Construction and Analysis of Boolean Functions of $2t+1$ Variables with Maximum Algebraic Immunity ⋆

Na Li and Wen-Feng Qi

Department of Applied Mathematics, Zhengzhou Information Engineering University, Zhengzhou, 450002, China
mylina_1980@yahoo.com.cn, wenfeng.qi@263.net

Abstract. In this paper, we study the construction of $(2t+1)$-variable Boolean functions with maximum algebraic immunity, and we also analyze some other cryptographic properties of this kind of functions, such as nonlinearity, resilience. We first identify several classes of this kind of functions. Further, some necessary conditions of this kind of functions which also have higher nonlinearity are obtained. In this way, a modified construction method is proposed to possibly obtain $(2t+1)$-variable Boolean functions which have maximum algebraic immunity and higher nonlinearity, and a class of such functions is also obtained. Finally, we present a sufficient and necessary condition of $(2t+1)$-variable Boolean functions with maximum algebraic immunity which are also 1-resilient.

Keywords: Algebraic attack, algebraic immunity, Boolean functions, balancedness, nonlinearity, resilience.

1 Introduction

The recent progress in research related to algebraic attacks [1,2,5,6] seems to threaten all LFSR-based stream ciphers. It is known that Boolean functions used in stream ciphers should have high algebraic degree [11]. However, a Boolean function may have low degree multiples even if its algebraic degree is high. By this fact it is possible to obtain an over-defined system of multivariate equations of low degree whose unknowns are the bits of the initialization of the LFSR(s). Then the secret key can be discovered by solving the system.

To measure the resistance to algebraic attacks, a new cryptographic property of Boolean functions called algebraic immunity (AI) has been proposed by W. Meier *et al.* [16]. When used in a cryptosystem, a Boolean function should have high AI. Now, it is known that the AI of an n-variable Boolean function is upper bounded by $\lceil \frac{n}{2} \rceil$ [6,16]. Balancedness, nonlinearity and correlation-immunity are three other important cryptographic criteria. In some sense, algebraic immunity is compatible with the former two criteria: a Boolean functions with low nonlinearity will have low AI [7,14], a Boolean function of an odd number of variables with maximum AI must be balanced [7]. The existence of links between algebraic immunity and correlation-immunity remains open.

Constructions of Boolean functions with maximum AI are obviously important. Further, it is more important to construct these functions which also satisfy

⋆ This work was supported by National Nature Science Foundation of China under Grant number 60373092.

some other criteria (such as balancedness, a high nonlinearity, a high correlation-immunity order, ...). Some classes of symmetric Boolean functions with maximum AI were obtained in [3] and [9], and it was shown in [12] that there is only one such symmetric function (besides its complement) when the number of input variables is odd. A construction keeping in mind the basic theory of algebraic immunity was presented in [9], which also provided some functions with maximum AI. In [4], Carlet introduced a general method (for any number of variables) and an algorithm (for an even number of variables) for constructing balanced functions with maximum AI. In [13], a method was proposed for constructing functions of an odd number of variables with maximum AI, which convert the problem of constructing such a function to the problem of finding an invertible submatrix of a $2^{n-1} \times 2^{n-1}$ matrix. And it was stated that any such function can be obtained by this method.

In this paper, we study the construction of $(2t+1)$-variable Boolean functions with maximum AI, and we also analyze some other cryptographic properties of this kind of functions. From the characteristic of the matrix used in the construction proposed in [13], we obtain some necessary or sufficient conditions of $(2t+1)$-variable Boolean functions with maximum AI. Further, by studying the Walsh spectra of this kind of functions, we obtain some necessary conditions of this kind of functions which also have higher nonlinearity and thus we propose a modified construction to obtain such functions. We finally present a sufficient and necessary condition of $(2t+1)$-variable Boolean functions with maximum AI which are also 1-resilient.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the set of all n-tuples of elements in the finite field $\mathbb{F}_2$. To avoid confusion with the usual sum, we denote the sum over $\mathbb{F}_2$ by $\oplus$.

A Boolean function of n variables is a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. Any n-variable Boolean function f can be uniquely expressed by a polynomial in $\mathbb{F}_2[x_1, \dots, x_n]/(x_1^2 - x_1, \dots, x_n^2 - x_n)$, which is called its algebraic normal form (ANF). The algebraic degree of f, denoted by $\deg(f)$, is the degree of this polynomial. Boolean function f can also be identified by a binary string of length 2^n, called its truth table, which is defined as

$$(f(0,0,\dots,0), f(1,0,\dots,0), f(0,1,\dots,0), \dots, f(1,1,\dots,1)).$$

Let

$$1_f = \{X \in \mathbb{F}_2^n | f(X) = 1\}, 0_f = \{X \in \mathbb{F}_2^n | f(X) = 0\}.$$

The set 1_f (resp. 0_f) is called the on set (resp. off set). The cardinality of 1_f, denoted by $wt(f)$, is called the Hamming wight of f. We say that an n-variable Boolean function f is balanced if $wt(f) = 2^{n-1}$. The Hamming distance between two functions f and g, denoted by $d(f,g)$, is the Hamming weight of $f \oplus g$. Let $S = (s_1, s_2, \dots, s_n) \in \mathbb{F}_2^n$, the Hamming weight of S, denoted by $wt(S)$, is the number of 1's in $\{s_1, s_2, \dots, s_n\}$.

Walsh spectra is an important tool for studying Boolean functions. Let $X = (x_1, \ldots, x_n)$ and $S = (s_1, \ldots, s_n)$ both belonging to $\mathbb{F}_2^n$ and their inner product $X \cdot S = x_1 s_1 \oplus \ldots \oplus x_n s_n$. Let f be a Boolean function of n variables. Then the Walsh transform of f is an integer valued function over $\mathbb{F}_2^n$ which is defined as

$$W_f(S) = \sum_{X \in \mathbb{F}_2^n} (-1)^{f(X) \oplus X \cdot S}.$$

Affine functions are those Boolean functions of degree at most 1. The nonlinearity of an n-variable Boolean function f is its Hamming distance from the set of all n-variable affine functions, i.e.,

$$nl(f) = \min\{d(f, g) | g \text{ is an affine function}\}.$$

The nonlinearity of f can be described by its Walsh spectra as $nl(f) = 2^{n-1} - \frac{1}{2}\max_{S \in \mathbb{F}_2^n} |W_f(S)|$. Correlation immune functions and resilient functions are two important classes of Boolean functions. A function is mth order correlation immune (resp. m-resilient) if and only if its Walsh spectra satisfies

$$W_f(S) = 0, \text{ for } 1 \leq wt(S) \leq m \quad (\text{resp. } 0 \leq wt(S) \leq m).$$

Definition 1. *[16] For a given n-variable Boolean function f, a nonzero n-variable Boolean function g is called an annihilator of f if $f \cdot g = 0$, and the algebraic immunity of f, denoted by $AI(f)$, is the minimum value of d such that f or $f \oplus 1$ admits an annihilating function of degree d.*

For convenience, two orderings on vectors and monomials are defined as follows.

Definition 2. *A vector ordering $<_v$ on $\mathbb{F}_2^n$ is defined as:*

let $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbb{F}_2^n$, then $(a_1, \ldots, a_n) <_v (b_1, \ldots, b_n)$ if and only if $\sum_{i=1}^n a_i < \sum_{i=1}^n b_i$, or $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$ and there exists $1 \leq i < n$ such that $a_i > b_i$, $a_j = b_j$ for $1 \leq j < i$.

Example 1. If $n = 3$, then $(0,0,0) <_v (1,0,0) <_v (0,1,0) <_v (0,0,1) <_v (1,1,0) <_v (1,0,1) <_v (0,1,1) <_v (1,1,1)$.

Definition 3. *A monomial ordering $<_m$ on $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 - x_1, \ldots, x_n^2 - x_n)$ is defined as:*

let $x_1^{a_1} \ldots x_n^{a_n}, x_1^{b_1} \ldots x_n^{b_n} \in \mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 - x_1, \ldots, x_n^2 - x_n)$, then $x_1^{a_1} \ldots x_n^{a_n} <_m x_1^{b_1} \ldots x_n^{b_n}$ if and only if $(a_1, \ldots, a_n) <_v (b_1, \ldots, b_n)$.

It is clear that $<_v$ and $<_m$ are both total orderings.

Let A be an $l \times l$ matrix, and integers $1 \leq i_1, i_2 \ldots, i_k \leq l, 1 \leq j_1, j_2 \ldots, j_k \leq l$. Denoted by $A_{(i_1, \ldots, i_k)}$ the $k \times l$ matrix with the rth $(1 \leq r \leq k)$ row vector equal to the i_rth row vector of A, and $A_{(i_1, \ldots, i_k; j_1, \ldots, j_k)}$ the $k \times k$ matrix with the rth $(1 \leq r \leq k)$ column vector equal to the j_rth column vector of $A_{(i_1, \ldots, i_k)}$.

3 Construction of Boolean functions with maximum AI

In this section, we briefly review the method to construct Boolean functions with maximum AI proposed in [13].

Let n be a positive integer, $X = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$. Let

$$v(X) = (1, x_1, \ldots, x_n, x_1x_2, \ldots, x_{n-1}x_n, \ldots\ldots, \\ x_1 \cdots x_{\lceil \frac{n}{2} \rceil - 1}, \ldots, x_{\lfloor \frac{n}{2} \rfloor + 2} \cdots x_n) \in \mathbb{F}_2^{\sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} \binom{n}{i}},$$

where the monomials are ordered according to the ordering $<_m$. It is clear that $\sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} \binom{n}{i} = 2^{n-1}$ when n is odd. Let f be an n-variable Boolean function, let $V(1_f)$ denote the $wt(f) \times \sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} \binom{n}{i}$ matrix with the set of row vectors $\{v(X) | X \in 1_f\}$, and $V(0_f)$ denote the $(2^n - wt(f)) \times \sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} \binom{n}{i}$ matrix with the set of row vectors $\{v(X) | X \in 0_f\}$.

Lemma 1. *[3,9] Let odd $n = 2t + 1$ and f be an n-variable Boolean function which satisfies*

$$f(X) = \begin{cases} a & \text{for } wt(X) \leq t \\ a \oplus 1 & \text{for } wt(X) > t \end{cases},$$

where $a \in \mathbb{F}_2$, then AI(f) $= t + 1$.

When $a = 1$, the function described in Lemma 1 is called the majority function, and we denote it by F_n. It is clear that F_n is balanced. We arrange the vectors in 1_{F_n} (resp. 0_{F_n}) according to the order $<_v$, and denote them by $X_1, \ldots, X_{2^{n-1}}$ (resp. $Y_1, \ldots, Y_{2^{n-1}}$), i.e. $X_1 <_v \ldots <_v X_{2^{n-1}}$ (resp. $Y_1 <_v \ldots <_v Y_{2^{n-1}}$). Let $X_j = (x_{j,1}, \ldots, x_{j,n})$ (resp. $Y_i = (y_{i,1}, \ldots, y_{i,n})$). The ith row vector of $V(1_{F_n})$ (resp. $V(0_{F_n})$) is $v(X_i)$ (resp. $v(Y_i)$).

The idea of the construction proposed in [13] is to obtain a new function by changing the values of the majority function at some vectors. The problem of finding out the appropriate vectors is converted to the problem of finding out a $k \times k$ invertible submatrix of the $2^{n-1} \times 2^{n-1}$ invertible matrix $W = V(0_{F_n})V(1_{F_n})^{-1}$.

Theorem 1. *[13] Let $n = 2t + 1$, and f an n-variable Boolean function. Then, AI(f)$= t + 1$ if and only if there exist integers $1 \leq i_1 < \ldots < i_k \leq 2^{n-1}, 1 \leq j_1 < \ldots < j_k \leq 2^{n-1}$, such that $f = f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ and $W_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ is invertible, where $f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ is defined as*

$$f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}(X) = \begin{cases} F_n(X) \oplus 1 & \text{if } X \in \{X_{j_1}, \ldots, X_{j_k}, Y_{i_1}, \ldots, Y_{i_k}\} \\ F_n(X) & \text{else} \end{cases}. \quad (1)$$

Construction 1 [13] Let $n = 2t + 1$. The following method can generate a Boolean function of n variables with maximum AI.

Step1: Select randomly an integer $1 \leq k \leq 2^{n-2}$ and k integers $1 \leq i_1 < \ldots < i_k \leq 2^{n-1}$.

Step2: Find out k integers $1 \le j_1 < \ldots < j_k \le 2^{n-1}$, such that the j_1th, $\ldots$, j_kth column vectors of $W_{(i_1,\ldots,i_k)}$ are linearly independent.

Then, the Boolean function $f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ defined by (1) has AI $t+1$.

Remark 1. 1) For any fixed $1 \le k \le 2^{n-2}$ and any k integers $1 \le i_1 < \ldots < i_k \le 2^{n-1}$, there always exist k integers $1 \le j_1 < \ldots < j_k \le 2^{n-1}$ such that $W_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ is invertible.

2) Any Boolean function of $2t+1$ variables with maximum AI can be constructed by this method.

For the rest of this paper, we always suppose $n = 2t+1$.

4 Properties of W and several classes of n-variable Boolean functions with maximum AI

In this section, we first show some important properties of the matrix $W = V(0_{F_n})V(1_{F_n})^{-1}$, then use these conclusions to obtain some necessary or sufficient conditions of n-variable Boolean function achieving maximum AI.

Let A be a $2^{n-1}\times 2^{n-1}$ matrix, and divide A into $(t+1)^2$ submatrixes, denoted by $A_{i,j}$, $1 \le i \le t+1$, $1 \le j \le t+1$, defined as

$$A_{i,j} = A_{(r_{i-1}+1,r_{i-1}+2\ldots,r_i;s_{j-1}+1,s_{j-1}+2\ldots,s_j)},$$

where

$$r_l = \begin{cases} 0 & \text{if } l=0 \\ \sum_{k=1}^{l}\binom{n}{t+k} & \text{if } l>0 \end{cases}, \quad s_l = \begin{cases} 0 & \text{if } l=0 \\ \sum_{k=0}^{l-1}\binom{n}{k} & \text{if } l>0 \end{cases}.$$

It is clear that the row (resp. column) vectors of $W_{i,j}$ correspond to the vectors in $\mathbb{F}_2^n$ with Hamming weight $i+t$ (resp. $j-1$).

Proposition 1. *[10] $V(1_{F_n})^{-1}$=$V(1_{F_n})$.*

Proposition 2. *Let $W = V(0_{F_n})V(1_{F_n})^{-1}$, then*

$$W_{i,j} = \begin{cases} \mathbf{0} & \text{if } \bigoplus_{r=0}^{t-j+1}\binom{t+i-j+1}{r} = 0 \\ V(0_{F_n})_{i,j} & \text{else} \end{cases}, \text{for } 1 \le i,j \le t+1,$$

where $\mathbf{0}$ denotes the matrix with all entries 0.

Proof. By Proposition 1, $W = V(0_{F_n})V(1_{F_n})^{-1} = V(0_{F_n})V(1_{F_n})$. Let $Y = (y_1,\ldots,y_n) \in 0_{F_n}$ and $wt(Y) = i > t$, $x_{r_1}\cdots x_{r_j}$ be a monomial of degree $j (0 \le j \le t)$. Denote the transpose of the column vector of $V(1_{F_n})$ corresponding to $x_{r_1}\cdots x_{r_j}$ by $u(x_{r_1}\cdots x_{r_j})$. That is, $u(x_{r_1}\cdots x_{r_j})$ is the evaluation of $x_{r_1}\cdots x_{r_j}$ at the vectors belonging to 1_{F_n}. We can represent $u(x_{r_1}\cdots x_{r_j})$ as

$$\begin{gathered}(g(1), g(x_1), \ldots, g(x_n), g(x_1x_2), g(x_1x_3), \ldots, \\ g(x_{n-1}x_n), \ldots, g(x_1\cdots x_t), \ldots, g(x_{t+2}\cdots x_n)),\end{gathered} \tag{2}$$

where g is a function on the monomials of degree at most t, which satisfies

$$g(x_1^{a_1}\cdots x_n^{a_n})=\begin{cases}1 \text{ if } x_{r_1}\cdots x_{r_j}|x_1^{a_1}\cdots x_n^{a_n}\\ 0 \quad\quad\quad\quad \text{else}\end{cases}. \tag{3}$$

On the other hand, we can also represent $v(Y)$ as

$$\begin{aligned}(h(1),h(x_1),\ldots,h(x_n),h(x_1x_2),h(x_1x_3),\ldots,\\ h(x_{n-1}x_n),\ldots,h(x_1\cdots x_t),\ldots,h(x_{t+2}\cdots x_n)),\end{aligned} \tag{4}$$

where h is a function on the monomials of degree at most t, which satisfies

$$h(x_1^{a_1}\cdots x_n^{a_n})=\begin{cases}1 \text{ if } x_1^{a_1}\cdots x_n^{a_n}|x_1^{y_1}\cdots x_n^{y_n}\\ 0 \quad\quad\quad\quad \text{else}\end{cases}. \tag{5}$$

Denote the inner product of $v(Y)$ and $u(x_{r_1}\cdots x_{r_j})$ by c.

If $y_{r_1},\ldots,y_{r_j}$ are not all 1, by (2), (3), (4) and (5), we have $c=0=h(x_{r_1}\cdots x_{r_j})$. If $y_{r_1},\ldots,y_{r_j}$ are all 1, we have $h(x_{r_1}\cdots x_{r_j})=1$ and

$$c=\bigoplus_{\substack{x_{r_1}\cdots x_{r_j}|x_1^{a_1}\cdots x_n^{a_n},\\ x_1^{a_1}\cdots x_n^{a_n}|x_1^{y_1}\cdots x_n^{y_n}\\ wt(a_1,\ldots,a_n)\leq t}} 1=\bigoplus_{r=0}^{t-j}\binom{i-j}{r}.$$

It is clear that the row (resp. column) vectors of $W_{i,j}$ correspond to the vectors in $\mathbb{F}_2^n$ with Hamming weight $i+t$ (resp. $j-1$). Therefore, we complete the proof.

Corollary 1. *1) For any $2\leq i\leq t+1$, $W_{i,t+2-i}=\mathbf{0}$.*

2) For any $1\leq j\leq t+1$, $W_{1,j}=V(0_{F_n})_{1,j}$.

3) For any $1\leq i\leq t+1$, $W_{i,t+1}=V(0_{F_n})_{i,t+1}$.

Proof. 1) If $2\leq i\leq t+1$ and $j=t+2-i$, then

$$\bigoplus_{r=0}^{t-j+1}\binom{t+i-j+1}{r}=\bigoplus_{r=0}^{i-1}\binom{2i-1}{r}=2^{2i-2} \bmod 2\ =0.$$

2) If $i=1$, then

$$\bigoplus_{r=0}^{t-j+1}\binom{t+i-j+1}{r}=\bigoplus_{r=0}^{t-j+1}\binom{t-j+2}{r}=2^{t-j+2}-1 \bmod 2\ =1.$$

3) If $j=t+1$, then

$$\bigoplus_{r=0}^{t-j+1}\binom{t+i-j+1}{r}=1.$$

We can obtain some necessary conditions of n-variable Boolean functions with maximum AI.

Theorem 2. *Let* $1 \le k \le 2^{n-1}$, $1 \le i_1 < \ldots < i_k \le 2^{n-1}$, $1 \le j_1 < \ldots < j_k \le 2^{n-1}$. *If there exist* $0 \le j \le t$, $t+1 \le i \le n$ *such that* $\bigoplus_{r=0}^{t-j} \binom{i-j}{r} = 0$, *and*

$$\#\{X \in \{X_{j_1}, \ldots, X_{j_k}\} | wt(X) = j\} + \#\{Y \in \{Y_{i_1}, \ldots, Y_{i_k}\} | wt(Y) = i\} > k,$$

then, $AI(f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}) < t+1$.

Proof. By Theorem 1, it is sufficient to show that $W_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ is not invertible. By Proposition 2 and the first condition, we have that $W_{i-t,j+1} = \mathbf{0}$. Then the second condition implies that $W_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ has a submatrix with the number of rows and columns greater than k whose entries are all 0. Therefore, $W_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ is not invertible.

Corollary 2. *Let* $1 \le k \le 2^{n-1}$, $1 \le i_1 < \ldots < i_k \le 2^{n-1}$, $1 \le j_1 < \ldots < j_k \le 2^{n-1}$. *If there exists* $0 \le r \le t-1$ *such that*

$$\#\{X \in \{X_{j_1}, \ldots, X_{j_k}\} | wt(X) = r\} + \#\{Y \in \{Y_{i_1}, \ldots, Y_{i_k}\} | wt(Y) = n-r\} > k,$$

then, $AI(f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}) < t+1$.

In the following of this section, several classes of n-variable Boolean functions with maximum AI are provided.

Theorem 3. *Let* $1 \le k \le 2^{n-1}$, $1 \le i_1 < \ldots < i_k \le 2^{n-1}$, $1 \le j_1 < \ldots < j_k \le 2^{n-1}$. *If the following conditions are both satisfied, then* $AI(f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}) = t+1$.

1) There exist $1 \le a_1 < \ldots < a_s \le n$, *such that* $x_{j_r,a_1} = \ldots = x_{j_r,a_s} = 0$ *for* $1 \le r \le k$.

2) For any X_{j_r} $(1 \le r \le k)$, *there exists correspondingly* $Y_{i_r{}'} \in \{Y_{i_1}, \ldots, Y_{i_k}\}$, *such that* $y_{i_r{}',a} = x_{j_r,a}$ *for* $a \notin \{a_1, \ldots, a_s\}$, *and*

$$\bigoplus_{l=0}^{t-wt(X_{j_r})} \binom{wt(Y_{i_r{}'}) - wt(X_{j_r})}{l} = 1.$$

Proof. If $X_{j_1}, \ldots, X_{j_k}$ and $Y_{i_1}, \ldots, Y_{i_k}$ satisfy the two conditions, then by Proposition 2, $W_{(i_1{}',\ldots,i_k{}';j_1,\ldots,j_k)}$ is in the form of lower triangular with all entries on the diagonal equal to 1. Therefore $W_{(i_1{}',\ldots,i_k{}';j_1,\ldots,j_k)}$ is invertible, which implies that $W_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ is invertible, and the result holds by Theorem 1.

Example 2. Let $n = 7$, $L_1 = \{(1,0,0,0,0,0,0), (0,1,1,0,0,0,0), (0,0,1,1,0,0,0), (1,1,1,0,0,0,0,)\} \subseteq 1_{F_n}$, $L_2 = \{(1,0,0,0,1,1,1), (0,1,1,0,1,1,0), (0,0,1,1,0,1,1), (1,1,1,0,1,1,1,)\} \subseteq 0_{F_n}$. Then the function

$$f(X) = \begin{cases} F_n(X) \oplus 1 & \text{if } X \in L_1 \cup L_2 \\ F_n(X) & \text{else} \end{cases}$$

has AI 4.

Theorem 4. *Let* $1 \le 2k \le 2^{n-1}$, $1 \le i_1 < \ldots < i_{2k} \le 2^{n-1}$, $1 \le j_1 < \ldots < j_{2k} \le 2^{n-1}$. $wt(X_{j_r}) = w_1$, $wt(Y_{i_r}) = w'_1$ *for* $1 \le r \le k$, *and* $wt(X_{j_r}) = w_2$, $wt(Y_{i_r}) = w'_2$ *for* $k+1 \le r \le 2k$. *If one of the following two conditions is satisfied, then* $AI(f_{(i_1,\ldots,i_{2k};j_1,\ldots,j_{2k})}) = t+1$.

1) $\bigoplus_{r=0}^{t-w_1} \binom{w'_2-w_1}{r}$ *and* $\bigoplus_{r=0}^{t-w_2} \binom{w'_1-w_2}{r}$ *are not both 1, and*

$$AI(f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}) = AI(f_{(i_{k+1},\ldots,i_{2k};j_{k+1},\ldots,j_{2k})}) = t+1.$$

2) $\bigoplus_{r=0}^{t-w_1} \binom{w'_1-w_1}{r}$ *and* $\bigoplus_{r=0}^{t-w_2} \binom{w'_2-w_2}{r}$ *are not both 1, and*

$$AI(f_{(i_1,\ldots,i_k;j_{k+1},\ldots,j_{2k})}) = AI(f_{(i_{k+1},\ldots,i_{2k};j_1,\ldots,j_k)}) = t+1.$$

Proof. Let M denote the $2k \times 2k$ matrix $W_{(i_1,\ldots,i_{2k};j_1,\ldots,j_{2k})}$. The first condition implies that $M_{(1,\ldots,k;1,\ldots,k)}$ and $M_{(k+1,\ldots,2k;k+1,\ldots,2k)}$ are both invertible, and at least one of $M_{(1,\ldots,k;k+1,\ldots,2k)}$ and $M_{(k+1,\ldots,2k;1,\ldots,k)}$ is $\mathbf{0}$. Then, M is invertible, and the result holds by Theorem 1.

If the second condition is satisfied, the result can be proved in the same way.

Example 3. Let $n = 7$, L_1=$\{(0,0,0,0,1,1,0),(0,0,0,0,1,0,1),(0,0,0,0,0,1,1),(1,1,0,0,1,0,0),(1,1,0,0,0,1,0),(1,1,0,0,0,0,1)\}$, L_2=$\{(1,1,0,0,1,1,0),(1,1,0,0,1,0,1),(1,1,0,0,0,1,1),(1,1,1,1,1,0,0),(1,1,1,1,0,1,0),(1,1,1,1,0,0,1)\}$. Then the function

$$f(X) = \begin{cases} F_n(X) \oplus 1 & \text{if } X \in L_1 \cup L_2 \\ F_n(X) & \text{else} \end{cases}$$

has AI 4.

Theorem 5. *Let* $1 \le k \le n$, $Y_{i_1}, \ldots, Y_{i_k}$ *belong to* 0_{F_n} *and their Hamming weight are* $w_1, \ldots, w_k$, *respectively. If*

1) $\bigoplus_{r=0}^{t-1} \binom{w_i-1}{r} = 1$ *for* $1 \le i \le k$, *and*

2) there exist $1 \le j_1 < \ldots < j_k \le n$, *such that the* j_1*th,* $\ldots$, j_k*th column of the matrix* $\begin{pmatrix} Y_{i_1} \\ \ldots \\ Y_{i_k} \end{pmatrix}$ *are linearly independent,*

then, $AI(f_{(i_1,\ldots,i_k;j_1+1,\ldots,j_k+1)}) = t+1$.

Proof. By Proposition 2, $W_{(i_1,\ldots,i_k;j_1+1,\ldots,j_k+1)}$ is invertible if the two conditions are both satisfied, then , and the result holds by Theorem 1.

Example 4. Let $n = 7$, L_1=$\{(1,0,0,0,0,0,0),(0,1,0,0,0,0,0),(0,0,1,0,0,0,0)\}$, L_2=$\{(1,0,1,0,1,1,1),(0,1,1,0,1,0,1),(1,1,1,1,0,1,0)\}$. Then the function

$$f(X) = \begin{cases} F_n(X) \oplus 1 & \text{if } X \in L_1 \cup L_2 \\ F_n(X) & \text{else} \end{cases}$$

has AI 4.

5 Nonlinearity and resilience of Boolean functions with maximum AI

At first, we give the Walsh spectra of majority functions. Note that although the first item and the case of $wt(S) = 1$ in the second item in the following lemma have been given in [9], we still give the proof for completeness.

Lemma 2. *Let $S \in \mathbb{F}_2^n$.*
1) If $wt(S)$ is even, then $W_{F_n}(S) = 0$.
2) If $wt(S)$ is odd, then

$$W_{F_n}(S) = (-1)^{(wt(S)+1)/2} 2 \binom{n-1}{t} \prod_{i=1}^{(wt(S)-1)/2} \frac{2i-1}{n-2i}.$$

Proof. Since $\sum_{wt(X)=i} (-1)^{S \cdot X} = K_i(wt(S), n)$, we have

$$W_{F_n}(S) = \sum_{i=t+1}^{n} K_i(wt(S), n) - \sum_{i=0}^{t} K_i(wt(S), n), \tag{6}$$

where $K_i(k, n)$ is the so-called Krawtchouk polynomial [15, Page 151, Part I] defined by

$$K_i(k, n) = \sum_{j=0}^{i} (-1)^j \binom{k}{j} \binom{n-k}{i-j}, i = 0, 1, \ldots, n.$$

Krawtchouk polynomials also have properties [15, Page 153, Part I] as follows.
P1. $K_i(k, n) = (-1)^k K_{n-i}(k, n)$.
P2. $\sum_{i=0}^{e} K_i(k, n) = K_e(k-1, n-1)$.
P3. $(n-k)K_i(k+1, n) = (n-2i)K_i(k, n) - kK_i(k-1, n)$ for nonnegative integers i and k.
If $wt(S)$ is even, then by (6) and P1, we have $W_{F_n}(S) = 0$.
If $wt(S)$ is odd, then by (6), P1 and P2, we have

$$W_{F_n}(S) = -2 \sum_{i=0}^{t} K_i(wt(S), n) = -2K_t(wt(S) - 1, n-1).$$

By the definition of Krawtchouk polynomials, we have $K_t(k, n-1) = 0$ if k is odd. Thus by P3, we have

$$\begin{aligned} W_{F_n}(S) &= (-1)^{(wt(S)-1)/2+1} 2K_t(0, n-1) \prod_{i=1}^{(wt(S)-1)/2} \frac{2i-1}{n-2i} \\ &= (-1)^{(wt(S)+1)/2} 2 \binom{n-1}{t} \prod_{i=1}^{(wt(S)-1)/2} \frac{2i-1}{n-2i}. \end{aligned}$$

Lemma 3. *Let $S, T \in \mathbb{F}_2^n$.*

1) If $wt(S) + wt(T) = n + 1$, then $W_{F_n}(S) = (-1)^t W_{F_n}(T)$.

2) If both $wt(S)$ and $wt(T)$ are odd, and $0 < wt(S) < wt(T) \le t + 1$, then $|W_{F_n}(S)| > |W_{F_n}(T)|$.

Proof. 1) Since Krawtchouk polynomials have the following property,

$$K_i(k, n) = (-1)^i K_i(n - k, n),$$

we have that

$$\begin{aligned} W_{F_n}(S) &= -2K_t(wt(S) - 1, n - 1) \\ &= -2(-1)^t K_t(n - 1 - (wt(S) - 1), n - 1) \\ &= -2(-1)^t K_t(wt(T) - 1, n - 1) = (-1)^t W_{F_n}(T). \end{aligned}$$

2) It is obvious from the second item of Lemma 2.

Remark 2. By Lemma 3, we have

$$\max_{T \in \mathbb{F}_2^n} |W_{F_n}(T)| = |W_{F_n}(S_1)| = |W_{F_n}(S_n)| = 2\binom{n-1}{t},$$

where $wt(S_1) = 1$, $wt(S_n) = n$. Therefore, $nl(F_n) = 2^{n-1} - \binom{n-1}{t}$ [9]. And

$$\max_{T \in \mathbb{F}_2^n, wt(T) \ne 1, n} |W_{F_n}(T)| = |W_{F_n}(S_3)| = |W_{F_n}(S_{n-2})| = \frac{2}{n-2}\binom{n-1}{t},$$

where $wt(S_3) = 3$, $wt(S_{n-2}) = n - 2$. We note that the difference between the maximal and the secondarily maximal absolute value of Walsh spectra is quite great, which is

$$2\frac{n-3}{n-2}\binom{n-1}{t}.$$

Algebraic immunity has the following relationship with nonlinearity.

Lemma 4. *[14] Let f be an n-variable Boolean function, $AI(f) = k$, then*

$$nl(f) \ge 2^{n-1} - \sum_{i=k-1}^{n-k} \binom{n-1}{i},$$

and this bound is tight.

Remark 3. Lemma 4 together with Remark 2 implies that F_n has the worst nonlinearity among all n-variable Boolean functions with maximum AI.

Theorem 6. *The Walsh spectra of $f = f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ is given by*

$$W_f(S) = W_{F_n}(S) - 4\left(\sum_{r=1}^{k} S \cdot X_{j_r} - \sum_{r=1}^{k} S \cdot Y_{i_r}\right).$$

Proof.

$$
\begin{aligned}
W_f(S) &= \sum_{r=1}^{2^{n-1}} (-1)^{f(X_r)+S\cdot X_r} + \sum_{r=1}^{2^{n-1}} (-1)^{f(Y_r)+S\cdot Y_r} \\
&= \sum_{r\in\{1,\ldots,2^{n-1}\}\setminus\{j_1,\ldots,j_k\}} (-1)^{F_n(X_r)+S\cdot X_r} + \sum_{r=1}^{k} (-1)^{F_n(X_{j_r})+1+S\cdot X_{j_r}} + \\
&\quad \sum_{r\in\{1,\ldots,2^{n-1}\}\setminus\{i_1,\ldots,i_k\}} (-1)^{F_n(Y_r)+S\cdot Y_r} + \sum_{r=1}^{k} (-1)^{F_n(Y_{i_r})+1+S\cdot Y_{i_r}} \\
&= W_{F_n}(S) - 2(\sum_{r=1}^{k} (-1)^{F_n(X_{j_r})+S\cdot X_{j_r}} + \sum_{r=1}^{k} (-1)^{F_n(Y_{i_r})+S\cdot Y_{i_r}}) \\
&= W_{F_n}(S) - 2(\sum_{r=1}^{k} (-1)^{1+S\cdot X_{j_r}} + \sum_{r=1}^{k} (-1)^{S\cdot Y_{i_r}}) \\
&= W_{F_n}(S) - 2(\sum_{r=1}^{k} (2S\cdot X_{j_r} - 1) + \sum_{r=1}^{k} (1 - 2S\cdot Y_{i_r})) \\
&= W_{F_n}(S) - 4(\sum_{r=1}^{k} S\cdot X_{j_r} - \sum_{r=1}^{k} S\cdot Y_{i_r}).
\end{aligned}
$$

From the above analysis in this section, some necessary conditions of Boolean functions with maximum AI and these functions which also have higher nonlinearity than that of F_n can be obtained.

Theorem 7. *Let* $1 \le k \le 2^{n-1}$, $1 \le i_1 < \ldots < i_k \le 2^{n-1}$, $1 \le j_1 < \ldots < j_k \le 2^{n-1}$. *If one of the following conditions is satisfied, then* $AI(f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}) < t+1$.

1) There exists $1 \le r \le n$, *such that* $x_{j_1,r} + \ldots + x_{j_k,r} > y_{i_1,r} + \ldots + y_{i_k,r}$.

2)If $n \equiv 1 \bmod 4$,

$$\#\{X \in \{X_{j_1},\ldots,X_{j_k}\} | wt(X) \textit{ is odd}\} > \#\{Y \in \{Y_{i_1},\ldots,Y_{i_k}\} | wt(Y) \textit{ is odd}\};$$

if $n \equiv 3 \bmod 4$,

$$\#\{X \in \{X_{j_1},\ldots,X_{j_k}\} | wt(X) \textit{ is odd}\} < \#\{Y \in \{Y_{i_1},\ldots,Y_{i_k}\} | wt(Y) \textit{ is odd}\}.$$

Proof. By Theorem 6, the first condition means that $|W_{f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}}(S)| > |W_{F_n}(S)|$ for $S = (\underbrace{0,\ldots,0}_{r-1},1,0,\ldots,0)$. Thus, we have $nl(f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}) < nl(F_n)$ by Remark 2 . Therefore, by Remark 3, we have $AI(f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}) < t+1$.

If the second condition is satisfied, then $|W_{f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}}(S)| > |W_{F_n}(S)|$ for $S = (1,1,\ldots,1)$. In the same way, the result can be proved.

Theorem 8. *Let* $f = f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ *be an* n*-variable Boolean function with AI* $t+1$. *If one of the following conditions is satisfied, then* f *has the worst nonlinearity among all* n*-variable Boolean functions with maximum AI.*

1) There exists $1 \le r \le n$, such that $x_{j_1,r} + \ldots + x_{j_k,r} = y_{i_1,r} + \ldots + y_{i_k,r}$.
2) $\#\{X \in \{X_{j_1}, \ldots, X_{j_k}\} | wt(X) \text{ is odd}\} = \#\{Y \in \{Y_{i_1}, \ldots, Y_{i_k}\} | wt(Y) \text{ is odd}\}$.

Proof. By Theorem 6, the first condition means that $|W_{f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}}(S)| = |W_{F_n}(S)|$ for $S = (\underbrace{0,\ldots,0}_{r-1},1,0,\ldots,0)$. Thus, we have $nl(f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}) \le nl(F_n)$ by Remark 2 . Therefore, by Remark 3, we have $nl(f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}) = nl(F_n)$, and the result is proved.

If the second condition is satisfied, then $|W_{f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}}(S)| = |W_{F_n}(S)|$ for $S = (1,1,\ldots,1)$. In the same way, the result can be proved.

Corollary 3. *For any $1 \le i,j \le 2^{n-1}$, if $AI(f_{(i;j)}) = t+1$ then $f_{(i;j)}$ has the worst nonlinearity among all n-variable Boolean functions with maximum AI.*

Proof. From Theorem 8, it is sufficient to consider the case of $i = 2^{n-1}, j = 1$, i.e. $X = (0,0,\ldots,0), Y = (1,1,\ldots,1)$. In this case, from the first item of Corollary 1 we have $AI(f_{(i;j)}) < t+1$ which contradicts the assumption.

Theorem 9. *If $1 \le k \le \frac{n-3}{4(n-2)}\binom{n-1}{t}$, then $nl(f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)})$ is given by*

$$2^{n-1} - \binom{n-1}{t} + 2\min\{\min_{1\le s\le n}(\sum_{r=1}^{k} y_{i_r,s} - \sum_{r=1}^{k} x_{j_r,s}), (-1)^t(N_1 - N_2)\},$$

where

$$N_1 = \#\{Y \in \{Y_{i_1},\ldots,Y_{i_k}\} | wt(Y) \text{ is odd }\},$$
$$N_2 = \#\{X \in \{X_{j_1},\ldots,X_{j_k}\} | wt(X) \text{ is odd }\}.$$

Proof. Denote $f_{(i_1,\ldots,i_k;j_1,\ldots,j_k;)}$ by f. From Theorem 6 we have,

$$|W_{F_n}(S)| - 4k \le |W_f(S)| \le |W_{F_n}(S)| + 4k.$$

Let $S, T \in \mathbb{F}_2^n$, and $wt(S) = 1$ or n, $wt(T) \notin \{1,n\}$. If $1 \le k \le \frac{n-3}{4(n-2)}\binom{n-1}{t}$, then by Remark 2,

$$|W_f(S)| \ge |W_{F_n}(S)| - 4k \ge |W_{F_n}(T)| + 4k \ge |W_f(T)|.$$

Therefore, we have $\max_{T\in\mathbb{F}_2^n}|W_f(T)| = \max_{wt(S)=1,n}|W_f(S)|$.

Case 1. $wt(S) = 1$ and $S = (\underbrace{0,\ldots,0}_{s-1},1,0,\ldots,0)$. By Theorem 6 we have

$$|W_f(S)| = 2\binom{n-1}{t} - 4(\sum_{r=1}^{k} y_{i_r,s} - \sum_{r=1}^{k} x_{j_r,s}).$$

Case 2. $wt(S) = n$. By Theorem 6 we have

$$|W_f(S)| = 2\binom{n-1}{t} - 4((-1)^t(N_1 - N_2)).$$

Hence the result follows from $nl(f) = 2^{n-1} - \frac{1}{2}\max_{S\in\mathbb{F}_2^n}|W_f(S)|$.

Now, we modify Construction 1 to construct n-variable Boolean functions with maximum AI and possibly having higher nonlinearity.

Construction 2 Step1: Select randomly an integer $1 \le k \le 2^{n-2}$ and k integers $1 \le i_1 < \ldots < i_k \le 2^{n-1}$, which satisfy

i) $\min\limits_{1\le s\le n} \sum\limits_{r=1}^{k} y_{i_r,s}$ is as large as possible;

ii) if $n \equiv 1 \bmod 4$, $\#\{Y \in \{Y_{i_1}, \ldots, Y_{i_k}\} | wt(Y)$ is odd $\}$ is as large as possible; if $n \equiv 3 \bmod 4$, $\#\{Y \in \{Y_{i_1}, \ldots, Y_{i_k}\} | wt(Y)$ is even $\}$ is as large as possible.

Step2: Find out k integers $1 \le j_1 < \ldots < j_k \le 2^{n-1}$, which satisfies

i) the j_1th, ..., j_kth column vectors of $W_{(i_1,\ldots,i_k)}$ are linearly independent;

ii) $a = \min\limits_{1\le s\le n} (\sum\limits_{r=1}^{k} y_{i_r,s} - \sum\limits_{r=1}^{k} x_{j_r,s})$ is as large as possible;

iii) if $n \equiv 1 \bmod 4$,

$$b = \#\{Y \in \{Y_{i_1}, \ldots, Y_{i_k}\} | wt(Y) \text{ is odd }\} - \#\{X \in \{X_{j_1}, \ldots, X_{j_k}\} | wt(X) \text{ is odd }\}$$

is as large as possible; if $n \equiv 3 \bmod 4$,

$$c = \#\{X \in \{X_{j_1}, \ldots, X_{j_k}\} | wt(X) \text{ is odd }\} - \#\{Y \in \{Y_{i_1}, \ldots, Y_{i_k}\} | wt(Y) \text{ is odd }\}$$

is as large as possible.

Then, the Boolean function $f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ defined by (1) has AI $t+1$ and has possibly a higher nonlinearity.

Remark 4. From Theorem 9, the function obtained by Construction 2 will has a higher nonlinearity than that of F_n if $1 \le k \le \frac{n-3}{4(n-2)}\binom{n-1}{t}$ and $a > 0$, $b > 0$ (if $n \equiv 1 \bmod 4$) or $c > 0$ (if $n \equiv 3 \bmod 4$), and it possibly has a nonlinearity equal to that of F_n if $k > \frac{n-3}{4(n-2)}$.

Further, the following theorem provides a class of n-variable Boolean functions with maximum AI which also have higher nonlinearity than that of F_n.

Theorem 10. *Let $n \equiv 3 \bmod 4$, $1 \le k \le \min\{n, \frac{n-3}{4(n-2)}\binom{n-1}{t}\}$, $Y_{i_1}, \ldots, Y_{i_k}$ belong to 0_{F_n} and their Hamming weights are $w_1, \ldots, w_k$, respectively. If*

1) $\bigoplus\limits_{r=0}^{t-1} \binom{w_i-1}{r} = 1$, $i = 1, \ldots, k$; and

2) $w_1, \ldots, w_k$ are not all odd; and

3) there exist $1 \le j_1 < \ldots < j_k \le n$, such that the j_1th, ..., j_kth columns of the matrix $\begin{pmatrix} Y_{i_1} \\ \ldots \\ Y_{i_k} \end{pmatrix}$ are linearly independent; and

4) for any $s \notin \{j_1, \ldots, j_k\}$, $y_{i_1,s} + \ldots + y_{i_k,s} \ge 1$; and for any $s \in \{j_1, \ldots, j_k\}$, $y_{i_1,s} + \ldots + y_{i_k,s} \ge 2$.

then, $AI(f_{(i_1,\ldots,i_k;j_1+1,\ldots,j_k+1)}) = t+1$ and $nl(f_{(i_1,\ldots,i_k;j_1+1,\ldots,j_k+1)}) \ge nl(F_n)+2$.

Example 5. The Boolean function defined in Example 4 has AI 4. And $nl(f) = nl(F_n) + 2$.

Finally, we obtain the following sufficient and necessary condition of Boolean functions with maximum AI which are also resilient functions.

Theorem 11. *Let $f = f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ be an n-variable Boolean function. Then, f is 1-resilient function if and only if*

$$\sum_{r=1}^{k} y_{i_r,s} - \sum_{r=1}^{k} x_{j_r,s} = \frac{1}{2}\binom{n-1}{t},$$

for $s = 1, \ldots, n$.

Corollary 4. *Let $f = f_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ be an n-variable Boolean function. Then, f is 1-resilient function and has AI $t+1$ if and only if*

$$\sum_{r=1}^{k} y_{i_r,s} - \sum_{r=1}^{k} x_{j_r,s} = \frac{1}{2}\binom{n-1}{t},$$

for $s = 1, \ldots, n$, and $W_{(i_1,\ldots,i_k;j_1,\ldots,j_k)}$ is invertible.

6 Conclusion

Possessing a high algebraic immunity is a necessary condition for Boolean functions used in stream ciphers against algebraic attacks. In this paper, some classes of $(2t+1)$-variable Boolean functions with maximum AI are obtained. Further, some necessary conditions of this kind of functions which also have higher nonlinearity are presented and thus a modified construction method is proposed to obtain such functions. Finally, a sufficient and necessary condition of $(2t+1)$-variable Boolean functions with maximum AI which are also 1-resilient is presented. However, it is still open that what is the highest nonlinearity of Boolean functions with maximum AI and how to construct Boolean functions which have maximum AI and the highest nonlinearity.

References

1. F. Armknecht. Improving fast algebraic attacks. In *FSE 2004*, volume 3017 of *Lecture Notes in Computer Science*, pages 65-82. Springer-Verlag, 2004.
2. F. Armknecht and M. Krause. Algebraic attacks on combiners with memory. In *Advances in Cryptology –CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 162-175. Springer-Verlag, 2003.
3. A. Braeken and B. Preneel. On the algebraic immunity of symmetric Boolean functions. In *INDOCRYPT 2005*, volume 3797 of *Lecture Notes in Computer Science*, pages 35-48. Springer-Verlag, 2005.
4. C. Carlet. A method of construction of balanced functions with optimum algebraic immunity. Available at http://eprint.iacr.org/2006/149.
5. N. Courtois. Fast algebraic attacks on stream ciphers with linear feedback. In *Advances in Cryptology –CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 176-194. Springer-Verlag, 2003.
6. N. Courtois and W. Meier. Algebraic attacks on stream ciphers with linear feedback. In *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 345-359. Springer-Verlag, 2003.

7. D. K. Dalai, K. C. Gupta and S. Maitra. Results on algebraic immunity for cryptographically significant Boolean functions. In *INDOCRYPT 2004*, volume 3348 of *Lecture Notes in Computer Science*, pages 92-106. Springer-Verlag, 2004.
8. D. K. Dalai, K. C. Gupta and S. Maitra. Cryptographically significant Boolean functions: construction and analysis in terms of algebraic immunity. In *FSE 2005*, volume 3557 of *Lecture Notes in Computer Science*, pages 98-111. Springer-Verlag, 2005.
9. D. K. Dalai, S. Maitra and S. Sarkar. Basic theory in construction of Boolean functions with maximum possible annihilator immunity. *Designs, Codes and Cryptography*, 40:41-58, 2006.
10. D. K. Dalai and S. Maitra. Reducing the Number of Homogeneous Linear Equations in Finding Annihilators. Available at http://eprint.iacr.org/2006/032.
11. C. Ding, G. Xiao and W. Shan. *The stability theory of stream ciphers.* Springer-Verlag, 1991.
12. N. Li and W. F. Qi. Symmetric Boolean functions depending on an odd number of variables with maximum algebraic immunity. *IEEE Transaction on Information Theory*, 52(5):2271-2273, May 2006.
13. N. Li and W. F. Qi. Construction and count of Boolean functions of an odd number of variables with maximum algebraic immunity. Available at http://arxiv.org/abs/cs.CR/0605139.
14. M. Lobanov. Tight bound between nonlinearity and algebraic immunity. Available at http://eprint.iacr.org/2005/441.
15. F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes.* Elsevier, North-Holland, 1977.
16. W. Meier, E. Pasalic and C. Carlet. Algebraic attacks and decomposition of Boolean functions. In *Advances in Cryptology –EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 474-491. Springer-Verlag, 2004.