functions to have nonlinearities near Sarkar-Maitra's bound can be made. This construction generates a small number of functions (compared to the Mariorana-McFarland construction). But it may be able to reach better algebraic immunities and *it should be studied further for this reason.*

Functions with Few Terms in Their Trace Representation. The so-called Gold function $tr\left(\alpha x^{2^r+1}\right)$ ($r \in \mathbb{N}$, n even) is bent if and only if $\alpha \notin \{x^{2^r+1}; x \in$

$F_{2^n}\}$. The Dillon function $tr\left(\alpha x^{2^{n/2}-1}\right)$ is bent if and only if the Kloosterman sum $\sum_{x\in F_{2^{n/2}}}(-1)^{tr_{n/2}(1/x+\alpha x)}$ is null, where $tr_{n/2}$ is the trace function on $F_{2^{n/2}}$, see [30]. Recent results prove the bentness of other functions with few terms in their trace representation. Namely, the functions:

- $tr\left(\alpha x^{4^k-2^k+1}\right)$, where (k,n)=1, n is not divisible by 3 and $\alpha \notin \{x^3; x \in F_{2^n}\}$, cf. [32];
- $tr\left(\alpha x^{2^{n/2}+2^{n/4+1}+1}\right)$, where $n \equiv 4$ [mod 8], $\alpha = \beta^5$, $\beta^4+\beta+1=0$, cf. [44];
- $tr\left(\alpha_1 x^{2^{n-1}+2^{n/2-1}} + \alpha_2 x^{3(2^{n/2}-1)+1}\right)$, where $n \equiv 4$ [mod 8], $\left(\alpha_1 + {\alpha_1}^{2^{n/2}}\right)^2$ $= {\alpha_2}^{2^{n/2}+1}$ and $\alpha_2 \in \{x^5; x \in F_{2^n}^*\}$, cf. [34];
- $tr\left(\alpha_1 x^{2^{n-1}+2^{n/2-1}} + \alpha_2 x^{3(2^{n/2}-1)+1}\right)$, where $\left(\alpha_1 + {\alpha_1}^{2^{n/2}}\right)^2 = {\alpha_2}^{2^{n/2}+1}$, $\alpha_2 \in F_{2^n}^*$ and $n \equiv 0$ or 2 or 6 [mod 8], cf. [34];
- $tr\left(\alpha_1 x^{2^{n-1}+2^{n/2-1}} + \alpha_2 x^{(2^{n/2-1}+2^{n/2-2}+1)(2^{n/2}-1)+1}\right)$, where $n \equiv 2$ [mod 4], $\left(\alpha_1 + {\alpha_1}^{2^{n/2}}\right)^2 = {\alpha_2}^{2^{n/2}+1}$, cf. [34];
- $tr\left(\alpha_1 x^{2^{n-1}+2^{n/2-1}} + \alpha_2 x^{\frac{2^{n/2-1}+1}{3}(2^{n/2}-1)+1}\right)$, where n is divisible by 4 and $\left(\alpha_1 + {\alpha_1}^{2^{n/2}}\right)^2 = {\alpha_2}^{2^{n/2}+1}$, cf. [34].

A last function, with more terms in its trace representation, and that we do not recall, is given in [43].

Computer experiment has been reported in [22] giving highly nonlinear balanced functions having high AI's. In Table 2, is computed the algebraic immunity of the function $tr(x^{2^n-2})$ (recall that the inverse function x^{2^n-2} is used as S-box in the AES) for $7 \le n \le 14$. This table shows that this fonction, even if good, is not optimal.

In Table 3 are listed balanced functions of three types: (1) balanced functions equal to the traces of power functions; (2) functions, denoted by *, obtained

Table 2. Computation of the nonlinearity and algebraic immunity for the inverse function for $6 \le n \le 14$

n	d	weight	degree	nonlinearity	alg. immunity
6	-1	32	5	24	3
7	-1	64	6	54	4
8	-1	128	7	112	4
9	-1	256	8	234	4
10	-1	512	9	480	5
11	-1	1024	10	980	5
12	-1	2048	11	1984	5
13	-1	4096	12	4006	6
14	-1	8192	13	8064	6

Table 3. Computation of the nonlinearity, algebraic degree and algebraic immunity for certain power functions $tr(x^d)$

n	d	weight	degree	nonlinearity	alg. immunity
8	31	128	5	112	4
8	39 (Kasami)	128^*	6	114	4
9	57 (Kasami)	256	4	224	4
9	59	256	5	240	5
9	115	256	5	240	5
10	241 (Kasami)	512	5	480	5
10	362	512	5	480	5
10	31 (Dillon)	512^*	9	486	5
10	339 (Dobbertin)	512^*	9	480	5
11	315	1024	6	992	6
12	993 (Kasami)	2048^*	11	2000	6
12	63 (Dillon)	2048^*	11	2000	6
12	636	2048^*	11	2000	6
13	993 (Kasami)	4096	6	4032	6
13	939	4096^{**}	12	4030	7
14	4033 (Kasami)	8192	7	8064	7
14	127 (Dillon)	8192^{**}	13	8088	7

from traces of power functions, which are not balanced (they have weight $2^{n-1} - 2^{n/2-1}$) and which are made balanced by replacing the first $2^{n/2-1}$ 0's by 1's (usually this construction leads to a function with a higher algebraic degree than the starting function); (3) functions, denoted by **, of the same kind as the previous ones, but for which were additionally inverted a small number of bits from 0 to 1 and reciprocally from 1 to 0 (this small modification does not affect too much the nonlinearity but may increase the AI by 1 in the case when the dimension of the annihilator of the Boolean function f or $1 + f$ is small).

3.2 Secondary Constructions

We shall call constructions with extension of the number of variables those constructions using functions on F_2^m, with $m < n$, to obtain functions on F_2^n.

General Constructions with Extension of the Number of Variables. All known secondary constructions of bent functions are particular cases of a general construction given in [8]:
Let m and r be two positive even integers. Let f be a Boolean function on F_2^{m+r} such that, for any element x' of F_2^r, the function on F_2^m:

$$f_{x'} : x \rightarrow f(x, x')$$

is bent. Then f is bent if and only if for any element u of F_2^m, the function

$$\varphi_u : x' \rightarrow \widetilde{f_{x'}}(u)$$

is bent on F_2^r.

A particular case of the general construction of bent functions given above is a construction due to Rothaus in [53]. We describe it because it will be related to the construction studied at the end of the present paper: if f_1, f_2, f_3 and $f_1 \oplus f_2 \oplus f_3$ are bent on F_2^m (m even), then the function defined on any element (x_1, x_2, x) of F_2^{m+2} by:

$$f(x_1, x_2, x) =$$

$$f_1(x)f_2(x) \oplus f_1(x)f_3(x) \oplus f_2(x)f_3(x) \oplus [f_1(x) \oplus f_2(x)]x_1 \oplus [f_1(x) \oplus f_3(x)]x_2 \oplus x_1x_2$$

is bent.

The classical secondary constructions of resilient functions are the following:

Direct Sums of Functions: if f is an r-variable t-resilient function and if g is an s-variable m-resilient function, then the function:

$$h(x_1, \ldots, x_r, x_{r+1}, \ldots, x_{r+s}) = f(x_1, \ldots, x_r) \oplus g(x_{r+1}, \ldots, x_{r+s})$$

is $(t + m + 1)$-resilient. This comes from the easily provable relation $\widehat{\chi_h}(a, b) = \widehat{\chi_f}(a) \times \widehat{\chi_g}(b)$, $a \in F_2^r$, $b \in F_2^s$. We have also $d^\circ h = \max(d^\circ f, d^\circ g)$ and, thanks to Relation (2), $N_h = 2^{r+s-1} - \frac{1}{2}(2^r - 2N_f)(2^s - 2N_g) = 2^r N_g + 2^s N_f - 2N_f N_g$.

We clearly have $\max(AI(f), AI(g)) \leq AI(h) \leq AI(f) + AI(g)$, since the restriction to an affine subspace E of the annihilator of a function is the annihilator of the restriction to E of the function (note that in the present case, at least one restriction is actually nonzero if the annihilator is nonzero), and since every product of an annihilator of $f + \epsilon$ with an annihilator of $g + \eta$ ($\epsilon, \eta \in F_2$) is an annihilator of $h + \epsilon + \eta$ (and, here, the direct product of a nonzero r-variable annihilator of f with a nonzero s-variable annihilator of g is nonzero since the two annihilators depend on disjoint sets of variables). The question seems open of determining general conditions under which the inequality $AI(h) \leq AI(f) + AI(g)$ can be proved to be an equality (which is clearly false in some cases, e.g. when $AI(f) + AI(g) > \max(d^\circ(f), d^\circ(g))$).

Note that, when the sum is not direct, the inequality $AI(f \oplus g) \leq AI(f) + AI(g)$ can be false: let h be an n-variable Boolean function and let l be an n-variable nonzero linear function, then the functions $f = hl$ and $g = h(l \oplus 1)$ have algebraic immunities at most 1, since $f(l \oplus 1) = gl = 0$, and their sum equals h. If $AI(h) > 2$, we obtain a counter-example. However, it involves non-balanced functions. A counter-example with balanced functions is as follows: let h be an n-variable balanced Boolean function and let l and l' be two distinct n-variable nonzero linear functions, such that the functions hll', $hl(l' \oplus 1)$, $h(l \oplus 1)l'$ and $h(l \oplus 1)(l' \oplus 1)$ are balanced. Then the functions $f = hll' \oplus (h \oplus 1)l(l' \oplus 1) + (l \oplus 1)(l' \oplus 1)$ and $g = l(l' \oplus 1) + h(l \oplus 1)l' + (h \oplus 1)(l \oplus 1)(l' \oplus 1)$ have algebraic immunities at most 2, since $f(l \oplus 1)l' = gll' = 0$, they are balanced and their sum equals h. If $AI(h) > 4$, we obtain a counter-example.

The secondary construction recently introduced in [29] consists in the direct sum of the starting function f and of a function g_k on $2k$ variables.

Siegenthaler's Construction: Let f and g be two Boolean functions on F_2^r. Consider the function

$$h(x_1, \ldots, x_r, x_{r+1}) = (x_{r+1} \oplus 1)f(x_1, \ldots, x_r) \oplus x_{r+1}g(x_1, \ldots, x_r)$$

on F_2^{r+1}. Then:

$$\widehat{\chi_h}(a_1,\ldots,a_r,a_{r+1}) = \widehat{\chi_f}(a_1,\ldots,a_r) + (-1)^{a_{r+1}}\,\widehat{\chi_g}(a_1,\ldots,a_r).$$

Thus, if f and g are m-resilient, then h is m-resilient; moreover, if for every $a \in F_2^r$ of Hamming weight $m+1$, we have $\widehat{\chi_f}(a)+\widehat{\chi_g}(a)=0$, then h is $(m+1)$-resilient. And we have: $N_h \geq N_f + N_g$. If f and g achieve maximum possible nonlinearity $2^{r-1}-2^{m+1}$ and if h is $(m+1)$-resilient, then the nonlinearity $2^r - 2^{m+2}$ of h is the best possible. If the supports of the Walsh transforms of f and g are disjoint, then we have $N_h = 2^{r-1} + \min(N_f, N_g)$; thus, if f and g achieve maximum possible nonlinearity $2^{r-1}-2^{m+1}$, then h achieves best possible nonlinearity $2^r - 2^{m+1}$.

The algebraic immunity of h has been studied in [29]:

- If $AI(f) \neq AI(g)$ then $AI(h) = \min\{AI(f), AI(g)\}+1$.
- If $AI(f) = AI(g) = d$, then $d \leq AI(h) \leq d+1$, and $AI(h)=d$ if and only if there exist $f_1, g_1 \in B_n$ of algebraic degree d such that $\{f * f_1 = 0, g * g_1 = 0\}$ or $\{(1+f)*f_1 = 0, (1+g)*g_1 = 0\}$ and $\deg(f_1+g_1) \leq d-1$.

We cannot say that Siegenthaler's construction is good or is bad in terms of algebraic immunity, since:

- a good construction is supposed to gain 1 (resp k) for the algebraic immunity when we add 2 (resp $2k$) variables, here we add only one;
- the construction is very general since every function can be obtained from it.

In practice, we could not obtain good algebraic immunity with it.

Siegenthaler [57] proposed, as a particular case of its (iterated) construction, to add to a given function f a linear function on disjoint variables for increasing its resiliency order. This does not allow achieving good algebraic immunity, since adding a linear function to f can increase the AI at most by one (an annihilator of f, multiplied by $l+1$ gives an annihilator of $f+l$).

Tarannikov's Construction: Let g be any Boolean function on F_2^r. Define the Boolean function h on F_2^{r+1} by

$$h(x_1,\ldots,x_r,x_{r+1}) = x_{r+1} \oplus g(x_1,\ldots,x_{r-1},x_r \oplus x_{r+1}).$$

The Walsh transform $\widehat{\chi_h}(a_1,\ldots,a_{r+1})$ is equal to

$$\sum_{x_1,\ldots,x_{r+1}\in F_2} (-1)^{a\cdot x \oplus g(x_1,\ldots,x_r)\oplus a_r x_r \oplus (a_r \oplus a_{r+1} \oplus 1)x_{r+1}}$$

where we write $a=(a_1,\ldots,a_{r-1})$ and $x=(x_1,\ldots,x_{r-1})$; it is null if $a_{r+1}=a_r$ and it equals $2\,\widehat{\chi_g}(a_1,\ldots,a_{r-1},a_r)$ if $a_r = a_{r+1}\oplus 1$. Thus: $N_h = 2\,N_g$; If g is m-resilient, then h is m-resilient. If, additionally, $\widehat{\chi_g}(a_1,\ldots,a_{r-1},1)$ is null for every vector $(a_1,\ldots,a_{r-1})$ of weight at most m, then h is $(m+1)$-resilient.

Generalizations: Tarannikov in [60], and after him, Pasalic et al. in [54] used this construction to design a more complex one, that we call *Tarannikov et al.'s construction*, and which allowed maximum tradeoff between resiliency, algebraic degree and nonlinearity. This construction uses two $(n-1)$-variable m-resilient functions f_1 and f_2 achieving Siegenthaler's and Sarkar et al.'s bounds to design an $(n+3)$-variable $(m+2)$-resilient function h also achieving these bounds, assuming that $f_1 + f_2$ has same degree as f_1 and f_2 and that the supports of the Walsh transforms of f_1 and f_2 are disjoint. The two restrictions $h_1(x_1, \ldots, x_{n+2}) = h(x_1, \ldots, x_{n+2}, 0)$ and $h_2(x_1, \ldots, x_{n+2}) = h(x_1, \ldots, x_{n+2}, 1)$ have then also disjoint Walsh supports, and these two functions can then be used in the places of f_1 and f_2. This leads to an infinite class of functions achieving Sarkar et al.'s and Siegenthaler's bounds. It has been proved in [2] that the n-variable functions constructed by this method attain $\mathbf{\Omega}(\sqrt{n})$ algebraic immunity (which is unfortunately bad).

Tarannikov et al.'s construction has been in its turn generalized (see [14]):

Theorem 1. *Let r, s, t and m be positive integers such that $t < r$ and $m < s$. Let f_1 and f_2 be two r-variable t-resilient functions. Let g_1 and g_2 be two s-variable m-resilient functions. Then the function $h(x,y) = f_1(x) \oplus g_1(y) \oplus (f_1 \oplus f_2)(x)\,(g_1 \oplus g_2)(y)$, $x \in F_2^r, y \in F_2^s$ is an $(r+s)$-variable $(t+m+1)$-resilient function. If f_1 and f_2 are distinct and if g_1 and g_2 are distinct, then the algebraic degree of h equals $\max(d^\circ f_1, d^\circ g_1, d^\circ(f_1 \oplus f_2) + d^\circ(g_1 \oplus g_2))$; otherwise, it equals $\max(d^\circ f_1, d^\circ g_1)$. The Walsh transform of h takes value*

$$\widehat{\chi_h}(a,b) = \frac{1}{2}\widehat{\chi_{f_1}}(a)\left[\widehat{\chi_{g_1}}(b) + \widehat{\chi_{g_2}}(b)\right] + \frac{1}{2}\widehat{\chi_{f_2}}(a)\left[\widehat{\chi_{g_1}}(b) - \widehat{\chi_{g_2}}(b)\right]. \qquad (7)$$

If the Walsh transforms of f_1 and f_2 have disjoint supports as well as those of g_1 and g_2, then

$$N_h = \min_{i,j \in \{1,2\}} \left(2^{r+s-2} + 2^{r-1} N_{g_j} + 2^{s-1} N_{f_i} - N_{f_i} N_{g_j}\right). \qquad (8)$$

In particular, if f_1 and f_2 have (optimum) nonlinearity $2^{r-1} - 2^{t+1}$ and have disjoint Walsh supports, if g_1 and g_2 have (optimum) nonlinearity $2^{s-1} - 2^{m+1}$ and have disjoint Walsh supports, if $f_1 + f_2$ has degree $r - t - 1$ and if $g_1 + g_2$ has degree $s - m - 1$, then h has degree $r + s - t - m - 2$ and nonlinearity $2^{r+s-1} - 2^{t+m+2}$, and thus achieves Siegenthaler's and Sarkar et al.'s bounds.

Note that function h, defined this way, is the concatenation of the four functions f_1, $f_1 \oplus 1$, f_2 and $f_2 \oplus 1$, in an order controled by $g_1(y)$ and $g_2(y)$. The proof of this theorem and examples of such pairs (f_1, f_2) (or (g_1, g_2)) can be found in [14]. This construction being very general since it generalizes all known secondary constructions, it is difficult to give bounds on the algebraic immunity of the resulting functions.

Other Constructions: There exists a secondary construction of resilient functions from bent functions (see [9]): let r be a positive integer, m a positive even integer and f a function such that, for any element x', the function: $f_{x'} : x \to f(x, x')$

is bent. If, for every element u of Hamming weight at most t, the function $\varphi_u : x' \to \widetilde{f_{x'}}(u)$ is $(t - w_H(u))$-resilient, then f is t-resilient (the converse is true).

Rothaus' construction has been modified in [9] into a construction of resilient functions: if f_1 is t-resilient, f_2 and f_3 are $(t-1)$-resilient and $f_1 \oplus f_2 \oplus f_3$ is $(t-2)$-resilient, then $f(x_1, x_2, x)$ is t-resilient (the converse is true). This construction does not seem able to produce functions with higher algebraic immunities than the functions used as building blocks.

Constructions Without Extension of the Number of Variables. Such constructions, by modifying the support of highly nonlinear resilient functions without decreasing their characteristics, may be appropriate for trying to increase the algebraic immunities of such functions, previously obtained by classical constructions. There exist, in the literature, four such constructions.

Modifying a Function on a Subspace: Dillon proves in [31] that if a binary function f is bent on F_2^n (n even) and if E is an $\frac{n}{2}$-dimensional flat on which f is constant, then, denoting by 1_E the indicator (i.e. the characteristic function) of E, the function $f \oplus 1_E$ is bent too. This is generalized in [6]:

Let $E = b \oplus E'$ be any flat in F_2^n (E', the direction of E, is a linear subspace of F_2^n). Let f be any bent function on F_2^n. The function $f^\star = f \oplus 1_E$ is bent if and only if one of the following equivalent conditions is satisfied :

1. for any x in $F_2^n \setminus E'$, the function: $y \mapsto f(y) \oplus f(x \oplus y)$ is balanced on E;
2. for any a in F_2^n, the restriction of the function $\widetilde{f}(x) \oplus b \cdot x$ to the flat $a \oplus E'^\perp$ is either constant or balanced.

If $f^\star$ is bent, then E has dimension greater than or equal to $r = n/2$ and the degree of the restriction of f to E is at most $dim(E) - r + 1$. If E has dimension r, then this last condition (i.e., the fact that the restriction of f to E is affine) is also sufficient and the function $\widetilde{f^\star}(x)$ is equal to :

$$\widetilde{f}(x) \oplus 1_{E'^\perp}(u \oplus x),$$

where u is any element of F_2^n such that for any x in $E : f(x) = u \cdot x \oplus \epsilon$.

This construction has been adapted to correlation-immune functions in [9]: let t, m and n any positive integers and f a t-th order correlation-immune function from F_2^n to F_2^m; assume there exists a subspace E of F_2^n, whose minimum nonzero weight is greater than t and such that the restriction of f to the orthogonal of E (i.e. the subspace of F_2^n: $E^\perp = \{u \in F_2^n \,|\, \forall x \in E,\, u \cdot x = 1\}$) is constant. Then f remains t-th order correlation-immune if we change its constant value on $E^\perp$ into any other one.

Hou-Langevin Construction: X.-D. Hou and P. Langevin have made in [39] a very simple observation: Let f be a Boolean function on F_2^n, n even. Let $\sigma = (\sigma_1, \cdots, \sigma_n)$ be a permutation on F_2^n such that

$$d_H\left(f, \sum_{i=1}^{n} a_i\,\sigma_i\right) = 2^{n-1} \pm 2^{\frac{n}{2}-1};\ \forall a \in F_2^n.$$

Then $f \circ \sigma^{-1}$ is bent.

A case of application of this fact, pointed out in [37], is when f belongs to Maiorana-McFarland class (3), with $\pi = id$ and when the coordinate functions of σ are all of the form $x_{i_1}y_{j_1} \oplus \ldots \oplus x_{i_k}y_{j_k} \oplus l(x,y) \oplus h(y)$, where $k < n/2$ and $i_l < j_l$ for every $l \leq k$; the function h is any Boolean function on $F_2^{n/2}$ and l is affine.

Another case of application is given in [39] when f has degree at most 3: assume that for every $i = 1, \cdots, n$, there exists a subset U_i of F_2^n and an affine function h_i such that:

$$\sigma_i(x) = \sum_{u \in U_i} (f(x) \oplus f(x \oplus u)) \oplus h_i(x).$$

Then $f \circ \sigma^{-1}$ is bent.

Only examples of potentially new bent functions have been deduced by Hou and Langevin from these results.

This idea of construction can be adapted to resilient functions:

If $d_H(f, \sum_{i=1}^{n} a_i\,\sigma_i) = 2^{n-1}$ for every $a \in F_2^n$ of weight at most k, then $f \circ \sigma^{-1}$ is k-resilient. This secondary construction needs strong hypothesis on the function used as buiding block to produce resilient functions. Further work seems necessary for designing functions for stream ciphers by using it.

Two Recent Constructions have been introduced in [24]. They will be recalled at Subsection 4.3.

4 A New Secondary Construction of Boolean Functions

4.1 A Modification of Rothaus' Construction

Rothaus' construction was the first non-trivial construction of bent functions to be obtained in the literature. It is still one of the most interesting known constructions nowadays, since the functions it produces can have degrees near $n/2$, even if the functions used as building blocks don't. But the constructed functions have a very particular form. It is possible to derive a construction having the same nice property but having not the same drawback, thanks to the following observation.

Given three Boolean functions f_1, f_2 and f_3, there is a nice relationship between their Walsh transforms and the Walsh transforms of two of their elementary symmetric related functions:

Lemma 1. *Let f_1, f_2 and f_3 be three Boolean functions on F_2^n. Let us denote by σ_1 the Boolean function equal to $f_1 \oplus f_2 \oplus f_3$ and by σ_2 the Boolean function equal to $f_1f_2 \oplus f_1f_3 \oplus f_2f_3$. Then we have $f_1 + f_2 + f_3 = \sigma_1 + 2\sigma_2$. This implies*

$$\widehat{\chi_{f_1}} + \widehat{\chi_{f_2}} + \widehat{\chi_{f_3}} = \widehat{\chi_{\sigma_1}} + 2\widehat{\chi_{\sigma_2}}. \qquad (9)$$

Proof. The fact that $f_1+f_2+f_3=\sigma_1+2\sigma_2$ (recall that these sums are calculated in $\mathbb{Z}$ and not mod 2) can be checked easily and directly implies $\chi_{f_1}+\chi_{f_2}+\chi_{f_3}=\chi_{\sigma_1}+2\chi_{\sigma_2}$, thanks to the equality $\chi_f=1-2f$ (valid for every Boolean function). The linearity of the Fourier transform with respect to the addition in $\mathbb{Z}$ implies then Relation (9). ◇

4.2 Deduced Constructions of Resilient Functions

We begin with resilient functions because the application of Lemma 1 is easy in this case. In the following theorem, saying that a function f is 0-order correlation immune does not impose any condition on f and saying it is 0-resilient means it is balanced.

Theorem 2. *Let n be any positive integer and k any non-negative integer such that $k\leq n$. Let f_1, f_2 and f_3 be three k-th order correlation immune (resp. k-resilient) functions. Then the function $\sigma_1=f_1\oplus f_2\oplus f_3$ is k-th order correlation immune (resp. k-resilient) if and only if the function $\sigma_2=f_1f_2\oplus f_1f_3\oplus f_2f_3$ is k-th order correlation immune (resp. k-resilient). Moreover:*

$$N_{\sigma_2}\geq\frac{1}{2}\left(N_{\sigma_1}+\sum_{i=1}^{3}N_{f_i}\right)-2^{n-1} \tag{10}$$

and if the Walsh supports of f_1, f_2 and f_3 are pairwise disjoint (that is, if at most one value $\widehat{\chi_{f_i}}(s)$, $i=1,2,3$ is nonzero, for every vector s), then

$$N_{\sigma_2}\geq\frac{1}{2}\left(N_{\sigma_1}+\min_{1\leq i\leq 3}N_{f_i}\right). \tag{11}$$

Proof. Relation (9) and the fact that for every nonzero vector a of weight at most k we have $\widehat{\chi_{f_i}}(a)=0$ for $i=1,2,3$ imply that $\widehat{\chi_{\sigma_1}}(a)=0$ if and only if $\widehat{\chi_{\sigma_2}}(a)=0$. Same property occurs for $a=0$ when f_1,f_2 and f_3 are resilient. Relation (9) implies the relation

$$\max_{s\in F_2^n}|\widehat{\chi_{\sigma_2}}(s)|\leq\frac{1}{2}\left(\sum_{i=1}^{3}\left(\max_{s\in F_2^n}|\widehat{\chi_{f_i}}(s)|\right)+\max_{s\in F_2^n}|\widehat{\chi_{\sigma_1}}(s)|\right)$$

and Relation (2) implies then Relation (10). If the Walsh supports of f_1, f_2 and f_3 are pairwise disjoint, then Relation (9) implies the relation

$$\max_{s\in F_2^n}|\widehat{\chi_{\sigma_2}}(s)|\leq\frac{1}{2}\left(\max_{1\leq i\leq 3}\left(\max_{s\in F_2^n}|\widehat{\chi_{f_i}}(s)|\right)+\max_{s\in F_2^n}|\widehat{\chi_{\sigma_1}}(s)|\right)$$

and Relation (2) implies then Relation (11). ◇

Remark: We have $\sigma_2=f_1\oplus(f_1\oplus f_2)(f_1\oplus f_3)$. Hence, another possible statement of Theorem 2 is: if f_1, $f_1\oplus f_2$ and $f_1\oplus f_3$ are k-th order correlation immune (resp. k-resilient) functions, then the function $f_1\oplus f_2\oplus f_3$ is k-th order correlation immune (resp. k-resilient) if and only if the function $f_1\oplus f_2f_3$ is k-th order correlation immune (resp. k-resilient).

We use now the invariance of the notion of correlation-immune (resp. resilient) function under translation to deduce an example of application of Theorem 2.

Proposition 2. *Let n be any positive integer and k any non-negative integer such that $k \leq n$. Let f and g be two k-th order correlation immune (resp. k-resilient) functions on F_2^n. Assume that there exist $a, b \in F_2^n$ such that $D_a f \oplus D_b g$ is constant. Then the function $h(x) = f(x) \oplus D_a f(x)(f(x) \oplus g(x))$, that is, $h(x) = \begin{cases} f(x) \text{ if } D_a f(x) = 0 \\ g(x) \text{ if } D_a f(x) = 1 \end{cases}$ is k-th order correlation immune (resp. k-resilient). Moreover:*

$$N_h \geq N_f + N_g - 2^{n-1} \tag{12}$$

and if the Walsh support of f is disjoint of that of g, then

$$N_h \geq \min\left(N_f, N_g\right). \tag{13}$$

Note that finding hihgly nonlinear resilient functions with disjoint supports is easy, by using Tarannikov et al.'s construction.

Proof. Let $D_a f \oplus D_b g = \epsilon$. Taking $f_1(x) = f(x)$, $f_2(x) = f(x+a)$ and $f_3(x) = g(x)$, the hypothesis of Theorem 2 is satisfied, since $\sigma_1(x) = D_a f(x) \oplus g(x) = D_b g(x) \oplus \epsilon \oplus g(x) = g(x+b) \oplus \epsilon$ is k-th order correlation immune (resp. k-resilient). Hence, $h(x) = f(x) \oplus D_a f(x)(f(x) \oplus g(x))$ is k-th order correlation immune (resp. k-resilient). Relation (12) is a direct consequence of Relation (10). Note that the Walsh support of f_2 equals that of $f_1 = f$, since we have $\widehat{\chi_{f_2}}(s) = (-1)^{a \cdot s} \widehat{\chi_f}(s)$ and that the Walsh support of σ_1 equals that of $f_3 = g$. Hence, if the Walsh support of f is disjoint of that of g, then Relation (9) implies the relation

$$\max_{s \in F_2^n} |\widehat{\chi_h}(s)| \leq \max\left(\max_{s \in F_2^n} |\widehat{\chi_f}(s)|, \max_{s \in F_2^n} |\widehat{\chi_g}(s)|\right)$$

and Relation (2) implies then Relation (13). ◇

Remarks:

1. The notion of resilient function being also invariant under any permutation of the input coordinates $x_1, \ldots, x_n$, Proposition 2 is also valid if we replace $D_a f$ by $f(x_1, \ldots, x_n) \oplus f(x_{\tau(1)}, \ldots, x_{\tau(n)})$ and $D_b g$ by $g(x_1, \ldots, x_n) \oplus g(x_{\tau'(1)}, \ldots, x_{\tau'(n)})$, where τ and τ' are two permutations of $\{1, \ldots, n\}$.
2. Computer experiment shows that the secondary construction of Theorem 2 and its particular case given in Proposition 2 can increase the algebraic immunity, while keeping the same resiliency order and the same nonlinearity. The reason is in the fact that the support of σ_2 (resp. h) is, in general, more complex than those of f_1, f_2 and f_3 (resp. f and g). *It would be nice finding a provable result illustrating this.*

A Deduced Primary Construction of Resilient Functions

Proposition 3. *let t and $n = r + s$ be any positive integers ($r > t > 0$, $s > 0$). Let g_1, g_2 and g_3 be any boolean functions on F_2^s and ϕ_1, ϕ_2 and ϕ_3 any mappings from F_2^s to F_2^r such that, for every element y in F_2^s, the vectors $\phi_1(y)$, $\phi_2(y)$, $\phi_3(y)$ and $\phi_1(y) \oplus \phi_2(y) \oplus \phi_3(y)$ have Hamming weights greater than t. Let us denote $f_1(x) = x \cdot \phi_1(y) \oplus g_1(y)$, $f_2(x) = x \cdot \phi_2(y) \oplus g_2(y)$ and $f_3(x) = x \cdot \phi_3(y) \oplus g_3(y)$. Then the function:*

$$f(x, y) = f_1(x)\, f_2(x) \ \oplus f_1(x)\, f_3(x) \oplus \ f_2(x)\, f_3(x)$$

is t-resilient.

Note that, if the sets $\phi_1(F_2^s)$, $\phi_2(F_2^s)$, and $\phi_3(F_2^s)$ are disjoint, Relation (5) implies that the Walsh supports of f_1, f_2 and f_3 are disjoint. Relation (11) of Theorem 2 is then satisfied. This implies that f can be (nearly) optimum with respect to Siegenthaler's and Sarkar et al.'s bounds. We have seen that a Maiorana-McFarland (nearly) optimum function has low degree and still lower AI. But here, the algebraic degree of f and its algebraic immunity may be higher than those of Maiorana-McFarland's (nearly) optimum functions. For instance, we obtained in [22] a balanced 14-variable function with algebraic degree 7, nonlinearity 7808, order of resiliency 5 and AI 6 by considering ϕ_1, ϕ_2, ϕ_3 from F_2^6 to F_2^8 such that for any $i \in \{1, 2, 3\}$ and any $x \in F_2^6$: $w_H(\phi_i(x)) \geq 6$ and such that $w_H(\phi_1(x) + \phi_2(x) + \phi_3(x)) \geq 6$.

Remark: We can also apply Theorem 2 to the class of resilient functions derived from the $\mathcal{PS}_{ap}$ construction: Let n and m be two positive integers, g_1, g_2 and g_3 three functions from F_{2^m} to F_2, ϕ a linear mapping from F_2^n to F_{2^m} and a an element of F_{2^m} such that $a \oplus \phi(y) \neq 0$, $\forall y \in F_2^n$.

Let b_1, b_2 and $b_3 \in F_2^n$ such that, for every z in F_{2^m}, $\phi^*(z) \oplus b_i$, $i = 1, 2, 3$ and $\phi^*(z) \oplus b_1 \oplus b_2 \oplus b_3$ have weight greater than t, where ϕ^* is the adjoint of ϕ, then the function

$$f(x, y) =$$
$$\left(g_1\left(\frac{x}{a \oplus \phi(y)}\right) \oplus b_1 \cdot y\right)\left(g_2\left(\frac{x}{a \oplus \phi(y)}\right) \oplus b_2 \cdot y\right) \oplus$$
$$\left(g_1\left(\frac{x}{a \oplus \phi(y)}\right) \oplus b_1 \cdot y\right)\left(g_3\left(\frac{x}{a \oplus \phi(y)}\right) \oplus b_3 \cdot y\right) \oplus$$
$$\left(g_2\left(\frac{x}{a \oplus \phi(y)}\right) \oplus b_2 \cdot y\right)\left(g_3\left(\frac{x}{a \oplus \phi(y)}\right) \oplus b_3 \cdot y\right)$$

is t-resilient. The complexity of the support of this function may permit getting a good algebraic immunity.

4.3 Constructing Bent Functions by Using Lemma 1

Applying Lemma 1 to the construction of bent functions is slightly less simple than for resilient functions. Nevertheless, we will deduce here again a secondary construction (we shall see that it generalizes a secondary construction obtained recently) and a primary construction.

Theorem 3. *Let n be any positive even integer. Let f_1, f_2 and f_3 be three bent functions. Denote by σ_1 the function $f_1 \oplus f_2 \oplus f_3$ and by σ_2 the function $f_1 f_2 \oplus f_1 f_3 \oplus f_2 f_3$. Then:*
1. if σ_1 is bent and if $\widetilde{\sigma_1} = \widetilde{f_1} \oplus \widetilde{f_2} \oplus \widetilde{f_3}$, then σ_2 is bent and $\widetilde{\sigma_2} = \widetilde{f_1}\widetilde{f_2} \oplus \widetilde{f_1}\widetilde{f_3} \oplus \widetilde{f_2}\widetilde{f_3}$;
2. if σ_2 is bent, or if more generally $\widehat{\chi_{\sigma_2}}(a)$ is divisible by $2^{n/2}$ for every a (e.g. if σ_2 is plateaued), then σ_1 is bent.

Proof. By hypothesis, we have for $i = 1, 2, 3$ and for every vector a: $\widehat{\chi_{f_i}}(a) = (-1)^{\widetilde{f_i}(a)}\, 2^{n/2}$.
1. If σ_1 is bent and if $\widetilde{\sigma_1} = \widetilde{f_1} \oplus \widetilde{f_2} \oplus \widetilde{f_3}$, then we have:

$$\widehat{\chi_{\sigma_1}}(a) = (-1)^{\widetilde{f_1}(a) \oplus \widetilde{f_2}(a) \oplus \widetilde{f_3}(a)}\, 2^{n/2}.$$

Relation (9) implies:

$$\begin{aligned}\widehat{\chi_{\sigma_2}}(a) &= \left[(-1)^{\widetilde{f_1}(a)} + (-1)^{\widetilde{f_2}(a)} + (-1)^{\widetilde{f_3}(a)} - (-1)^{\widetilde{f_1}(a) \oplus \widetilde{f_2}(a) \oplus \widetilde{f_3}(a)}\right] 2^{(n-2)/2} \\ &= (-1)^{\widetilde{f_1}(a)\widetilde{f_2}(a) \oplus \widetilde{f_1}(a)\widetilde{f_3}(a) \oplus \widetilde{f_2}(a)\widetilde{f_3}(a)} 2^{n/2}.\end{aligned}$$

2. If $\widehat{\chi_{\sigma_2}}(a)$ is divisible by $2^{n/2}$ for every a, then the number $\widehat{\chi_{\sigma_1}}(a)$, equal to $\left[(-1)^{\widetilde{f_1}(a)} + (-1)^{\widetilde{f_2}(a)} + (-1)^{\widetilde{f_3}(a)}\right] 2^{n/2} - 2\widehat{\chi_{\sigma_2}}(a)$, is congruent with $2^{n/2}$ mod $2^{n/2+1}$ for every a. This is sufficient to imply that σ_1 is bent, according to Lemma 1 of [7]. ◇

Remark: Here again, it is possible to state Theorem 3 slightly differently. For instance, if f_1, $f_1 \oplus f_2$ and $f_1 \oplus f_3$ are three bent functions such that $f_1 \oplus f_2 f_3$ has Walsh spectrum divisible by $2^{n/2}$, then $\sigma_1 = f_1 \oplus f_2 \oplus f_3$ is bent. Notice that a sufficient condition for $f_1 \oplus f_2 f_3$ having Walsh spectrum divisible by $2^{n/2}$ is that $f_2 f_3 = 0$ or that $f_2 \preceq f_3$ (i.e. that the support of f_3 includes that of f_2). In particular, if f is a bent function and if E and F are two disjoint $(n/2)$-dimensional flats on which f is affine, the function $f \oplus 1_E \oplus 1_F$ is bent.

Theorem 3 and Lemma 1 imply as particular cases two secondary constructions of bent functions, recently obtained in [24]:

Corollary 1. *[24] Let f and g be two bent functions on F_2^n (n even). Assume that there exists $a \in F_2^n$ such that $D_a f = D_a g$. Then the function $f(x) \oplus D_a f(x)(f(x) \oplus g(x))$ is bent and has dual $\widetilde{f}(x) \oplus (a \cdot x)(\widetilde{f}(x) \oplus \widetilde{g}(x))$.*

Indeed, taking $f_1(x) = f(x)$, $f_2(x) = f(x + a)$ and $f_3(x) = g(x)$, the hypothesis of Alinea 1 of Theorem 3 is satisfied: $\sigma_1(x) = D_a f(x) \oplus g(x) = D_a g(x) \oplus g(x) = g(x + a)$ is bent and we have $\widetilde{\sigma_1}(x) = a \cdot x \oplus \widetilde{g}(x) = \widetilde{f_1}(x) \oplus \widetilde{f_2}(x) \oplus \widetilde{f_3}(x)$. Hence, $\sigma_2(x) = f(x) \oplus D_a f(x)(f(x) \oplus g(x))$ is bent (note that the dual of f_2 equals $\widetilde{f_1} \oplus a \cdot x$). ◇

Remarks:

1. Applying Corollary 1 to the duals of f and g gives that, if f and g are two bent functions on F_2^n such that there exists $a \in F_2^n$ such that $D_a \widetilde{f} = D_a \widetilde{g}$, then the function $f(x) \oplus (a \cdot x)(f(x) \oplus g(x))$ is bent.

2. More generally than in Corollary 1, let L be an affine automorphism of F_2^n. We know that, for every bent function f, the function $f \circ L$ is bent and admits as dual $\widetilde{f} \circ L^*$, where L^* is the adjoint operator of L^{-1} (such that, for every $x, y \in F_2^n$, we have $x \cdot L^{-1}(y) = L^*(x) \cdot y$). Then if f and g are two bent functions such that $\begin{cases} f(x) \oplus f \circ L(x) \oplus g(x) \oplus g \circ L(x) = 0, \forall x \in F_2^n \\ \widetilde{f}(x) \oplus \widetilde{f} \circ L^*(x) \oplus \widetilde{g}(x) \oplus \widetilde{g} \circ L^*(x) = 0, \forall x \in F_2^n; \end{cases}$, then the function $fg \oplus (f \oplus g)(f \circ L)$ is bent and its dual equals $\widetilde{f}\widetilde{g} \oplus (\widetilde{f} \oplus \widetilde{g})(\widetilde{f} \circ L^*)$. Indeed, taking $f_1 = f$, $f_2 = f \circ L$ and $f_3 = g$, we have $\sigma_1 = g \circ L$ and therefore $\widetilde{\sigma}_1 = \widetilde{g} \circ L^* = \widetilde{f_1} \oplus \widetilde{f_2} \oplus \widetilde{f_3}$ and $\sigma_2 = fg \oplus (f \oplus g)(f \circ L)$.

Proposition 4. *[24] Let n be any positive even integer. Let f and g be two plateaued functions of the same amplitude $2^{n/2+1}$, whose Walsh transform's supports S_f and S_g are two distinct cosets of the same vector subspace E of F_2^n. Let a be an element of F_2^n such that the cosets $a + S_f$ and $a + S_g$ are both distinct of S_f and S_g. Then the function $f(x) \oplus (a \cdot x)(f(x) \oplus g(x))$ is bent.*

Proof. Set $f_1(x) = f(x)$, $f_2(x) = f(x) \oplus a \cdot x$ and $f_3(x) = g(x)$. We have: $\sigma_1(x) = a \cdot x \oplus g(x)$. Hence, f_1, f_2, f_3 and σ_1 are four plateaued functions of amplitude $2^{n/2+1}$, whose Walsh transform's supports equal $S_f, a + S_f, S_g$ and $a + S_g$. The cosets $S_f, S_g, a + S_f$ and $a + S_g$ constituting a partition of F_2^n (note that E has necessarily co-dimension 2), Relation (9) implies that $\sigma_2(x) = f(x) \oplus (a \cdot x)(f(x) \oplus g(x))$ is bent. ◇

An Example Related to Proposition 4: The Kerdock Code. Partially-bent functions (see [5]) give a way of constructing plateaued functions[2]; they are defined as follows: two vector subspaces E (of even dimension) and F are chosen in F_2^n such that their sum is direct and equals F_2^n; for every $x \in E$ and every $y \in F$, we define $f(x + y) = g(x) \oplus l(y)$, where g is bent on E and l is linear on F. All quadratic functions (that is, functions of algebraic degrees at most 2) are of this type (F is then the kernel of their associated symplectic form; see [45, 5]). If F (often called the kernel of f) has dimension 2, then f is plateaued with amplitude $2^{n/2+1}$ and its Walsh transform's support S_f is a flat (of co-dimension 2) whose direction equals $F^\perp$. Hence, we can choose two vectors a and b such that $\{S_f, a+S_f, b+S_f, a+b+S_f\}$ is a partition of F_2^n. We define then $f_1(x) = f(x), f_2(x) = f(x) \oplus a \cdot x$, and $f_3(x) = f(x) \oplus b \cdot x$. We have $(f_1 \oplus f_2 \oplus f_3)(x) = f(x) \oplus (a+b) \cdot x$ and the hypothesis of Lemma 1 (that is, the hypothesis of Proposition 4 with $g(x) = f(x) \oplus b \cdot x)$ is satisfied. We deduce that the function $f(x) \oplus (a \cdot x)(b \cdot x)$ is bent. In the sequel, we shall call *Kerdock-like construction* this construction $(f, a, b) \mapsto \sigma_2$. The fact that it always provides bent functions is not new, but this is exactly how the bent functions in the Kerdock code are constructed (see [45]). We show now how (revisiting an observation from [24]). Denoting $m = n - 1 = 2t + 1$, the elements of F_2^n are identified to ordered pairs (x, ϵ) with $x \in F_{2^m}$ and $\epsilon \in F_2$. Then we define $f(x, \epsilon) = tr(\sum_{i=1}^{t} x^{2^i+1})$, where tr is the trace function from F_{2^m} to F_2. This function is quadratic and its kernel F (more precisely here, the kernel of its associated symplectic form)

[2] Another way is by using Maiorana-McFarland construction (4) with ϕ injective.

equals (see [45]) the vector space $\{(x,\epsilon)\in F_{2^m}\times F_2/\, x+tr(x)=0\}=\{\mathbf{0},\mathbf{1}\}\times F_2$, where $\mathbf{0},\mathbf{1}\in F_{2^m}$. This kernel has dimension 2 and the Walsh transform's support S_f of f is therefore a flat of dimension $n-2$ (whose direction equals $F^\perp$). So we can apply Kerdock-like construction. Recall that the notion of bent function is independent of the choice of the inner product. So we can choose $(x,\epsilon)\cdot(y,\eta)=tr(xy)\oplus\epsilon\eta$. The choice of $a=(\mathbf{0},1)$, $b=(\mathbf{1},0)$ in the Kerdock-like construction shows that the function $\sigma_2(x,\epsilon)=tr(\sum_{i=1}^t x^{2^i+1})\oplus\epsilon tr(x)$ is bent. Obviously, for every $u\in F_{2^m}^*$, the function $(x,\epsilon)\mapsto\sigma_2(ux,\epsilon)$ is also bent (note that it is obtained through the Kerdock-like construction from $f_u(x,\epsilon)=tr(\sum_{i=1}^t (ux)^{2^i+1})$, $a=(\mathbf{0},1)$ and $b=(u,0)$). A property which is specific to Kerdock codes (and that could not be obtained with non-quadratic functions until now) is that the sum $(x,\epsilon)\mapsto\sigma_2(ux,\epsilon)\oplus\sigma_2(vx,\epsilon)$ of two distinct such functions is still bent. Let us check this: the quadratic function $f_u\oplus f_v$ has kernel $\{(x,\epsilon)\in F_{2^m}\times F_2/\,(u^2+v^2)x+utr(ux)+vtr(vx)=0\}=E_{u,v}\times F_2$, where $E_{u,v}$ has dimension at most 2 (since the equation $(u^2+v^2)x+utr(ux)+vtr(vx)=0$ has at most 4 solutions). Since we know that the kernel of a quadratic function must have even co-dimension (and hence, here, even dimension), the dimension of $E_{u,v}$ must equal 1. The function $\sigma_2(ux,\epsilon)\oplus\sigma_2(vx,\epsilon)$ can then be obtained through the Kerdock-like construction from the function $f_u\oplus f_v$ and the vectors $a=(\mathbf{0},1)$ and $b=(u+v,0)$. The hypothesis of Proposition 4 is satisfied thanks to the fact that b does not belong to $E_{u,v}^\perp$ (this can be checked by showing that $E_{u,v}^\perp=\{(u^2+v^2)y+utr(uy)+vtr(vy);\, y\in F_{2^m}\}$).

A Primary Construction of Bent Functions Deduced from Theorem 3

Proposition 5. *Let n be any positive even integer. Let π_1, π_2, π_3 be three permutations on $F_2^{n/2}$ such that $\pi_1\oplus\pi_2\oplus\pi_3$ is also a permutation and such that the inverse of $\pi_1\oplus\pi_2\oplus\pi_3$ equals $\pi_1^{-1}\oplus\pi_2^{-1}\oplus\pi_3^{-1}$. Then the function*

$$f(x,y)=[x\cdot\pi_1(y)]\,[x\cdot\pi_2(y)]\oplus[x\cdot\pi_1(y)]\,[x\cdot\pi_3(y)]\oplus[x\cdot\pi_2(y)]\,[x\cdot\pi_3(y)]$$

is bent.

The proof is a direct consequence of the first alinea of Theorem 3 and of the properties of Maiorana-McFarland's class recalled above. Note that the result is still valid if an affine function g in y is added to the $x\cdot\pi_i(y)$'s in the expression of $f(x,y)$.

It is also easy to apply Theorem 3 to class $\mathcal{PS}_{ap}$: the condition on the dual of σ_1 is automatically satisfied if σ_1 is bent. But this does not lead to new functions, since if $f_i(x,y)=g_i(x\,y^{2^{\frac{n}{2}}-2})$ for $i=1,2,3$, then σ_1 and σ_2 have the same forms.

4.4 A Generalization of Lemma 1

Lemma 1 can be generalized to more than 3 functions. This leads to further methods of constructions.

Proposition 6. *Let $f_1, \ldots, f_m$ be Boolean functions on F_2^n. For every positive integer l, let σ_l be the Boolean function defined by*

$$\sigma_l = \bigoplus_{1\leq i_1<\ldots<i_l\leq m} \prod_{j=1}^{l} f_{i_j} \quad \text{if } l \leq m \text{ and } \sigma_l = 0 \text{ otherwise.}$$

Then we have $f_1 + \ldots + f_m = \sum_{i\geq 0} 2^i\, \sigma_{2^i}$. Denoting by $\widehat{f}$ the Fourier transform of f, that is, $\widehat{f}(s) = \sum_{x\in F_2^n} f(x)(-1)^{x\cdot s}$, this implies $\widehat{f_1}+\ldots+\widehat{f_m} = \sum_{i\geq 0} 2^i\, \widehat{\sigma_{2^i}}$. Moreover, if $m+1$ is a power of 2, say $m+1 = 2^r$, then

$$\widehat{\chi_{f_1}} + \ldots + \widehat{\chi_{f_m}} = \sum_{i=0}^{r-1} 2^i\, \widehat{\chi_{\sigma_{2^i}}}. \tag{14}$$

Proof. Let x be any vector of F_2^n and $j = \sum_{k=1}^{m} f_k(x)$. According to Lucas' Theorem (cf. [45]), the binary expansion of j is $\sum_{i\geq 0} \left[2^i \left(\binom{j}{2^i} \text{ [mod 2]}\right)\right]$. It is a simple matter to check that $\binom{j}{2^i}$ [mod 2] $= \sigma_{2^i}(x)$. Thus, $f_1 + \ldots + f_m = \sum_{i\geq 0} 2^i\, \sigma_{2^i}$. The linearity of the Walsh transform with respect to the addition in $\mathbb{Z}$ implies then directly $\widehat{f_1} + \ldots + \widehat{f_m} = \sum_{i\geq 0} 2^i\, \widehat{\sigma_{2^i}}$.

If $m+1 = 2^r$, then we have $m = \sum_{i=0}^{r-1} 2^i$. Thus, we deduce $\chi_{f_1} + \ldots + \chi_{f_m} = \sum_{i=0}^{r-1} 2^i\, \chi_{\sigma_{2i}}$ from $f_1 + \ldots + f_m = \sum_{i=0}^{r-1} 2^i\, \sigma_{2^i}$. The linearity of the Walsh transform implies then relation (14). ◇

Corollary 2. *Let n be any positive integer and k any non-negative integer such that $k \leq n$. Let $f_1, \ldots, f_7$ be k-th order correlation immune (resp. k-resilient) functions. If two among the functions $\sigma_1 = f_1 \oplus \ldots \oplus f_7$, $\sigma_2 = f_1f_2 \oplus f_1f_3 \oplus \ldots \oplus f_6f_7$ and $\sigma_4 = \bigoplus_{1\leq i_1<\ldots<i_4\leq 7} \prod_{j=1}^{l} f_{i_j}$ is k-th order correlation immune (resp. k-resilient) then the third one is k-th order correlation immune (resp. k-resilient).*

The proof is similar to the proof of Theorem 2.

Corollary 3. *Let n be any positive even integer and $f_1, \ldots, f_m$ ($m \leq 7$) be bent functions on F_2^n.*

- *Assume that σ_1 is bent, and that, for every $a \in F_2^n$, the number $\widehat{\chi_{\sigma_4}}(a)$ is divisible by $2^{n/2}$. Then:*
  - *if $m = 5$ and $\widetilde{\sigma_1} = \widetilde{f_1} \oplus \ldots \oplus \widetilde{f_5} \oplus 1$ then σ_2 is bent;*
  - *if $m = 7$ and $\widetilde{\sigma_1} = \widetilde{f_1} \oplus \ldots \oplus \widetilde{f_7}$, then σ_2 is bent;*
- *Assume that $m \in \{5, 7\}$ and that, for every $a \in F_2^n$, the number $\widehat{\chi_{\sigma_4}}(a)$ is divisible by $2^{n/2-1}$ and the number $\widehat{\chi_{\sigma_2}}(a)$ is divisible by $2^{n/2}$, then σ_1 is bent.*

Proof. By hypothesis, we have for $i = 1, \ldots, m$ and for every vector $a \neq 0$: $\widehat{\chi_{f_i}}(a) = -2\widehat{f_i}(a) = (-1)^{\widetilde{f_i}(a)}\, 2^{n/2}$.

- If σ_1 is bent and, for every $a \in F_2^n$, the number $\widehat{\chi_{\sigma_4}}(a)$ is divisible by $2^{n/2}$, then $\widehat{\chi_{\sigma_2}}(a)$ is congruent with $\left[(-1)^{\widetilde{f_1}(a)} + \ldots + (-1)^{\widetilde{f_m}(a)} - (-1)^{\widetilde{\sigma_1}(a)}\right]$ $2^{n/2-1}$ modulo $2^{n/2+1}$, for every $a \neq 0$.

  If $m = 5$ and $\widetilde{\sigma_1} = \widetilde{f_1} \oplus \ldots \oplus \widetilde{f_5} \oplus 1$ then, denoting by k the Hamming weight of the word $(\widetilde{f_1}(a), \ldots, \widetilde{f_5}(a))$, the number $\widehat{\chi_{\sigma_2}}(a)$ is congruent with $[5 - 2k + (-1)^k]\, 2^{n/2-1}$ modulo $2^{n/2+1}$.

  If $m = 7$ and $\widetilde{\sigma_1} = \widetilde{f_1} \oplus \ldots \oplus \widetilde{f_7}$ then, denoting by k the Hamming weight of the word $(\widetilde{f_1}(a), \ldots, \widetilde{f_7}(a))$, the number $\widehat{\chi_{\sigma_2}}(a)$ is congruent with $[7 - 2k - (-1)^k]\, 2^{n/2-1}$ modulo $2^{n/2+1}$. So, in both cases, we have $\widehat{\chi_{\sigma_2}}(a) \equiv 2^{n/2}$ [mod $2^{n/2+1}$], and σ_2 is bent, according to Lemma 1 of [7] (which is equivalent to saying that a Boolean function f is bent if and only if $\widehat{\chi_f}(a)$ is congruent with $2^{n/2}$ modulo $2^{n/2+1}$, for every $a \neq 0$; indeed, $a \neq 0$ is sufficient thanks to Parseval's relation).
- If, for every $a \in F_2^n$, the number $\widehat{\chi_{\sigma_4}}(a)$ is divisible by $2^{n/2-1}$ and the number $\widehat{\chi_{\sigma_2}}(a)$ is divisible by $2^{n/2}$, then, for every $a \neq 0$, the number $\widehat{\chi_{\sigma_1}}(a)$ is congruent with $\left[(-1)^{\widetilde{f_1}(a)} + \ldots + (-1)^{\widetilde{f_m}(a)}\right]$ $2^{n/2}$ mod $2^{n/2+1}$. Since $m \in \{5, 7\}$, it is then congruent with $2^{n/2}$ mod $2^{n/2+1}$ and σ_1 is bent, according to Lemma 1 of [7]. ◇

References

1. E.F. Assmus and Key, J. D. *Designs and their Codes*, Cambridge Univ. Press.
2. A. Botev and Y. Tarannikov. Lower bounds on algebraic immunity for recursive constructions of nonlinear filters. Preprint 2004.
3. P. Camion, C. Carlet, P. Charpin, N. Sendrier, On correlation-immune functions, *Advances in Cryptology: Crypto '91, Proceedings, Lecture Notes in Computer Science*, V. 576, pp. 86-100, 1991.
4. A. Canteaut and Trabbia, M. Improved fast correlation attacks using parity-check equations of weight 4 and 5, *Advanced in Cryptology-EUROCRYPT 2000. Lecture notes in computer science* 1807, pp. 573-588, 2000.
5. C. Carlet. Partially-bent functions, *Designs Codes and Cryptography*, 3, 135-145 (1993) and proceedings of CRYPTO' 92, Advances in Cryptology, Lecture Notes in Computer Science 740, Springer Verlag, pp. 280-291, 1993.
6. C. Carlet. Two new classes of bent functions, *EUROCRYPT' 93, Advances in Cryptology, Lecture Notes in Computer Science* 765, Springer Verlag, pp. 77-101, 1994.
7. C. Carlet. Generalized Partial Spreads, *IEEE Transactions on Information Theory*, vol 41, number 5, pp. 1482-1487, 1995.
8. C. Carlet. A construction of bent functions. *Finite Fields and Applications, London Mathematical Society*, Lecture Series 233, Cambridge University Press, pp. 47-58, 1996.
9. C. Carlet. More correlation-immune and resilient functions over Galois fields and Galois rings. *Advances in Cryptology, EUROCRYPT' 97, Lecture Notes in Computer Science* 1233, 422-433, Springer Verlag, 1997.
10. C. Carlet. Recent results on binary bent functions. *International Conference on Combinatorics, Information Theory and Statistics; Journal of Combinatorics, Information and System Sciences*, Vol. 24, Nos. 3-4, pp. 275-291, 1999.

11. C. Carlet. On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions, *Proceedings of SETA'01* (Sequences and their Applications 2001), Discrete Mathematics and Theoretical Computer Science, Springer, pp. 131-144, 2001.
12. C. Carlet. A larger Class of Cryptographic Boolean Functions via a Study of the Maiorana-McFarland Construction. *Advances in Cryptology - CRYPT0 2002, no. 2442 in Lecture Notes in Computer Science*, pp. 549-564, 2002.
13. C. Carlet. On the confusion and diffusion properties of Maiorana-McFarland's and extended Maiorana-McFarland's functions. *Special Issue "Complexity Issues in Coding and Cryptography", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday, Journal of Complexity* 20, pp. 182-204, 2004.
14. C. Carlet. On the secondary constructions of resilient and bent functions. Proceedings of the Workshop on Coding, Cryptography and Combinatorics 2003, published by Birkhäuser Verlag, K. Feng, H. Niederreiter and C. Xing Eds., pp. 3-28, 2004.
15. C. Carlet. On the degree, nonlinearity, algebraic thickness and non-normality of Boolean functions, with developments on symmetric functions. *IEEE Transactions on Information Theory*, vol. 50, pp. 2178-2185, 2004.
16. C. Carlet. Concatenating indicators of flats for designing cryptographic functions. *Design, Codes and Cryptography* volume 36, Number 2, pp.189 - 202, 2005.
17. C. Carlet. Designing bent functions and resilient functions from known ones, without extending their number of variables. Proceedings of International Symposium on Information Theory 2005.
18. 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 (winter 2005-2006).
19. C. Carlet, D. K. Dalai, K. C. Gupta and S. Maitra. Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction. Preprint.
20. C. Carlet, H. Dobbertin and G. Leander. Normal extensions of bent functions. *IEEE Transactions on Information Theory*, vol. 50, no. 11, pp. 2880-2885, 2004.
21. C. Carlet and P. Gaborit. Hyper-bent functions and cyclic codes. To appear in the Journal of Combinatorial Theory, Series A, 2005.
22. C. Carlet and P. Gaborit. On the construction of balanced Boolean functions with a good algebraic immunity. Proceedings of International Symposium on Information Theory 2005. To appear.
23. C. Carlet and P. Sarkar. Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions. *Finite fields and Applications* 8, pp. 120-130, 2002.
24. C. Carlet and J.L. Yucas. Piecewise Constructions of Bent and Almost Optimal Boolean Functions. To appear in *Designs, Codes and Cryptography*, 2005.
25. N. Courtois. Fast Algebraic Attacks on Stream Ciphers with Linear Feedback. *Advances in cryptology–CRYPTO 2003, Lecture Notes in Computer Science* 2729, pp. 177-194, Springer, 2003.
26. N. Courtois and W. Meier. Algebraic Attacks on Stream Ciphers with Linear Feedback. *Advances in cryptology–EUROCRYPT 2003, Lecture Notes in Computer Science* 2656, pp. 346-359, Springer, 2002.
27. 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.
28. D. K. Dalai, K. C. Gupta and S. Maitra. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions. Indocrypt 2004, pp. 92–106, number 3348 in Lecture Notes in Computer Science, Springer Verlag, 2004.

29. D. K. Dalai, K. C. Gupta and S. Maitra. Cryptographically Significant Boolean functions: Construction and Analysis in terms of Algebraic Immunity. *Fast Software Encryption 2005, Lecture Notes in Computer Science* 3557, pp. 98-111, 2005.
30. J. F. Dillon. *Elementary Hadamard Difference sets.* Ph. D. Thesis, Univ. of Maryland, 1974.
31. J. F. Dillon. Elementary Hadamard Difference sets, *Proc. Sixth S-E Conf. Comb. Graph Theory and Comp.*, F. Hoffman et al. (Eds), Winnipeg Utilitas Math, pp. 237-249, 1975.
32. J. F. Dillon and H. Dobbertin. New cyclic difference sets with Singer parameters. Finite Fields and Their Applications 10, pp. 342-389, 2004.
33. H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. *Fast Software Encryption, Second International Workshop*, Lecture Notes in Computer Science 1008, pp. 61-74, 1995.
34. H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke and P. Gaborit. Construction of Bent Functions via Niho Power Functions. To appear in the *Journal of Combinatorial Theory, Series A*, 2005.
35. G. Gong. On Existence and Invariant of Algebraic Attacks. Technical report, 2004. http://www.cacr.math.uwaterloo.ca/techreports/2004/corr2004-17.pdf
36. P. Hawkes and G. G. Rose. Rewriting variables: the complexity of fast algebraic attacks on stream ciphers. Cryptology ePrint Archive, Report 2004/081, 2004. http://eprint.iacr.org/2004/081.
37. X.-D. Hou. New constructions of bent functions, *International Conference on Combinatorics, Information Theory and Statistics; Journal of Combinatorics, Information and System Sciences*, Vol. 24, Nos. 3-4, pp. 275-291, 1999.
38. X.-D. Hou. Group actions on binary resilient functions. Appl. Algebra Eng. Commun. Comput. 14(2), pp. 97-115, 2003.
39. X.-D. Hou and P. Langevin. Results on bent functions, *Journal of Combinatorial Theory, Series A*, 80, pp. 232-246, 1997.
40. T. Johansson and Jönsson, F. Improved fast correlation attack on stream ciphers via convolutional codes. *Advances in Cryptology - EUROCRYPT'99, number 1592 in Lecture Notes in Computer Science*, pp. 347-362, 1999.
41. T. Johansson and Jönsson, F. Fast correlation attacks based on turbo code techniques. *Advances in Cryptology - CRYPTO'99, number 1666 in Lecture Notes in Computer Science*, pp. 181-197, 1999.
42. K. Khoo, G.-E. Tan, H.-K. Lee and G. Gong. Comparision of Boolean function design. Proceedings of International Symposium on Information Theory 2005.
43. G. Leander. Bent functions with 2^r Niho exponents. *Proceedings of the Workshop on Coding and Cryptography* 2005, Bergen, pp. 454-461, 2005.
44. G. Leander. Monomial bent functions. *Proceedings of the Workshop on Coding and Cryptography* 2005, Bergen, pp. 462-470, 2005.
45. F. J. Mac Williams and N. J. Sloane. *The theory of error-correcting codes*, Amsterdam, North Holland, 1977.
46. S. Maity and S. Maitra. Minimum distance between bent and 1-resilient Boolean functions. *Proceedings of Fast Software Encryption* 2004, LNCS 3017, pp. 143-160, 2004.
47. W. Meier and O. Staffelbach. Nonlinearity Criteria for Cryptographic Functions, *Advances in Cryptology, EUROCRYPT' 89, Lecture Notes in Computer Science 434, pp. 549-562, Springer Verlag*, 1990.
48. W. Meier, E. Pasalic and C. Carlet. Algebraic attacks and decomposition of Boolean functions. *Advances in Cryptology, EUROCRYPT 2004, Lecture Notes in Computer Science, Springer Verlag* 3027, pp. 474-491, 2004.

49. D. Olejár and M. Stanek. "On cryptographic properties of random Boolean functions." Journal of Universal Computer Science, vol. 4, No.8, pp. 705-717, 1998.
50. E. Pasalic and S. Maitra. A Maiorana-McFarland type construction for resilient Boolean functions on n variables (n even) with nonlinearity $> 2^{n-1} - 2^{n/2} + 2^{n/2-2}$. *Proceedings of the Workshop on Coding and Cryptography 2003*, pp. 365-374, 2003.
51. Olsen, J. D., Scholtz, R. A. and L. R. Welch. Bent function sequences, *IEEE Trans. on Inf. Theory* , vol IT- 28, n° 6, 1982.
52. E. Pasalic. Degree optimized resilient Boolean functions from Maiorana-McFarland class. In *9th IMA Conference on Cryptography and Coding*, 2003.
53. O. S. Rothaus. On "bent" functions, *J. Comb. Theory*, 20A, 300-305, 1976.
54. E. Pasalic, T. Johansson, S. Maitra and P. Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity. *Proceedings of the Workshop on Coding and Cryptography* 2001, published by *Electronic Notes in Discrete Mathematics*, Elsevier, vo. 6, pp. 425-434, 2001.
55. P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. *Advances in Cryptology - EUROCRYPT 2000*, no. 1807 in Lecture Notes in Computer Science, Springer Verlag, pp. 485-506, 2000.
56. P. Sarkar and S. Maitra. Nonlinearity Bounds and Constructions of Resilient Boolean Functions. *CRYPTO 2000, LNCS* Vol. 1880, ed. Mihir Bellare, pp. 515-532, 2000.
57. T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information theory*, V. IT-30, No 5, pp. 776-780, 1984.
58. Siegenthaler, T. Decrypting a Class of Stream Ciphers Using Ciphertext Only. *IEEE Transactions on Computer, V. C-34*, No 1, pp. 81-85, 1985.
59. L. Simpson, E. Dawson, J. Golic and W. Millan. LILI Keystream generator, *P roceedings of SAC'2000, Lecture Notes in Computer Science* 1807, Springer, pp. 248-261, 2001; cf. www.isrc.qut.edu.au/lili/.
60. Y. V. Tarannikov. On resilient Boolean functions with maximum possible nonlinearity. *Proceedings of INDOCRYPT 2000, Lecture Notes in Computer Science* 1977, pp. 19-30, 2000.
61. Xiao Guo-Zhen and Massey, J. L. A Spectral Characterization of Correlation-Immune Combining Functions. *IEEE Trans. Inf. Theory*, Vol IT 34, n° 3, pp. 569-571, 1988.
62. Y. Zheng and X. M. Zhang. Plateaued functions. *ICICS'99, Lecture Notes in Computer Science*, Heidelberg, Ed., Springer-Verlag, vol. 1726, pp. 284-300, 1999.