An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity

Claude Carlet[1] and Keqin Feng[2]

[1] Department of Mathematics, University of Paris 8 (MAATICAH), 93526 - Saint-Denis cedex 02, France; e-mail: claude.carlet@inria.fr.
[2] Department of Mathematical Sciences, Tsinghua University, Beijing China 100084; e-mail: kfeng@math.tsinghua.edu.cn (Supported by the NSFC grant 60433050 and the 973 grant of China 2004CB 3180004).

Abstract. After the improvement by Courtois and Meier of the algebraic attacks on stream ciphers and the introduction of the related notion of algebraic immunity, several constructions of infinite classes of Boolean functions with optimum algebraic immunity have been proposed. All of them gave functions whose algebraic degrees are high enough for resisting the Berlekamp-Massey attack and the recent Rønjom-Helleseth attack, but whose nonlinearities either achieve the worst possible value (given by Lobanov's bound) or are slightly superior to it. Hence, these functions do not allow resistance to fast correlation attacks. Moreover, they do not behave well with respect to fast algebraic attacks. In this paper, we study an infinite class of functions which achieve an optimum algebraic immunity. We prove that they have an optimum algebraic degree and a much better nonlinearity than all the previously obtained infinite classes of functions. We check that, at least for small values of the number of variables, the functions of this class have in fact a very good nonlinearity and also a good behavior against fast algebraic attacks.

Keywords: Algebraic attack, Boolean function, Stream cipher

1 Introduction

Before this century, the Boolean functions used in the combiner and filter models of stream ciphers (see description *e.g.* in [9]) had mainly to be balanced, to have a high algebraic degree, a high nonlinearity and, in the case of the combiner model, a high correlation immunity (in the case of the filter model, a correlation immunity of order 1 is commonly considered as sufficient; in most cases, it is easily achieved without losing the other properties, by replacing the function by a linearly equivalent one). These properties could be satisfied by functions of about 10 variables. But the algebraic attacks introduced by Courtois and Meier [15] (or more properly speaking improved by them, since the idea of algebraic attacks comes already from Shannon), which have allowed cryptanalysing several

stream ciphers [1, 12, 13, 15, 25] have led to more constraints on the functions, and obliged to increase the number of variables up to at least 13 variables and in practice much more (maybe 20). The property needed for resisting the standard algebraic attack of Courtois and Meier [15] is a high algebraic immunity [33]: for a given Boolean function f on n variables, any nonzero Boolean function g such that $f * g = 0$ or $(1+f) * g = 0$ should have high algebraic degree, where $*$ is the multiplication of functions inherited from multiplication in $\mathbb{F}_2$, the finite field with two elements. The best possible algebraic immunity of n-variable functions is $\lceil \frac{n}{2} \rceil$ [15]. It has been proved in [19] that, for all $a < 1$, when n tends to infinity, $AI(f)$ is almost surely greater than $\frac{n}{2} - \sqrt{\frac{n}{2} \ln \left(\frac{n}{a \ln 2}\right)}$. Hence, random functions behave well with respect to the algebraic immunity (but this does not mean that functions with good algebraic immunity are easy to construct).
Having a high algebraic immunity is not sufficient for resisting the fast algebraic attacks introduced by Courtois in [13]: if one can find g of low degree and $h \neq 0$ of reasonable degree such that $f * g = h$, then a fast algebraic attack (FAA) is feasible. No result is known on the behavior of random functions against FAA.
Even a high resistance to fast algebraic attacks is not sufficient, since algebraic attacks on the augmented function [23] can be efficient when fast algebraic attacks are not. The resistance to these attacks is not properly speaking a property of the function used in a cipher and studying the resistance of the cipher to them obliges to consider all possible update functions (of the linear part of the pseudorandom generator).

It is a difficult challenge to find functions achieving all of the necessary criteria and the research of such functions has taken a significant delay with respect to cryptanalyses. The research of Boolean functions that can resist algebraic attacks, the Berlekamp-Massey attack and the fast correlation attacks has not given fully satisfactory results: we know that functions achieving optimal or suboptimal algebraic immunity and in the same time balancedness, high algebraic degree and high nonlinearity must exist thanks to the results of [19, 37]. Such functions have been found with sufficient numbers of variables thanks to Algorithm 1 of [2] (others can be found by using the algorithm of [20]). But the functions given in [2] belong to classes which have not, potentially, a good asymptotic algebraic immunity (see [35]), and there remains to see whether these functions behave well against fast algebraic attacks. No infinite class of functions with good algebraic immunity and good nonlinearity has been exhibited so far.

There are, up to now, two main infinite classes of Boolean functions achieving optimum algebraic immunity. The first one contains functions in even numbers n of variables and is obtained by an iterative construction. The constructed functions have been further studied in [10], where it is shown that their algebraic degrees are close to n but their nonlinearity is $2^{n-1} - \binom{n-1}{\frac{n}{2}}$, which is insufficient. Moreover, they are not balanced (but it is possible to build balanced functions from these ones) and are weak against fast algebraic attacks [2, 18]. The second class contains symmetric functions (whose values depend only on the Hamming weight of the input vectors) [3, 18] or functions whose values depend on the Hamming weight of the input vectors except for a few inputs [7]. The nonlinearities of these functions are often not exceeding $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$ and when they do, they are not much greater than this number, see [11]. They are still weaker against fast algebraic attacks [2]. The functions constructed in [28, 29] seem to have worse nonlinearity than those of [7]. Apart from these infinite classes, some power functions with sub-optimal algebraic immunity, in at most 20 variables, have been exhibited in [2, Table 1]. The behavior of these functions against fast algebraic attacks has not been investigated so far.

In the present paper, we show that an infinite class of balanced functions with optimal algebraic immunity, which has been considered in [22] for showing the tightness of bounds on the algebraic immunity of vectorial functions, has potentially a good nonlinearity. We give a very simple proof of the optimal algebraic immunity of these functions. We show that they have also optimal algebraic degree and we prove a lower bound on their nonlinearities which is much larger than the best nonlinearities of the infinite classes of functions with optimal algebraic immunity found so far. However, this bound is not enough for saying these functions have good nonlinearities. We compute for small values of n the exact values of the nonlinearity, which are very good and much bigger than the lower bound, and we also check for these values of n that the functions behave well against fast algebraic attacks. This is the first time a function (and moreover a whole infinite class of functions) seems able to satisfy all of the main criteria for being used as a filtering function in a stream cipher.

The rest of the paper is organized as follows. In Section 2, we recall the necessary background. In Section 3, we give a simple proof that the functions of the class have optimal algebraic immunity. In Section 4, we calculate the univariate representation of the functions and deduce their algebraic degree. We prove a lower bound on their nonlinearity. We give also the exact values of the nonlinearity for small values of n. In Section 5, we give the results of computer investigations suggesting a good immunity of the functions against fast algebraic attacks.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$, and B_n the set of n-variable (Boolean) functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The basic representation of a Boolean function $f(x_1, \cdots, x_n)$ is by the output column of its truth table, i.e., a binary string of length 2^n,

$$[f(0,0,\cdots,0), f(1,0,\cdots,0), f(0,1,\cdots,0), f(1,1,\cdots,0), \cdots, f(1,1,\cdots,1)].$$

The *Hamming weight* $\mathrm{wt}(f)$ of a Boolean function $f \in B_n$ is the weight of this string, that is, the size of the support $\mathrm{Supp}(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ of the function. The *Hamming distance* $\mathrm{d_H}(f, g)$ between two Boolean functions f and g is the Hamming weight of their difference $f + g$ (by abuse of notation, we use $+$ to denote the addition on $\mathbb{F}_2$, i.e., the XOR). We say that a Boolean function f is *balanced* if its truth table contains an equal number of 1's and 0's, that is, if its Hamming weight equals 2^{n-1}.

Any Boolean function has a unique representation as a multivariate polynomial over $\mathbb{F}_2$, called the *algebraic normal form* (ANF), of the special form:

$$f(x_1, \cdots, x_n) = \sum_{I \subseteq \{1,2,\cdots,n\}} a_I \prod_{i \in I} x_i.$$

The *algebraic degree*, $\deg(f)$, is the global degree of this polynomial, that is, the number of variables in the highest order term with non zero coefficient. A Boolean function is affine if it has degree at most 1. The set of all affine functions is denoted by A_n.

We shall need another representation of Boolean functions, by univariate polynomials over the field $\mathbb{F}_{2^n}$. We identify the field $\mathbb{F}_{2^n}$ and the vector space $\mathbb{F}_2^n$: this field being an n-dimensional $\mathbb{F}_2$-vector space, we can choose a basis $(\beta_1, \cdots, \beta_n)$ and identify every element $x = \sum_{i=1}^n x_i\beta_i \in \mathbb{F}_{2^n}$ with the n-tuple of its coordinates $(x_1, \cdots, x_n) \in \mathbb{F}_2^n$. Every function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ (and in particular every Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$) can then be uniquely represented as a polynomial $\sum_{j=0}^{2^n-1} a_j x^j$ where $a_j \in \mathbb{F}_{2^n}$. Indeed, the mapping which maps every such polynomial to the corresponding function from $\mathbb{F}_{2^n}$ to itself is $\mathbb{F}_{2^n}$-linear, injective (since a non-zero polynomial of degree at most $2^n - 1$ over a field cannot have more than $2^n - 1$ zeroes in this field) and therefore surjective since the $\mathbb{F}_{2^n}$-vector spaces of these polynomials and of the functions from $\mathbb{F}_{2^n}$ to itself have the same dimension 2^n. The function is Boolean if and only if the functions $f(x)$ and $(f(x))^2$ are represented by the same polynomial, that is, if $a_0, a_{2^n-1} \in \mathbb{F}_2$ and, for every $i = 1, \cdots, 2^n - 2$, we have $a_{2j} = (a_j)^2$, where $2j$ is taken mod $2^n - 1$. Then the algebraic degree of the function equals the maximum *2-weight* $w_2(j)$ of j such that $a_j \neq 0$, where the 2-weight of j equals the number of 1's in its binary expansion. We briefly recall why, since the algebraic degree is an important parameter and we will need this when studying the functions. Writing $j = \sum_{s=0}^{n-1} j_s 2^s$, we have the equalities:

$$\begin{aligned} f(x) &= \sum_{j=0}^{2^n-1} a_j \left(\sum_{i=1}^n x_i \beta_i \right)^j \\ &= \sum_{j=0}^{2^n-1} a_j \left(\sum_{i=1}^n x_i \beta_i \right)^{\sum_{s=0}^{n-1} j_s 2^s} \\ &= \sum_{j=0}^{2^n-1} a_j \prod_{s=0}^{n-1} \left(\sum_{i=1}^n x_i \beta_i^{2^s} \right)^{j_s} ; \end{aligned}$$

expanding these products, simplifying and decomposing again over the basis $(\beta_1, \ldots, \beta_n)$ gives the ANF of F; this proves that the algebraic degree is upper bounded by the number $\max\{w_2(j);\ a_j \neq 0\}$, and it cannot be strictly smaller, because the number of those functions from $\mathbb{F}_{2^n}$ to itself of algebraic degrees at most d equals the number of those univariate polynomials $\sum_{j=0}^{2^n-1} a_j x^j$, $a_j \in \mathbb{F}_{2^n}$, such that $\max_{j=0,\ldots,2^n-1/\ a_j \neq 0} w_2(j) \leq d$.

In this representation, the elements of A_n are all the functions $tr(ax)$, $a \in \mathbb{F}_{2^n}$, where tr is the trace function: $tr(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}$.

Any Boolean function should have high algebraic degree to allow the cryptosystem resisting the Berlekamp-Massey attack [21].

Boolean functions used in cryptographic systems must have high nonlinearity to withstand fast correlation attacks (see e.g. [6, 34]). The *nonlinearity* of an n-variable function f is its distance to the set of all n-variable affine functions, i.e.,

$$nl(f) = \min_{g \in A_n} (\mathrm{d_H}(f, g)).$$

This parameter can be expressed by means of the Walsh transform. Let $x = (x_1, \cdots, x_n)$ and $\lambda = (\lambda_1, \cdots, \lambda_n)$ both belong to $\mathbb{F}_2^n$ and $\lambda \cdot x$ be the usual inner product in $\mathbb{F}_2^n$: $\lambda \cdot x = \lambda_1 x_1 + \cdots + \lambda_n x_n \in \mathbb{F}_2$, or any other inner product in $\mathbb{F}_2^n$. Let $f(x)$ be a Boolean function in n variables. The *Walsh transform* (depending on the choice of the inner product) of $f(x)$ is the integer valued function over $\mathbb{F}_2^n$ defined as

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \lambda \cdot x}.$$

If we identify the vector space $\mathbb{F}_2^n$ with the field $\mathbb{F}_{2^n}$, then we can take for inner product: $\lambda \cdot x = tr(\lambda x)$.
A Boolean function f is balanced if and only if $W_f(0) = 0$. The nonlinearity of f can also be given by

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_2^n} |W_f(\lambda)|.$$

For every n-variable function f we have $nl(f) \leq 2^{n-1} - 2^{n/2-1}$.

Algebraic attacks have been introduced recently (see [15]). They recover the secret key, or at least the initialization of the cipher, by solving a system of multivariate algebraic equations. The idea that the key bits can be characterized as the solutions of such a system comes from C. Shannon [39]. In practice, for cryptosystems which are robust against the usual attacks, this system is too complex to be solved (its equations being highly nonlinear). In the case of stream ciphers, we can get a very overdefined system (i.e. a system with a number of linearly independent equations much greater than the number of unknowns). In the combiner or the filter model, with a linear part of size N and with an n-variable Boolean function f as combining or filtering function, there exists a linear permutation $L : \mathbb{F}_2^N \mapsto \mathbb{F}_2^N$ and a linear mapping $L' : \mathbb{F}_2^N \mapsto \mathbb{F}_2^n$ such that, denoting by $u_1, \cdots, u_N$ the initialisation and by $(s_i)_{i \geq 0}$ the pseudo-random sequence output by the generator, we have, for every $i \geq 0$:

$$s_i = f(L' \circ L^i(u_1, \cdots, u_N)).$$

The number of equations can then be much larger than the number of unknowns. This makes less complex the resolution of the system by using Groebner basis, and even allows linearizing the system (i.e. obtaining a system of linear equations by replacing every monomial of degree greater than 1 by a new unknown); the resulting linear system has however too many unkwnowns and cannot be solved. Courtois and Meier have had a simple but very efficient idea. Assume that there exist functions $g \neq 0$ and h of low degrees (say, of degrees at most d) such that $f * g = h$. We have then, for every $i \geq 0$:

$$s_i \, g(L' \circ L^i(u_1, \cdots, u_N)) = h(L' \circ L^i(u_1, \cdots, u_N)).$$

This equation in $u_1, \cdots, u_N$ has degree at most d, since L and L' are linear, and the system of equations obtained after linearization can then be solved by Gaussian elimination. Low degree relations have been shown to exist for several well known constructions of stream ciphers, which were immune to all previously known attacks.
It has been shown [15, 33] that the existence of such relations is equivalent to that of non-zero functions g of low degrees such that $f * g = 0$ or $(f + 1) * g = 0$. This led to the following definition.

Definition 1. *For $f \in B_n$, we define $AN(f) = \{g \in B_n \,|\, f * g = 0\}$. Any function $g \in AN(f)$ is called an annihilator of f. The algebraic immunity (AI) of f is the minimum degree of all the nonzero annihilators of f and of all those of $f + 1$. We denote it by $AI(f)$.*

Note that $AI(f) \leq \deg(f)$, since $f * (1 + f) = 0$. Note also that the algebraic immunity, as well as the nonlinearity and the degree, is affine invariant (i.e. is invariant under composition by an affine automorphism). As shown in [15], we have $AI(f) \leq \lceil \frac{n}{2} \rceil$.

The complexity of the standard algebraic attack on the combiner model or the filter model using a nonlinear function f equals roughly $O(D^3)$ in time and $O(D)$ in data, where $D = \sum_{i=0}^{AI(f)} \binom{N}{i}$, where N is the size of the linear part of the pseudo-random generator.

If a function has optimal algebraic immunity $\lceil \frac{n}{2} \rceil$ with n odd, then it is balanced (see e.g. [10]). Whatever is n, a high value of $AI(f)$ automatically implies that the nonlinearity is not very low: M. Lobanov has obtained in [31] the following tight lower bound:

$$nl(f) \geq 2 \sum_{i=0}^{AI(f)-2} \binom{n-1}{i}.$$

However, this bound does not assure that the nonlinearity is high enough:
• For n even and $AI(f) = \frac{n}{2}$, it gives $nl(f) \geq 2^{n-1} - 2\binom{n-1}{n/2-1} = 2^{n-1} - \binom{n}{n/2}$ which is much smaller than the best possible nonlinearity $2^{n-1} - 2^{n/2-1}$ and, more problematically, much smaller than the asymptotic almost sure nonlinearity of Boolean functions, which is, when n tends to ∞, located in the neighbourhood

of $2^{n-1} - 2^{n/2-1}\sqrt{2n\ln 2}$ (see [37]); the nonlinearity reached by the known functions with optimal AI is equal to (or is close to) that of the majority function which maps an input vector $x \in \mathbb{F}_2^n$ to 1 if its weight is not smaller (resp. is strictly greater) than $n/2$ and 0 otherwise (the two versions are affinely equivalent) and of the iterative construction recalled in [10] : $2^{n-1} - \binom{n-1}{n/2} = 2^{n-1} - \frac{1}{2}\binom{n}{n/2}$; it is a little better than what gives Lobanov's bound but it is insufficient. Some functions exhibited in [11, 28, 29] have better nonlinearities but the increasement is not quite significant.
• For n odd and $AI(f) = \frac{n+1}{2}$, Lobanov's bound gives $nl(f) \geq 2^{n-1} - \binom{n-1}{(n-1)/2} \simeq 2^{n-1} - \frac{1}{2}\binom{n}{(n-1)/2}$ which is a little better than in the n even case, but still far from the average nonlinearity of Boolean functions; the nonlinearity of the majority function matches this bound; here again, some functions exhibited in [11, 28, 29] have better nonlinearities but the increasement is not sufficient.

A high algebraic immunity is a necessary but not sufficient condition for robustness against all kinds of algebraic attacks. Indeed, if one can find g of low degree and $h \neq 0$ of reasonable degree such that $f * g = h$, then a fast algebraic attack is feasible, see [13, 1, 24] (note however that fast algebraic attacks need more data than standard ones). This has been exploited in [14] to present an attack on SFINKS [4] and we can say that with this attack, which comes in addition to the standard algebraic attack, Courtois has made very difficult the work of the designer. Since $f * g = h$ implies $f * h = f * f * g = f * g = h$, we see that h is then an annihilator of $f + 1$ and if $h \neq 0$, then its degree is at least equal to the algebraic immunity of f. So summarizing, we shall say that the function behaves well with respect to fast algebraic attacks if there exists k (which can be small with respect to n, but not too small) such that, for every nonzero function g of algebraic degree at most k, the function $h = f * g$ has algebraic degree significantly greater than $\lceil \frac{n}{2} \rceil$. It has been shown in [13] that when $e + d \geq n$, there must exist g of degree at most e and h of degree at most d such that $f * g = h$. Hence, an n-variable function f can be considered as optimal with respect to fast algebraic attacks if there do not exist two functions $g \neq 0$ and h such that $f * g = h$ and $\deg(g) + \deg(h) < n$ with $\deg(g) < n/2$. The question of the existence of such functions was completely open until the present paper.

The pseudo-random generator must also resist algebraic attacks on the augmented function [23], that is, on the vectorial function $F(x)$ whose coordinate functions are $f(x), f(L(x)), \cdots, f(L^{m-1}(x))$, where L is the (linear) update function of the linear part of the generator. Algebraic attacks can be more efficient when applied to the augmented function rather than to the function f itself. The efficiency of the attack depends not only on the function f, but also on the update function (and naturally also on the choice of m), since for two different update functions L and L', the vectorial functions $F(x)$ and $F'(x) = (f(x), f(L'(x)), ..., f(L'^{m-1}(x))$ are not linearly equivalent (neither equivalent in the more general sense called CCZ-equivalence, that is, affine equivalence of the graphs of the functions). Testing the behavior of a function with respect to this attack is therefore a long term work (all possible update functions have to be investigated).

A new version of algebraic attack has been found recently by S. Rønjom and T. Helleseth [38] and is very efficient. Its time complexity is roughly $O(\mathcal{D})$, where $\mathcal{D} = \sum_{i=0}^{\deg(f)} \binom{N}{i}$, where N is the size of the linear part of the pseudo-random generator. But it needs much more data than standard algebraic attacks: $O(\mathcal{D})$ also! When f has degree close to n and algebraic immunity close to $\frac{n}{2}$, this is the square of what is needed by standard algebraic attacks. However, this attack obliges the designer to choose a function with very high degree.

The functions used in the combiner model must be additionally highly resilient (that is, balanced and correlation immune of a high order; see definition *e.g.* in [9]) to withstand correlation attacks. It seems quite difficult to achieve all of the necessary criteria including this one, and for this reason, the filter generator seems more appropriate.

3 The infinite class and its algebraic immunity

We shall show that, for every n, the Boolean function on $\mathbb{F}_{2^n}$ whose support equals $\{0\}\cup\{\alpha^i;\ i=0,\cdots,2^{n-1}-2\}$, where α is a primitive element of $\mathbb{F}_{2^n}$, has optimal algebraic immunity. This function (or more precisely its complement) makes thinking of the majority function but we shall see that it is in fact quite different since it has much better nonlinearity and it behaves much better with respect to fast algebraic attacks too.

Theorem 1. *Let n be any integer such that $n \geq 2$ and α a primitive element of the field F_{2^n}.*
Let f be the Boolean function on $\mathbb{F}_{2^n}$ whose support is $\{0,1,\alpha,\cdots,\alpha^{2^{n-1}-2}\}$. Then f has optimal algebraic immunity $\lceil n/2\rceil$.

Proof.
Let g be any Boolean function of algebraic degree at most $\lceil n/2\rceil-1$. Let $g(x)=\sum_{i=0}^{2^n-1} g_i x^i$ be its univariate representation in the field $\mathbb{F}_{2^n}$, where $g_i \in \mathbb{F}_{2^n}$ is null if the 2-weight $w_2(i)$ of i is at least $\lceil n/2\rceil$ (which implies in particular that $g_{2^n-1}=0$).
If g is an annihilator of f, then we have $g(\alpha^i)=0$ for every $i=0,\cdots,2^{n-1}-2$, that is, the vector $(g_0,\cdots,g_{2^n-2})$ belongs to the Reed-Solomon code over $\mathbb{F}_{2^n}$ of zeroes $1,\alpha,\cdots,\alpha^{2^{n-1}-2}$ (the Reed-Solomon code of zeroes $\alpha^\ell,\cdots,\alpha^{\ell+r}$ equals by definition the set of vectors $(g_0,\cdots,g_{2^n-2})$ of $\mathbb{F}_{2^n}^{2^n-1}$ such that these elements are zeroes of the polynomial $\sum_{i=0}^{2^n-2} g_i X^i$, see [32]; there exists an equivalent definition where Reed-Solomon codes are given by evaluating polynomials at points but we shall not need it).
According to the BCH bound, if g is non-zero, then the vector $(g_0,\cdots,g_{2^n-2})$ has Hamming weight at least 2^{n-1}. The general proof of this lower bound can

be found in [32] as well. For self-completeness, we briefly recall how it can be simply proved in our framework. By definition, we have:

$$\begin{pmatrix} g(1) \\ g(\alpha) \\ g(\alpha^2) \\ \vdots \\ g(\alpha^{2^n-2}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^n-2} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(2^n-2)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{2^n-2} & \alpha^{2(2^n-2)} & \cdots & \alpha^{(2^n-2)(2^n-2)} \end{pmatrix} \times \begin{pmatrix} g_0 \\ g_1 \\ g_2 \\ \vdots \\ g_{2^n-2} \end{pmatrix}$$

which implies (since for every $0 \leq i, j \leq 2^n - 2$, the sum $\sum_{k=0}^{2^n-2} \alpha^{(i-j)k}$ equals 1 if $i = j$ and 0 otherwise):

$$\begin{pmatrix} g_0 \\ g_1 \\ g_2 \\ \vdots \\ g_{2^n-2} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-(2^n-2)} \\ 1 & \alpha^{-2} & \alpha^{-4} & \cdots & \alpha^{-2(2^n-2)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{-(2^n-2)} & \alpha^{-2(2^n-2)} & \cdots & \alpha^{-(2^n-2)(2^n-2)} \end{pmatrix} \times \begin{pmatrix} g(1) \\ g(\alpha) \\ g(\alpha^2) \\ \vdots \\ g(\alpha^{2^n-2}) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{-(2^{n-1}-1)} & \alpha^{-2^{n-1}} & \cdots & \alpha^{-(2^n-2)} \\ \vdots & \vdots & \cdots & \vdots \\ \alpha^{-(2^{n-1}-1)(2^n-2)} & \alpha^{-2^{n-1}(2^n-2)} & \cdots & \alpha^{-(2^n-2)(2^n-2)} \end{pmatrix} \times \begin{pmatrix} g(\alpha^{2^{n-1}-1}) \\ g(\alpha^{2^{n-1}}) \\ \vdots \\ g(\alpha^{2^n-2}) \end{pmatrix}$$

Suppose that at least 2^{n-1} of the g_i's are null. Then, $g(\alpha^{2^{n-1}-1}), \cdots, g(\alpha^{2^n-2})$ satisfy a homogeneous system of linear equations whose matrix is a $2^{n-1} \times 2^{n-1}$ Vandermonde matrix and whose determinant is therefore non-null. This implies that $g(\alpha^{2^{n-1}-1}), \cdots, g(\alpha^{2^n-2})$ and therefore g must then be null, a contradiction. Hence the vector $(g_0, \cdots, g_{2^n-2})$ has weight at least 2^{n-1}.

Moreover, suppose that this vector has Hamming weight 2^{n-1} exactly. Then $g(x) = \sum_{\substack{0 \leq i \leq 2^n-2 \\ w_2(i) \leq (n-1)/2}} x^i$ and n is odd (so that $g(x)$ can have 2^{n-1} terms); but this contradicts the fact that $g(0) = 0$. We deduce that the vector $(g_0, \cdots, g_{2^n-2})$ has Hamming weight strictly greater than 2^{n-1}, leading to a contradiction with the fact that g has algebraic degree at most $\lceil n/2 \rceil - 1$, since the number of integers of 2-weight at most $\lceil n/2 \rceil - 1$ is not strictly greater than 2^{n-1}.

Let g be now a non-zero annihilator of $f + 1$. The vector $(g_0, \cdots, g_{2^n-2})$ belongs then to the Reed-Solomon code over $\mathbb{F}_{2^n}$ of zeroes $\alpha^{2^{n-1}-1}, \cdots, \alpha^{2^n-2}$. According to the BCH bound (which can be proven similarly as above), this vector has then Hamming weight strictly greater than 2^{n-1}. We arrive to the same contradiction. Hence, there does not exist a non-zero annihilator of f or $f + 1$ of algebraic degree at most $\lceil n/2 \rceil - 1$ and f has then (optimal) algebraic immunity $\lceil n/2 \rceil$. □

Remark.

1. We have proved in fact that f admits no non-zero annihilator whose univariate representation has at most 2^{n-1} non-zero coefficients.

2. The same proof shows that, for every even n, denoting $D = \sum_{i=0}^{n/2-1}\binom{n}{i} = 2^{n-1} - \binom{n-1}{n/2}$, if the support of f contains $\{0, \alpha^i, \alpha^{i+1}, \cdots \alpha^{i+D-2}\}$ and if the support of $f + 1$ contains $\{\alpha^j, \alpha^{i+1}, \cdots \alpha^{j+D-1}\}$ for suitable parameters i, j, then the function f also has optimal AI. Moreover, for every n and every positive integer D, if $\text{Supp}(f) \supseteq \{0, \alpha^i, \alpha^{i+1}, \cdots \alpha^{i+D-2}\}$ and $\text{Supp}(f+1) \supseteq \{\alpha^j, \alpha^{i+1}, \cdots \alpha^{j+D-1}\}$ for suitable parameters i, j, then the function f has AI at least k such that $D \geq \sum_{i=0}^{k-1}\binom{n}{i}$. Hence, we can build functions with sub-optimal algebraic immunity. Sub-optimality is sometimes better than optimality in cryptography, when it allows avoiding a too strong structure of the function. Here, this allows constructing a balanced function of algebraic immunity $\lceil \frac{n}{2} \rceil - 1$ (for instance) and whose support is not made exclusively of consecutive powers of a primitive element.

3. Note that the function of Theorem 1 is not *a priori* linearly equivalent to the Boolean function whose support equals the set of the binary expansions of the integers in the range $[0; 2^{n-1} - 1]$. Indeed, for general $i = \sum_{k=0}^{n-1} 2^{i_k}$, $j = \sum_{k=0}^{n-1} 2^{j_k}$ there is no bilinear relationship between $tr(\alpha^{i+j})$ and $i_0 j_0 + \cdots + i_{n-1} j_{n-1}$. This means that the inner products in both frameworks are not linearly linked.

4 Algebraic degree and nonlinearity of the function

We shall see now that the algebraic degree of the function of Theorem 1 is cryptographically quite satisfactory and that its nonlinearity is provably much better than for the previously known functions with optimal algebraic immunity. However, the lower bound we obtain gives a value which is not high enough for saying that the function has good nonlinearity. Nevertheless, for the values of n for which we could compute the exact value of the nonlinearity, it is quite satisfactory too.

Theorem 2. *The univariate representation of the function f of Theorem 1 equals*

$$1 + \sum_{i=1}^{2^n-2} \frac{\alpha^i}{(1+\alpha^i)^{1/2}}\, x^i \qquad (1)$$

where $u^{1/2} = u^{2^{n-1}}$. Hence, f has algebraic degree $n-1$ (which is optimal for a balanced function).

Proof. Let $f(x) = \sum_{i=0}^{2^n-1} f_i\, x^i$ be the univariate representation of f. We have $f_0 = f(0) = 1$, $f_{2^n-1} = 0$ (since f has even Hamming weight and therefore algebraic degree at most $n-1$) and for every $i \in \{1, \cdots, 2^n - 2\}$:

$$f_i = \sum_{j=0}^{2^n-2} f(\alpha^j)\, \alpha^{-ij} = \sum_{j=0}^{2^{n-1}-2} \alpha^{-ij} = \frac{1 + \alpha^{-i(2^{n-1}-1)}}{1+\alpha^{-i}} =$$

$$\left(\frac{1+\alpha^{-i(2^n-2)}}{1+\alpha^{-2i}}\right)^{1/2} = \left(\frac{1+\alpha^{i}}{1+\alpha^{-2i}}\right)^{1/2} = \frac{\alpha^i}{(1+\alpha^i)^{1/2}}.$$

This proves Relation (1). We can see that $f_{2^n-2} \neq 0$ and therefore f has algebraic degree $n-1$. □

Remark. Computing the expression of Theorem 2 has high complexity. Actually, the complexity of computing $f(x)$ is comparable to computing the discrete log since the latter can be obtained by computing n outputs to f (with a dichotomic method).

Theorem 3. *Let f be defined as in Theorem 1, then:*

$$nl(f) \geq 2^{n-1} + \frac{2^{n/2+1}}{\pi} \ln\left(\frac{\pi}{4(2^n-1)}\right) - 1 \approx 2^{n-1} - \frac{2\ln 2}{\pi}\, n\, 2^{n/2}.$$

Proof.

$$\begin{aligned}
nl(f) &= 2^{n-1} - \frac{1}{2}\max_{\lambda\in\mathbb{F}_2^n} |W_f(\lambda)| \qquad (2)\\
&= 2^{n-1} - \frac{1}{2}\max_{0\neq\lambda\in\mathbb{F}_2^n} |W_f(\lambda)| \quad (\text{since } W_f(0)=0)\\
&= 2^{n-1} - \max_{\lambda\in\mathbb{F}_{2^n}^*} \left|\sum_{x\notin supp(f)} (-1)^{tr(\lambda x)}\right|\\
&\qquad (\text{since } (-1)^f = 2\,(f+1)-1 \text{ and } \sum_{x\in\mathbb{F}_2^n}(-1)^{\lambda\cdot x}=0)\\
&= 2^{n-1} - \max_{\lambda\in\mathbb{F}_{2^n}^*} |S_\lambda|
\end{aligned}$$

where

$$S_\lambda = \sum_{i=2^{n-1}-1}^{2^n-2} (-1)^{tr(\lambda\alpha^i)} \quad (\lambda\in\mathbb{F}_{2^n}^*) \qquad (3)$$

Let $\zeta = e^{\frac{2\pi\sqrt{-1}}{2^n-1}}$ be a primitive (2^n-1)-th root of 1 in the complex field $\mathbb{C}$, χ be the multiplicative character of $\mathbb{F}_{2^n}$ defined by $\chi(\alpha^j) = \zeta^j$ $(0 \leq j \leq 2^n-2)$ and $\chi(0) = 0$. We define the Gauss sum:

$$G(\chi^\mu) = \sum_{x\in\mathbb{F}_{2^n}^*} \chi^\mu(x)(-1)^{tr(x)} \quad (0 \leq \mu \leq 2^n-2)$$

It is well-known (see [30]) that $G(\chi^0) = -1$ and $|G(\chi^\mu)| = 2^{\frac{n}{2}}$ for $1 \leq \mu \leq 2^n-2$. By Fourier transformation we have

$$(-1)^{tr(\alpha^j)} = \frac{1}{2^n-1}\sum_{\mu=0}^{2^n-2} G(\chi^\mu)\overline{\chi}^\mu(\alpha^j) \quad (0 \leq j \leq 2^n-2)$$

Let $\lambda = \alpha^l$ $(0 \leq l \leq 2^n - 2)$ and $q = 2^n$. Then $\overline{\chi}^\mu(\lambda\alpha^i) = \zeta^{-\mu(l+i)}$ and by (3),

$$\begin{aligned}
S_\lambda &= \frac{1}{q-1} \sum_{\mu=0}^{q-2} G(\chi^\mu) \sum_{i=\frac{q}{2}-1}^{q-2} \overline{\chi}^\mu(\lambda\alpha^i) \\
&= \frac{1}{q-1} \sum_{\mu=0}^{q-2} G(\chi^\mu) \sum_{i=\frac{q}{2}-1}^{q-2} \zeta^{-\mu(l+i)} \\
&= \frac{1}{q-1} \left(\sum_{\mu=1}^{q-2} G(\chi^\mu) \zeta^{-\mu l} \, \frac{\zeta^{-\mu(\frac{q}{2}-1)} - 1}{1 - \zeta^{-\mu}} - \frac{q}{2} \right)
\end{aligned}$$

Therefore, for $\lambda \in \mathbb{F}_q^*$,

$$\begin{aligned}
|S_\lambda| &\leq \frac{1}{q-1} \left(\sum_{\mu=1}^{q-2} |G(\chi^\mu)| \cdot \frac{\left| \sin \frac{\pi\mu\left(\frac{q}{2}-1\right)}{q-1} \right|}{\sin \frac{\pi\mu}{q-1}} + \frac{q}{2} \right) \\
&\leq \frac{1}{q-1} \left(\sum_{\mu=1}^{q-2} |G(\chi^\mu)| \cdot \frac{1}{\sin \frac{\pi\mu}{q-1}} + \frac{q}{2} \right) \\
&= \frac{1}{q-1} \left(2\sqrt{q} \sum_{\mu=1}^{\frac{q}{2}-1} \left(\sin \frac{\pi\mu}{q-1} \right)^{-1} + \frac{q}{2} \right)
\end{aligned}$$

since $\sin(\pi - u) = \sin(u)$. By convexity of the function $\frac{1}{\sin t}$, we have, for $0 \leq \theta < t$ and $t + \theta \leq \pi$:

$$\frac{1}{\sin(t-\theta)} + \frac{1}{\sin(t+\theta)} \geq \frac{2}{\sin\ t}.$$

Then we deduce

$$\int_{t-\frac{\theta}{2}}^{t+\frac{\theta}{2}} \frac{du}{\sin\ u} \geq \frac{\theta}{\sin\ t}$$

and taking $\theta = \frac{\pi}{q-1}$:

$$\begin{aligned}
\sum_{\mu=1}^{\frac{q}{2}-1} \left(\sin \frac{\pi\mu}{q-1} \right)^{-1} &\leq \frac{q-1}{\pi} \sum_{\mu=1}^{\frac{q}{2}-1} \int_{\frac{\pi\mu}{q-1} - \frac{\pi}{2(q-1)}}^{\frac{\pi\mu}{q-1} + \frac{\pi}{2(q-1)}} \frac{du}{\sin\ u} \\
&= \frac{q-1}{\pi} \int_{\frac{\pi}{2(q-1)}}^{\frac{\pi}{2}} \frac{du}{\sin\ u}.
\end{aligned}$$

Set $t(x) = \tan(x/2)$. We have $\sin x = \frac{2t(x)}{1+t^2(x)}$ and therefore $\frac{1}{\sin x} = \frac{t'(x)}{t(x)}$. Hence a primitive of $1/\sin x$ equals $\ln(|\tan(x/2)|)$. This implies

$$\begin{aligned}
2^{n-1} - \max S_\lambda &\geq 2^{n-1} - \left(2^{n/2+1} \left[\frac{1}{\pi} \ln(\tan(x/2)) \right]_{\frac{\pi}{2(2^n-1)}}^{\frac{\pi}{2}} + 1 \right) \\
&= 2^{n-1} + \frac{2^{n/2+1}}{\pi} \ln\left(\tan\left(\frac{\pi}{4(2^n-1)} \right) \right) - 1 \\
&\geq 2^{n-1} + \frac{2^{n/2+1}}{\pi} \ln\left(\frac{\pi}{4(2^n-1)} \right) - 1 \\
&\left(\text{since } \tan x \geq x;\ \forall x \in \left[0; \frac{\pi}{2}\right[\right) \\
&\approx 2^{n-1} - \frac{2\ln 2}{\pi} n\, 2^{n/2}.
\end{aligned}$$

□

Remarks.
1. The lower bound given by Theorem 3 shows that the nonlinearity of our function f is provably considerably better (at least asymptotically) than those of the previously found functions. Moreover, we checked for small values of n that the exact value of $nl(f)$ is much better than what gives this lower bound and better than the nonlinearity of random functions and that it seems quite sufficient for resisting fast correlation attacks (for these small values of n, it behaves as $2^{n-1} - 2^{n/2}$). We give in Table 1 below, for n ranging from 6 to 11, the values of the nonlinearity of f compared with Lobanov's lower bound (when applied with optimal algebraic immunity), with the best nonlinearities of those functions with optimal AI known before the present paper, with the lower bound of Theorem 3, and with the upper bound $2^{n-1} - 2^{n/2-1}$.
2. We have seen that the computation of the value of $f(x)$ has high complexity. The power functions seen in [2, Table 1] may be better in practice for being used with a high number of variables, if their behavior against fast algebraic attacks can be proved good. Our construction might be useful with different designs, using less variables. It would be nice to find other infinite classes with the same qualities and which would be more easily computable.

n	6	7	8	9	10	11
Lobanov's bound	12	44	58	186	260	772
Best nl of fcts with optimal AI known before	22	48	98	196	400	798
The bound of Theorem 3	10	28	70	163	366	798
The values of the nl of fct f of Theorem 1	*24*	*54*	*112*	*232*	*478*	*980*
The upper bound $2^{n-1} - 2^{n/2-1}$	28	58	120	244	496	1001

Table 1. The values of the nonlinearity of f compared with Lobanov's lower bound and with the upper bound $2^{n-1} - 2^{n/2-1}$

5 Immunity against fast algebraic attacks

Computer investigations made using [2, Algorithm 2] suggest the following properties of the class of functions of Theorem 1:

- No nonzero function g of degree at most e and no function h of degree at most d exist such that $f * g = h$, when $(e, d) = (1, n - 2)$ for n odd and $(e, d) = (1, n - 3)$ for n even. This has been checked for $n \leq 12$ and we conjecture it for every n.
- For $e > 1$, pairs (g, h) of degrees (e, d) such that $e + d < n - 1$ were never observed. Precisely, the non-existence of such pairs could be checked exhaustively for $n \leq 9$ and $e < n/2$, for $n = 10$ and $e \leq 3$ and for $n = 11$ and $e \leq 2$. This suggests that this class of functions, even if not always optimal against fast algebraic attacks, has a very good behavior.

The instance with $n = 9$ turns out to be optimal. To the best of our knowledge, this is the first time where a function with optimal immunity against FAA's can be observed.

Conclusion

The functions of Theorem 1 seem to gather all the properties needed for allowing the stream ciphers using them as filtering functions to resist all the main attacks (the Berlekamp-Massey and Rønjom-Helleseth attacks, fast correlation attacks, standard and fast algebraic attacks). They are the only functions of this kind found so far.

Acknowledgement

The authors thank Sihem Mesnager for her help in computing the nonlinearities of the function and for a nice improvement of a first version of our lower bound on the nonlinearity. We thank also Simon Fischer for his precious help in computing the immunities to fast algebraic attacks of the function and Xiangyong Zeng for a nice observation.

References

1. Armknecht, F.: Improving fast algebraic attacks, Fast Software Encryption, Lecture Notes in Computer Science, vol. 3017 pp. 65-82. Springer, Verlag (2004).
2. Armknecht, F., Carlet, C., Gaborit, P., Künzli, S., Meier,W. and Ruatta, O.: 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.
3. Braeken, A., Preneel, B.: On the algebraic immunity of symmetric Boolean functions, Progress in Cryptology–Indocrypt 2005, Lecture Notes in Computer Science, vol. 3797 pp. 35-48. Springer, Verlag (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.

4. Braeken, A., Lano, J., Mentens, N., Preneel, B. and Verbauwhede, I.: SFINKS: A Synchronous stream cipher for restricted hardware environments. SKEW - Symmetric Key Encryption Workshop, 2005.
5. Canteaut, A.: Open problems related to algebraic attacks on stream ciphers, Coding and Cryptography, Lecture Notes in Computer Science, vol. 3969 pp. 120-134. Springer, Verlag (2006).
6. Canteaut, A., Trabbia, M.: Improved fast correlation attacks using parity-check equations of weight 4 and 5, Advances in Cryptology–EUROCRYPT 2000, Lecture Notes in Computer Science, vol. 1807 pp. 573-588. Springer (2000).
7. Carlet, C.: A method of construction of balanced functions with optimum algebraic immunity. Cryptology ePrint Archive, http://eprint.iacr.org/2006/149. To appear in the proceedings of the Wuyi Workshop on Coding and Cryptology, published by World Scientific Publishing Co. in its series of Coding and Cryptology.
8. Carlet, C.: On the higher order nonlinearities of algebraic immune functions, Advances in Cryptology–CRYPTO 2006, Lecture Notes in Computer Science, vol. 4117 pp. 584-601. Springer (2006).
9. Carlet, C. 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
10. Carlet, C., Dalai, D.K., Gupta, K.C., Maitra, S.: Algebraic immunity for cryptographically significant Boolean functions: analysis and construction. IEEE Trans. Inform. Theory 52(7), 3105-3121 (2006).
11. Carlet, C., Zeng, X. and Li, C.: Further properties of several classes of Boolean functions with optimum algebraic immunity. Preprint, IACR e-print archive 2007/370.
12. Cho, J.Y., Pieprzyk, J.: Algebraic attacks on SOBER-t32 and SOBER-128, Fast Software Encryption, Lecture Notes in Computer Science, vol. 3017 pp. 49-64. Springer, Verlag (2004).
13. Courtois, N.: Fast algebraic attacks on stream ciphers with linear feedback, Advances in Cryptology–CRYPTO 2003, Lecture Notes in Computer Science, vol. 2729 pp. 176-194. Springer, Verlag (2003).
14. Courtois, N.: Cryptanalysis of SFINKS. In *ICISC 2005*. Also available at Cryptology ePrint Archive, http://eprint.iacr.org/, Report 2005/243, 2005.
15. Courtois, N., Meier, W.: Algebraic attacks on stream ciphers with linear feedback, Advances in Cryptology–Eurocrypt 2003, Lecture Notes in Computer Science, vol. 2656 pp. 345-359. Springer, Verlag (2003).
16. Courtois, N., Pieprzyk, J.: Cryptanalysis of block ciphers with overdefined systems of equations, Advances in Cryptology–ASIACRYPT 2002, Lecture Notes in Computer Science, vol. 2501 pp. 267-287. Springer, Verlag (2002).
17. Dalai, D.K., Gupta, K.C., Maitra, S.: Cryptographically significant Boolean functions: construction and analysis in terms of algebraic immunity, Fast Software Encryption, Lecture Notes in Computer Science, vol. 3557 pp. 98-111. Springer, Verlag (2005).
18. Dalai, D.K., Maitra, S., Sarkar, S.: Basic theory in construction of Boolean functions with maximum possible annihilator immunity. Des. Codes Cryptogr. 40(1), 41-58 (2006).

19. Didier, F.: 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.
20. Didier, F.: Using Wiedemann's algorithm to compute the immunity against algebraic and fast algebraic attacks. Proceedings of Indocrypt 2006, LNCS 4329, pp. 236-250.
21. Ding, C., Xiao, G., Shan, W.: The Stability Theory of Stream Ciphers, Lecture Notes in Computer Science, vol. 561. Springer, Verlag (1991).
22. Feng, K., Liao, Q. and Yang, J.: Maximal values of generalized algebraic immunity. To appear in Designs, Codes and Cryptography.
23. Fischer, S. and Meier, W.: Algebraic Immunity of S-boxes and Augmented Functions. Proceedings of Fast Software Encryption 2007. Lecture Notes in Comput. Sci. 4593, pp. 366-381.
24. Hawkes, P. and Rose, G.: Rewriting Variables: The Complexity of Fast Algebraic Attacks on Stream Ciphers. In M. K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004, LNCS 3152*, pp. 390–406. Springer Verlag, 2004.
25. Lee, D.H., Kim, J., Hong, J., Han, J.W., Moon, D.: Algebraic attacks on summation generators, Fast Software Encryption, Lecture Notes in Computer Science, vol. 3017 pp. 34-48. Springer, Verlag (2004).
26. Li, N., Qi, W.F.: Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity, Advances in Cryptology–ASIACRYPT 2006, Lecture Notes in Computer Science, vol. 4284 pp 84-98. Springer (2006).
27. Li, N. and Qi, W. F. "Symmetric Boolean functions depending on an odd number of variables with maximum algebraic immunity," *IEEE Transactions on Information theory*, vol. 52, no. 5, pp. 2271-2273, 2006.
28. Li, N. and Qi, W.-Q. Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity. *Proceedings of Asiacrypt 2006*, Lecture Notes in Computer Science 4284, pp. 84-98, 2006.
29. Li, N., Qu, L., Qi, W.-F., Feng, G., Li, C. and Xie, D.. On the construction of Boolean functions with optimal algebraic immunity. *IEEE Transactions on Information Theory*, vol. 54, No. 3, pp. 1330-1334, 2008.
30. Lidl, R. and Niederreiter, H. *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, Reading, Massachussetts (1983)
31. Lobanov, M.: Tight bound between nonlinearity and algebraic immunity. Paper 2005/441 in http://eprint.iacr.org/
32. MacWilliams, F.J., Sloane, N.J.: The Theory of Error-Correcting Codes. Amsterdam, The Netherlands: North-Holland (1977).
33. Meier, W., Pasalic, E., Carlet, C.: Algebraic attacks and decomposition of Boolean functions, Advances in Cryptology–EUROCRYPT 2004, Lecture Notes in Computer Science, vol. 3027 pp. 474-491. Springer, Verlag (2004).
34. Meier, W. and Staffelbach, O. Fast correlation attacks on stream ciphers. *Advances in Cryptology, EUROCRYPT'88, Lecture Notes in Computer Science* 330, pp. 301-314, 1988.
35. Nawaz,Y., Gong, G., and Gupta, K. Upper Bounds on Algebraic Immunity of Power Functions. Proceeding of Fast Software Encryption 2006, Lecture Notes in Computer Science 4047, pp. 375-389.
36. L. Qu, C. Li, and K. Feng, "Note on symmetric Boolean functions with maximum algebraic immunity in odd number of variables," *IEEE Transactions on Information theory*, vol. 53, no. 8, pp. 2908-2910, Aug. 2007.
37. Rodier, F.: Asymptotic nonlinearity of Boolean functions. *Designs, Codes and Cryptography*, no 40:1 2006, pp 59-70.

38. Rønjom, S., Helleseth, T.: A new attack on the filter generator. IEEE Trans. Inform. Theory 53(5) 1752-1758 (2007).
39. Shannon, C. E. Communication theory of secrecy systems. *Bell system technical journal*, 28, pp. 656-715, 1949.