Construction of Rotation Symmetric Boolean Functions with Maximum Algebraic Immunity on Odd Number of Variables

Sumanta Sarkar and Subhamoy Maitra

Applied Statistics Institute
Indian Statistical Institute
203 B T Road, Kolkata 700108, India
Email: {sumanta_r, subho}@isical.ac.in

Abstract. In this paper we present a theoretical construction of Rotation Symmetric Boolean Functions (RSBFs) on odd number of variables with maximum possible AI and further these functions are not symmetric. Our RSBFs are of better nonlinearity than the existing theoretical constructions with maximum possible AI . To get very good nonlinearity, which is important for practical cryptographic design, we generalize our construction to a construction cum search technique in the RSBF class. We find 7, 9, 11 variable RSBFs with maximum possible AI having nonlinearities 56, 240, 984 respectively with very small amount of search after our basic construction.

Keywords: Algebraic Immunity, Boolean Function, Nonlinearity, Nonsingular Matrix, Rotational Symmetry, Walsh Spectrum.

1 Introduction

Algebraic attack has received a lot of attention recently in studying the security of Stream ciphers as well as Block ciphers [1, 3, 4, 6, 7, 11, 10, 8, 23, 2, 18, 9]. One necessary condition to resist this attack is that the Boolean function used in the cipher should have good algebraic immunity (AI). It is known [10, 33] that for any n-variable Boolean function, maximum possible AI is $\lceil \frac{n}{2} \rceil$.

So far a few theoretical constructions of Boolean functions with optimal AI have been presented in the literature. In [14], the first ever construction of Boolean functions with maximum AI was proposed. Later, the construction of Symmetric Boolean functions with maximum AI was given in [17, 5]. For odd number of input variables, majority functions are the examples of symmetric functions with maximum AI . Recently in [25], the idea of modifying symmetric functions to get other functions with maximum AI is proposed using the technique of [16].

An n-variable Boolean function which is invariant under the action of the cyclic group C_n on the set $\{0, 1\}^n$ is called Rotation Symmetric Boolean functions (RSBFs). We denote the class of all n-variable RSBFs as $S(C_n)$. On the other hand, an n-variable Symmetric Boolean function is one which is invariant under the action of the Symmetric group S_n on the set $\{0,1\}^n$ and we denote the class of all n-variable Symmetric Boolean functions as $S(S_n)$. The class $S(C_n)$ has been shown to be extremely rich as the class contains Boolean functions with excellent cryptographic as well as combinatorial significance [12, 15, 19, 21, 20, 22, 30, 31, 34, 36, 37]. As for example, in [21, 22], 9-variable Boolean functions with nonlinearity 241 have been discovered in $S(C_9)$ which had been open for a long period. Also an RSBF has a short representation which is interesting for the design purpose of ciphers. Since $C_n \subset S_n$, we have $S(S_n) \subset S(C_n)$. Therefore all the Symmetric functions with maximum AI are also examples of RSBFs with maximum AI . The class $S(C_n) \setminus S(S_n)$ becomes quite huge for larger n. However, so far there has been no known construction method available which gives n-variable RSBFs belonging to $S(C_n) \setminus S(S_n)$, having the maximum AI . It has been proved in [26, 35], that the majority function is the only possible symmetric Boolean function on odd number of variables which has maximum AI . Hence, there is a need to get a theoretical construction method which provides new class of RSBFs with maximum AI , which are not symmetric.

In this paper we present a construction method (Construction 1) that generates RSBFs on odd variables (≥ 5) with maximum AI , which are not symmetric. Note that up to 3 variables, RSBFs are all symmetric, and that is the reason we concentrate on $n \geq 5$. In this construction, n-variable majority function is considered and its outputs are toggled at the inputs of the orbits of size $\lfloor \frac{n}{2} \rfloor$ and $\lceil \frac{n}{2} \rceil$ respectively. These orbits are chosen in such a manner that a sub matrix associated to these points is nonsingular. This idea follows the work of [16], where the sub matrix was introduced to reduce the complexity for determining AI of a Boolean function. We also show that the functions of this class have nonlinearity $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor} + 2$ which is better than $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$, the lower bound [27] on nonlinearity of any n (odd) variable function with maximum AI ; further the general theoretical constructions [14, 17, 5] could only achieve this lower bound so far.

We present a generalization of the Construction 1 in Construction 2 which is further generalized in Construction 3. In each of the generalizations we release the restrictions on choosing orbits and achieve better nonlinearity of the constructed RSBFs with maximum AI . We present instances of RSBFs having nonlinearities equal to or slightly less than $2^{n-1} - 2^{\frac{n-1}{2}}$ for odd n, $5 \leq n \leq 15$.

2 Basics of Boolean functions

Let us denote $V_n = \{0,1\}^n$. An n-variable Boolean function f can be seen as a mapping $f : V_n \rightarrow V_1$. By truth table of a Boolean function on n input variables $(x_1, \ldots, x_n)$, we mean the 2^n length binary string

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

We denote the set of all n-variable Boolean functions as $\mathcal{B}_n$. Obviously $|\mathcal{B}_n| = 2^{2^n}$. The *Hamming weight* of a binary string T is the number of 1's in T, denoted by $wt(T)$. An n-variable Boolean function f is said to be *balanced* if its truth table contains an equal number of 0's and 1's, i.e., $wt(f) = 2^{n-1}$. Also, the *Hamming distance* between two equidimensional binary strings T_1 and T_2 is defined by $d(T_1, T_2) = wt(T_1 \oplus T_2)$, where $\oplus$ denotes the addition over $GF(2)$. Support of f denoted by *supp*(f) is the set of inputs $x \in V_n$ such that $f(x) = 1$.

An n-variable Boolean function $f(x_1, \ldots, x_n)$ can be considered to be a multivariate polynomial over $GF(2)$. This polynomial can be expressed as a sum of products representation of all distinct k-th order products $(0 \leq k \leq n)$ of the variables. More precisely, $f(x_1, \ldots, x_n)$ can be written as

$$a_0 \oplus \bigoplus_{1 \leq i \leq n} a_i x_i \oplus \bigoplus_{1 \leq i < j \leq n} a_{ij} x_i x_j \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where the coefficients $a_0, a_i, a_{ij}, \ldots, a_{12\ldots n} \in \{0, 1\}$. This representation of f is called the *algebraic normal form* (ANF) of f. The number of variables in the highest order product term with nonzero coefficient is called the *algebraic degree*, or simply the degree of f and denoted by $deg(f)$.

Let $x = (x_1, \ldots, x_n)$ and $\omega = (\omega_1, \ldots, \omega_n)$ both belonging to V_n and $x \cdot \omega = x_1\omega_1 \oplus \ldots \oplus x_n\omega_n$. Let $f(x)$ be a Boolean function on n variables. Then the *Walsh transform* of $f(x)$ is an integer valued function over V_n which is defined as

$$W_f(\omega) = \sum_{x \in V_n} (-1)^{f(x) \oplus x \cdot \omega}.$$

The Walsh spectrum of f is the multiset $\{W_f(\omega) | \omega \in V_n\}$. In terms of Walsh spectrum, the nonlinearity of f is given by

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in V_n} |W_f(\omega)|.$$

Symmetric Boolean functions n-variable are the ones which are invariant under the action of the Symmetric group S_n on V_n, i.e., for $\mu, \nu \in V_n$, if $wt(\mu) = wt(\nu)$ then $f(\mu) = f(\nu)$. In [17], analysis of the Walsh spectra of the Symmetric functions has been done in terms of Krawtchouk polynomial. Krawtchouk polynomial [28, Page 151, Part I] of degree i is given by $K_i(k, n) = \sum_{j=0}^{i} (-1)^j \binom{k}{j} \binom{n-k}{i-j}$, $i = 0, 1, \ldots, n$. It is known that for a fixed $\omega \in V_n$, such that $wt(\omega) = k$, $\sum_{wt(x)=i} (-1)^{\omega \cdot x} = K_i(k, n)$. Thus it can be checked that if f is an n-variable Symmetric function, then for $wt(\omega) = k$, $W_f(\omega) = \sum_{i=0}^{n} (-1)^{re_f(i)} K_i(k, n)$, where $re_f(i)$ is the value of f at an input of weight i. It is also known that for a symmetric function f on n variables and $\mu, \nu \in V_n$, $W_f(\mu) = W_f(\nu)$, if $wt(\mu) = wt(\nu)$. Note that $K_i(k, n)$ is the (i, k)-th element of the Krawtchouk matrix (KR_M) of order $(n+1) \times (n+1)$. Thus Walsh spectrum of f can be determined as $(ref[0], \ldots, ref[n]) \times (KR_M[0], \ldots, KR_M[n])$, where each $KR_M[k]$, $(0 \leq k \leq n)$ is a column vector of KR_M.

A nonzero n-variable Boolean function g is called an annihilator of an n-variable Boolean function f if $f * g = 0$. We denote the set of all annihilators of f by $AN(f)$. Then algebraic immunity of f, denoted by $\mathcal{AI}_n(f)$, is defined [33] as the degree of the minimum degree annihilator among all the annihilators of f or $1 \oplus f$, i.e., $\mathcal{AI}_n(f) = \min\{\deg(g) : g \neq 0,\ g \in AN(f) \cup AN(1 \oplus f)\}$. We repeat that the maximum possible algebraic immunity of f is $\lceil \frac{n}{2} \rceil$.

2.1 Rotation Symmetric Boolean Functions

We consider the action of the Cyclic group C_n on the set V_n. Let $x = (x_1, \ldots, x_n)$ be an element of V_n and $\rho_n^i \in C_n$, where $i \geq 0$. Then C_n acts on V_n as follows,

$$\rho_n^i(x_1, x_2, \ldots, x_{n-1}, x_n) = (x_{1+i}, x_{2+i}, \ldots, x_{n-1+i}, x_{n+i}),$$

where $k + i$ $(1 \leq k \leq n)$ takes the value $k + i \bmod n$ with the only exception that when $k + i \equiv 0 \bmod n$, then we will assign $k + i \bmod n$ by n instead of 0. This is to cope up with the input variable indices $1, \ldots, n$ for $x_1, \ldots, x_n$. An n-variable Boolean function f is called *Rotation Symmetric Boolean function (RSBF)* if it is invariant under the action of C_n, i.e., for each input $(x_1, \ldots, x_n) \in V_n$, $f(\rho_n^i(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n)$ for $1 \leq i \leq n - 1$. We denote the orbit generated by $x = (x_1, \ldots, x_n)$ under this action as O_x, therefore, $O_x = \{\rho_n^i(x_1, \ldots, x_n) | 1 \leq i \leq n\}$ and the number of such orbits is denoted by g_n. Thus the number of n-variable RSBFs is 2^{g_n}. Let ϕ be Euler's *phi*-function, then it can be shown by Burnside's lemma that (see also [36]) $g_n = \frac{1}{n} \sum_{k|n} \phi(k)\, 2^{\frac{n}{k}}$.

An *orbit* is completely determined by its *representative element* $\Lambda_{n,i}$, which is the lexicographically first element belonging to the orbit [37] and we define the weight of the orbit is exactly the same as weight of the representative element. These representative elements are again arranged lexicographically as $\Lambda_{n,0}, \ldots, \Lambda_{n,g_n-1}$. Note that for any n, $\Lambda_{n,0} = (0, 0, \ldots, 0)$ (the all zero input), $\Lambda_{n,1} = (0, 0, \ldots, 1)$ (the input of weight 1) and $\Lambda_{n,g_n-1} = (1, 1, \ldots, 1)$ (the all 1 input). Thus an n-variable RSBF f can be represented by the g_n length string $f(\Lambda_{n,0}), \ldots, f(\Lambda_{n,g_n-1})$ which we call RSTT of f and denote it by $RSTT_f$.

In [37] it was shown that the Walsh spectrum of an RSBF f takes the same value for all elements belonging to the same orbit, i.e., $W_f(\mu) = W_f(\nu)$ if $\mu \in O_\nu$. Therefore the Walsh spectrum of f can be represented by the g_n length vector $(wa_f[0], \ldots, wa_f[g_n])$ where $wa_f[j] = W_f(\Lambda_{n,j})$. In analyzing the Walsh spectrum of an RSBF, the ${}_n\mathcal{A}$ matrix has been introduced [37]. The matrix ${}_n\mathcal{A} = ({}_n\mathcal{A}_{i,j})_{g_n \times g_n}$ is defined as ${}_n\mathcal{A}_{i,j} = \sum_{x \in O_{\Lambda_{n,i}}} (-1)^{x \cdot \Lambda_{n,j}}$, for an n-variable RSBF. Using this $g_n \times g_n$ matrix, the Walsh spectrum for an RSBF can be calculated as $W_f(\Lambda_{n,j}) = \sum_{i=0}^{g_n-1} (-1)^{f(\Lambda_{n,i})}\, {}_n\mathcal{A}_{i,j}$.

Let's have an example.

Example 1. Take $n = 5$. Then $g_n = 8$. The orbit representative elements are respectively $\{(0,0,0,0,0), (0,0,0,0,1), (0,0,0,1,1), (0,0,1,0,1), (0,0,1,1,1), (0,1,0,1,1), (0,1,1,1,1), (1,1,1,1,1)\}$. Then the matrix ${}_n\mathcal{A}$ is as follows

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 5 & 3 & 1 & 1 & -1 & -1 & -3 & -5 \\ 5 & 1 & 1 & -3 & 1 & -3 & 1 & 5 \\ 5 & 1 & -3 & 1 & -3 & 1 & 1 & 5 \\ 5 & -1 & 1 & -3 & -1 & 3 & 1 & -5 \\ 5 & -1 & -3 & 1 & 3 & -1 & 1 & -5 \\ 5 & -3 & 1 & 1 & 1 & 1 & -3 & 5 \\ 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 \end{bmatrix}$$

3 Existing results related to annihilators

We take the degree graded lexicographic order "$<^{dgl}$" on the set of all monomials on n-variables $\{x_{m_1} \dots x_{m_k} : 1 \leq k \leq n, 1 \leq m_1, \dots, m_k \leq n\}$, i.e., $x_{m_1} x_{m_2} \dots x_{m_k} < x_{r_1} x_{r_2} \dots x_{r_l}$ if either $k < l$ or $k = l$ and there is $1 \leq p \leq k$ such that $m_k = r_k$, $m_{k-1} = r_{k-1}, \dots, m_{p+1} = r_{p+1}$ and $m_p < r_p$. For example, for $n = 7$, $x_1 x_3 x_6 <^{dgl} x_1 x_2 x_4 x_5$ and $x_1 x_3 x_6 <^{dgl} x_1 x_4 x_6$.

Let $v_{n,d}(x) = (m_1(x), m_2(x), \dots, m_{\sum_{i=0}^{d} \binom{n}{i}}(x))$, where $m_i(x)$ is the i-th monomial as in the order ($<^{dgl}$) evaluated at the point $x = (x_1, x_2, \dots, x_n)$.

Definition 1. *Given a Boolean function f on n-variables, let $M_{n,d}(f)$ be the $wt(f) \times \sum_{i=0}^{d} \binom{n}{i}$ matrix defined as*

$$M_{n,d}(f) = \begin{bmatrix} v_{n,d}(P_1) \\ v_{n,d}(P_2) \\ \vdots \\ v_{n,d}(P_{wt(f)}) \end{bmatrix}$$

where $0 \leq d \leq n$, $P_i \in supp(f)$, $1 \leq i \leq wt(f)$ and $P_1 <^{dgl} P_2 <^{dgl} \cdots <^{dgl} P_{wt(f)}$.

Let f be an n-variable Boolean function. Let a nonzero n-variable function g be an annihilator of f, i.e., $f(x_1, \dots, x_n) * g(x_1, \dots, x_n) = 0$ for all $(x_1, \dots, x_n) \in V_n$. That means,

$$g(x_1, \dots, x_n) = 0 \text{ if } f(x_1, \dots, x_n) = 1. \tag{1}$$

If the degree of the function g is less than equal to d, then the ANF of g is of the form

$$g(x_1, \dots, x_n) = a_0 + \sum_{i=0}^{n} a_i x_i + \cdots + \sum_{1 \leq i_1 < i_2 \cdots < i_d \leq n} a_{i_1, \dots, i_d} x_{i_1} \cdots x_{i_d},$$

where $a_0, a_1, \dots, a_{12}, \dots a_{n-d+1, \dots, n}$ are from $\{0, 1\}$ not all zero. Then the relation 1 gives a homogeneous linear equation

$$a_0 + \sum_{i=0}^{n} a_i x_i + \cdots + \sum_{1 \leq i_1 < i_2 \cdots < i_d \leq n} a_{i_1, \dots, i_d} x_{i_1} \cdots x_{i_d} = 0, \tag{2}$$

with $a_0, a_1, \ldots, a_{12}, \ldots a_{n-d+1,\ldots,n}$ as variables for each input $(x_1, \ldots, x_n) \in supp(f)$ and thus $wt(f)$ homogeneous linear equations in total. If this system of equations has a nonzero solution, then g having the coefficients in its ANF which is the solution of this system of equations is an annihilator of f of degree less than or equal to d. Note that in this system of equations $M_{n,d}(f)$ is the coefficient matrix. Then it is clear that if the rank of $M_{n,d}(f)$ is equal to $\sum_{i=0}^{d} \binom{n}{i}$, f does not posses any annihilator. If for $d = \lfloor \frac{n}{2} \rfloor$, both of f and $1 \oplus f$ do not have any annihilator of degree less than or equal to d, then f has maximum algebraic, i.e., $\lceil \frac{n}{2} \rceil$.

Theorem 1. *[16] Let g be an n-variable Boolean function defined as $g(x) = 1$ if and only if $wt(x) \leq d$ for $0 \leq d \leq n$. Then $M_{n,d}(g)^{-1} = M_{n,d}(g)$, i.e., $M_{n,d}(g)$ is a self inverse matrix.*

3.1 Existence of RSBFs with maximum AI on odd variables

Let us start with a few available results on n-variable Boolean functions with maximum AI . Henceforth we will consider the $<^{dgl}$ ordering of the inputs of V_n unless stated.

Proposition 1. *[13] An odd variable Boolean function with maximum* AI *must be balanced.*

Proposition 2. *[24] Let f be an n (odd) variable Boolean function. Then* AI *of f is $\lceil \frac{n}{2} \rceil$ if and only if f is balanced and $M_{n,\lceil \frac{n}{2} \rceil - 1}(f)$ has full rank.*

Definition 2. *The n (odd) variable Boolean function f with*

$$f(X) = \begin{cases} a \text{ if } wt(X) \leq \lceil \frac{n}{2} \rceil - 1, \\ a \oplus 1 \text{ if } wt(X) \geq \lceil \frac{n}{2} \rceil. \end{cases}$$

is called the Majority function.

Note that the Majority function is a Symmetric Boolean function and it has been proved [5, 17] that this function has maximum algebraic immunity, i.e., $\lceil \frac{n}{2} \rceil$. We take $a = 1$ and call the corresponding n-variable Majority function as G_n. Weight of this function is 2^{n-1}. Then both of the matrices $M_{n,\lceil \frac{n}{2} \rceil - 1}(G_n)$ and $M_{n,\lceil \frac{n}{2} \rceil - 1}(1 \oplus G_n)$ are of the order $2^{n-1} \times 2^{n-1}$ and nonsingular. Now we take a look at a construction of an n-variable Boolean function having maximum AI by modifying some outputs of the Majority function G_n.

Let $\{X_1, \ldots, X_{2^{n-1}}\}$ and $\{Y_1, \ldots, Y_{2^{n-1}}\}$ be the support of G_n and $1 \oplus G_n$ respectively. Suppose $X^j = \{X_{j_1}, \ldots, X_{j_k}\}$ and $Y^i = \{Y_{i_1}, \ldots, Y_{i_k}\}$. Construct the function F_n as

$$F_n(X) = \begin{cases} 1 \oplus G_n(X), \text{ if } X \subset X^j \cup Y^i, \\ G_n(X), \text{ elsewhere.} \end{cases}$$

In rest of the paper, we denote an n-variable Boolean function constructed as above by F_n.

Proposition 3. *The function F_n has maximum* AI *if and only if the two k-sets X^j and Y^i be such that $M_{n,\lceil \frac{n}{2} \rceil -1}(F_n)$ is nonsingular.*

Proof. It follows from Proposition 2. □

This idea was first proposed in [16] and using this idea, a few classes of Boolean functions on odd variables with maximum AI have been demonstrated in [25].

Let's have a quick look at a result from linear algebra.

Theorem 2. *Let V be a vector space over the field F of dimension τ and $\{\alpha_1, \ldots, \alpha_\tau\}$ and $\{\beta_1, \ldots, \beta_\tau\}$ are two bases of V. Then for any k $(1 \leq k \leq \tau)$, there will be a pair of k-sets $\{\beta_{a_1}, \ldots, \beta_{a_k}\}$ and $\{\alpha_{b_1}, \ldots, \alpha_{b_k}\}$ such that the set $\{\alpha_1, \ldots, \alpha_\tau\} \cup \{\beta_{a_1}, \ldots, \beta_{a_k}\} \setminus \{\alpha_{b_1}, \ldots, \alpha_{b_k}\}$ will be a basis of V.*

The row vectors $v_{n,\lfloor \frac{n}{2} \rfloor}(X_1), \ldots, v_{n,\lfloor \frac{n}{2} \rfloor}(X_{2^{n-1}})$ of $M_{n,\lfloor \frac{n}{2} \rfloor}(G_n)$ form a basis of the vector space V_{n-1}. Similarly the row vectors $v_{n,\lfloor \frac{n}{2} \rfloor}(Y_1), \ldots, v_{n,\lfloor \frac{n}{2} \rfloor}(Y_{2^{n-1}})$ of $M_{n,\lfloor \frac{n}{2} \rfloor}(1 \oplus G_n)$ also form a basis of the vector space V_{n-1}. By finding two k-sets (which always exist by Theorem 2) $\{v_{n,\lfloor \frac{n}{2} \rfloor}(X_{j_1}), \ldots, v_{n,\lfloor \frac{n}{2} \rfloor}(X_{j_k})\}$ and $\{v_{n,\lfloor \frac{n}{2} \rfloor}(Y_{i_1}), \ldots, v_{n,\lfloor \frac{n}{2} \rfloor}(Y_{i_k})\}$, one can construct an n-variable Boolean function F_n with maximum algebraic immunity if and only if the corresponding matrix $M_{n,\lfloor \frac{n}{2} \rfloor}(F_n)$ is nonsingular. Complexity of checking the nonsingularity of the matrix $M_{n,\lfloor \frac{n}{2} \rfloor}(F_n)$ is $O((\sum_{t=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{t})^3)$, i,e., this construction will take huge time for larger n. But this task can be done with lesser effort by forming a matrix, $W = M_{n,\lfloor \frac{n}{2} \rfloor}(1 \oplus G_n) \times (M_{n,\lfloor \frac{n}{2} \rfloor}(G_n))^{-1}$ and checking a sub matrix of it. Since $(M_{n,\lfloor \frac{n}{2} \rfloor}(G_n))^{-1} = M_{n,\lfloor \frac{n}{2} \rfloor}(G_n)$, then $W = M_{n,\lfloor \frac{n}{2} \rfloor}(1 \oplus G_n) \times M_{n,\lfloor \frac{n}{2} \rfloor}(G_n)$. We have the following proposition.

Proposition 4. *[16] Let A be a nonsingular $m \times m$ binary matrix where the row vectors are denoted as $v_1, \ldots, v_m$. Let U be a $k \times m$ matrix, $k \leq m$, where the vectors are denoted as $u_1, \ldots, u_k$. Let $Z = UA^{-1}$, be a $k \times m$ binary matrix. Consider that a matrix A' is formed from A by replacing the rows $v_{i_1}, \ldots, v_{i_k}$ of A by the vectors $u_1, \ldots, u_k$. Further consider the $k \times k$ matrix Z' is formed by taking the j_1-th, j_2-th, …, j_k-th columns of Z. Then A' is nonsingular if and only if Z' is nonsingular.*

From the construction of F_n it is clear that it is balanced. Now construct the matrix $W = M_{n,\lfloor \frac{n}{2} \rfloor}(1 \oplus G_n) \times M_{n,\lfloor \frac{n}{2} \rfloor}(G_n)$. Consider A to be the matrix $M_{n,\lfloor \frac{n}{2} \rfloor}(G_n)$ and let U be the matrix formed by i_1-th, …, i_k-th rows of $M_{n,\lfloor \frac{n}{2} \rfloor}(1 \oplus G_n)$ which are the row vectors $v_{n,\lfloor \frac{n}{2} \rfloor}(Y_{i_1}), \ldots, v_{n,\lfloor \frac{n}{2} \rfloor}(Y_{i_k})$ respectively. Now replace the j_1-th, …, j_k-th rows of $M_{n,\lfloor \frac{n}{2} \rfloor}(G_n)$ which are respectively the row vectors $v_{n,\lfloor \frac{n}{2} \rfloor}(X_{j_1}), \ldots, v_{n,\lfloor \frac{n}{2} \rfloor}(X_{j_k})$ by the rows of U and form the new matrix A'. Note that A' is exactly the $M_{n,\lfloor \frac{n}{2} \rfloor}(F_n)$ matrix. Let $W_{|Y^i| \times |X^j|}$ be the matrix formed by taking i_1-th, …, i_k-th rows and j_1-th, …, j_k-th columns of W. Then $M_{n,\lfloor \frac{n}{2} \rfloor}(F_n)$ is nonsingular if and only if $W_{|Y^i| \times |X^j|}$ is nonsingular. Thus we have the following theorem.

Theorem 3. *The function F_n has maximum algebraic immunity if and only if the sub matrix $W_{|Y^i| \times |X^j|}$ is nonsingular.*

The following proposition characterizes W.

Proposition 5. *[16] The (q,p)-th element of the matrix W is given by*

$$W_{(q,p)} = \begin{cases} 0, \ \textit{if}\ WS(X_p) \not\subseteq WS(Y_q), \\ \displaystyle\sum_{t=0}^{\lfloor \frac{n}{2} \rfloor - wt(X_p)} \binom{wt(Y_q) - wt(X_p)}{t} \bmod 2, \ \textit{else} \ ; \end{cases}$$

where $WS((x_1,\ldots,x_n)) = \{i : x_i = 1\} \subseteq \{1,\ldots,n\}$.

4 New class of RSBFs with maximum AI

Since up to 3 variables all the RSBFs are symmetric, we consider $n \geq 5$.

Proposition 6. *Given odd n, all the orbits O_μ generated by $\mu = (\mu_1,\ldots,\mu_n) \in V_n$ of weight $\lfloor \frac{n}{2} \rfloor$ or $\lceil \frac{n}{2} \rceil$ have n elements.*

Proof. From [36], it is known that if $gcd(n, wt(\mu)) = 1$, then the orbit O_μ contains n elements. Since $gcd(n, \lfloor \frac{n}{2} \rfloor) = gcd(n, \lceil \frac{n}{2} \rceil) = 1$, the result follows. □

Now we present the construction.

Construction 1

1. *Take odd $n \geq 5$.*
2. *Take an element $x \in V_n$ of weight $\lfloor \frac{n}{2} \rfloor$ and generate the orbit O_x.*
3. *Choose an orbit O_y by an element $y \in V_n$ of weight $\lceil \frac{n}{2} \rceil$ such that*

   for each $x' \in O_x$ there is a unique $y' \in O_y$ where $WS(x') \subset WS(y')$.
4. *Construct*

$$R_n(X) = \begin{cases} G_n(X) \oplus 1, \ \textit{if}\ X \in O_x \cup O_y, \\ G_n(X), \ \textit{elsewhere} \ . \end{cases}$$

Henceforth, we will consider R_n as the function on n (≥ 5 and odd) variables obtained from Construction 1. We have the following theorem.

Theorem 4. *The function R_n is an n-variable RSBF with maximum AI .*

Proof. R_n is obtained by toggling all outputs of G_n corresponding to the inputs belonging to the two orbits O_x and O_y. Therefore R_n is an RSBF on n variables. By Proposition 6, we have $|O_x| = |O_y|$. Also it is clear that $G_n(X) = 1$ for all $X \in O_x$ and $G_n(X) = 0$ for all $X \in O_y$. So $wt(R_n) = 2^{n-1} - |O_x| + |O_y| = 2^{n-1}$. Thus R_n is a balanced RSBF on n-variables.

Let us now investigate the matrix $W_{|O_y| \times |O_x|}$. We reorder the elements in O_x and O_y as $x^{(1)},\ldots,x^{(|O_x|)}$ and $y^{(1)},\ldots,y^{(|O_y|)}$ respectively where $WS(x^{(p)}) \subset WS(y^{(p)})$, for all $1 \leq p \leq |O_x| = |O_y|$. As $WS(x^{(p)}) \not\subseteq WS(y^{(q)})$ for all $q \in \{1,\ldots,|O_y|\} \setminus \{p\}$, then by Proposition 5, the value of $W_{(q,p)} = 0$, for all $q \in$

$\{1, \ldots, |O_y|\} \backslash \{p\}$. Again by Proposition 5, the value of $W_{(p,p)}$ can be determined as

$$W_{(p,p)} = \sum_{t=0}^{\lfloor \frac{n}{2} \rfloor - wt(x^{(p)})} \binom{wt(y^{(p)}) - wt(x^{(p)})}{t} = \sum_{t=0}^{\lfloor \frac{n}{2} \rfloor - \lfloor \frac{n}{2} \rfloor} \binom{\lceil \frac{n}{2} \rceil - \lfloor \frac{n}{2} \rfloor}{t} = 1.$$

Thus the matrix $W_{|O_y| \times |O_x|}$ is a diagonal matrix where all the diagonal elements are all equal to 1. Hence $W_{|O_y| \times |O_x|}$ is nonsingular. Therefore Theorem 3 implies that R_n has maximum AI . □

Example 2. Take $n = 5$. Consider $x = (1, 0, 0, 1, 0)$ and $y = (1, 0, 0, 1, 1)$ and generate the orbits

$$\begin{aligned} O_x &= \{(1,0,0,1,0), (0,1,0,0,1), (1,0,1,0,0), (0,1,0,1,0), (0,0,1,0,1)\} \text{ and} \\ O_y &= \quad \{(1,0,0,1,1), (1,1,0,0,1), (1,1,1,0,0), (0,1,1,1,0), (0,0,1,1,1)\}. \end{aligned}$$

Here, for each $x' \in O_x$, there is a unique $y' \in O_y$ such that $WS(x') \subset WS(y')$. Precisely,

$$\begin{aligned} &WS((1,0,0,1,0)) \subset WS((1,0,0,1,1)), WS((0,1,0,0,1)) \subset WS((1,1,0,0,1)), \\ &WS((1,0,1,0,0)) \subset WS((1,1,1,0,0)), WS((0,1,0,1,0)) \subset WS((0,1,1,1,0)), \\ &WS((0,0,1,0,1)) \subset WS((0,0,1,1,1)). \end{aligned}$$

Therefore by Theorem 4, the function

$$R_n(X) = \begin{cases} G_n(X) \oplus 1, & \text{if } X \in O_x \cup O_y, \\ G_n(X), & \text{elsewhere }, \end{cases}$$

is a 5-variable RSBF with maximum AI , i.e., 3.

It is known [27] that for an n (odd) variable Boolean function f with maximum AI , we have $nl(f) \geq 2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$. Therefore nonlinearity of the function R_n will be at least $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$. Let us now examine the exact nonlinearity of R_n.

Theorem 5. *The nonlinearity of the function R_n is $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor} + 2$.*

Proof. As per the assumptions of Construction 1, $n \geq 5$ and it is odd; and weights of the orbits O_x and O_y are respectively $\lfloor \frac{n}{2} \rfloor$ and $\lceil \frac{n}{2} \rceil$. Now G_n being a symmetric function, it is also RSBF. So R_n can be viewed as a function, which is obtained by toggling the outputs of the RSBF G_n corresponding to the orbit O_x and O_y. From [17], we know that $nl(G_n) = 2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$. Also it is known that the maximum absolute Walsh spectrum value of G_n, i.e., $2\binom{n-1}{\lfloor \frac{n}{2} \rfloor}$ occurs at the inputs corresponding to the orbits of weight 1 and n. We denote an element of V_n by Λ^n. Note that when, $wt(\Lambda^n) = n$, the value of $W_{G_n}(\Lambda^n)$ is $-2\binom{n-1}{\lfloor \frac{n}{2} \rfloor}$ or $2\binom{n-1}{\lfloor \frac{n}{2} \rfloor}$ according as $\lfloor \frac{n}{2} \rfloor$ is even or odd, and for $(wt(\Lambda^n) = 1)$, $W_{G_n}(\Lambda^n) = -2\binom{n-1}{\lfloor \frac{n}{2} \rfloor}$.

Let us first find the relation between the values of $W_{R_n}(\Lambda^n)$ and $W_{G_n}(\Lambda^n)$.

$$\begin{aligned}
W_{R_n}(\Lambda^n) = & \sum_{\zeta \in V_n \setminus \{O_x \cup O_y\}} (-1)^{R_n(\zeta)}(-1)^{\zeta\cdot\Lambda^n} + \sum_{\zeta\in O_x} (-1)^{R_n(\zeta)}(-1)^{\zeta\cdot\Lambda^n} \\
& + \sum_{\zeta\in O_y} (-1)^{R_n(\zeta)}(-1)^{\zeta\cdot\Lambda^n} \\
= & \sum_{\zeta \in V_n \setminus \{O_x \cup O_y\}} (-1)^{G_n(\zeta)}(-1)^{\zeta\cdot\Lambda^n} + \sum_{\zeta\in O_x} (-1)^{1\oplus G_n(\zeta)}(-1)^{\zeta\cdot\Lambda^n} \\
& + \sum_{\zeta\in O_y} (-1)^{1\oplus G_n(\zeta)}(-1)^{\zeta\cdot\Lambda^n} \\
= & \sum_{\zeta \in V_n \setminus \{O_x \cup O_y\}} (-1)^{G_n(\zeta)}(-1)^{\zeta\cdot\Lambda^n} - \sum_{\zeta\in O_x} (-1)^{G_n(\zeta)}(-1)^{\zeta\cdot\Lambda^n} \\
& - \sum_{\zeta\in O_y} (-1)^{G_n(\zeta)}(-1)^{\zeta\cdot\Lambda^n} \\
= & \sum_{\zeta\in V_n} (-1)^{G_n(\zeta)}(-1)^{\zeta\cdot\Lambda^n} - 2\sum_{\zeta\in O_x} (-1)^{1}(-1)^{\zeta\cdot\Lambda^n} - 2\sum_{\zeta\in O_y} (-1)^{0}(-1)^{\zeta\cdot\Lambda^n} \\
= & W_{G_n}(\Lambda^n) + 2\sum_{\zeta\in O_x} (-1)^{\zeta\cdot\Lambda^n} - 2\sum_{\zeta\in O_y} (-1)^{\zeta\cdot\Lambda^n} \qquad (3)
\end{aligned}$$

Consider that $wt(\Lambda^n) = 1$. It can be proved that for any two orbits O_μ and O_ν of weight $\lfloor \frac{n}{2} \rfloor$ and $\lceil \frac{n}{2} \rceil$ respectively, $\sum_{\zeta\in O_\mu}(-1)^{\zeta\cdot\Lambda} = 1$ and $\sum_{\zeta\in O_\nu}(-1)^{\zeta\cdot\Lambda} = -1$. Thus $\sum_{\zeta\in O_x}(-1)^{\zeta\cdot\Lambda} = 1$ and $\sum_{\zeta\in O_y}(-1)^{\zeta\cdot\Lambda} = -1$. Therefore from Equation 3 we get, $W_{R_n}(\Lambda^n) = -2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} + 4$.

Let us now check the Walsh spectrum value $W_{R_n}(\Lambda^n)$ for $wt(\Lambda^n) = n$. We do it in the following two cases.

CASE I : $\lfloor \frac{n}{2} \rfloor$ is even.

We have, $\sum_{\zeta\in O_x}(-1)^{\zeta\cdot\Lambda^n} = |O_x| = n$, since $\zeta\cdot\Lambda^n$ is $\lfloor \frac{n}{2} \rfloor$ which is even. Again for $\zeta \in O_y$, we have, $\zeta\cdot\Lambda^n = \lceil \frac{n}{2} \rceil$ which is odd, so $\sum_{\zeta\in O_y}(-1)^{\zeta\cdot\Lambda^n} = |O_y| = -n$. Therefore from Equation 3, we get $W_{R_n}(\Lambda^n) = -2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} + 2n + 2n = -2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} + 4n$.

CASE II : $\lfloor \frac{n}{2} \rfloor$ is odd.

Using the similar argument as applied in the previous case, we can show that $\sum_{\zeta\in O_x}(-1)^{\zeta\cdot\Lambda^n} = -n$ and $\sum_{\zeta\in O_y}(-1)^{\zeta\cdot\Lambda^n} = n$. Therefore from Equation 3, we get $W_{R_n}(\Lambda^n) = 2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} - 2n - 2n = 2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} - 4n$.

Note that $2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} > 4n$, except for the case $n = 5$. Therefore for both of the cases and for $n \geq 7$, $|W_{R_n}(\Lambda^n)| = 2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} - 4n$. Also $2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} - 4n < 2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} - 4$, for $n \geq 7$. This implies that $|W_{R_n}(\Lambda^n)| \leq |W_{R_n}(\Delta^n)|$ for $n \geq 7$, where $\Delta^n \in V_n$ is an input of weight 1. For $n = 5$, $2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} = 12$ and thus, $W_{R_n}(\Lambda^n) = -8 = W_{R_n}(\Delta^n)$. Therefore, $|W_{R_n}(\Lambda^n)| \leq |W_{R_n}(\Delta^n)|$ for all $n \geq 5$.

Let us check the Walsh spectrum values of R_n at the other inputs, i.e., except inputs of weight 1 and n. For $n \geq 7$, the second maximum absolute value in the Walsh spectrum of G_n occurs at the inputs of weight 3 and $n-2$. The exact value at weight 3 input is $\mathcal{C} = [\binom{n-3}{\frac{n-1}{2}} - 2\binom{n-3}{\frac{n-1}{2}-1} + \binom{n-3}{\frac{n-1}{2}-2}]$, whereas at the input of weight $n-2$, the exact value is $\mathcal{C}$ when $\lfloor \frac{n}{2} \rfloor$ is even and it is $-\mathcal{C}$ when $\lfloor \frac{n}{2} \rfloor$ is odd. Equation 3 implies that when $wt(\Lambda^n) = 3$ or $n-2$, $|W_{R_n}(\Lambda^n)|$ can attain value maximum up to $|W_{G_n}(\Lambda^n)| + 4n$, i.e., $\binom{n-3}{\frac{n-1}{2}} - 2\binom{n-3}{\frac{n-1}{2}-1} + \binom{n-3}{\frac{n-1}{2}-2} + 4n$. But it is clear that, $\binom{n-3}{\frac{n-1}{2}} - 2\binom{n-3}{\frac{n-1}{2}-1} + \binom{n-3}{\frac{n-1}{2}-2} + 4n \leq 2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} - 4 = |W_{R_n}(\Delta^n)|$.

Now looking at the Matrix ${}_n\mathcal{A}$ for $n = 5$, (Given in Example 1) we can verify that for any choice of two orbits O_x and O_y assumed in Construction 1, the absolute Walsh spectrum value of R_n, for all the inputs Λ^n of weight 3 is 8 which is equal to $|W_{R_n}(\Delta^n)|$.

Therefor for all $n \geq 5$, maximum absolute Walsh Spectrum value of R_n is $2\binom{n-1}{\lfloor \frac{n}{2} \rfloor} - 4$. Hence, $nl(R_n) = 2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor} + 2$. □

5 Generalization of Construction 1

The idea of the Construction 1 can be generalized as follows.

Construction 2 *Take orbits $O_{z_1}, \ldots, O_{z_k}$ with $G_n(z_i) = 1$, for $z_i \in V_n, 1 \leq i \leq k$ and $O_{w_1}, \ldots, O_{w_l}$ with $G_n(w_i) = 0$ for $w_i \in V_n, 1 \leq i \leq l$. Assume that,*

1. $\sum_{t=0}^{k} |O_{z_t}| = \sum_{t=0}^{l} |O_{w_t}|$.
2. *for each $x' \in \cup_{t=0}^{k} O_{z_t}$ there is a unique $y' \in \cup_{t=0}^{l} O_{w_t}$ such that $WS(x') \subset WS(y')$.*
3. $\sum_{t=0}^{\lfloor \frac{n}{2} \rfloor - wt(x')} \binom{wt(y')-wt(x')}{t}$ *is odd, for any $x' \in \cup_{t=0}^{k} O_{z_t}$ and corresponding $y' \cup_{t=0}^{l} O_{w_t}$ such that $WS(x') \subset WS(y')$.*

Then construct,

$$R'_n(X) = \begin{cases} G_n(X) \oplus 1, & \text{if } X \in \{\cup_{t=0}^{k} O_{z_t}\} \bigcup \{\cup_{t=0}^{l} O_{w_t}\} \\ G_n(X), & \text{elsewhere .} \end{cases}$$

Then we have the following theorem.

Theorem 6. *The function R'_n is an n-variable RSBF with maximum* AI .

Proof. Following the same argument as used in Theorem 4 we can prove that $W_{|\cup_{t=0}^{k} O_{z_t}| \times |\cup_{t=0}^{l} O_{w_t}|}$ is a diagonal matrix whose diagonal elements are all equal to 1, i.e., it is nonsingular. Hence the proof. □

Following is an example of an RSBF of this class.

Example 3. Take $n = 7$. Consider $z_1 = (0,0,0,1,1,0,1), z_2 = (0,0,1,0,1,0,1)$ and $w_1 = (0,0,0,1,1,1,1), w_2 = (0,0,1,0,1,1,1)$ and generate the orbits

$$\begin{aligned} O_{z_1} = \{&(0,0,0,1,1,0,1),(0,0,1,1,0,1,0),(0,1,1,0,1,0,0),(1,1,0,1,0,0,0),\\ &(1,0,1,0,0,0,1),(0,1,0,0,0,1,1),(1,0,0,0,1,1,0)\}; \end{aligned}$$

$$\begin{aligned} O_{z_2} = \{&(0,0,1,0,1,0,1),(0,1,0,1,0,1,0),(1,0,1,0,1,0,0),(0,1,0,1,0,0,1),\\ &(1,0,1,0,0,1,0),(0,1,0,0,1,0,1),(1,0,0,1,0,1,0)\}; \end{aligned}$$

$$\begin{aligned} O_{w_1} = \{&(0,0,0,1,1,1,1),(0,0,1,1,1,1,0),(0,1,1,1,1,0,0),(1,1,1,1,0,0,0),\\ &(1,1,1,0,0,0,1),(1,1,0,0,0,1,1),(1,0,0,0,1,1,1)\}; \end{aligned}$$

$$\begin{aligned} O_{w_2} = \{&(0,0,1,0,1,1,1),(0,1,0,1,1,1,0),(1,0,1,1,1,0,0),(0,1,1,1,0,0,1),\\ &(1,1,1,0,0,1,0),(1,1,0,0,1,0,1),(1,0,0,1,0,1,1)\}. \end{aligned}$$

Here for each $x' \in O_{z_1} \cup O_{z_2}$, there exists a unique $y' \in O_{w_1} \cup O_{w_2}$ such that $WS(x') \subset WS(y')$ and $\sum_{t=0}^{\lfloor \frac{n}{2} \rfloor - wt(x')} \binom{wt(y')-wt(x')}{t}$ is odd. Then construct,

$$R'_n(X) = \begin{cases} G_n(X) \oplus 1, \text{ if } X \in \{O_{z_1} \cup O_{z_2}\} \bigcup \{O_{w_1} \cup O_{w_2}\} \\ G_n(X), \text{ elsewhere }. \end{cases}$$

Then by Theorem 6, R'_n is an 7-variable RSBF with maximum AI , i.e., 4.

As in Construction 2, outputs of G_n are toggled at more inputs, one can expect better nonlinearity than the Construction 1.

For 7-variable functions with maximum AI 3, the lower bound on nonlinearity is 44 [27] and that is exactly achieved in the existing theoretical construction [14, 17, 5]. Our Construction 1 provides the nonlinearity 46. Further we used Construction 2 to get all possible functions R'_n and they provide the nonlinearity 48.

5.1 Further generalization

We further release the restrictions in Construction 2 in choosing the orbits $O_{z_1}, \ldots, O_{z_2}$ and $O_{w_1}, \ldots, O_{w_k}$ such that for each $x' \in \cup_{t=0}^{k} O_{z_t}$ there is a unique $y' \in \cup_{t=0}^{l} O_{w_t}$ such that $WS(x') \subset WS(y')$. The construction is as follows

Construction 3 *Take $n \geq 5$ and odd. Consider the orbits $O_{z_1}, \ldots, O_{z_k}$ and $O_{w_1}, \ldots, O_{w_k}$ such that the sub matrix $W_{|\cup_{t=0}^{k} O_{z_t}| \times |\cup_{t=0}^{l} O_{w_t}|}$ is nonsingular. Then construct,*

$$R''_n(X) = \begin{cases} G_n(X) \oplus 1, \text{ if } X \in \{\cup_{t=0}^{k} O_{z_t}\} \bigcup \{\cup_{t=0}^{l} O_{w_t}\} \\ G_n(X), \text{ elsewhere }. \end{cases}$$

Then we have the following theorem.

Theorem 7. *The function R''_n is an n-variable RSBF with maximum* AI .

Construction 3 will provide all the RSBFs with maximum AI . In this case we need a heuristic to search through the space of RSBFs with maximum AI as the exhaustive search may not be possible as number of input variables n increases.

One may note that it is possible to use these techniques to search through the space of general Boolean functions, but that space is much larger (2^{2^n}) compared to the space of RSBFs $(\approx 2^{\frac{2^n}{n}})$ and getting high nonlinearity after a small amount of search using a heuristic is not expected.

We present a simple form of heusristic as follows that we run for several iterations.

1. Start with a RSBF n having maximum AI using Construction 1.
2. We choose two orbits of same sizes having different output values and toggle the outputs corresponding to both the orbits (this is to keep the function balanced).
3. If the modified function is of maximum AI and having better nonlinearity than the previous ones, then we store that as the best function.

By this heuristic, we achieve 7, 9, 11 variable RSBFs with maximum possible AI having nonlinearities 56, 240, 984 respectively with very small amount of search. Note that these nonlinearities are either equal or close to $2^{n-1} - 2^{\frac{n-1}{2}}$. We are currently working on better search heuristics.

6 Conclusion

In this paper, we present the construction (Construction 1) of Rotation Symmetric Boolean functions on $n \geq 5$ (odd) variables with maximum possible algebraic immunity. Then we generalize this construction idea. We determine the nonlinearity of the RSBFs constructed in Construction 1 and find that the nonlinearity is 2 more than the lower bound of nonlinearity of n (odd) variable Boolean functions with maximum algebraic immunity. Prior to our construction, the existing theoretical constructions could achieve only the lower bound. We also included little amount of search with the construction method to get RSBFs having maximum possible AI and very high nonlinearity. With minor modifications, our method will work for RSBFs on even number of variables. This will be available in the full version of this paper.

References

1. F. Armknecht. Improving Fast Algebraic Attacks. In *Fast Software Encryption, FSE 2004*, number 3017 in Lecture Notes in Computer Science, pages 65–82. Springer-Verlag, 2004.
2. F. Armknecht, C. Carlet, P. Gaborit, S. Kuenzli, W. Meier and O. Ruatta. Efficient computation of algebraic immunity for algebraic and fast algebraic attacks. In *Advances in Cryptology - Eurocrypt 2006*, number 4004 in Lecture Notes in Computer Science. Springer-Verlag, 2006.
3. L. M. Batten. Algebraic Attacks over GF(q). In *Progress in Cryptology - Indocrypt 2004*, number 3348 in Lecture Notes in Computer Science, pages 84–91. Springer-Verlag, 2004.
4. A. Braeken and B. Praneel. Probabilistic algebraic attacks. In *10th IMA international conference on cryptography and coding, 2005*, number 3796 in Lecture Notes in Computer Science, pages 290–303. Springer-Verlag, 2005.
5. A. Braeken and B. Praneel. On the Algebraic Immunity of Symmetric Boolean Functions. In *Indocrypt 2005*, number 3797 in Lecture Notes in Computer Science, pages 35–48. Springer Verlag, 2005. An earlier version is available at Cryptology ePrint Archive: report 2005/245, http://eprint.iacr.org/2005/245.

6. J. H. Cheon and D. H. Lee. Resistance of S-Boxes against Algebraic Attacks. In *Fast Software Encryption, FSE 2004*, number 3017 in Lecture Notes in Computer Science, pages 83–94. Springer-Verlag, 2004.
7. J. Y. Cho and J. Pieprzyk. Algebraic Attacks on SOBER-t32 and SOBER-128. In *Fast Software Encryption, FSE 2004*, number 3017 in Lecture Notes in Computer Science, pages 49–64. Springer Verlag, 2004.
8. N. Courtois. Fast Algebraic Attacks on Stream Ciphers with Linear Feedback. In *Advances in Cryptology - Crypto 2003*, number 2729 in Lecture Notes in Computer Science, pages 176–194. Springer-Verlag, 2003.
9. N. Courtois, B. Debraize and E. Garrido. On Exact Algebraic [Non-]Immunity of S-boxes Based on Power Functions. In *Australasian Conference on Information Security and Privacy, ACISP 2006.* To be published in Lecture Notes in Computer Science. Springer-verlag, 2006.An earlier version is available at Cryptology ePrint Archive: report 2005/203, http://eprint.iacr.org/2005/203.
10. N. Courtois and W. Meier. Algebraic Attacks on Stream Ciphers with Linear Feedback. In *Advances in Cryptology - Eurocrypt 2003*, number 2656 in Lecture Notes in Computer Science, pages 345–359. Springer Verlag, 2003.
11. N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In *Advances in Cryptology - Asiacrypt 2002*, number 2501 in Lecture Notes in Computer Science, pages 267–287. Springer Verlag, 2002. Modified and extended version is available in Cryprology ePrint Archive: report 2002/044, http://eprint.iacr.org/2002/044/.
12. T. W. Cusick and P. Stănică. Fast Evaluation, Weights and Nonlinearity of Rotation-Symmetric Functions. *Discrete Mathematics*, Volume 258, 289–301, 2002.
13. D. K. Dalai, K. C. Gupta and S. Maitra. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions. In *Progress in Cryptology - Indocrypt 2004*, number 3348 in Lecture Notes in Computer Science, pages 92–106. Springer Verlag, 2004.
14. D. K. Dalai, K. C. Gupta and S. Maitra. Cryptographically Significant Boolean functions: Construction and Analysis in terms of Algebraic Immunity. In *Fast Software Encryption, FSE 2005*, number 3557 in Lecture Notes in Computer Science, pages 98–111. Springer-Verlag 2005.
15. D. K. Dalai, S. Maitra and S. Sarkar. Results on rotation symmetric Bent functions. *Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA'06*, publications of the universities of Rouen and Havre, 137–156, 2006.
16. D. K. Dalai and S. Maitra. Reducing the Number of Homogeneous Linear Equations in Finding Annihilators. Accepted in International Conference on sequences and their applications, SETA 2006, to be held in September 24 – 28, 2006 Beijing, China, to be published in number 4086 in Lecture Notes in Computer Science, Springer-verlag. An extended version is available at Cryptology ePrint Archive: report 2006/032, http://eprint.iacr.org/2006/032.
17. D. K. Dalai, S. Maitra and S. Sarkar. Basic Theory in Construction of Boolean Functions with Maximum Possible Annihilator Immunity. *Design, Codes and Cryptography* 40(1):41–58, July 2006. A preliminary version is available at Cryptology ePrint Archive: report 2005/229, http://eprint.iacr.org/2005/229.
18. F. Didier and J. Tillich. Computing the Algebraic Immunity Efficiently. In *Fast Software Encryption, FSE 2006*, to be published in Lecture Notes in Computer Science. Springer-Verlag, 2006.

19. M. Hell, A. Maximov and S. Maitra. On efficient implementation of search strategy for rotation symmetric Boolean functions. *Ninth International Workshop on Algebraic and Combinatorial Coding Theory, ACCT 2004*, Black Sea Coast, Bulgaria, 2004.
20. S. Kavut, S. Maitra, M. D. Yücel. Autocorrelation spectra of balanced boolean functions on odd number input variables with maximum absolute value $< 2^{\frac{n+1}{2}}$. *Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA 06*, publications of the universities of Rouen and the Havre, 73–86, 2006.
21. S. Kavut, S. Maitra and M. D. Yücel. There exist Boolean functions on n (odd) variables having nonlinearity $> 2^{n-1} - 2^{\frac{n-1}{2}}$ if and only if $n > 7$. IACR eprint server, *http://eprint.iacr.org/2006/181.*
22. S. Kavut, S. Maitra S. Sarkar and M. D. Yücel. Enumeration of 9-variable Rotation Symmetric Boolean Functions having Nonlinearity > 240. *INDOCRYPT - 2006*, Lecture Notes in Computer Science, Volume 4329, Springer-Verlag, 266–279, 2006.
23. D. H. Lee, J. Kim, J. Hong, J. W. Han and D. Moon. Algebraic Attacks on Summation Generators. In *Fast Software Encryption, FSE 2004*, number 3017 in Lecture Notes in Computer Science, pages 34–48. Springer Verlag, 2004.
24. 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.
25. N. Li and W. F. Qi. Construction and Analysis of Boolean functions of $2t + 1$ variables with maximum algebraic immunity. In *Advances in Cryptology, Asiacrypt 1992*, number 4284 in Lecture Notes in Computer Science, pages 84–98. Springer-Verlag, 2006.
26. N. Li and W. F. Qi. Symmetric Boolean functions depending on an odd number of variables with maximum algebraic immunity. In *IEEE Transaction on Information Theory*,IT-52(5):2271-2273, May 2006.
27. M. Lobanov. Tight bound between nonlinearity and algebraic immunity. *Cryptology ePrint Archive, eprint.iacr.org, No. 2005/441*, 2005.
28. F. J. MacWillams and N. J. A. Sloane. *The Theory of Error Correcting Codes.* North Holland, 1977.
29. S. Maitra. Correlation immune Boolean functions with very high nonlinearity. *Cryptology ePrint Archive, eprint.iacr.org, No. 2000/054*, October 27, 2000.
30. A. Maximov, M. Hell and S. Maitra. Plateaued Rotation Symmetric Boolean Functions on Odd Number of Variables. *First Workshop on Boolean Functions: Cryptography and Applications, BFCA 05*, publications of the universities of Rouen and Havre, 83–104, 2005.
31. A. Maximov. Classes of Plateaued Rotation Symmetric Boolean functions under Transformation of Walsh Spectra. *International Workshop on Coding and Cryptography 2005*, 325–334. See also IACR eprint server, *http://eprint.iacr.org/2004/354.*
32. W. Meier and O. Staffelbach. Fast correlation attack on stream ciphers. In *Advances in Cryptology - EUROCRYPT'88*, volume 330, pages 301–314. Springer-Verlag, May 1988.
33. 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.
34. J. Pieprzyk and C. X. Qu. Fast Hashing and Rotation-Symmetric Functions. *Journal of Universal Computer Science* Volume 5, 20–31, 1999.

35. L. Qu, C. Li, and K. Feng. A note on symmetric Boolean functions with maximum algebraic immunity in odd number of variables. Preprint, 2006.
36. P. Stănică and S. Maitra. Rotation Symmetric Boolean Functions – Count and Cryptographic Properties. In *R. C. Bose Centenary Symposium on Discrete Mathematics and Applications*, December 2002. Electronic Notes in Discrete Mathematics, Elsevier, volume 15.
37. P. Stănică, S. Maitra and J. Clark. Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions. In *Fast Software Encryption, FSE 2004*, number 3017 in Lecture Notes in Computer Science, pages 161–177. Springer-Verlag, 2004.