On the Algebraic Immunity of Symmetric Boolean Functions

An Braeken and Bart Preneel

Katholieke Universiteit Leuven
Dept. Elect. Eng.-ESAT/SCD-COSIC,
Kasteelpark Arenberg 10, 3001 Heverlee, Belgium
{an.braeken,bart.preneel}@esat.kuleuven.be

Abstract. In this paper, we analyse the algebraic immunity of symmetric Boolean functions. We identify a set of lowest degree annihilators for symmetric functions and propose an efficient algorithm for computing the algebraic immunity of a symmetric function. The existence of several symmetric functions with maximum algebraic immunity is proven. In this way, a new class of function which have good implementation properties and maximum algebraic immunity is found. We also investigate the existence of symmetric functions with high nonlinearity and reasonable order of algebraic immunity. Finally, we give suggestions how to use symmetric functions in a stream cipher.

1 Introduction

Symmetric functions have the property that the function value is determined by the weight of the vector. Therefore, a symmetric function in n variables can be defined by a vector of length $n+1$ which represents the function values of the different weights of the vectors. For this reason, symmetric functions are very interesting functions in order to obtain low memory in software. Also in hardware implementation, only a low number of gates is required [15]. Properties such as balancedness and resiliency, propagation characteristics and nonlinearity are studied in [1]. It is shown that these functions do not behave very good in general with respect to a combination of the properties nonlinearity, degree, and resiliency, which are important properties for resisting distinguishing and correlation attacks.
In 2002, several successfull algebraic attacks on stream ciphers were proposed. The success of these attacks do not mainly depend on the classical properties of nonlinearity or resiliency, but mainly on the weak behaviour with respect to the property of algebraic immunity. In this paper we study the resistance against algebraic attacks for the symmetric functions. We identify a set of lowest degree annihilators of a symmetric function. Since the size of this set is very small in comparison with the general case, the algorithm for computing the algebraic immunity of a symmetric function becomes much more efficient. We prove the existence of several symmetric functions with optimal algebraic immunity. The idea is then to use these functions which have good algebraic immunity in combination with highly nonlinear functions as building block in the design of a stream cipher.
First, Sect. 2 deals with some background on Boolean functions and more in particular on symmetric Boolean functions. In Sect. 3, we investigate the algebraic immunity of homogeneous symmetric functions. Based on the identification of a set of lowest degree annihilators of a symmetric function, we propose an algorithm for computing the algebraic immunity of symmetric functions in Sect. 4. Sect. 5 presents the proofs on several symmetric functions which possess maximum algebraic immunity. In Sect. 6, we investigate the existence of symmetric functions with reasonable AI and better nonlinearity as the symmetric functions with maximum AI. Finally, we conclude in Sect. 7 by summerizing the good and bad properties of symmetric functions when used in a concrete design. We also present some open problems.

2 Background

Let us first recall the basic background on Boolean functions together with some properties of symmetric Boolean functions which were proven in [13].
Let $\mathbb{F}_2^n$ be the set of all n-tuples of elements in the field $\mathbb{F}_2$ (Galois field with two elements), endowed with the natural vector space structure over $\mathbb{F}_2$. An element $\overline{u} = (u_0, \ldots, u_{n-1})$ in $\mathbb{F}_2^n$ can be represented by an integer $\mathbb{Z}_{2^n}$ belonging to the interval $[0, 2^n - 1]$, *i.e.*, $u = \sum_{i=0}^{n-1} u_i 2^i$. We will use both notations interchangeable in the rest of the paper.

A Boolean function f on $\mathbb{F}_2^n$ is a mapping from $\mathbb{F}_2^n$ onto $\mathbb{F}_2$. It can be uniquely represented by the truth table (TT) which is the vector of length 2^n consisting of its function values. The weight $\mathrm{wt}(\overline{v})$ of a vector $\overline{v} \in \mathbb{F}_2^n$ is defined as the number of nonzero positions.
Another unique representation, called the ANF, is a polynomial in $\mathbb{F}_2[x_0,\ldots,x_{n-1}]/(x_0^2-x_0,\ldots,x_{n-1}^2-x_{n-1})$.

$$f(\overline{x}) = \bigoplus_{(a_0,\ldots,a_{n-1})\in\mathbb{F}_2^n} h(a_0,\ldots,a_{n-1})x_0^{a_0}\ldots x_{n-1}^{a_{n-1}}, \quad h(\overline{a}) = \sum_{\overline{x}\preceq\overline{a}} f(\overline{x}), \text{for any } \overline{a}\in\mathbb{F}_2^n\,,$$

where $\overline{x} \preceq \overline{a}$ means that $x_i \leq a_i$ for all $0 \leq i \leq n-1$. The degree of the polynomial determines the algebraic degree of this function. Basically, the ANF of a function consists of the modulo 2 sum of polynomials $(x_0 \oplus a_0 \oplus 1)\cdots(x_{n-1}\oplus a_{n-1}\oplus 1)$ for all $\overline{a} \in \mathbb{F}_2^n$ such that $f(\overline{a}) = 1$. Denote the all-zero function or vector by $\overline{0}$ and the all-one function or vector by $\overline{1}$.
The Walsh transform W_f of a function f on $\mathbb{F}_2^n$ is defined as the real valued transformation

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

From the Walsh transform, we derive the property of nonlinearity $N_f = 2^{n-1} - \frac{1}{2}\max_{\overline{w}\in\mathbb{F}_2^n} W_f(\overline{w})$, which represents the smallest distance between a Boolean function and any affine function.
As response on the algebraic attacks, Meier et al. [10] introduced the concept of algebraic immunity (AI) for a Boolean function f on $\mathbb{F}_2^n$. This measure defines the lowest degree of a non-zero function g from $\mathbb{F}_2^n$ into $\mathbb{F}_2$ for which $f\cdot g = \overline{0}$ or $(f\oplus\overline{1})\cdot g = \overline{0}$. The function g for which $f \cdot g = \overline{0}$ is called an *annihilator function* of f. The set of all annihilators of f is denoted by $An(f)$. The AI is upper bounded by $\lceil \frac{n}{2} \rceil$ as proven in [3].
Symmetric Boolean functions have the property that the function value of all vectors with the same weight is equal. Consequently, the truth table of the symmetric function on $\mathbb{F}_2^n$ can be replaced by a vector v_f of length $n+1$ where the components $v_f(i)$ for $0 \leq i \leq n$ represent the function value for vectors of weight i. The vector v_f is called the value vector (VV) of the symmetric function f.
Also the ANF representation for a symmetric function can be replaced by a shorter form [1, Prop. 2], called the simplified ANF (SANF). Denote the homogeneous symmetric function, which is the function that contains all terms of degree i for $0 \leq i \leq n$, by σ_i. Then, the SANF is a polynomial in $\mathbb{F}_2[x_0,\ldots,x_{n-1}]/(x_0^2-x_0,\ldots,x_{n-1}^2-x_{n-1})$ with basis elements the homogeneous symmetric functions σ_i for $0 \leq i \leq n$:

$$f(\overline{x}) = \bigoplus_{i=0}^{n} \lambda_f(i)\sigma_i, \lambda_f(i) = \sum_{k\preceq i} v_f(k), \text{for } 0 \leq i \leq n\,.$$

The vector $\lambda_f = (\lambda_f(0),\ldots,\lambda_f(n))$ is called the simplified ANF vector (SANF vector).

3 Algebraic Immunity of Homogeneous Symmetric Boolean Functions

Although the affine equivalence classes with representatives the homogeneous symmetric functions of degree $n-2$ and $n-3$ have rather high distance to low order degree functions (see [8]), it does not mean that they possess high security against algebraic attacks. Therefore, we will show in this section upper bounds on the algebraic immunity of σ_{n-2} and σ_{n-3}.

Lemma 1. *The product of two homogeneous symmetric functions with degree a and b is again a homogeneous symmetric function with degree equal to $\overline{a} \vee \overline{b}$.*

Proof. Let $f = \sigma_a\sigma_b$. For any $0 \leq i \leq n$, $v_f(i) = 1$ iff $\overline{a} \preceq \overline{i}$ and $\overline{b} \preceq \overline{i}$ by Lucas' theorem [7], or in other words iff $(\overline{a}\vee\overline{b}) \preceq \overline{i}$. Consequently, $v_{\sigma_a\sigma_b} = v_{\sigma_{a\vee b}}$. □

By applying the previous theorem, we obtain the following factorisation of a homogeneous symmetric Boolean function.

Theorem 1. *Let $\overline{a} = (a_0,\ldots,a_{n-1}) \in \mathbb{F}_2^n$, then the homogeneous symmetric function σ_a on $\mathbb{F}_2^n$ can be factorized in $\sigma_a = \sigma_{2^{a_0}}\sigma_{2^{a_1}}\cdots\sigma_{2^{a_{n-1}}}$.*

This theorem enables us to immediately derive the following general result on the AI of homogeneous symmetric functions.

Corollary 1. *Let σ_a be the homogeneous symmetric function with $0 \leq a \leq n$ on $\mathbb{F}_2^n$ where $2^{j-1} \leq n < 2^j$. Define $i \in \{0, \ldots, j-1\}$ as the smallest integer for which $a_i \neq 0$. Then the AI of σ_a is less or equal than 2^i. An annihilator of degree 2^i is given by $\sigma_{2^i} \oplus 1$.*

Example 1. Consider σ_3 on $\mathbb{F}_2^n$ with $n \geq 3$. The $\mathrm{AI}(\sigma_3) = \mathrm{AI}(\sigma_1\sigma_2) = 1$. Consequently $\sigma_1 \oplus \overline{1}$ is a corresponding lowest degree annihilator of degree 1.

Theorem 2. *The homogeneous symmetric function $\sigma_{2^{j-1}}$ on $\mathbb{F}_2^n$ where $2^{j-1} \leq n < 2^j - 1$, can be written as $\sigma_{2^{j-1}} = \sigma_{2^{j-1}}(\sigma_{n-(2^{j-1}-1)} \oplus \overline{1})(\sigma_{n-(2^{j-1}-2)} \oplus \overline{1}) \cdots (\sigma_{2^{j-1}-1} \oplus \overline{1})$.*

Proof. The proof follows immediately from the fact that $v_{\sigma_{n-c}}(k) = 0$ for all $n - 2^{j-1} + 1 \leq c \leq 2^{j-1} - 1$ and $2^{j-1} \leq k \leq n$. □

Corollary 2. *Let $2^{j-1} \leq n < 2^j - 1$. The algebraic immunity of σ_a with $a \equiv 1 \mod 2^{j-1}$ in $\mathbb{F}_2^n$ is less or equal than $n - (2^{j-1} - 1)$. An annihilator of degree equal to $n - (2^{j-1} - 1)$ is given by $\sigma_{n-(2^{j-1}-1)}$.*

Example 2. For $8 \leq n < 15$, we have that

$$\begin{aligned}
n = 8:&\ \sigma_8 = \sigma_8(\sigma_1 \oplus \overline{1}) \cdots (\sigma_7 \oplus \overline{1}),\\
n = 9:&\ \sigma_8 = \sigma_8(\sigma_2 \oplus \overline{1}) \cdots (\sigma_7 \oplus \overline{1}),\\
&\ \vdots\\
n = 14:&\ \sigma_8 = \sigma_8(\sigma_7 \oplus \overline{1}).
\end{aligned}$$

Note that Corollary 2 can be made stronger by taking also the upper bound of Corollary 1 into account. Finally, as a direct application of corollaries 2 and 1, we derive an upper bound on the AI of the symmetric function σ_d for $d = n - 2$ and $n - 3$.

Corollary 3. *If n is odd, then the AI of σ_{n-2} is equal to 1. If $n = 4k$ with $k \geq 1$, then the AI of σ_{n-2} is equal to 2. If $n = 2^i + 2$ for $i \geq 2$, then $AI(\sigma_{n-2}) \leq 3$. Finally, if $n = 2^{i+1}k + 2^i + 2$, then $AI(\sigma_{n-2}) \leq 2^i$ for $k \geq 1, i \geq 2$.*

Corollary 4. *If n is even, then the AI of σ_{n-3} is equal to 1. If $n = 4k + 1$ with $k \geq 1$, then the AI of σ_{n-3} is equal to 2. If $n = 2^i + 3$ for $i \geq 2$, then $AI(\sigma_{n-3}) \leq 4$. Finally, if $n = 2^{i+1}k + 2^i + 3$, then $AI(\sigma_{n-3}) \leq 2^i$ for $k \geq 1, i \geq 2$.*

Moreover, the set of dimensions in which a homogeneous symmetric function that can reach the maximum algebraic immunity exists, is very small.

Corollary 5. *The only homogeneous symmetric function with maximum algebraic immunity is equal to $\sigma_{2^{j-1}}$ in dimensions $n = 2^j, 2^j - 1, 2^j - 2$. For all other dimensions no homogeneous symmetric functions with maximum AI exist.*

Proof. From corollaries 1 and 2, we derive that the homogeneous symmetric function $\sigma_{2^{j-1}}$ in dimension n with $2^{j-1} < n \leq 2^j$ is the only function for which the maximum AI can be reached, since all other homogeneous symmetric functions can be decomposed into the product of homogeneous symmetric functions of smaller degree. However, by Theorem 2, we derive that for $n = 2^j - 3$ holds that $\sigma_{2^{j-1}} = \sigma_{2^{j-1}}(\sigma_{2^j-3-2^{j-1}+1} \oplus \overline{1}) \cdots (\sigma_{2^{j-1}-1} \oplus \overline{1})$. Since $2(2^j - 2^{j-1} - 2) < 2^j - 3$, this function has an annihilator of degree strictly less than $\lceil \frac{n}{2} \rceil$. Trivially, the same argument holds for all dimensions $2^{j-1} + 1 \leq n \leq 2^j - 3$. □

We will show in Section 5 that these functions have indeed maximum AI.

4 Annihilators of Symmetric Functions

We first distinguish a set of annihilators of a symmetric function. Based on this set, we propose an efficient algorithm for computing the AI of a symmetric Boolean function.

Denote the homogeneous symmetric function of degree i which depends on the j variables $\{x_{n-j}, x_{n-j+1}, \ldots, x_{n-1}\}$ with $j \geq i$ by σ_i^j. We also use the notation of P_k^l to represent the set of polynomials where each polynomial contains all k variables $\{x_0, \ldots, x_{k-1}\}$ and consists of the product of at most l factors where every factor is either the sum of two variables, one variable, or the complement of one variable. Consequently $\lceil \frac{k}{2} \rceil \leq l$. Note that the variables in the polynomials P_k^l play the same role, which means that changing the indices of the variables do not introduce new polynomials in P_k^l. Therefore, we define the role of the variables $\{x_0, \ldots, x_{k-1}\}$ in the polynomials of P_k^l as follows. Depending on l, the first factors involving the first variables (starting from $x_0, x_1, \ldots$) may consist of one variable, the complement of one variable or the sum of two variables. The following factors may consist of one variable and the sum of two variables, while the last factors consist of the sum of two variables.

Example 3. If $\lceil \frac{k}{2} \rceil = l$, only the polynomial $(x_0 \oplus x_1)(x_2 \oplus x_3) \cdots (x_{k-2} \oplus x_{k-1})$ for k even and the polynomial $x_0(x_1 \oplus x_2)(x_3 \oplus x_4) \cdots (x_{k-2} \oplus x_{k-1})$ for k odd belongs to $P_k^{\lceil \frac{k}{2} \rceil}$. If $\lceil \frac{k}{2} \rceil = l - 1$, the polynomials $x_0 x_1 (x_2 \oplus x_3) \cdots (x_{k-2} \oplus x_{k-1})$, $(x_0 \oplus 1) x_1 (x_2 \oplus x_3) \cdots (x_{k-2} \oplus x_{k-1})$, $(x_0 \oplus 1)(x_1 \oplus 1)(x_2 \oplus x_3) \cdots (x_{k-2} \oplus x_{k-1})$, $(x_0 \oplus x_1)(x_2 \oplus x_3) \cdots (x_{k-2} \oplus x_{k-1})$, belong to $P_k^{\lceil \frac{k}{2} \rceil + 1}$ for k even.

The goal of this section is to show that at least one of the lowest degree annihilators with degree strictly less than $\lceil \frac{n}{2} \rceil$ of a symmetric function on $\mathbb{F}_2^n$ is a linear combination of the polynomials of the form for n even:

$$\sigma_0^2 P_{n-2}^{\frac{n}{2}-1}, \sigma_0^3 P_{n-3}^{\frac{n}{2}-1}, \ldots, \sigma_0^{n-1} P_1^{\frac{n}{2}-1}, \sigma_0,$$
$$\sigma_1^4 P_{n-4}^{\frac{n}{2}-2}, \ldots, \sigma_1^{n-1} P_1^{\frac{n}{2}-2}, \sigma_1, \ldots, \sigma_{\frac{n}{2}-2}^{n-2} P_2^1, \sigma_{\frac{n}{2}-2}^{n-1} P_1^1, \sigma_{\frac{n}{2}-2}, \sigma_{\frac{n}{2}-1},$$

and for n odd:

$$\sigma_0^1 P_{n-1}^{\lceil \frac{n}{2} \rceil -1}, \sigma_0^2 P_{n-2}^{\lceil \frac{n}{2} \rceil -1}, \ldots, \sigma_0^{n-1} P_1^{\lceil \frac{n}{2} \rceil -1}, \sigma_0,$$
$$\sigma_1^3 P_{n-3}^{\lceil \frac{n}{2} \rceil -2}, \ldots, \sigma_1^{n-1} P_1^{\lceil \frac{n}{2} \rceil -2}, \sigma_1, \ldots, \sigma_{\lceil \frac{n}{2} \rceil -2}^{n-2} P_2^1, \sigma_{\lceil \frac{n}{2} \rceil -2}^{n-1} P_1^1, \sigma_{\lceil \frac{n}{2} \rceil -2}, \sigma_{\lceil \frac{n}{2} \rceil -1}.$$

Due to the fact that $\lceil \frac{k}{2} \rceil \leq l$, the restrictions of the functions σ_k for $k \in \{0, \ldots, \lceil \frac{n}{2} \rceil - 1\}$ need to be considered starting from dimension $2k+2$ for n even and dimension $2k+1$ for n odd in order to obtain annihilators of degree less or equal than $\lceil \frac{n}{2} \rceil - 1$. We will call this set of annihilators AN_S. We now give some examples of such annihilators.

Example 4. Let $n = 16$, and suppose f is a symmetric Boolean function on $\mathbb{F}_2^n$ with value vector v_f which satisfies $v_f(i) = 0$ for $i \in \{6, 7, 10, 11\}$. Then the function $g(\overline{x}) = \sigma_2^9 x_0 (x_1 \oplus x_2)(x_3 \oplus x_4)(x_5 \oplus x_6)$ represents an annihilator of the function f. This follows from the fact that σ_2^9 is equal to 1 only for vectors in $\mathbb{F}_2^9$ with weight equal to 2,3,6,7. The function $x_0(x_1 \oplus x_2)(x_3 \oplus x_4)(x_5 \oplus x_6)$ is equal to 1 only for a subset of vectors in $\mathbb{F}_2^7$ with weight 4. Consequently the function g is equal to 1 only for a subset of vectors of weight 6,7,10,11.

If the value vector in the coordinates 2 and 6 is equal to c where $c \in \{0, 1\}$ for a symmetric function f in 10 variables, then $(x_0 \oplus 1)(\sigma_2^9 \oplus \sigma_3^9)$ represents an annihilator with degree 3 of f if $c = 0$, or $f \oplus \overline{1}$ if $c = 1$.

Annihilators of symmetric functions are equal to 0 for all vectors of certain weight which belong to the support of the corresponding symmetric function. But the annihilators can be 0 or 1 for vectors which do not belong to the support of the symmetric function. Therefore, an example of an annihilator is the one which consists of the product of a symmetric function which is restricted to the last $n-k$ variables in order to guarantee that the function value is 1 for vectors of the same weight, together with a polynomial that depends on the other k variables and which is 1 for a subset of vectors with fixed weight. The polynomials P_k^l of the annihilators AN_S are constructed in such way that they are equal to 1 only for a subset of vectors which have exactly the same weight. We will prove that the annihilators in AN_S have lowest possible degree by showing that if one of the factors of the polynomial P_k^l would consist of more than 3 variables (in order to decrease the degree), then there also exists an annihilator of the set AN_S whose support is contained in the support of this annihilator and which has smaller or equal degree. Therefore, we first prove Lemma 2.

Remark 1. We note that the annihilators of AN_S do not determine the complete basis of the ideal of annihilators with degree strictly less than $\lceil \frac{n}{2} \rceil$ of a symmetric function. For instance, the function $x_0\sigma_3$ on $\mathbb{F}_2^{10}$ is annihilator of all symmetric functions on $\mathbb{F}_2^{10}$ for which $v_f(4) = v_f(8) = 0$. But also the function $x_0\sigma_3^9 \in \mathrm{AN}_S$ satisfies this property. Both functions are linearly independent. In general, if $x_0\sigma_1, \ldots, x_0 \cdots x_{\lceil \frac{n}{2} \rceil - 3}\sigma_1, \ldots, x_0\sigma_{\lceil \frac{n}{2} \rceil - 2}$ is annihilator of degree less than $\lceil \frac{n}{2} \rceil$, then also the functions $x_0\sigma_1^{n-1}, \ldots, x_0 \cdots x_{\lceil \frac{n}{2} \rceil - 3}\sigma_1^{n - \lceil \frac{n}{2} \rceil + 2}, \ldots, x_0\sigma^{n-1}_{\lceil \frac{n}{2} \rceil - 2}$. Also note that the variables of the polynomials P_k^l play the same role in the representation, and that they only depend on the first k variables. This is possible due to the symmetry of the symmetric function. Since we are only interested in the existence of at least one annihilator in order to determine the AI of the function, we can restrict us for the search of annihilators into the set AN_S.

Lemma 2. *Let $r \geq 3$ and $n \geq r - 1$. Define S_i^n as the symmetric function on n variables of degree i,*

$$S_i^n = \bigoplus_{0 \leq k \leq i} c_k^S \sigma_k^n \text{ where } c_k^S \in \{0, 1\} \text{ for all } 0 \leq k \leq i.$$

Denote the set of weights in the support of S_i^n by V_S. Define also $S_{i-(r-1)}^{n-(r-1)} = \bigoplus_{0 \leq k \leq i} c_k^S \sigma_{k-(r-1)}^{n-(r-1)}$ where $\sigma_i = 0$ for $i < 0$ and denote its support of the value vector by $V_{S'}$. Then

$$\{a + r - 1 : a \in V_{S'}\} \subseteq \{a, a + 2, \ldots, a + r - 1 : a \in V_S\} \tag{1}$$

$$\{a + r : a \in V_{S'}\} \subseteq \{a + 1, a + 3, \ldots, a + r : a \in V_S\} \tag{2}$$

Proof. Note that Equation (2) follows from Equation (1). The theorem is based on the fact that for $k \geq 1$ we have that

$$\{a, a + 2, \ldots, a + 2k : a \in \ \mathrm{sup}(\sigma_{2k+1})\} = \{a + 2k : a \in \ \mathrm{sup}(\sigma_1)\},.$$

Indeed, both sets contain all odd numbers starting from $2k+1$. For the set on the right, this is clear. For the set on the left, we have to check if there is a gap between two consecutive odd numbers. In general, we will say that there is a k-gap in between two consecutive elements a, b of the sets defined above if there are k odd numbers missing between a and b. Let us call a sequence of all zeros, a run. The value vector of the function σ_{2k+1} has a run of length $2k + 1$. This is the longest run since the period of σ_{2k+1} is equal to $2^{\lceil \log_2(2k+1) \rceil}$ and $2^{\lceil \log_2(2k+1) \rceil - 1} \leq 2k + 1$ together with $\sigma_{2k+1}(2^{\lceil \log_2(2k+1) \rceil}) = 1$.
More in general, we have that for all $l \geq 1$:

$$L = \{a, a + 2, \ldots, a + 2l : a \in \ \mathrm{sup}(\sigma_{2k+1})\} \supseteq \{a + 2l : a \in \ \mathrm{sup}(\sigma_{2k+1-2l})\} = R.$$

For $l = k$, the sets R and L contain all odd elements starting from $2k + 1$ as explained above. For $l = k - 1$, the set R contains all elements in the support of σ_3 shifted over $2k - 2$ positions, while the set L contains all elements on the shifting positions 0, 2, 4, until $2k - 2$ of the elements in the support of σ_{2k+1}. Therefore, the set R has a 1-gap in between two consecutive elements of its set. The set L has at most a 1-gap in between two consecutive elements. For $l = k - 2$, the set R contains all elements in the support of σ_5 shifted over $2k - 4$ positions, while the set L contains all elements on the shifting positions 0, 2, 4, until $2k - 4$ of the elements in the support of σ_{2k+1}. Therefore, the sets R and L have at most a 2-gap in between two consecutive elements of its set. This process continues until $l = 1$. For $l = 1$, the set R contains all elements in the support of σ_{2k-1} shifted over 2 positions, while the set L contains all elements in the support of σ_{2k+1} together with the elements on the shifting position 2. Therefore, both sets have at most a $(k - 1)$-gap in between two consecutive elements. If there is a gap in between two consecutive elements of the set L, then it will coincide with a gap in between two consecutive elements of the set R. This follows from the fact that $\sigma_{2k+1-2l}$ has degree $2l$ smaller than σ_{2k+1} and the function values of $\sigma_{2k+1-2l}$ are shifted over $2l$ positions in the set R.
The same principle can be applied for the support of σ_{2k} versus the support of σ_0 and the support of σ_{2k-2l} versus the support of σ_{2k} for $k \geq 1$ and $l \geq 1$:

$$\{a, a + 2, \ldots, a + 2k : a \in \ \mathrm{sup}(\sigma_{2k})\} = \{a + 2k : a \in \ \mathrm{sup}(\sigma_0)\}$$

$$L = \{a, a + 2, \ldots, a + 2l : a \in \ \mathrm{sup}(\sigma_{2k})\} \supseteq \{a + 2l : a \in \ \mathrm{sup}(\sigma_{2k-2l})\} = R.$$

Finally, we have to show that the theorem also holds for any symmetric function. First note that the value vector of any symmetric function S of degree d has a run of lenght at most d. Therefore the largest gap in the set L is equal to $d-2l$. The value vector of the symmetric function S' of degree $d-2l$ has a run of length at most $d-2l$. Since the support of S' is shifted over $2l$ positions, the gap of the set corresponding with S will coincide with the gap of the set corresponding with S'. $\square$

Example 5. Let $n=10, r=3$. The support of the value vector of the function $\sigma_0^{10}\oplus\sigma_1^{10}\oplus\sigma_2^{10}\oplus\sigma_5^{10}$ belongs to $V_S=\{0,3,4,5,8\}$. The support of the value vector of $\sigma_0^8\oplus\sigma_3^8$ belongs to $V_{S'}=\{0,1,2,4,5,6,8\}$. Following the theorem, it holds that $\{2,3,4,6,7,8,10\}\subseteq\{0,2,3,4,5,6,7,8,10\}$.

Directly from Lemma 2, we derive that

Corollary 6. *Let r be odd and $r\geq 3$, then the support of $S_i^{n-r}(x_0\oplus\cdots\oplus x_{r-1})$ contains the support of $S_{i-(r-1)}^{n-(2r-1)}x_0(x_1\oplus x_2)\cdots(x_{2r-3}\oplus x_{2r-2})$. The support of $S_i^{n-r}(x_0\oplus\cdots\oplus x_{r-1}\oplus 1)$ contains the support of $S_{i-(r-1)}^{n-(2r-1)}(x_0\oplus 1)(x_1\oplus x_2)\cdots(x_{2r-3}\oplus x_{2r-2})$. Both have the same degree $i+1$.*
Let r be even and $r\geq 4$, then the support of $S_i^{n-r}(x_0\oplus\cdots\oplus x_{r-1})$ contains the support of $S_{i-(r-2)}^{n-(2r-2)}(x_0\oplus x_1)(x_2\oplus x_3)\cdots(x_{2r-3}\oplus x_{2r-4})$. Both have the same degree $i+1$. The support of $S_i^{n-r}(x_0\oplus\cdots\oplus x_{r-1}\oplus 1)$ contains the support of $S_{i-r}^{n-2r}(x_0\oplus x_1)(x_2\oplus x_3)\cdots(x_{2r-1}\oplus x_{2r-2})$. The latest function has degree i in comparison with degree $i+1$ of the first function. This equation also holds for $r=2$.

Consequently, we can conclude that if one or more factors of the polynomial P_k^l would consist of the complement of two terms or more than three terms, then there always exists an annihilator of AN_S which has degree smaller or equal and whose support is contained in the support of that annihilator. Since the set of homogeneous symmetric functions σ_i for $0\leq i\leq n$ represent a basis for generating the whole set of symmetric functions on $\mathbb{F}_2^n$, where the weight of the basis elements is the smallest possible, we can conclude from the structure of the elements in the set AN_S that one of the lowest degree annihilators of a homogeneous symmetric function is again a homogeneous symmetric function.

Corollary 7. *Let $2^{j-1}-1\leq n<2^j$ and $\overline{a}\in\mathbb{F}_2^n$. Assume $i\in\{0,\dots,j-1\}$ be the smallest integer such that $a_i\neq 0$. The AI of σ_a is equal to $\min\{2^{a_i}, n-(2^{j-1}-1)+(a_{j-1}\oplus 1)(2^{j-1}-1)\}$.*

Let us now compute the number of polynomials in the set AN_S.

Theorem 3. *The number N of polynomials in AN_S is equal to*

$$N=2\sum_{i=1}^{\lceil\frac{n}{2}\rceil-1}(2^i-1)+2^{\lceil\frac{n}{2}\rceil}-1\,.$$

Proof. We will compute the number for n even. In a similar way, the result is obtained for n odd. Denote R_k^n for n even and $0\leq k\leq\frac{n}{2}-1$ as the sum of all elements which have σ_k^i for $i=2k+2,\dots,n$ as factor, *i.e.*, the sum of all elements of the sets $P_i^{\frac{n}{2}-k-1}$ for $i=0,\dots,n-(2k+2)$:

$$R_k^n=\sum_{i=0}^{n-(2k+2)}|P_i^{\frac{n}{2}-k-1}|\,.$$

For $i=n-(2k+2)$, there is exactly one element in $P_{n-(2k+2)}^{\frac{n}{2}-k-1}$, namely the polynomial $(x_1\oplus x_2)\cdots(x_{n-2k-2}\oplus x_{n-2k-3})$. Every decrease of i until $i=\frac{n}{2}-k-1$ with 1 gives one more degree of freedom, which leads to a factor of two more for the possible polynomials in $P_i^{\frac{n}{2}-k-1}$. For instance, suppose the polynomial $P_i^{\frac{n}{2}}-k-1$ has the form $(x_1\oplus x_2)(x_3\oplus x_4)\cdots$ at step i. After removing one variable at step $i-1$, we have two more possible elements in $P_{i-1}^{\frac{n}{2}-k-1}$ namely $x_1(x_2\oplus x_3)\cdots$ and $(x_1\oplus 1)(x_2\oplus x_3)\cdots$. Removing another variable leads again to two more possible polynomials: $(x_1\oplus x_2)\cdots$, $x_1x_2\cdots$, $(x_1\oplus 1)x_2\cdots$, $(x_1\oplus 1)(x_2\oplus 1)\cdots$. For $i<\frac{n}{2}-k-1$, due to the smaller number of variables, the total number of polynomials decreases again with a factor of 2. Therefore, we have that for $0\leq k\leq\frac{n}{2}-1$:

$$R_k^n=2\sum_{i=0}^{\frac{n}{2}-k-2}2^i+2^{\frac{n}{2}-k-1}\,.$$

Consequently, the total number of terms belonging to class 2 is equal to

$$N=\sum_{k=0}^{\frac{n}{2}-1}R_k^n=2\sum_{i=1}^{\lceil\frac{n}{2}\rceil-1}(2^i-1)+2^{\lceil\frac{n}{2}\rceil}-1\,.$$

$\square$

Example 6. For $n = 14$, we have that

$$\begin{aligned}
&\sigma_0 \rightarrow (|P^6_{12}|, \ldots, |P^6_0|) = (1, 2, 4, 8, 16, 32, 64, 32, 16, 8, 4, 2, 1)\\
&\sigma_1 \rightarrow (|P^5_{10}|, \ldots, |P^5_0|) = (1, 2, 4, 8, 16, 32, 16, 8, 4, 2, 1)\\
&\sigma_2 \rightarrow (|P^4_8|, \ldots, |P^5_0|) = (1, 2, 4, 8, 16, 8, 4, 2, 1)\\
&\sigma_3 \rightarrow (|P^3_6|, \ldots, |P^3_0|) = (1, 2, 4, 8, 4, 2, 1)\\
&\sigma_4 \rightarrow (|P^2_4|, \ldots, |P^2_0|) = (1, 2, 4, 2, 1)\\
&\sigma_5 \rightarrow (|P^1_2|, \ldots, |P^1_0|) = (1, 2, 1)\\
&\sigma_6 \rightarrow |P^0_0| = 1
\end{aligned}$$

4.1 Algorithm for Computing AI

As shown in the previous section, one of the lowest degree annihilators of degree less than $\lceil \frac{n}{2} \rceil$ consists of a linear combination of N polynomials where N is equal to the number of elements of AN_S as determined in Theorem 3. This number is much smaller than the number of all polynomials of degree less than $\lceil \frac{n}{2} \rceil$ which is equal to $\sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} \binom{n}{i}$. Table 1 shows the comparison between both numbers for dimensions $n = 2k$ with $5 \leq k \leq 10$. We can conclude that the difference increases with the dimension.

Table 1. Comparison of the size of annihilator-set

n	10	12	14	16	18	20
$\sum_{i=0}^{\lceil \frac{n}{2} \rceil - 1} \binom{n}{i}$	386	1 586	6 476	26 333	106 762	431 910
$\lvert \mathrm{AN}_S \rvert$	83	177	376	1 005	2 539	3 824

The main goal of the algorithm that computes the AI of a function consists in finding suitable linear combinations within these terms. Consequently, roughly speaking the complexity for computing the AI of a symmetric function can be upper bounded by $N^{2.81}$, where 2.81 corresponds with the exponent for Gaussian elimination. Moreover, the additional tricks presented in [10] can be used to accelerate the algorithm even further. Due to the fact that we have much less functions to combine in the algorithm for computing the AI of a symmetric function, the AI of any arbitrary symmetric function can be computed for much larger dimensions.
Instead of checking the whole set of 2^{n+1} symmetric functions for functions with maximum AI, we first present some properties on the value vector of a symmetric function with maximum AI. These properties can be immediately derived from the existence of the annihilators AN_S.

4.2 Properties

Theorem 4. *Let f be a symmetric Boolean function on $\mathbb{F}_2^n$ with value vector v_f. If $v_f(\lceil \frac{n}{2} \rceil - 1) = v_f(\lceil \frac{n}{2} \rceil + 1)$ for all n, or in addition for n odd $v_f(\lceil \frac{n}{2} \rceil - 2) = v_f(\lceil \frac{n}{2} \rceil)$, then f can not have maximum AI.*

Proof. One can easily check that the function

$$\begin{aligned}
(x_0 \oplus x_1)(x_2 \oplus x_3) \cdots (x_{n-6} \oplus x_{n-5})\sigma_1^4 &\quad \text{if } n \text{ is even}\\
(x_0 \oplus x_1)(x_2 \oplus x_3) \cdots (x_{n-5} \oplus x_{n-4})(\sigma_1^3 \oplus c\sigma_0^3), c \in \mathbb{F}_2, &\quad \text{if } n \text{ is odd}
\end{aligned}$$

is 1 only in a subset of vectors with weight $\lceil \frac{n}{2} \rceil - 1$ and $\lceil \frac{n}{2} \rceil + 1$ for n even and n odd with $c = 0$. Similar for n odd and $c = 1$, the function is 1 only in a subset of vectors with weight $\lceil \frac{n}{2} \rceil - 2$ and $\lceil \frac{n}{2} \rceil$. Consequently, this function represents an annihilator of f or $f \oplus \overline{1}$. □

Example 7. For $n = 7$, consider the functions $(x_0 \oplus x_1)(x_2 \oplus x_3)(x_4 \oplus x_5 \oplus x_6)$ and $(x_0 \oplus x_1)(x_2 \oplus x_3)(x_4 \oplus x_5 \oplus x_6 \oplus 1)$. The first one has value 1 only in a subset of vectors with weight 3 and 5. The second function has value 1 only in a subset of vectors with weight 2 and 4. Therefore, all symmetric functions or their complements on $\mathbb{F}_2^7$ with value vector $v_f(3) = v_f(5)$ or $v_f(2) = v_f(4)$ can be annihilated by these functions. For $n = 8$, the function $(x_0 \oplus x_1)(x_2 \oplus x_3)(x_4 \oplus x_5 \oplus x_6 \oplus x_7)$ has value 1 only in vectors of weight 3 and 5.

Theorem 5. *Let $2^j \leq n < 2^{j+1} - 1$ where $j \geq 1$ and f be a symmetric Boolean function on $\mathbb{F}_2^n$ with value vector v_f. Define for all $0 \leq i < 2^{j-1}$ the set $V_i = \{l : l \equiv i \mod 2^{j-1} \text{ for } 0 \leq l < n\}$. If there exists $i \in \{0, \ldots, 2^{j-1} - 1\}$ such that $v_f(k) = 0$ (resp. 1) for all $k \in V_i$, then the AI of f is smaller or equal than $2^{j-1} - 1$. For $n = 2^{j+1} - 1$ where $j \geq 1$, the value vector of f should be of the form $(\overline{a}|\overline{a}^c)$ where $\overline{a} \in \mathbb{F}_2^j$ in order to reach the maximum AI.*

Proof. Let $2^j \leq n < 2^{j+1} - 1$. If the condition of the theorem is not satisfied, then there exist coefficients $c_0, \ldots, c_{2^{j-1}-1} \in \mathbb{F}_2$ such that $c_0\sigma_0 \vee c_1\sigma_1 \vee c_2\sigma_2 \cdots \vee c_{2^{j-1}-1}\sigma_{2^{j-1}-1}$ represents an annihilator of degree strictly less than 2^{j-1} of the function f (if value vector is equal to 0 in V_i) or an annihilator of the function $f \oplus \overline{1}$ (if value vector is equal to 1 in V_i). Similar for $n = 2^{j+1} - 1$. □

Example 8. For $n = 7$, the symmetric function σ_3 satisfies $v_{\sigma_3}(3) = 1, v_{\sigma_3}(7) = 1$ and 0 elsewhere. Consequently, σ_3 is annihilator of the symmetric functions f (or their complements) on $\mathbb{F}_2^7$ which satisfy $v_f(3) = v_f(7)$. Also if for the symmetric function on $\mathbb{F}_2^7$ one of the equalities $v_f(2) = v_f(6)$, $v_f(1) = v_f(5)$, $v_f(0) = v_f(4)$, is satisfied, then no maximum AI can be obtained because $\sigma_2 \oplus \sigma_3$, $\sigma_1 \oplus \sigma_3$, and $\sigma_0 \oplus \sigma_1 \oplus \sigma_2 \oplus \sigma_3$ respectively represent the corresponding annihilators. Therefore, $v_f = (a_0, a_1, a_2, a_3, a_0 \oplus 1, a_1 \oplus 1, a_2 \oplus 1, a_3 \oplus 1)$ with $a_0, a_1, a_2, a_3 \in \{0, 1\}$ for symmetric functions with maximum AI in 7 variables.

Finally, we want to mention that also the condition on the weight of a Boolean function is very strong for symmetric functions in odd number of variables.

Theorem 6. *[4] Let f be a Boolean function on $\mathbb{F}_2^n$. If $wt(f) < \sum_{i=0}^{d} \binom{n}{i}$ or $2^n - wt(f) < \sum_{i=0}^{d} \binom{n}{i}$, then the AI of f is less or equal than d.*

Consequently, maximum AI can only be obtained for balanced functions if n is odd. A large set of balanced functions in n odd are the trivially balanced functions, *i.e.*, the functions with value vector $v_f(i) = v_f(n - i)$ for all $0 \leq i \leq \lfloor \frac{n}{2} \rfloor$. In fact, the trivially balanced functions form the whole set of balanced functions for n odd and $n \leq 128$, except in dimensions $n \in \{13, 29, 31, 33, 35, 41, 47, 61, 63, 73, 97, 103\}$ as shown in [14].

4.3 Experiments

For the computation of the AI, we can use a more efficient algorithm than the algorithm of [10] as explained above and thus reach higher dimensions.
If n is odd, the condition of trivially balancedness is very powerful. We checked until $n \leq 17$ and can conclude that the only trivially balanced functions with maximum AI have value vector v_f such that

$$v_f(i) = \begin{cases} 0 \text{ for } i < \lceil \frac{n}{2} \rceil \\ 1 \text{ for } i \geq \lceil \frac{n}{2} \rceil . \end{cases} \tag{3}$$

In [12], the complete set of non-trivially balanced functions for $n = 13$ is described. From this description, we derive that the AI of the non-trivial balanced functions in 13 variables is less or equal than 3 due to Theorem 5. Therefore, we conclude that all symmetric functions in n odd and $n \leq 17$ with maximum AI have value vector defined by (3). We will prove in the next section that a symmetric function with such value vector always has maximal AI for every n odd. Moreover, it can be easily proven that for $n = 2^i - 1, 2^i + 1$, with $i \geq 2$, only the trivially balanced functions with value vector determined by (3) have maximum AI. In these dimensions, the property of Theorem 5 is very powerful.
For n even, we found more symmetric functions with maximum AI. In the next section, we will theoretically prove the maximum AI for some of these functions. The theorems will cover all symmetric functions with maximum AI in dimensions less or equal than 12 and all but one in dimensions 14 and 16. We refer to Appendix for the complete set of symmetric Boolean functions with maximum AI in dimensions $n = 6, 8, 10, 12, 14, 16$.

5 Symmetric Functions with Maximum AI

In this section, we prove the existence of several symmetric functions with maximum AI for all dimensions n.
Let us first recall that the property of AI is invariant under affine transformation in the input variables, *i.e.*, $f(\overline{x})$ and $f(\overline{x}A \oplus \overline{b})$, where A is an $n \times n$ nonsingular matrix and $\overline{b} \in \mathbb{F}_2^n$ will have the same AI. This follows from the fact that if g is annihilator of f, then $g(\overline{x}A \oplus \overline{b})$ is annihilator of $f(\overline{x}A \oplus \overline{b})$.
However, the AI of two functions $f(\overline{x})$ and $f(\overline{x}) \oplus \overline{c} \cdot \overline{x}$ with $\overline{c} \in \mathbb{F}_2^n$ can differ at most with 1. This can be easily seen as follows. Let g be annihilator of f such that $f(\overline{x}) \cdot g(\overline{x}) = 0$, then $g(\overline{x})(\overline{c} \cdot \overline{x} \oplus \overline{1})$ is annihilator of $(f(\overline{x}) \oplus \overline{c} \cdot \overline{x})$ because $(f(\overline{x}) \oplus \overline{c} \cdot \overline{x})g(\overline{x})(\overline{c} \cdot \overline{x} \oplus \overline{1}) = f(\overline{x})g(\overline{x})(\overline{c} \cdot \overline{x} \oplus 1) \oplus (\overline{c} \cdot \overline{x})g(\overline{x})(\overline{c} \cdot \overline{x} \oplus \overline{1}) = 0$. The last equality follows from the fact that $\overline{c} \cdot \overline{x} \oplus \overline{1}$ is annihilator of $\overline{c} \cdot \overline{x}$.
We now investigate the affine transformations on the input variables which will transform a symmetric function into a new symmetric function.

Theorem 7. *In n even, the only binary linear transformation on the input variables of a symmetric function that will compute a new symmetric function on $\mathbb{F}_2^n$ is the transformation $T = \overline{x} \mapsto \overline{x}A$, where A is a nonsingular $n \times n$ matrix over $\mathbb{F}_2$ with the property that the sum of the elements in each row and column of A is equal to $n-1$. In n odd, no such transformations exist.*
The transformation $(x_0, \ldots, x_{n-1}) \mapsto (x_0 \oplus 1, \ldots, x_{n-1} \oplus 1)$ for all n will map a symmetric function with value vector v_f to a symmetric function with value vector equal to the reverse of this value vector, i.e., v_f^r.

Proof. A minimal requirement for a binary linear transformation $x \mapsto \overline{x}A$ which maps a symmetric function onto a symmetric function is that the weight W of the columns and rows of A is equal, since all variables play the same role in a symmetric function. If W is greater than 1 and smaller than $n-1$, the transformation is not bijective or does not lead to a symmetric function.
Consider n even and $W = n-1$. If $wt(\overline{x})$ is odd and equal to i, then we show that $wt(\overline{x}A)$ is equal to $n-i$. Denote by $V = \{i : x_i \neq 0\}$. The coordinates j with $j \in \{0, \ldots, n-1\}$ in the vector $\overline{x}A$ are 1 if and only if the elements on the corresponding column j of A are 1 exactly on the i positions of the set V. (Note that it is not possible that there are $i-2k$ with $k \geq 1$ elements in the columns of A which are 1 and $2k$ elements which are 0 due to the fact that $W = n-1$.) The number of such columns in A is equal to $\binom{n-i}{n-i-1} = n-i$ for i odd and $1 \leq i \leq n-1$.
Now we show that if $wt(\overline{x})$ is even and equal to i, then $wt(\overline{x}A) = i$. Denote by $V = \{i : x_i \neq 0\}$. The coordinates j with $j \in \{0, \ldots, n-1\}$ in the vector $\overline{x}A$ are 1 if and only if the elements on the corresponding column j of A are 1 on exactly $i-1$ positions of the set V. There are $\binom{i}{i-1} = i$ possibilities for this to occur.
For n odd, the transformation T is not bijective which follows immediately from the fact that vectors of weight 0 and n are both mapped onto vectors of weight 0.
Finally, since the transformation $(x_0, \ldots, x_{n-1}) \mapsto (x_0 \oplus 1, \ldots, x_{n-1} \oplus 1)$ maps a vector of weight i onto a vector of weight $n-i$, this transformation corresponds to the mapping of $v_f(i)$ onto $v_f(n-i)$ for every i with $0 \leq i \leq n$. ☐

We now present three basic classses of symmetric functions with maximum AI.

Class 1

Theorem 8. *The symmetric function f in $\mathbb{F}_2^n$ with value vector*

$$v_f(i) = \begin{cases} 0 \text{ for } i < \lceil \frac{n}{2} \rceil \\ 1 \text{ else} \end{cases} \tag{4}$$

has maximum AI. Let us denote this function f by F_k where k is equal to the threshold $\lceil \frac{n}{2} \rceil$.

Proof. First we show that the function $F_{\lceil \frac{n}{2} \rceil} \oplus \overline{1}$ only has annihilators of degree greater or equal than $\lceil \frac{n}{2} \rceil$. The annihilators of $F_{\lceil \frac{n}{2} \rceil} \oplus \overline{1}$ are 0 in all vectors of weight less than $\lceil \frac{n}{2} \rceil$. Consequently, the terms which appear in the ANF of the function correspond with vectors of weight greater or equal than $\lceil \frac{n}{2} \rceil$ by definition of the ANF. Thus, no linear combination can be found in order to decrease the degree of the resulting function.

As explained above, $F_{\lceil\frac{n}{2}\rceil}$ and $F_{\lceil\frac{n}{2}\rceil}\oplus\overline{1}$ are affine equivalent under affine transformation (complementation) in the input variables for n odd. For n even, the function $F_{\lceil\frac{n}{2}\rceil}$ is affine equivalent with $F_{\lceil\frac{n}{2}\rceil+1}\oplus\overline{1}$. The proof explained above can also be applied on the annihilators of the function $F_{\lceil\frac{n}{2}\rceil+1}\oplus\overline{1}$ for n even since $v_{F_{\lceil\frac{n}{2}\rceil}\oplus\overline{1}}\preceq v_{F_{\lceil\frac{n}{2}\rceil+1}\oplus\overline{1}}$. The theorem follows then from the fact that functions which are affine equivalent in the input variables have the same number of annihilators of fixed degree. □

Remark 2. The maximum AI of this class of symmetric functions was independently proven in [5] using a different proof method.

For n even, we prove that also the function which only differs from the threshold function $F_{\lceil\frac{n}{2}\rceil}$ in the function value of the vector $(1,\ldots,1)$ has maximum AI. Denote the zero vector on $\mathbb{F}_2^{n+1}$ with 1 on position i by $\overline{e}_i$ for $0\leq i\leq n$.

Theorem 9. *The symmetric function f with value vector $v_{F_{\lceil\frac{n}{2}\rceil}}\oplus\overline{e}_n$ in $\mathbb{F}_2^n$ for n even has maximum AI. The degree of f is equal to n if $n\neq 2^i$ for $i\geq 1$ and equal to 2^{i-1} else.*

Proof. First in a similar way as Theorem 8, we can prove that $f\oplus\overline{1}$ can not have annihilators of degree strictly less than $\lceil\frac{n}{2}\rceil$, since $v_{F_{\lceil\frac{n}{2}\rceil}\oplus\overline{1}}\subseteq v_{f\oplus\overline{1}}$.

Second, the proof that also f has no annihilators of degree less than $\lceil\frac{n}{2}\rceil$, is reduced to the proof on the affine equivalent function f', which is obtained from f after the transformation $(x_0,\ldots,x_{n-1})\mapsto(x_0\oplus 1,\ldots,x_{n-1}\oplus 1)$. The function values of annihilators of f' should be 0 for all vectors with weight $1,\ldots,\lfloor\frac{n}{2}\rfloor$ and can be 0 or 1 for vectors of weight 0 and weight $\lfloor\frac{n}{2}\rfloor+1,\ldots,n$. The terms in the ANF corresponding with vectors of weight $\lfloor\frac{n}{2}\rfloor+1,\ldots,n$ have degree greater or equal than $\lfloor\frac{n}{2}\rfloor+1$, while the terms corresponding with the zero vector have degrees from 0 until n. Consequently for n even, any linear combination of the term corresponding with the zero vector and terms corresponding with vectors of weight greater or equal than $\frac{n}{2}+1$ will still contain terms of weight $\frac{n}{2}$. Therefore, there are no annihilators of degree strictly less than $\frac{n}{2}$ for n even. This statement does not hold for n odd, since $\lfloor\frac{n}{2}\rfloor<\lceil\frac{n}{2}\rceil$. Moreover, for n odd, the existence of annihilators of degree less than $\lceil\frac{n}{2}\rceil$ can also be easily understood from the fact that the requirement of balancedness is not satisfied. □

Class 2
For $n\geq 8$ and even, we can distinguish another class of symmetric functions with maximum AI. These symmetric functions differ from $F_{\frac{n}{2}}$ in two symmetric positions such that they possess the same weight as $F_{\frac{n}{2}}$. Denote by $\overline{s}_i$ the all zero vector on $\mathbb{F}_2^{n+1}$ with 1 on positions $i,n-i$ for $0\leq i<\frac{n}{2}$.

Theorem 10. *Let $n=2k$ and $k\geq 4$. The symmetric function f with value vector $v_{F_{\frac{n}{2}}}\oplus\overline{s}_{k-4}$ on $\mathbb{F}_2^n$ has maximum AI.*

Proof. We first show that $f\oplus\overline{1}$ has no annihilators of degree less than $\lceil\frac{n}{2}\rceil$. Suppose that there exists an annihilator g of degree less than $\lceil\frac{n}{2}\rceil$ of this function:

$$g(\overline{x})=a_0\oplus\bigoplus_{0\leq i_1\leq n-1}a_{i_1}x_{i_1}\oplus\cdots\oplus\bigoplus_{0\leq i_1<\cdots<i_{k-1}\leq n-1}a_{i_1,\ldots,i_{k-1}}x_{i_1}\cdots x_{i_{k-1}}\,.$$

Then, the annihilator g should satisfy that $g(\overline{a})=0$ for all $\overline{a}\in\mathbb{F}_2^n$ such that $\mathrm{wt}(\overline{a})\in\{0,1,2,\ldots,k-1,k+4\}\setminus\{k-4\}$. This property for the weights $\{0,1,2,\ldots,k-1\}\setminus\{k-4\}$ translates in the following equations for the coefficients of the ANF of g:

$$\begin{aligned}
a_0&=0\\
a_{i_1}&=0 && \text{for all } 0\leq i_1\leq n-1;\\
&\ \vdots\\
a_{i_1,\ldots,i_{k-5}}&=0 && \text{for all } 1\leq i_1<\cdots<i_{k-5}\leq n;\\
a_{i_1,\ldots,i_{k-3}}&=a_{i_1,\ldots,i_{k-4}}\oplus\cdots\oplus a_{i_2,\ldots,i_{k-3}} && \text{for all } 0\leq i_1<\cdots<i_{k-3}\leq n-1;\\
a_{i_1,\ldots,i_{k-2}}&=a_{i_1,\ldots,i_{k-4}}\oplus\cdots\oplus a_{i_3,\ldots,i_{k-2}} && \text{for all } 0\leq i_1<\cdots<i_{k-2}\leq n-1;\\
a_{i_1,\ldots,i_{k-1}}&=a_{i_1,\ldots,i_{k-4}}\oplus\cdots\oplus a_{i_4,\ldots,i_{k-1}} && \text{for all } 0\leq i_1<\cdots<i_{k-1}\leq n-1.
\end{aligned}\tag{5}$$

For all vectors of weight $k+4$ with 1 on positions $i_1, \ldots, i_{k+4}$, where $0 \leq i_1 < \cdots < i_{k+4} \leq n-1$ we derive the equation

$$a_{i_1,\ldots,i_{k-4}} \oplus \cdots \oplus a_{i_9,\ldots,i_{k+4}} = 0\,. \tag{6}$$

This equation is found as follows. The annihilator consists of a linear combination of terms of degree less than $k-1$. By the system of equations (5), these terms are either zero or linear combinations of terms of degree $k-4$. Therefore, we count the number of times a fixed term of degree $k-4$ will appear in the resulting equation. For instance the term $a_{i_1,\ldots,i_{k-4}}$ will appear due to terms of the form $a_{i_1,\ldots,i_{k-4},x,y,z}, a_{i_1,\ldots,i_{k-4},x,y}, a_{i_1,\ldots,i_{k-4},x}, a_{i_1,\ldots,i_{k-4}}$, where $x, y, z \in \{k-3, \ldots, k+4\}$. The total number of such terms is equal to $\binom{8}{3} + \binom{8}{2} + \binom{8}{1} + \binom{8}{0} \equiv 1 \mod 2$, which explains Equation (6). Consequently, we obtain a homogeneous system of $\binom{2k}{k+4}$ equations corresponding to all vectors with weight $k+4$ and $\binom{2k}{k-4}$ unknowns corresponding with the coefficients of the terms of weight $k-4$. Since the equations are linearly independent, the number of equations is equal to the number of unknowns: $\binom{2k}{k-4} = \binom{2k}{k+4}$.
The property $\binom{j+4}{j-4} \equiv 1 \mod 2$ for $5 \leq j \leq k$ for all $k \geq 5$ holds by Lucas' Theorem [7]. For $j = k$, this implies that the number of terms in the equation is odd. For $j \in \{5, \ldots, k-1\}$, this implies that the number of terms with $k-j$ variables fixed in the equation is odd. Therefore, we conclude that the only solution for the coefficients of the terms of degree $k-4$ is zero. Following the system of equations (5), g reduces to the zero function.
In a similar way, one can show that the affine equivalent function f', obtained after complementing all input variables, also has no non-zero annihilators of degree less than $\frac{n}{2}$ due to $v_{f\oplus\overline{1}} \preceq v_{f'}$. □

Again, the symmetric functions f which differ from the functions presented in Theorem 10 only in the all-one vector have maximum AI for $n \geq 10$. This can be obtained by using the proof technique of Theorem 9 for showing the non-existence of annihilators with degree less than $\frac{n}{2}$ for f and the proof technique of Theorem 10 for $f \oplus \overline{1}$.

Theorem 11. *Let $n = 2k$ and $k \geq 5$. The symmetric function f with value vector $v_{F_{\frac{n}{2}}} \oplus \overline{s}_{k-4} \oplus \overline{e}_n$ on $\mathbb{F}_2^n$ has maximum AI. The degree of f is equal to n if $n \neq 2^i$ with $i \geq 1$ and equal to 2^{i-1} else.*

We also present another class of functions which differs from $F_{\frac{n}{2}}$ in two symmetric positions. These functions coincide with the function defined in Theorem 9 for $n = 8$.

Theorem 12. *Let f be a symmetric function on $\mathbb{F}_2^n$ with n even. If $\binom{n}{\frac{n}{2}} \equiv 1 \mod 4$, then the function with value vector $v_{F_{\frac{n}{2}}} \oplus \overline{s}_0$ has maximum AI.*

Proof. In a similar way as the proof of Theorem 10, we derive that the coefficients with degree between 1 and $\frac{n}{2} - 1$ of an annihilator g of $f \oplus \overline{1}$ and f' (f' is function obtained from f after complementing the input variables) are all equal to a_0. From the vector of weight n, we derive that $a_0 = 0$ if and only if the number of terms in the equation is odd, and thus $\sum_{i=0}^{\frac{n}{2}-1} \binom{n}{i} = 2^{n-1} - \frac{1}{2}\binom{n}{\frac{n}{2}}$ is odd. □

Example 9. The numbers $n = 2^i$ for $i \geq 3$ satisfy the property that $\binom{n}{\frac{n}{2}} \equiv 1 \mod 4$.

Class 3

For n even, the third class of functions with maximum AI differs from $F_{\frac{n}{2}}$ in only one position. Therefore these functions have weight different from the weight of the functions of class 1 or 2.

Theorem 13. *Let f be a symmetric function on $\mathbb{F}_2^n$ with n even. For $1 \leq i < \lfloor \frac{n}{4} \rfloor$, if $\binom{\frac{n}{2}+t-i}{t} \equiv 1 \mod 2$ for all $t \in \{1, \ldots, i\}$, then the function f with value vector $v_{F_{\frac{n}{2}}} \oplus \overline{e}_{n-i}$ has maximium AI.*

Proof. Since $v_{F_{\frac{n}{2}}\oplus\overline{1}} \preceq v_{f\oplus\overline{1}}$, we refer to Theorem 8 for the proof that the function $f\oplus\overline{1}$ has no annihilators of degree less than $\frac{n}{2}$. To prove the same for f, we consider the affine equivalent function f' which has value vector equal to the reverse. In the same way as the proof of theorem 10, the coefficients of degree less than i are equal to 0 and the coefficients of degrees between $i+1$ and $\frac{n}{2}$ can be expressed as the sum of terms of degree i (see Equation (5)). Now the contradiction follows from the equations derived from the vectors of weight $\frac{n}{2}$. The equations are homogeneous and consist of the sum of all terms in $\frac{n}{2}$ variables of degree i. Therefore, if the condition $\binom{\frac{n}{2}+t-i}{t} \equiv 1 \mod 2$ for $1 \leq t \leq i$ is satisfied, no subset of coefficients can be equal to 1. As a consequence, the zero function is the only annihilator of degree less than $\frac{n}{2}$. □

Example 10. For $n = 14$, since $\binom{7}{1} \equiv 1 \mod 2$, the function value vector $v_{F_7} \oplus \overline{e}_{13}$ has maximum AI. Also $\binom{7}{3} \equiv 1 \mod 2$, $\binom{6}{2} \equiv 1 \mod 2$, $\binom{5}{1} \equiv 1 \mod 2$, and thus the function with value vector $v_{F_7} \oplus \overline{e}_{11}$ represents a function with maximum AI.

Functions Derived From Classes 1, 2, and 3

For n even, the symmetric functions from classes 1, 2, and 3 can be used to derive other symmetric functions by means of the affine transformation $(x_0, \ldots, x_{n-1}) \mapsto (x_0 \oplus x_1 \oplus \cdots \oplus x_{n-2}, x_1 \oplus x_2 \oplus \cdots \oplus x_{n-1}, \ldots, x_{n-1} \oplus x_0 \oplus \cdots \oplus x_{n-3})$. As already explained, this transformation maps vectors of odd weight i to vectors with weight $n - i$. If the weight is even, then nothing is changed.

Corollary 8. *Let f be a symmetric functions on $\mathbb{F}_2^n$ which belongs to class 1 or 2. If $n = 4k$, then $f \oplus \sigma_1$ has maximum AI. If $n = 4k+2$, then the symmetric function with value vector $v_{f\oplus\sigma_1} \oplus \overline{e}_{\frac{n}{2}}$ has maximum AI.*
Let f be a symmetric functions on $\mathbb{F}_2^n$ which belongs to class 3. If $n = 4k$, then the function with value vector $v_{f\oplus\sigma_1} \oplus c\overline{e}_{n-i}$, where $c = 1$ if i is odd and $c = 0$ otherwise, has maximum AI. If $n = 4k + 2$, then the function with value vector $v_{f\oplus\sigma_1} \oplus \overline{e}_{\frac{n}{2}} \oplus c\overline{e}_{n-i}$, where $c = 1$ if i is odd and $c = 0$ otherwise has maximum AI.

Remark 3. We want to note that the symmetric Boolean functions f derived from the function $F_{\lceil \frac{n}{2} \rceil}$ and also $F_{\lceil \frac{n}{2} \rceil} \oplus \sigma_n$ if n is even have very simple annihilators. For instance, it can be easily seen that the functions $x_{i_1} \cdots x_{i_{\lceil \frac{n}{2} \rceil}}$ with $0 \le i_1 < i_2 < \cdots < i_{\lceil \frac{n}{2} \rceil} \le n-1$ are annihilators of $F_{\lceil \frac{n}{2} \rceil} \oplus \overline{1}$. Moreover, they form exactly the basis of the set of annihilators for $F_{\lceil \frac{n}{2} \rceil} \oplus \overline{1}$. The basis of the annihilators of $F_{\lceil \frac{n}{2} \rceil} \oplus \sigma_n \oplus \overline{1}$ consists of the elements $\{x_0 \cdots x_{\lceil \frac{n}{2} \rceil - 1} \oplus x_{i_1} \cdots x_{i_{\lceil \frac{n}{2} \rceil}} : 0 \le i_1 < i_2 < \cdots < i_{\lceil \frac{n}{2} \rceil} \le n-1, (i_1, \ldots, i_{\lceil \frac{n}{2} \rceil}) \neq (0, \ldots, \lceil \frac{n}{2} \rceil - 1)\}$.
A high number of terms in the equations is another important criteria for the algebraic attacks. Therefore, one should be very careful in choosing the taps of the filter function and the taps of the LFSR when using these symmetric functions in a filter generator. The annihilators of the affine equivalent functions are more complicated. However, this does not change the situation, since one can always replace the filter generator by an equivalent generator with different initial state and connection polynomial of the LFSR and with filter function equal to the affine equivalent one (see [6]).
Annihilators of degree $\frac{n}{2}$ of symmetric functions which belong to classes 2 or 3 are more complicated and consist of more terms.

Properties

Properties such as degree, weight and maximum value in the Walsh spectrum of the functions from classes 1, 2, and 3 for n even are summerized in Table 2. The property of degree can be easily derived by using Proposition 2 and Proposition 4 of [1]. The nonlinearity of the functions is immediately derived from the weight since one can show that $\max_{\overline{w}\in\mathbb{F}_2^n} |W_f(\overline{w})| = |W_f(\overline{0})|$. This is proven in detail by Dalai *et. al* in [5].

Table 2. Properties of Symmetric function on $\mathbb{F}_2^n$ with Maximum AI for n even

Function	Degree	weight	max $\lvert W_f \rvert$
$F_{\frac{n}{2}}$	$2^{\lfloor \log_2 n \rfloor}$	$2^{n-1} + \frac{1}{2}\binom{n}{\frac{n}{2}}$	$\binom{n}{\frac{n}{2}}$
$F_{\frac{n}{2}} \oplus \overline{s}_{\frac{n}{2}-4}$	$2^{\lfloor \log_2 n \rfloor}$	$2^{n-1} + \frac{1}{2}\binom{n}{\frac{n}{2}}$	$\binom{n}{\frac{n}{2}}$
$F_{\frac{n}{2}} \oplus \overline{e}_{n-i}$	$\ge n - i$	$2^{n-1} + \frac{1}{2}\binom{n}{\frac{n}{2}} - \binom{n}{n-i}$	$\binom{n}{\frac{n}{2}} - 2\binom{n}{n-i}$

The functions from class 1 for n odd are trivially balanced. The nonlinearity of these functions is equal to $2^{n-1} - \binom{n-1}{\frac{n-1}{2}}$. This follows from the fact that the restriction to the subspace $x_n = 0$ (resp. $x_n = 1$) is equal to the symmetric function (resp. complement of symmetric function) of class 1 in $\mathbb{F}_2^{n-1}$. As mentioned in [1], trivially balanced functions satisfy the property that the derivative with respect to the all one vector is constant, *i.e.*, $D_{\overline{1}}f = \overline{1}$. Also $W_f(\overline{v}) = 0$ for all vectors $\overline{v}$ of even weight.

6 AI and Nonlinearity of Symmetric Functions

Since the nonlinearity of functions with maximum AI is rather small, we also investigated the existence of symmetric functions with suboptimal AI and better nonlinearity.
Let us first investigate if there exists symmetric functions with the highest or suboptimal nonlinearity that satisfy a reasonable order of AI. It has been pointed out in [9] that the only symmetric functions with maximum nonlinearity ($2^{n-1}-2^{\frac{n}{2}-1}$ for n even and $2^{n-1}-2^{\frac{n-1}{2}}$ for n odd) are quadratic functions. Therefore, their AI is upperbounded by 2. In [1], symmetric functions with suboptimal nonlinearity are determined. Based on Theorem 1 and Theorem 2, we derive that symmetric functions with suboptimal nonlinearity as determined in [1] have AI upper bounded by 3.

Theorem 14. *The symmetric Boolean functions on $\mathbb{F}_2^n$ with SANF equal to $c_0\sigma_0 \oplus c_1\sigma_1 \oplus \sigma_3 \oplus \cdots \oplus \sigma_{n-2} \oplus \sigma_{n-1}$, where $c_0, c_1 \in \mathbb{F}_2$ have nonlinearity equal to $2^{n-1}-\frac{1}{2}(2^{\lfloor\frac{n+1}{2}\rfloor}+4)$. The AI of these functions is upper bounded by 3.*

Proof. The coefficient c_0 can be 0 or 1, since the AI of a function f is defined as the lowest degree annihilator of f or $f \oplus \overline{1}$. For $c_1 = 0$, if $n = 4k, 4k+3$, $\sigma_1 \oplus \sigma_2$ represents an annihilator of the function. If $n = 4k+1, 4k+2$, the function can be annihilated by $(\sigma_1 \oplus \sigma_2)(x_0 \oplus 1)$.
If $c_1 = 1$, for $n = 4k, 4k+1$, the function σ_2 represents an annihilator, while for $n = 4k+2, 4k+3$, the function $\sigma_2(x_0 \oplus 1)$ can annihilate the function.
This follows from the equalities, $\sigma_1\sigma_3 = \sigma_2\sigma_3$, $\sigma_1\sigma_{4k+i} = \sigma_{4k+i+1}$, with $i \in \{0,2\}$, $\sigma_2\sigma_{4k+i} = \sigma_{4k+i+2}$, for $i \in \{0,1\}$, and $\sigma_n(x_0 \oplus \overline{1}) = \overline{0}$. □

In a similar way, we also derive an uppperbound on the AI of another class of functions with suboptimal nonlinearity.

Theorem 15. *The symmetric Boolean functions on $\mathbb{F}_2^n$ with SANF equal to $c_0\sigma_0 \oplus c_1\sigma_1 \oplus \sigma_2 \oplus \sigma_n$ or $c_0\sigma_0 \oplus c_1\sigma_1 \oplus \sigma_3 \oplus \cdots \oplus \sigma_{n-1} \oplus \sigma_n$, where $c_0, c_1 \in \mathbb{F}_2$ have nonlinearity equal to $2^{n-1}-\frac{1}{2}(2^{\lfloor\frac{n+1}{2}\rfloor}+2)$. The AI of these functions is upper bounded by 3.*

Therefore, we need to work from the other direction, i.e., to search in the set of functions with suboptimal AI the class of functions with the best nonlinearity. From computer experiments, we derive that for dimensions 10,12, and 14, no symmetric function exists which has AI equal to $\frac{n}{2}-1$ and better nonlinearity as the functions with maximum nonlinearity. For $n = 8$ and 16, several functions could be found with AI equal to $\frac{n}{2}-1$ and slightly better nonlinearity. For instance, the best nonlinearity of a function with maximum AI equal to 7 in $n = 16$ is 27804 in comparison with 26333 for a function with maximum AI.
If n is odd and equal to 9, 11, 13, 15, and 17, we could distinguish one class of functions which have the best possible nonlinearity for a symmetric function with AI one less than the maximum. They have value vector equal to $v_{F_{\lceil\frac{n}{2}\rceil}} \oplus \overline{s}_{\lceil\frac{n}{2}\rceil-5}$ for $n = 2k+1$ with $4 \le k \le 8$. The proof on the AI is basically the same as in Theorem 10. Note that for dimensions greater or equal than 19, this function does not satisfy anymore that the AI is equal to $\lceil\frac{n}{2}\rceil-1$. These functions are all trivially balanced but the gain in nonlinearity in comparison with the functions that have maximum AI is marginally. The maximum of the Walsh value differs only a factor of $4\left(\binom{n-1}{\lceil\frac{n}{2}\rceil-5}-\binom{n-1}{\lceil\frac{n}{2}\rceil-6}\right)$.
However, the difference in nonlinearity between functions with maximum AI and functions with lower AI increases much more if one considers functions with smaller AI equal to $\frac{n}{2}-2$. We can distinguish one class of symmetric functions which have the best possible nonlinearity when the AI is equal to $\lceil\frac{n}{2}\rceil-2$. We checked until dimension 18 and only in dimension 10, we could find one function which has slightly better nonlinearity (468 compared to 476). The value vector of this class of symmetric functions is build up as follows. We start in dimension 1 with the value vector $(1,0)$. If the dimension is even, we obtain the value vector depending on the dimension n:

- If $4(2^{2i}-1) < n < 4(2^{2i+1}-1)$ for $i \ge 0$: We add the bit 1 on the left.
- If $4(2^{2i-1}-1) < n < 4(2^{2i}-1)$ for $i \ge 1$: We add the bit 0 on the left.
- If $n = 4(2^{2i}-1)$ for $i \ge 1$: We add the bit 1 on the left.
- If $n = 4(2^{2i-1}-1)$ for $i \ge 1$: We add the bit 0 on the left.

In odd dimensions, we complete the value vector such that a trivially balanced function is obtained. Consequently, the value vector consists of k different subvectors $\overline{s}_i$ for $1 \le i \le k$, i.e., $v_f = (\overline{s}_1, \ldots, \overline{s}_k)$. The two middle subvectors $\overline{s}_{\lceil\frac{k}{2}\rceil}, \overline{s}_{\lceil\frac{k}{2}\rceil+1}$ have size equal to 2. The following two subvectors going from the middle to the second vector $\overline{s}_2$ and second last vector $\overline{s}_{k-2}$ have size 4, 8,... Every subvector is either the all-zero or the all-one vector and two consecutive subvectors are different. The construction is illustrated in Table 3 with some examples for dimensions n with $9 \leq n \leq 17$. From the construction, we immediately derive a formula for the weight in function of the dimension:

$$wt(f) = 2^{n-1} - \frac{1}{2}\binom{n}{\frac{n}{2}} + (-1)^{i+1} \sum_{i \geq 2} \binom{n}{\frac{n}{2} - (2^i - 2)},$$

where $\binom{n}{l} = 0$ if $l < 0$. The proof for the AI can be performed with the same method as before. Basically the inner part of the value vector $(1, 1, 0, 0)$ will be responsable for the AI. Also the maximum value in the Walsh spectrum is given in the table. Note that the maximum value is reached in the zero vector for symmetric functions of dimesions $2k$ for $k \geq 7$, which means that the nonlinearity can be derived from the weight of these functions.

Table 3. Symmetric functions with suboptimal AI equal to $n - 2$

n	v_f	AI	weight	max$\lvert W_f \rvert$
8	(0,0,0,1,1,0,0,1,1)	2	121	18
9	(0,0,0,1,1,0,0,1,1,1)	3	256	36
10	(0,0,0,1,1,0,0,1,1,1,1)	3	506	44
11	(0,0,0,0,1,1,0,0,1,1,1,1)	4	1024	88
12	(1,0,0,0,0,1,1,0,0,1,1,1,1)	4	2 080	112
13	(1,0,0,0,0,1,1,0,0,1,1,1,1,0)	5	4 096	224
14	(1,1,0,0,0,0,1,1,0,0,1,1,1,1,0)	5	8 464	544
15	(1,1,0,0,0,0,1,1,0,0,1,1,1,1,0,0)	6	16 384	1088
16	(1,1,1,0,0,0,0,1,1,0,0,1,1,1,1,0,0)	6	34 221	2 906
17	(1,1,1,1,0,0,0,0,1,1,0,0,1,1,1,1,0,0)	7	65 536	4 192

We want to note that this class is not satisfying in order to obtain symmetric functions with good nonlinearity and reasonable AI. Computing the measure for normalized nonlinearity for a Boolean function in n variables, $\epsilon = \frac{\max|W_f|}{2^n}$ shows that this value reaches its maximum $\epsilon = 2^{-5,19}$ for dimensions 12 and 13. For dimensions greater or equal than 14, this value slightly decreases. These functions in dimension 12 and 13 have a too small AI, namely equal to 4 and 5 respectively. It seems that it is not possible to obtain a sufficient order of AI (in the order of 7) together with a reasonable nonlinearity (in the order of $\epsilon = 2^{-9}$) for symmetric functions which depend on less than 32 variables. Therefore, we need to search for another way to increase the nonlinearity of the symmetric functions. One method for this, is explained in the next section.

7 Open Questions and Remarks

7.1 Good Properties

The symmetric functions presented in the previous section have a high AI, which is important for the resistance against algebraic attacks. On the other hand, the functions suffer from the problems of nonbalancedness and low nonlinearity. Therefore, we propose to make use of the construction of the direct sum. Let us first recall the properties of the direct sum of two functions.

Direct Sum (See e.g. [11] for the derivation of the properties.) Let $f_1 : \mathbb{F}_2^{n_1} \to \mathbb{F}_2$ and $f_2 : \mathbb{F}_2^{n_2} \to \mathbb{F}_2$ be Boolean functions. Consider the Boolean function $f : \mathbb{F}_2^{n_1} \times \mathbb{F}_2^{n_2} : (\overline{x}, \overline{y}) \mapsto f(\overline{x}, \overline{y}) = f_1(\overline{x}) \oplus f_2(\overline{y})$. Then

- $\mathrm{wt}(f) = 2^{n_2}\,\mathrm{wt}(f_1) + 2^{n_1}\,\mathrm{wt}(f_2) - 2\,\mathrm{wt}(f_1)\,\mathrm{wt}(f_2)$
- $\deg(f) = \max(\deg(f_1), \deg(f_2))$
- $W_f(\overline{x}, \overline{y}) = W_{f_1}(\overline{x}) W_{f_2}(\overline{y})$
- If f_1 is t_1-resilient and f_2 is t_2-resilient, then f is $(t_1 + t_2 + 1)$-resilient.
- $N_f \geq 2^{n_2} N_{f_1} + 2^{n_1} N_{f_2} - 2 N_{f_1} N_{f_2}$

Moreover, for the AI of the direct sum, we have the following theorem.

Theorem 16. *Let f be equal to $f(x,y) = f_1(x) \oplus f_2(y) : \mathbb{F}_2^{n_1+n_2} \to \mathbb{F}_2$. Then the AI of f is determined by*

$$\max\{\mathrm{AI}(f_1), \mathrm{AI}(f_2)\} \leq \mathrm{AI}(f) \leq \min\{\max\{\deg(f_1), \deg(f_2)\}, \mathrm{AI}(f_1) + \mathrm{AI}(f_2)\}\,.$$

Proof. The annihilators of f are of the form $f' = g(f_1 \oplus f_2 \oplus \overline{1})$, where g is an arbitrary function on $\mathbb{F}_2^{n_1+n_2}$. We now look at the different possibilities of g and determine the degree of f', in order to obtain the upper bound on the AI.

- The function g is the identity function. Since f_1 and f_2 depend on different variables, $\deg(f') = \max\{\deg(f_1), \deg(f_2)\}$.
- The function $g = f_1'$ (or $g = f_2'$) is annihilator of f_1 (or f_2). Then, $f' = f_1' f_2 \oplus f_1'$ (or $f' = f_2' f_1 \oplus f_2'$), and thus $\deg(f') = \deg(f_1') + \deg(f_2)$ (or $\deg(f') = \deg(f_1) + \deg(f_2')$).
- The function $g = f_1' f_2'$ is the product of the annihilators of f_1 and f_2. Then, $f' = f_1' f_2'$, and thus $\deg(f') = \deg(f_1') + \deg(f_2')$.

The lower bound is easily explained by the fact that f_1 and f_2 depend on different sets of variables. $\square$

Corollary 9. *If f is a Boolean function on $\mathbb{F}_2^n$ which has maximum AI, than $f \oplus x_{n+1}$ has also maximum AI if n is odd.*

In order to overcome the problem of non-balancedness for the class of symmetric functions in n even, we propose to add by the direct sum a linear function which depends on one or more variables. In this way, also the resiliency of the function increases, which may play a favorable role in the resynchronization of the cipher.
The nonlinearity of the symmetric functions is too small to provide reasonable security against distinguishing and correlation attacks. Although by taking the direct sum with a function of high nonlinearity, a lower bound can be obtained. Examples of functions with high nonlinearity and which have still reasonable hardware complexity are the power functions. Since the AI of the power functions is not optimal as shown in [2], the combination with a symmetric function would be a cheap solution to overcome that problem.

7.2 Problems

It is clear that a symmetric function has lots of structure. Therefore, it is an interesting research question whether this structure can be exploited in an attack. Also, the use of the direct sum of two functions has been pointed out as a possible weakness in the design. But again, no attack is known for this.
There are two straightforward ways to destroy the symmetry and to still maintain a large set of the properties such as nonlinearity, AI and degree. The first way is by affine transformation on the input variables which keeps the AI, nonlinearity and degree invariant. However, this method is not a good solution, since one can construct an equivalent cipher, with different initial state and different connection polynomial for the LFSR(s) where the function is again symmetric (see [6]). The second way is to add an affine function, which keeps the nonlinearity and degree invariant, but will decrease the AI with 1 in general. For this transformation, it is not immediately clear how to rewrite it to an equivalent scheme where the symmetric function is again obtained.
Finally, as further work, we propose to apply similar techniques for the study of the AI of rotation symmetric functions.

Acknowledgement

We thank Anne Canteaut and Marion Videau for their useful comments and suggestions. This work was supported in part by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government and by the European Commission through the IST Programme under Contract IST2002507932 ECRYPT. An Braeken is an F.W.O. Research Assistant, sponsored by the Fund for Scientific Research - Flanders (Belgium).

References

1. A. Canteaut and M. Videau. Symmetric boolean functions. *IEEE Transactions on Information Theory*, 2005.
2. C. Carlet and P. Gaborit. On the construction of balanced boolean functions with a good algebraic immunity. Proceedings of First Workshop on Boolean Functions : Cryptography and Applications, Mars 2005, Rouen, 2005.
3. 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. Eli Biham, editor, Springer, 2003.
4. D.K. Dalai, K.C. Gupta, and S. Maitra. Results on algebraic immunity for cryptographically significant Boolean functions. In *Progress in Cryptology — INDOCRYPT 2004*, volume 3348 of *Lecture Notes in Computer Science*, pages 92–106. Anne Canteaut, editor, Springer, 2004.
5. D.K. Dalai, S. Maitra, and S. Sarkar. Basic theory in construction of boolean functions with maximum possible annihilator immunity. http://eprint.iacr.org/2005/229/.
6. C. Ding, G. Xiao, and W. Shan. *Stability Theory of Stream Ciphers*. Springer, 1991. ISBN 3-540-54973-0, 0-387-54973-0.
7. N.J. Fine. Binomial coefficients modulo a prime. *Mathematical Association of America Monthly*, pages 589–592, December 1947.
8. T. Iwata and K. Kurosawa. Probabilistic higher order differential attack and higher order bent functions. In *Advances in Cryptology — ASIACRYPT 1999*, volume 1716 of *Lecture Notes in Computer Science*, pages 62–74. Kwok-Yan Lam and Eiji Okamoto and Chaoping Xing, editors, Springer, 1999.
9. S. Maitra and P. Sarkar. Maximum nonlinearity of symmetric Boolean functions on odd number of variables. *IEEE Transactions on Information Theory*, IT-48(9):2626–2630, 2002.
10. 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. Christian Cachin and Jan Camenisch, editors, Springer, 2004.
11. P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. In *Advances in Cryptology — EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 488–511. Bart Preneel, editor, Springer, 2000.
12. P. Sarkar and S. Maitra. Balancedness and correlation immunity of symmetric boolean functions. *Electronics Notes in Discrete Mathematics*, 15:178–183, 2002.
13. M. Videau. On some properties of symmetric Boolean functions. In *IEEE International Symposium on Information Theory, 2004, Proceedings*, page 500. Daniel J. Costello and Jr. Bruce Hajek, editors, IEEE Press.
14. J. von zur Gathen and J.R. Roche. Polynomials with two values. *Combinatorica*, 17(3):345–362, 1997.
15. I. Wegener. *The Complexity of Boolean Functions.* Wiley, 1987.

Functions with Maximum AI for Dimensions 6,10,12,14,16

We present the complete set of symmetric functions with maximum AI in dimensions 6,10,12,14,16. The functions are ordered in groups of size 4. The first function f_1 of the group can be seen as the representative of that group, since the three other functions are obtained from this function. The second function f_2 is derived from f_1 by complementing all input variables and thus has value vector which is the reverse of the value vector of f_1. The third function f_3 is obtained from f_1 by applying the affine transformation presented in Theorem 7 and the fourth function f_4 has value vector equal to the reverse of the value vector of f_3. All symmetric functions in the table are normalised in order to satisfy the property $v_f(0) = 0$. For every function, we computed the SANF-vector, weight, and maximum value of the Walsh spectrum.

Table 4. Symmetric function in Dimension 6 with Maximum AI

v_f	weight	SANF vector	max $\|W_f\|$
(0,0,0,1,1,1,1)	42	(0,0,0,1,1,0,0)	20
(0,0,0,0,1,1,1)	22	(0,0,0,0,1,0,0)	20
(0,1,0,1,1,0,1)	42	(0,1,0,0,1,0,0)	20
(0,1,0,0,1,0,1)	22	(0,1,0,1,1,0,0)	20
(0,0,0,1,1,1,0)	41	(0,0,0,1,1,0,1)	18
(0,1,1,1,0,0,0)	41	(0,1,1,1,0,1,1)	18
(0,1,0,1,1,0,0)	41	(0,1,0,0,1,0,1)	18
(0,0,1,1,0,1,0)	41	(0,0,1,0,0,1,1)	18
(0,0,0,1,1,0,1)	36	(0,0,0,1,1,1,0)	12
(0,1,0,0,1,1,1)	28	(0,1,0,1,1,1,0)	12

Table 5. Symmetric function in Dimension 8 with Maximum AI

v_f	weight	SANF vector	max $\|W_f\|$
(0,0,0,0,1,1,1,1,1)	163	(0,0,0,0,1,0,0,0,1)	70
(0,0,0,0,0,1,1,1,1)	93	(0,0,0,0,0,1,1,1,1)	70
(0,1,0,1,1,0,1,0,1)	163	(0,1,0,0,1,0,0,0,1)	70
(0,1,0,1,0,0,1,0,1)	93	(0,1,0,0,0,1,1,1,1)	70
(0,0,0,0,1,1,1,1,0)	162	(0,0,0,0,1,0,0,0,0)	68
(0,1,1,1,1,0,0,0,0)	162	(0,1,1,1,1,0,0,0,0)	68
(0,1,0,1,1,0,1,0,0)	162	(0,1,0,0,1,0,0,0,0)	68
(0,0,1,0,1,1,0,1,0)	162	(0,0,1,1,1,0,0,0,0)	68
(0,1,1,1,1,0,0,0,1)	163	(0,1,1,1,1,0,0,0,1)	70
(0,1,1,1,0,0,0,0,1)	93	(0,1,1,1,0,1,1,1,1)	70
(0,0,1,0,1,1,0,1,1)	163	(0,0,1,1,1,0,0,0,1)	70
(0,0,1,0,0,1,0,1,1)	93	(0,0,1,1,0,1,1,1,1)	70

Table 6. Symmetric function in Dimension 10 with Maximum AI

v_f	weight	SANF vector	max $\|W_f\|$
(0,0,0,0,0,1,1,1,1,1,1)	638	(0,0,0,0,0,1,1,1,1,0,0)	252
(0,0,0,0,0,0,1,1,1,1,1)	386	(0,0,0,0,0,0,1,0,1,0,0)	252
(0,1,0,1,0,1,1,0,1,0,1)	638	(0,1,0,0,0,0,1,0,1,0,0)	252
(0,1,0,1,0,0,1,0,1,0,1)	386	(0,1,0,0,0,1,1,1,1,0,0)	252
(0,0,0,0,0,1,1,1,1,1,0)	637	(0,0,0,0,0,1,1,1,1,0,1)	250
(0,1,1,1,1,1,0,0,0,0,0)	637	(0,1,1,1,1,1,0,1,0,1,1)	250
(0,1,0,1,0,1,1,0,1,0,0)	637	(0,1,0,0,0,0,1,0,1,0,1)	250
(0,0,1,0,1,1,0,1,0,1,0)	637	(0,0,1,1,1,0,0,0,0,1,1)	250
(0,1,0,0,0,1,1,1,1,0,0)	637	(0,1,0,1,0,0,1,0,1,0,1)	250
(0,0,1,1,1,1,0,0,0,1,0)	637	(0,0,1,0,1,0,0,0,0,1,1)	250
(0,0,0,1,0,1,1,0,1,1,0)	637	(0,0,0,1,0,1,1,1,1,0,1)	250
(0,1,1,0,1,1,0,1,0,0,0)	637	(0,1,1,0,1,1,0,1,0,1,1)	250
(0,1,0,0,0,1,1,1,1,0,1)	638	(0,1,0,1,0,0,1,0,1,0,0)	252
(0,1,0,0,0,0,1,1,1,0,1)	386	(0,1,0,1,0,1,1,1,1,0,0)	252
(0,0,0,1,0,1,1,0,1,1,1)	638	(0,0,0,1,0,1,1,1,1,0,0)	252
(0,0,0,1,0,0,1,0,1,1,1)	386	(0,0,0,1,0,0,1,0,1,0,0)	252
(0,0,0,0,0,1,1,1,1,0,1)	628	(0,0,0,0,0,1,1,1,1,1,0)	232
(0,1,0,0,0,0,1,1,1,1,1)	396	(0,1,0,1,0,1,1,1,1,1,0)	232
(0,0,0,1,0,1,1,0,1,0,1)	628	(0,0,0,1,0,1,1,1,1,1,0)	232
(0,1,0,1,0,0,1,0,1,1,1)	396	(0,1,0,0,0,1,1,1,1,1,0)	232

Table 7. Symmetric function in Dimension 12 with Maximum AI

v_f	weight	SANF vector	max $\|W_f\|$
(0,0,0,0,0,0,1,1,1,1,1,1,1)	2510	(0,0,0,0,0,0,1,0,1,0,0,0,0)	924
(0,0,0,0,0,0,0,1,1,1,1,1,1)	1586	(0,0,0,0,0,0,0,1,1,0,0,0,0)	924
(0,1,0,1,0,1,1,0,1,0,1,0,1)	2510	(0,1,0,0,0,0,1,0,1,0,0,0,0)	924
(0,1,01,0,1,0,0,1,0,1,0,1)	1586	(0,1,0,0,0,0,0,1,1,0,0,0,0)	924
(0,0,0,0,0,0,1,1,1,1,1,1,0)	2509	(0,0,0,0,0,0,1,0,1,0,0,0,1)	922
(0,1,1,1,1,1,1,0,0,0,0,0,0)	2509	(0,1,1,1,1,1,1,0,0,0,1,1,1)	922
(0,1,0,1,0,1,1,0,1,0,1,0,0)	2509	(0,1,0,0,0,0,1,0,1,0,0,0,1)	922
(0,0,1,0,1,0,1,1,0,1,0,1,0)	2509	(0,0,1,1,1,1,1,0,0,0,1,1,1)	922
(0,0,1,0,0,0,1,1,1,1,0,1,0)	2509	(0,0,1,1,0,0,0,1,1,0,0,0,1)	922
(0,1,0,1,1,1,1,0,0,0,1,0,0)	2509	(0,1,0,0,1,1,0,1,0,1,1,1,1)	922
(0,1,1,1,0,1,1,0,1,0,0,0,0)	2509	(0,1,1,1,0,0,0,1,1,0,0,0,1)	922
(0,0,0,0,1,0,1,1,0,1,1,1,0)	2509	(0,0,0,0,1,1,0,1,0,1,1,1,1)	922
(0,0,1,0,0,0,1,1,1,1,0,1,1)	2510	(0,0,1,1,0,0,0,1,1,0,0,0,0)	924
(0,0,1,0,0,0,0,1,1,1,0,1,1)	1586	(0,0,1,1,0,0,1,0,1,0,0,0,0)	924
(0,1,1,1,0,1,1,0,1,0,0,0,1)	2510	(0,1,1,1,0,0,0,1,1,0,0,0,0)	924
(0,1,1,1,0,1,0,0,1,0,0,0,1)	1586	(0,1,1,1,0,0,1,0,1,0,0,0,0)	924
(0,0,0,0,0,0,1,1,1,1,0,1,1)	2444	(0,0,0,0,0,0,1,0,1,0,1,1,0)	792
(0,0,1,0,0,0,0,1,1,1,1,1,1)	1652	(0,0,1,1,0,0,1,0,1,0,1,1,0)	792
(0,1,0,1,0,1,1,0,1,0,0,0,1)	2444	(0,1,0,0,0,0,1,0,1,0,1,1,0)	792
(0,1,1,1,0,1,0,0,1,0,1,0,1)	1652	(0,1,1,1,0,0,1,0,1,0,1,1,0)	792

Table 8. Symmetric function in Dimension 14 with Maximum AI

v_f	weight	SANF vector	max $\|W_f\|$
(0,0,0,0,0,0,0,1,1,1,1,1,1,1,1)	9908	(0,0,0,0,0,0,0,1,1,0,0,0,0,0,0)	3432
(0,0,0,0,0,0,0,0,1,1,1,1,1,1,1)	6476	(0,0,0,0,0,0,0,0,1,0,0,0,0,0,0)	3432
(0,1,0,1,0,1,0,1,1,0,1,0,1,0,1)	9908	(0,1,0,0,0,0,0,0,1,0,0,0,0,0,0)	3432
(0,1,0,1,0,1,0,0,1,0,1,0,1,0,1)	6476	(0,1,0,0,0,0,0,1,1,0,0,0,0,0,0)	3432
(0,0,0,0,0,0,0,1,1,1,1,1,1,1,0)	9907	(0,0,0,0,0,0,0,1,1,0,0,0,0,0,1)	3434
(0,1,1,1,1,1,1,1,0,0,0,0,0,0,0)	9907	(0,1,1,1,1,1,1,1,0,1,1,1,1,1,1)	3434
(0,1,0,1,0,1,0,1,1,0,1,0,1,0,0)	9907	(0,1,0,0,0,0,0,1,0,0,0,0,0,0,1)	3434
(0,0,1,0,1,0,1,1,0,1,0,1,0,1,0)	9907	(0,0,1,1,1,1,1,0,0,1,1,1,1,1,1)	3434
(0,0,0,1,0,0,0,1,1,1,1,0,1,1,0)	9907	(0,0,0,1,0,0,0,0,1,0,0,0,0,0,1)	3434
(0,1,1,0,1,1,1,1,0,0,0,1,0,0,0)	9907	(0,1,1,0,1,1,1,0,0,1,1,1,1,1,1)	3434
(0,1,0,0,0,1,0,1,1,0,1,1,1,0,0)	9907	(0,1,0,1,0,0,0,1,1,0,0,0,0,0,1)	3434
(0,0,1,1,1,0,1,1,0,1,0,0,0,1,0)	9907	(0,0,1,0,1,1,1,1,0,1,1,1,1,1,1)	3434
(0,0,0,1,0,0,0,1,1,1,1,0,1,1,1)	9908	(0,0,0,1,0,0,0,0,1,0,0,0,0,0,0)	3432
(0,0,0,1,0,0,0,0,1,1,1,0,1,1,1)	6476	(0,0,0,1,0,0,0,1,1,0,0,0,0,0,0)	3432
(0,1,0,0,0,1,0,1,1,0,1,1,1,0,1)	6476	(0,1,0,1,0,0,0,1,1,0,0,0,0,0,0)	3432
(0,1,0,0,0,1,0,0,1,0,1,1,1,0,1)	9907	(0,1,0,1,0,0,0,0,1,0,0,0,0,0,0)	3432
(0,0,0,0,0,0,0,1,1,1,1,0,1,1,1)	9544	(0,0,0,0,0,0,0,1,1,0,0,1,0,0,0)	2704
(0,0,0,1,0,0,0,0,1,1,1,1,1,1,1)	6840	(0,0,0,1,0,0,0,1,1,0,0,1,0,0,0)	2704
(0,1,0,0,0,1,0,1,1,0,1,0,1,0,1)	9544	(0,1,0,0,0,0,0,0,1,0,0,1,0,0,0)	2704
(0,1,0,1,0,1,0,0,1,0,1,1,1,0,1)	6840	(0,1,0,1,0,0,0,0,1,0,0,1,0,0,0)	2704
(0,0,0,0,0,0,0,1,1,1,1,1,1,0,1)	9894	(0,0,0,0,0,0,0,1,1,0,0,0,0,1,0)	3404
(0,1,0,0,0,0,0,0,1,1,1,1,1,1,1)	6490	(0,1,0,1,0,1,0,1,1,0,0,1,0,1,0)	3404
(0,1,0,1,0,1,0,0,1,0,1,0,1,1,1)	9894	(0,1,0,0,0,0,0,0,1,0,0,0,0,1,0)	3404
(0,0,0,1,0,1,0,1,1,0,1,0,1,0,1)	6490	(0,0,0,1,0,1,0,0,1,0,0,1,0,1,0)	3404
(0,0,0,1,0,0,0,1,1,1,1,0,1,0,1)	9894	(0,0,0,1,0,0,0,0,1,0,0,0,0,1,0)	3404
(0,1,0,1,0,0,0,0,1,1,1,0,1,1,1)	6490	(0,1,0,0,0,1,0,0,1,1,0,1,0,1,0)	3404
(0,1,0,0,0,1,0,0,1,0,1,1,1,1,1)	9894	(0,1,0,1,0,0,0,1,1,0,0,0,0,1,0)	3404
(0,0,0,0,0,1,0,1,1,0,1,1,1,0,1)	6490	(0,0,0,0,0,1,0,1,1,1,0,1,0,1,0)	3404

Table 9. Symmetric function in Dimension 16 with Maximum AI

v_f	weight	SANF vector	max $\lvert W_f \rvert$
(0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,1)	39203	(0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1)	12870
(0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1)	26333	(0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1)	12870
(0,1,0,1,0,1,0,1,1,0,1,0,1,0,1,0,1)	39203	(0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1)	12870
(0,1,0,1,0,1,0,1,0,0,1,0,1,0,1,0,1)	26333	(0,1,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1)	12870
(0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,0)	39202	(0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0)	12868
(0,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0)	39202	(0,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0)	12868
(0,1,0,1,0,1,0,1,1,0,1,0,1,0,1,0,0)	39202	(0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0)	12868
(0,0,1,0,1,0,1,0,1,1,0,1,0,1,0,1,0)	39202	(0,0,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0)	12868
(0,0,0,0,1,0,0,0,1,1,1,1,0,1,1,1,0)	39202	(0,0,0,0,1,1,1,1,1,0,0,0,0,0,0,0,0)	12868
(0,1,1,1,0,1,1,1,1,0,0,0,1,0,0,0,0)	39202	(0,1,1,0,0,0,0,0,1,0,0,0,0,0,0,0,0)	12868
(0,1,0,1,1,1,0,1,1,0,1,0,0,0,1,0,0)	39202	(0,1,0,0,1,1,1,1,1,0,0,0,0,0,0,0,0)	12868
(0,0,1,0,0,0,1,0,1,1,0,1,1,1,0,1,0)	39202	(0,0,1,0,0,0,0,0,1,0,0,0,0,0,0,0,0)	12868
(0,0,0,0,1,0,0,0,1,1,1,1,0,1,1,1,1)	39203	(0,0,0,0,1,1,1,1,1,0,0,0,0,0,0,0,1)	12870
(0,0,0,0,1,0,0,0,0,1,1,1,0,1,1,1,1)	26333	(0,0,0,0,1,1,1,1,0,1,1,1,1,1,1,1,1)	12870
(0,1,0,1,1,1,0,1,1,0,1,0,0,0,1,0,1)	39203	(0,1,0,0,1,1,1,1,1,0,0,0,0,0,0,0,1)	12870
(0,1,0,1,1,1,0,1,0,0,1,0,0,0,1,0,1)	26333	(0,1,0,0,1,1,1,1,0,1,1,1,1,1,1,1,1)	12870
(0,1,1,1,1,1,1,1,0,0,0,0,0,0,0,0,1)	26333	(0,1,1,1,1,1,1,1,0,1,1,1,1,1,1,1,1)	12870
(0,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,1)	39203	(0,1,1,1,1,1,1,1,1,0,0,0,0,0,0,0,1)	12870
(0,0,1,0,1,0,1,0,0,1,0,1,0,1,0,1,1)	26333	(0,0,1,1,1,1,1,1,0,1,1,1,1,1,1,1,1)	12870
(0,0,1,0,1,0,1,0,1,1,0,1,0,1,0,1,1)	39203	(0,0,1,1,1,1,1,1,1,0,0,0,0,0,0,0,1)	12870
(0,1,1,1,0,1,1,1,0,0,0,1,0,0,0,1)	26333	(0,1,1,1,0,0,0,0,1,1,1,1,1,1,1,1)	12870
(0,1,1,1,0,1,1,1,1,0,0,0,1,0,0,0,1)	39203	(0,1,1,1,0,0,0,0,1,0,0,0,0,0,0,0,1)	12870
(0,0,1,0,0,0,1,0,0,1,0,1,1,1,0,1,1)	26333	(0,0,1,1,0,0,0,0,0,1,1,1,1,1,1,1,1)	12870
(0,0,1,0,0,0,1,0,1,1,0,1,1,1,0,1,0)	39203	(0,0,1,1,0,0,0,0,1,0,0,0,0,0,0,0,1)	12870