Construction of Balanced Functions without Extending Their Number of Variables

Aïssa. Belmeguenaï, Noureddine. Doghmane, and Khaled. Mansouri

***Abstract*— In this work, we first give a general method which can get a large class of balanced Boolean functions with reasonably high nonlinearity, larger than that obtained by Lobanov. Then, we study the secondary construction of Boolean functions without extending their number of variables, introduced recently by Carlet. This gives interesting cryptographic properties in terms of balancedness, nonlinearity and algebraic immunity. We conclude the paper by proving that the algebraic immunity of the constructed functions is better than among of the starting functions.**

***Index Terms*—Algebraic immunity, Boolean function, nonlinearity, resiliency.**

I. Introduction

Boolean functions, when used in stream cipher (combiner model or filter model), are required to have good cryptographic properties. Some of the important properties are balancedness, a high algebraic degree, a high non linearity and in the case of the combiner model, a reasonably high correlation immunity. These properties ensure that the functions are resistant against correlation attacks [1] and linear cryptanalysis [2].

Recently, algebraic attacks [8], [9], [10], [11], [12], [13], [14] have been observed that a Boolean function f used as a cryptographic primitive, must have a high algebraic immunity. But not sufficient property for Boolean function used in stream ciphers. It is an important topic to construct Boolean functions with optimum algebraic immunity. But these functions must also satisfy the other criteria recalled above for being likely to be used in stream ciphers.

Non linearity is the most important property among those cryptographic properties on Boolean function used in stream ciphers. In [15], Lobanov proved that $Nf \geq 2\sum_{i=0}^{AI(f)-2}\binom{n-1}{i}$ for every n-variable Boolean functions. Moreover, by constructing a family of Boolean function achieving the equality $Nf = 2\sum_{i=0}^{AI(f)-2}\binom{n-1}{i}$, he proved that this lower bound cannot be improved further. The result of [15] and theorem 2 of [16] give a new reason why one should not use functions f with low nonlinearity, since in that case $AI_n(f)$ would be low. However, they do not ensure that if f has high algebraic immunity (for instance an optimum one $AI_n(f) = \left[\frac{n}{2}\right]$) then its nonlinearity will be high. Indeed, the result of [15] implies then that f has nonlinearity at least $2\sum_{i=0}^{\left[\frac{n}{2}\right]-2}\binom{n-1}{i}$, that is, $2^{n-1} - \binom{n-1}{\frac{n-1}{2}}$ if n is odd and $2^{n-1} - \binom{n-1}{\frac{n}{2}-1} - \binom{n-1}{\frac{n}{2}}$ if n is even.

The object of this work is double. In the first time, it is a question of studying the non linearity and the algebraic immunity of a n-variable function. General method which can get a large class of Boolean functions are considered. All these functions have algebraic immunity at least k, where $k \prec\prec \left[\frac{n}{2}\right]$ is any integer. We study their Walsh transforms. Furthermore, by choosing suitable parameters, we show that some infinite classes of balanced functions can have non linearity significantly larger than $2^{n-1} - \binom{n-1}{\frac{n}{2}-1} - \binom{n-1}{\frac{n}{2}}$. Thus, we use Carlet's construction [17] to construct Boolean functions with better cryptographic properties, which gives the guidance for the design of balanced Boolean functions to resist algebraic attack, and helps to design good cryptographic primitives of cryptosystems.

Manuscript received May, 2008.

A. Belmeguenaï is with the Laboratory of applied automatic, Department of electronics, Faculty of Science and Engineering August 20- 55 Skikda University LP 26 El-hadeik Avenue, Algeria (e-mail: belmeguenaiaissa@yahoo.fr).

N. Doghmane is with the Department of electronics, Faculty of Science and Engineering Badji Mokhtar University - Annaba LP 12, Algeria (e-mail: ndoghmane@univ-annaba.org).

K. Mansouri is with the Department of electronics, Faculty of Science and Engineering Badji Mokhtar University - Annaba LP 12, Algeria (e-mail: mansouri.khaled@ voila.fr).

The paper is organized as follows. Section 2 gives preliminaries. In section 3, we give a general methode to get a large numerous Boolean functions with algebraic immunity at $k \prec\prec \left[\frac{n}{2}\right]$ and have important nonlinearity. In section 4 we deduce balanced functions with nonlinearity, larger than that obtained by Lobanov. In section 5, we use construction introduced by Carlet [17] to derive construction of balanced functions with reasonably high nonlinearity and we show that, the algebraic immunity of the constructed functions is better than among of the starting functions. Section 6 concludes the study.

II. PRELIMINARIES

A Boolean function on n-variable may be viewed as a mapping from F_2^n in to F_2. The set of all n-variable Boolean functions is denoted by B_n. By $\oplus$ we denote sum modulo 2. The Hamming weight $wt(f)$ of a Boolean function f on F_2^n is the size of its *support* $\{x \in F_2^n;\, f(x)=1\}$. The Hamming distance $d(f,g)$ between two Boolean functions f and g is the Hamming weight of their difference $f \oplus g$, $d(f,g)=wt(f \oplus g)$. An n-variable Boolean function f has unique algebraic normal form (A.N.F): $f(x_1,...,x_n)=a_0+\sum_{i=0}^{n} a_i x_i +$ $\sum_{1\le i\prec j\le n} a_{ij}x_i x_j + ... + a_{12...n}x_1x_2...x_n$.

Where the coefficients a_0, a_i, a_{ij} ,.., $a_{12...n}$ belong to F_2.

The algebraic degree of Boolean function f, denoted by $d°(f)$, is defined as the number of variables in the highest order term with nonzero coefficient. If algebraic degree of f is smaller than or equal to one then f is called affine function. An affine function with a constant term equal to zero is called a linear function. Many properties of Boolean functions can be described by the Walsh-Hadamard transform. Let f be Boolean function on F_2^n. Then the Walsh-Hadamard transform of f is defined as:

$$\forall u \in F_2^n, Wf(u)=\sum_{x\in F_2^n}(-1)^{f(x)}(-1)^{u.x}. \qquad (1)$$

Where $x.u = x_1.u_1 + ... + x_n.u_n$ denotes the usual scalar product of vectors u and x.

The nonlinearity Nf of a n-variable function f is the minimum distance from the set of all n-variable affine functions, it equal to:

$$Nf = 2^{n-1}-\frac{1}{2}\max_{u\in F_2^n}|Wf(u)|. \qquad (2)$$

Boolean functions used in cipher system must have high nonlinearity to prevent correlation and linear attacks [18], [19], [20], [1]. A Boolean function f on F_2^n is balanced if $wt(f)=wt(f\oplus 1)$. In other words, f is balanced if and only if $wt(f)=2^{n-1}$. Correlation immune functions and resilient functions are two important classes of Boolean functions. Xiao and Massey [21] provided a spectral characterization of correlation immune and t-*th* order resilient functions. A function f is t-*th* order correlation immune if and only if its Walsh transform satisfies: $Wf(u)=0$, for $1\le wt(u)\le t$, where $wt(u)$ denotes the Hamming weight of *u*, and f is t-resilient if moreover $Wf(0)=0$. $\forall u\in F_2^n$, $0\le wt(u)\le t$.

The algebraic immunity of a Boolean function f is the smaller degree of non null function g such that $f*g=0$ or $(1\oplus f)*g=0$. Otherwise, the minimum value of d such that f or $1\oplus f$ admits an annihilator of degree d. We denoted by $AI_n(f)$ the algebraic immunity of a Boolean function f. It is shown in [13] and [10] that algebraic immunity of a Boolean function f is at most $\left[\frac{n}{2}\right]$.

Notation: $x\oplus y=(x_1\oplus y_1, x_2\oplus y_2,..., x_n\oplus y_n)$, where $x=(x_1,x_2,...,x_n)$, $y=(y_1,y_2,...,y_n)\in F_2^n$; $1\oplus x=(1\oplus x_1, 1\oplus x_2,...,1\oplus x_n)$ is the bitwise complement of $x=(x_1,x_2,...,x_n)$.

It is known that for a fixed every vector $u\in F_2^n$ such that $wt(u)=m$, we have

$$\sum_{x\in F_2^n / wt(x)=i}(-1)^{u\cdot x}=\sum_{j=0}^{i}(-1)^j\binom{m}{j}\binom{n-m}{i-j}=K_i(m,n). \qquad (3)$$

Where $K_i(x,n)$ is the Krawtchouk polynomial [22].

Proposition 1:

1) $K_0(m,n)=1, K_1(m,n)=n-2m$;
2) $(i+1)K_{i+1}(m,n)=(n-2m)K_i(m,n)-$ $(n-i+1)k_{i-1}(m,n)$;
3) $(n-m)K_i(m+1,n)=(n-2i)K_i(m,n)-$ $mk_i(m-1,n)$;
4) $K_i(m,n)=(-1)^i K_{n-i}(n-m,n)$.

The following lemmas will be used to prove the results in the paper.

Lemma 1: [23] For $1\le i\le \left[\frac{n-1}{2}\right]$ and $1\le m\le n-1, |K_i(m,n)|\le K_i(1,n)$.

Lemma 2: For every two integers n and $m \geq 0$: we have

1) $\begin{pmatrix} n \\ 0 \end{pmatrix} = 1$;

2) $\begin{pmatrix} n \\ n \end{pmatrix} = 1$;

3) $\begin{pmatrix} n \\ m \end{pmatrix} = 0$, for every $m \succ n$;

4) $2^n = \begin{pmatrix} n \\ 0 \end{pmatrix} + \begin{pmatrix} n \\ 1 \end{pmatrix} + \ldots + \begin{pmatrix} n \\ n-1 \end{pmatrix} + \begin{pmatrix} n \\ n \end{pmatrix}$;

5) $\begin{pmatrix} n+1 \\ m+1 \end{pmatrix} = \begin{pmatrix} n \\ m+1 \end{pmatrix} + \begin{pmatrix} n \\ m \end{pmatrix}$, for every $n \geq 0$ and $m \geq 0$.

Lemma 3: [17] Let f_1, f_2 and f_3 be three Boolean functions on F_2^n. We denoted by α_1 the Boolean function equal to $f_1 \oplus f_2 \oplus f_3$ and by α_2 the Boolean function equal to $f_1 f_2 \oplus f_1 f_3 \oplus f_2 f_3$. Then we have $f_1 + f_2 + f_3 = \alpha_1 + 2\alpha_2$. This implies

$$Wf_1 + Wf_2 + Wf_3 = W\alpha_1 + 2W\alpha_2. \qquad (4)$$

Lemma 4: Let k, n be any two positive integers such that $k \prec\prec \left[\frac{n}{2}\right]$. For $1 \leq i \leq k-1$,

$$K_i(1,n) \leq K_i(0,n). \qquad (5)$$

Proof: Note that $K_i(0,n) = \begin{pmatrix} n \\ i \end{pmatrix}$, $K_i(1,n) = \begin{pmatrix} n-1 \\ i \end{pmatrix} - \begin{pmatrix} n-1 \\ i-1 \end{pmatrix}$. For $i = 0$, we have $K_0(0,n) = K_0(1,n) = 1$. For $i = 1$, $K_1(0,n) = n$ and $K_1(1,n) = n-2$.

Suppose that $K_i(1,n) \leq K_i(0,n)$ true for $1 \leq i \leq k-2$. $K_{k-1}(0,n) = \begin{pmatrix} n \\ k-1 \end{pmatrix}$. By lemma 2 (Item 5), we have

$$K_{k-1}(0,n) = \begin{pmatrix} n \\ k-1 \end{pmatrix} = \begin{pmatrix} n-1 \\ k-1 \end{pmatrix} + \begin{pmatrix} n-1 \\ k-2 \end{pmatrix} \geq$$

$$\begin{pmatrix} n-1 \\ k-1 \end{pmatrix} - \begin{pmatrix} n-1 \\ k-2 \end{pmatrix} + \begin{pmatrix} n-1 \\ k-2 \end{pmatrix} - \begin{pmatrix} n-1 \\ k-3 \end{pmatrix}$$

$$= \begin{pmatrix} n-1 \\ k-1 \end{pmatrix} - \begin{pmatrix} n-1 \\ k-3 \end{pmatrix} \geq \begin{pmatrix} n-1 \\ k-1 \end{pmatrix} - \begin{pmatrix} n-1 \\ k-2 \end{pmatrix} = K_{k-1}(1,n).$$

Hence, the inequalities (5) true for $1 \leq i \leq k-1$.

III. CONSTRUCTION OF BOOLEAN FUNCTIONS

The idea of our construction comes from the following.

Construction 1: Let k, n be any two positive integers such that $k \prec\prec \left[\frac{n}{2}\right]$. Let g and f be two Booleans functions of B_n with the following conditions.

1) g equal zero for $wt(x) \prec k$ and $wt(x) \succ n-k$,

2) $$f(x) = \begin{cases} 0 & if \quad wt(x) \prec k \\ g(x) & if \quad k \leq wt(x) \leq n-k \\ 1 & if \quad wt(x) \succ n-k \end{cases}$$

Then we have the following important result.

Lemma 5: Let $f \in B_n$ be a function as described in Construction 1. Then $AI_n(f) \geq k$.

Proof: We first show that the function $1 \oplus f$ has not a nonzero annihilator of degree less than k.

Write the possible annihilator h of the function $1 \oplus f$ of degree at most $k-1$ by means of indeterminate coefficients:

$$h = a_0 + \sum_{i=0}^{n} a_i x_i + \sum_{1 \leq i \prec j \leq n} a_{ij} x_i x_j + \ldots + a_{12\ldots k-1} x_1 x_2 \ldots x_{k-1}$$

The function h is the annihilator of $1 \oplus f$ if only if $1 \oplus f(x) = 1$ follows $h(x) = 0$. We obtain the system of homogeneous linear equations on the coefficients of the function h:

$h(x) = 0$

for all vectors x of Hamming weight less than or equals $k-1$. Since $h(0,\ldots,0) = 0$, we have $a_0 = 0$. Since $h(x) = 0$ if $wt(x) = 1$, we have $a_i = a_0 = 0$. Applying the induction on the weight of vectors we, obtain that all coefficients of h are zeros, hence, $h \equiv 0$. i.e $1 \oplus f$ has not a nonzero annihilator of degree less than k.

Now, we prove that f has not annihilator of degree less than k. Suppose f has an annihilator H of degree less than k. That is, $f(x) * H(x) = 0$, i.e., $H(x) = 0$ when $f(x) = 1$. Note that, if $g(x) = 1$, we have $H(x) = 0$ for every vector $x \in F_2^n$ such that $wt(x) \geq k$. Define H_1 as $H_1(x) = H(1 \oplus x)$, i.e., $H(x) = H_1(1 \oplus x)$. This gives $\deg(H_1) = \deg(H) \prec k$. Hence, we have $(1 \oplus f(x)) * H_1(1 \oplus x) = 0$. So, $1 \oplus f$ has an annihilator of degree less than k, which is a contradiction.

If $g(x)=0$, then $H(x)=0$ for every vector $x\in F_2^n$ such that $wt(x)\succ n-k$. Define H_2 as $H_2(x)=H(1\oplus x)$, i.e., $H(x)=H_2(1\oplus x)$. This gives, $\deg(H_2)=\deg(H)\prec k$. Hence, we have $(1\oplus f(x))*H_2(1\oplus x)=0$. So, $1\oplus f$ has an annihilator of degree less than k, which is a contradiction.

Lemma 6: Let $f\in B_n$ be a function as described in Construction 1. Then

$$\sum_{i=0}^{k-1}\binom{n}{i}\le wt(f)\le\sum_{i=0}^{n-k}\binom{n}{i}. \qquad (6)$$

Lemma 7: Let $f\in B_n$ be a function as described in Construction 1. Then the value of the Walsh transform of f at every $u\in F_2^n$ equals:

$$Wf(u)=\begin{cases} Wg(u)-2\displaystyle\sum_{x\in F_2^n\,/\,wt(x)\prec k}(-1)^{u\cdot x} & for\ \ even\ \ wt(u)\\ Wg(u)+2\displaystyle\sum_{x\in F_2^n\,/\,wt(x)\prec k}(-1)^{u\cdot x} & for\ \ odd\ \ wt(u)\end{cases}$$

(7)

Proof: For every vector $u\in F_2^n$, we have

$$Wf(u)=\sum_{x\in F_2^n}(-1)^{f(x)\oplus u\cdot x}$$

$$=\sum_{x\in F_2^n\,/\,wt(x)\prec k}(-1)^{0\oplus u\cdot x}+\sum_{x\in F_2^n\,/\,k\le wt(x)\le n-k}(-1)^{g(x)\oplus u\cdot x}+\sum_{x\in F_2^n\,/\,wt(x)\succ n-k}(-1)^{1\oplus u.x}$$

$$=\sum_{x\in F_2^n\,/\,wt(x)\prec k}(-1)^{0\oplus u\cdot x}+\sum_{x\in F_2^n}(-1)^{g(x)\oplus u\cdot x}$$

$$-\sum_{x\in F_2^n\,/\,wt(x)\prec k}(-1)^{0\oplus u\cdot x}-\sum_{x\in F_2^n\,/\,wt(x)\succ n-k}(-1)^{0\oplus u\cdot x}+\sum_{x\in F_2^n\,/\,wt(u)\succ n-k}(-1)^{1\oplus u\cdot x}$$

$$=\sum_{x\in F_2^n}(-1)^{g(x)\oplus u\cdot x}-\sum_{x\in F_2^n\,/\,wt(x)\prec k}(-1)^{u\oplus u\cdot x}+\sum_{x\in F_2^n\,/\,wt(x)\prec k}(-1)^{1\oplus u\oplus u\cdot x}$$

$$=\begin{cases} Wg(u)-2\displaystyle\sum_{x\in F_2^n\,/\,wt(x)\prec k}(-1)^{u\cdot x} & for\ \ even\ \ wt(u)\\ Wg(u)+2\displaystyle\sum_{x\in F_2^n\,/\,wt(x)\prec k}(-1)^{u\cdot x} & for\ \ odd\ \ wt(u)\end{cases}.$$

IV. Deduced BALANCED FUNCTIONS

We use the result of Lemma 7 to study the nonlinearity and balancedness for a class of functions based on Construction 1.

Theorem 1: Let k,n be any two positive integers such that $k\prec\prec\left[\frac{n}{2}\right]$. Let $f\in B_n$ be a function as defined by Construction 1. Then, if $Wt(g)=\frac{1}{2}\sum_{i=k}^{n-k}\binom{n}{i}$, then f is balanced. Moreover

$$Nf\ \ge Ng-\binom{n}{k-1}. \qquad (8)$$

Proof: Relation (7) and the fact that for every vector $u=0$ implies relation

$$Wf(0)=Wg(0)-2\sum_{i=0}^{k-1}\binom{n}{i}\ =2^n-2wt(g)-2\sum_{i=0}^{k-1}\binom{n}{i}$$

$=\sum_{i=k}^{n-k}\binom{n}{i}-2wt(g)$ Imply that $Wf(0)=0$ if only if $Wt(g)=\frac{1}{2}\sum_{i=k}^{n-k}\binom{n}{i}$: f *is* balanced.

Relation (3), relation (7) and the fact that for every vector $u\in F_2^n$ implies relation

$$\max_{u\in F_2^n}|Wf(u)|\le\max_{u\in F_2^n}|Wg(u)|+2\max_{u\in F_2^n}|K_{k-1}(wt(u),n)|. \qquad (9)$$

From lemma 1, one has

$$\max_{u\in F_2^n}|K_{k-1}(wt(u),n)|=\max(|K_{k-1}(1,n)|,|K_{k-1}(n,n)|)\quad .$$

From proposition 1 (Item 4), we have $K_i(m,n)=(-1)^iK_i(n-m,n)$, this give $K_{k-1}(n,n)=(-1)^{k-1}K_{k-1}(0,n)$, we have

$$\max_{u\in F_2^n}|K_{k-1}(wt(u),n)|=\max(|K_{k-1}(1,n)|,|K_{k-1}(0,n)|). \qquad (10)$$

By using relations (9) and (10), we have

$$\max_{u\in F_2^n}|Wf(u)|\le\max_{u\in F_2^n}|Wg(u)|+2\max\left(\max_{u\in F_2^n}|K_{k-1}(1,n)|,\max_{u\in F_2^n}|K_{k-1}(0,n)|\right)$$

and relation (5) implies the relation

$$\max_{u\in F_2^n}|Wf(u)|\le\max_{u\in F_2^n}|Wg(u)|+2\binom{n}{k-1}. \qquad (11)$$

Using relation (2), we deduce relation (8).

In the following corollary 1, we will show that the nonlinearity of function $f\in B_n$ as described in construction 1 can achieve the best possible nonlinearity, larger than obtained by Lobanov [15].

Corollary 1: Let n be even integer. Let $f\in B_n$ be Boolean function as described in construction 1. If g is bent and if $Wt(g)=\frac{1}{2}\sum_{i=k}^{n-k}\binom{n}{i}$. Then f is balanced function has nonlinearity at least $2^{n-1}-2^{\frac{n}{2}-1}-\binom{n}{k-1}$.

Note that in [15] it was constructed the balanced function f of even number n of variables with the maximum possible algebraic immunity $k = \left[\frac{n}{2}\right]$ and nonlinearity $2^{n-1} - \binom{n-1}{\frac{n}{2}-1} - \binom{n-1}{\frac{n}{2}}$. Our corollary1 proved that it is possible to design class of balanced functions with algebraic immunity $k \prec\prec \left[\frac{n}{2}\right]$ achieve nonlinearity at least $2^{n-1} - 2^{\frac{n}{2}-1} - \binom{n}{k-1}$, significantly larger than $2^{n-1} - \binom{n-1}{\frac{n}{2}-1} - \binom{n-1}{\frac{n}{2}}$. We give in table 1, for $n \geq 18$ and even, the few values on Nf of bound of corollary 1 and in table 2 we give the values of nonlinearity $2^{n-1} - \binom{n-1}{\frac{n}{2}-1} - \binom{n-1}{\frac{n}{2}} \approx 2^{n-1} - \frac{2^{n+1}}{\sqrt{2\pi n}}$ obtained in [15].

The bound of corollary 1 is better than the bound of [15] for every $n \geq 22$ even and for every value of $2 \leq k \leq 5$ (see table 1 and table 2).

Remark 1: The family of functions described by construction 1 is very general. It is easy to see that construction 1 makes possible to define a large class of Boolean functions with algebraic immunity at least $k \prec\prec \left[\frac{n}{2}\right]$ and an important nonlinearity. For example if $k = \left[\frac{n}{2}\right]$, we get class of Boolean functions f of n -variable achieving the nonlinearity $Nf = 2\sum_{i=0}^{\left[\frac{n}{2}\right]-2} \binom{n-1}{i}$ giving in [15]. Thus, by choosing suitable parameters, for even n, bent function g and $Wt(g) = \frac{1}{2}\sum_{i=k}^{n-k}\binom{n}{i}$, we show that some infinite classes of balanced functions can have non linearity significantly larger than $2^{n-1} - \binom{n-1}{\frac{n}{2}-1} - \binom{n-1}{\frac{n}{2}}$. For instance, for bent function g, $k = 2$ and $Wt(g) = \frac{1}{2}\sum_{i=k}^{n-k}\binom{n}{i}$. Then, the function f of even number n of variables is balanced has nonlinearity at least $2^{n-1} - 2^{\frac{n}{2}-1} - n \approx 2^{n-1} - o\left(2^{\frac{n}{2}-1}\right)$, best possible non linearity.

Lobanov’s bound does not guarantee that having a high resistance to the correlation attacks. Indeed, such resistance needs a high nonlinearity, from table 2, we see Lobanov’s bound $2^{n-1} - \binom{n-1}{\frac{n}{2}-1} - \binom{n-1}{\frac{n}{2}} \approx 2^{n-1} - \frac{2^{n+1}}{\sqrt{2\pi n}}$ is not quite satisfactory. But the bound of corollary 1, show that having a reasonable high algebraic immunity and important nonlinearity. Moreover, for every $n \geq 28$ even and for every value of $k \geq 7$, the algebraic immunity $k \geq 7$ is a strong property, not only with respect to the resistance to algebraic attacks, but also with respect to the resistance to higher order attacks.

V. CONSTRUCTION BALANCED FUNCTIONS WITHEOUT EXTENDING THEIR NUMBER OF VARIABLES

We use now the results of Lemma 3 and lemma 7 and the construction [17] to construct Boolean functions with better cryptographic properties, which gives the guidance for the design of balanced Boolean functions to resist algebraic attack, and helps to design good cryptographic primitives of cryptosystems.

Theorem 2: Let k,n be any two positive integers such that $k \prec\prec \left[\frac{n}{2}\right]$. Let g_1, g_2 and g_3 be three Boolean functions on F_2^n equals zero for $wt(x) \prec k$ and $wt(x) \succ n-k$. We denoted by σ_1 the Boolean function equal to $g_1 \oplus g_2 \oplus g_3$.

Let $$f_1(x) = \begin{cases} 0 \quad if \quad wt(x) \prec k \\ g_1(x) \quad if \quad k \leq wt(x) \leq n-k \\ 1 \quad if \quad wt(x) \succ n-k \end{cases},$$

$$f_2(x) = \begin{cases} 0 \quad if \quad wt(x) \prec k \\ g_2(x) \quad if \quad k \leq wt(x) \leq n-k \\ 1 \quad if \quad wt(x) \succ n-k \end{cases}$$ and

$$f_3(x)=\begin{cases}0 \quad if \quad wt(x)\prec k\\ g_3(x) \quad if \quad k\le wt(x)\le n-k\\ 1 \quad if \quad wt(x)\succ n-k\end{cases}$$ three balanced functions. Then the function $\alpha_1 = f_1 \oplus f_2 \oplus f_3$ is balanced if only if the function $\alpha_2 = f_1 f_2 \oplus f_1 f_3 \oplus f_2 f_3$ is balanced. Moreover

$$N\alpha_2 \ge \frac{1}{2}\left(\sum_{i=1}^{3} Ng_i + N\sigma_1\right) - 2\binom{n}{k-1} - 2^{n-1} \qquad (12)$$

if the Walsh support of f_1, f_2 and f_3 are pairwise disjoint, then $N\alpha_2 \ge \frac{1}{2}\left(\min_{1\le i\le 3} Ng_i + N\sigma_1\right) - \binom{n}{k-1}$. (13)

Proof: Relation (4) and the fact that for every vector $u = 0$, we have $Wf_i(0) = 0$, for $i = 1,2,3$ imply that $W\alpha_1(0) = 0$ if only if $W\alpha_2 = 0$. Relations (4) and the fact that for every vector $u \in F_2^n$ implies relation

$$\max_{u\in F_2^n}\left|W\alpha_2(u)\right| \le \frac{1}{2}\left(\sum_{i=1}^{3}\left(\max_{u\in F_2^n}\left|Wf_i(u)\right|\right) + \max_{u\in F_2^n}\left|W\alpha_1(u)\right|\right)$$

and relation (11) implies

$$\max_{u\in F_2^n}\left|W\alpha_2(u)\right| \le \frac{1}{2}\left(\sum_{i=1}^{3}\left(\max_{u\in F_2^n}\left|Wg_i(u)\right|\right) + 6\binom{n}{k-1} + \max_{u\in F_2^n}\left|W\sigma_1(u)\right| + 2\binom{n}{k-1}\right)$$

, using relation (2), we have

$$2^n - 2N\alpha_2 \le \frac{1}{2}\left(4\times 2^n - 2\sum_{i=1}^{3} Ng_i - 2N\sigma_1 + 8\binom{n}{k-1}\right)$$

or equivalent relation (12).

If at most one value $Wf_i(u) = 0$, for $i = 1,2,3$ is nonzero, then relation (4) implies the relation

$$\max_{u\in F_2^n}\left|W\alpha_2(u)\right| \le \frac{1}{2}\left(\max_{1\le i\le 3}\left(\max_{u\in F_2^n}\left|Wf_i(u)\right|\right) + \max_{u\in F_2^n}\left|W\alpha_1(u)\right|\right)$$

, relation (11) implies

$$\max_{u\in F_2^n}\left|W\alpha_2(u)\right| \le \frac{1}{2}\left(\max_{1\le i\le 3}\left(\max_{u\in F_2^n}\left|Wg_i(u)\right|\right) + 2\binom{n}{k-1} + \max_{u\in F_2^n}\left|W\sigma_1(u)\right| + 2\binom{n}{k-1}\right)$$

and relation (2) implies then relation (13).

Now, we study an algebraic immunity of Boolean functions α_2. We will prove the function α_2 in theorem 2 can have better algebraic immunity than f_1, f_2, f_3 and α_1. Given $f \in B_n$, we denote by $AN_n(f)$ the set of non null $p \in B_n$ with lowest possible degree such that $p * f = 0$ or $p * (1 \oplus f) = 0$.

Proposition 2: Let

$$f_1(x)=\begin{cases}0 \quad if \quad wt(x)\prec k\\ g_1(x) \quad if \quad k\le wt(x)\le n-k\\ 1 \quad if \quad wt(x)\succ n-k\end{cases},$$

$$f_2(x)=\begin{cases}0 \quad if \quad wt(x)\prec k\\ g_2(x) \quad if \quad k\le wt(x)\le n-k\\ 1 \quad if \quad wt(x)\succ n-k\end{cases}$$ and

$$f_3(x)=\begin{cases}0 \quad if \quad wt(x)\prec k\\ g_3(x) \quad if \quad k\le wt(x)\le n-k\\ 1 \quad if \quad wt(x)\succ n-k\end{cases}$$ be three

Boolean functions on F_2^n have respectively algebraic degree r_1, r_2 and r_3. Let $\alpha_2(x) = f_1(x)f_2(x) \oplus f_1(x)f_3(x) \oplus f_2(x)f_3(x)$ be Boolean function. Then

1) $k \le AI_n(\alpha_2) \le k + \min(r_1, r_2, r_3)$

2) if $r_1 = r_2 = r_3 = r$ then

$$k \le AI_n(\alpha_2) \le k + r$$

Proof: From lemma 5, we have $k \le AI_n(f_1) = AI_n(f_2) = AI_n(f_3)$.

Let $\sigma_2 = g_1 g_2 \oplus g_1 g_3 \oplus g_2 g_3$. Note that, $\alpha_2(x) = f_1(x)f_2(x) \oplus f_1(x)f_3(x) \oplus f_2(x)f_3(x)$

$$=\begin{cases}0 \quad if \quad wt(x)\prec k\\ \sigma_2(x) \quad if \quad k\le wt(x)\le n-k\\ 1 \quad if \quad wt(x)\succ n-k\end{cases}.$$

From lemma 5, we have

$$k \le AI_n(\alpha_2) \qquad (14)$$

Let $p_1 \in AN_n(f_1)$. If $f_1 * p_1 = 0$, then $(f_2 \oplus f_3)\alpha_2 * p_1 = 0$. If $(1 \oplus f_1) * p_1 = 0$, then $(f_2 \oplus f_3)(1 \oplus \alpha_2) * p_1 = 0$. This gives inequalities:

$$AI_n(\alpha_2) \le k + \min(r_2, r_3) \qquad (15)$$

Let $p_2 \in AN_n(f_2)$. If $f_2 * p_2 = 0$, then $(f_1 \oplus f_3)\alpha_2 * p_2 = 0$. If $(1\oplus f_2) * p_2 = 0$, then $(f_1 \oplus f_3)(1\oplus \alpha_2) * p_2 = 0$. This gives inequalities:

$$AI_n(\alpha_2) \le k + \min(r_1, r_3) \qquad (16)$$

Let $p_3 \in A_n(f_3)$. If $f_3 * p_3 = 0$, then $(f_1 \oplus f_2)\alpha_2 * p_3 = 0$. If $(1\oplus f_3) * p_3 = 0$ then $(f_1 \oplus f_2)(1\oplus \alpha_2) * p_3 = 0$. This gives inequalities:

$$AI_n(\alpha_2) \le k + \min(r_1, r_2) \qquad (17)$$

Equations (15), (16) and (17) give inequalities on the right. Item 2 is direct consequence of item 1.

Table 1: The best lower bounds of balanced function *f* for $Ng = 2^{n-1} - 2^{\frac{n}{2}-1}$

n	*m=3*	*m=4*	*m=5*
18	130663	130000	127756
20	523586	522636	518931
22	2095897	2094588	2088813
24	8386284	8384536	8375934
26	33550011	33547736	33535386
28	134209158	134206260	134189061
30	536854093	536850468	536827123
32	2147450384	2147445920	2147414920

Table 2: The best lower bounds of balanced function *f* of [15]

n	*Nf*
18	81751
20	339517
22	1383228
24	5653936
26	23044039
28	93729726
30	380348781
32	1541277961

VI. CONCLUSIONS

We presented a general method of Boolean functions which can get a large class of Boolean functions with reasonably high nonlinearity. It is possible to specify the parameters n and g, to define class of balanced functions of even number n of variables with an algebraic immunity $k \prec\prec \left[\frac{n}{2}\right]$ that achieves nonlinearity at least $2^{n-1} - 2^{\frac{n}{2}-1} - \binom{n}{k-1}$, significantly larger than that obtained by Lobanov. Then, we study the secondary construction of Boolean functions without extending their number of variables, introduced recently by Carlet. This gives interesting cryptographic properties in terms of balancedness, nonlinearity and algebraic immunity. We prove that, the algebraic immunity of the constructed functions is better than among of the starting functions.

References

[1] T. Siegenthaler, “Decrypting a class of stream ciphers using cipher text only”, *IEEE Transactions on Computers*, C-34, N°1:81–85, January 1985.

[2] C. Ding, G. Xiao, and W. Shan, “The stability theory of stream ciphers”, *Number 561, Lecture Notes in Computer Science*, Springer Verlag, August 1991.

[3] O. S. Rothaus, “On bent functions”, *Journal of Combinatorial Theory*, Series A20, pp. 300-305.

[4] T. Siegenthaler, “Correlation-immunity of nonlinear combining functions for cryptographic applications”, *IEEE Transactions on Information Theory*, IT-30, N°5:776–780, September 1984.

[5] P. Sarkar and S. Maitra, “Nonlinearity bounds and construction of resilient Boolean functions”, *In: Advances in Cryptology - EUROCRYPT 2000*, vol. 1880 in Lecture Notes in Computer Science, pages 515–532. Springer Verlag, 2000

[6] Y. V. Tarannikov, “On resilient Boolean functions with maximum possible nonlinearity”, *Proceedings of INDOCRYPT 2000,* lecture Notes in Computer Science 1977, pp19-30, 2000.

[7] Y. Zheng and X. M. Zhang, “Improving upper bound on the non linearity of high order correlation immune functions”, *Proceedings of Selected Areas in Cryptography 2000*, Lecture Notes in computer Science 2012, pp262- 274, 2001.

[8] J. Y. Cho and J. Pieprzyk, “Algebraic Attacks on SOBER-t32 and SOBER-128”*, In FSE 2004, number 3017 in Lecture Notes in Computer Science,* pages 49–64. Springer Verlag, 2004.

[9] N. Courtois and J. Pieprzyk,” Cryptanalysis of block ciphers with overde-fined systems of equations”, *In Advances in Cryptology – ASIACRYPT 2002,* number 2501 in Lecture Notes in Computer Science, pages 267–287. Springer Verlag, 2002.

[10] 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. 345-359, Springer, 2003.

[11] 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.

[12] D. H. Lee et al, “Algebraic Attacks on Summation Generators”, *In FSE 2004,* number 3017 in Lecture Notes in Computer Science, pages 34–48. Springer Verlag, 2004.

[13] W. Meier, E. Pasalic and C. Carlet, “Algebraic attacks and decomposition of Boolean functions” *In Advances in Cryptology - EUROCRYPT 2004,* number 3027 in Lecture Notes in Computer Science, pages 474–491. Springer Verlag, 2004.

[14] F. Armknecht, “Improving Fast algebraic Attacks”, *In FSE 2004,* number 3017 in lecture Notes in computer Science, pages 65-82. Springer Verlag, 2004.

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

[16] C. Carlet, D. K. Dalai, K. C. Gupta, S. Maitra, "Algebraic immunity for cryptographically Significant Boolean functions: analysis and construction", *IEEE Transaction on information theory*, vol XX, N° Y, 2006.

[17] C. Carlet, "Improving the algebraic immunity of resilient and nonlinear functions and constructing bent functions. IACR eprint server, http://eprint.iacr.org, 2004/276. See also the extended abstract entitled Designing bent functions and resilient functions from known ones, without extending their number of variables", *in the proceedings of ISIT* 2005.

[18] A. Canteaut and M. Trabbia, "Improved fast correlation attacks using parity-check equations of weight 4 and 5", *Advanced in Cryptology-EUROCRYPT 2000*. Lecture notes in computer science 1807 (2000), pp. 573-588.

[19] *T. Johansson and F. Jonsson*, "Improved fast correlation attack on stream ciphers via convolutional codes", *Advances in Cryptology - EUROCRYPT'99*, number 1592 in Lecture Notes in Computer Science (1999), pp. 347–362.

[20] T. Johansson and F. Jonsson, "Fast correlation attacks based on turbo code techniques" , *Advances in Cryptology - CRYPTO'99*, number 1666 in Lecture Notes in Computer Science (1999), pp. 181–197.

[21] G. Z. Xiao 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.

[22] F. J. MacWilliams and N. J. Sloane, "The Theory of Error-Correcting Codes", Amsterdam, The Netherlands:North-Holland, 1977.

[23] C. Carlet et al. "Further Properties of several classes of Boolean functions with optimum algebraic immunity". Cryptology eprint archive http://eprint.iacr. org/), 2007.