Information and Computation 208 (2010) 341–350

Contents lists available at ScienceDirect

Information and Computation

journal homepage: www.elsevier.com/locate/ic

9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class☆

Selçuk Kavut*, Melek Diker Yücel

Department of Electrical Engineering and Institute of Applied Mathematics, Middle East Technical University – ODTÜ, 06531 Ankara, Turkey

ARTICLE INFO

Article history:
Received 12 December 2008
Revised 5 August 2009
Available online 4 January 2010

Keywords:
Boolean functions
Combinatorial problems
Cryptography
Dihedral symmetry
Nonlinearity
Rotational symmetry

ABSTRACT

We give a new lower bound to the covering radius of the first order Reed–Muller code $RM(1,n)$, where $n \in \{9, 11, 13\}$. Equivalently, we present the n-variable Boolean functions for $n \in \{9, 11, 13\}$ with maximum nonlinearity found till now. In 2006, 9-variable Boolean functions having nonlinearity 241, which is strictly greater than the bent concatenation bound of 240, have been discovered in the class of Rotation Symmetric Boolean Functions (RSBFs) by Kavut, Maitra and Yücel. To improve this nonlinearity result, we have firstly defined some subsets of the n-variable Boolean functions as the generalized classes of "k-RSBFs and k-DSBFs (k-Dihedral Symmetric Boolean Functions)", where k is a positive integer dividing n. Secondly, utilizing a steepest-descent like iterative heuristic search algorithm, we have found 9-variable Boolean functions with nonlinearity 242 within the classes of both 3-RSBFs and 3-DSBFs. Thirdly, motivated by the fact that RSBFs are invariant under a special permutation of the input vector, we have classified all possible permutations up to the linear equivalence of Boolean functions that are invariant under those permutations.

1. Introduction

On odd number of input variables n, constructing Boolean functions with maximum possible nonlinearity is an open problem in the area of cryptography and combinatorics. The problem is also related to the upper bound $\lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \rfloor$ on the covering radius of the first order Reed–Muller code [3], which is later improved [4] as $2\lfloor 2^{n-2} - 2^{\frac{n}{2}-2} \rfloor$. Boolean functions on even number of input variables n, attaining the maximum nonlinearity of $\left(2^{n-1} - 2^{\frac{n}{2}-1}\right)$ are called the bent functions [5]. For odd n, the nonlinearity value $\left(2^{n-1} - 2^{\frac{n-1}{2}}\right)$ is known as the *bent concatenation bound*. In Table 1, we present the bent concatenation bound for $7 \leqslant n \leqslant 15$, together with recent nonlinearity results [4,6–9].

For odd $n \leqslant 7$, it is known that the maximum nonlinearity is equal to the bent concatenation bound [10,11]. However, in 1983, using combinatorial techniques and search methods, Patterson and Wiedemann [9] constructed 15-variable Boolean functions with nonlinearity 16,276, exceeding the bent concatenation bound by 20. Utilizing those 15-variable functions it is possible to obtain functions with nonlinearity $\left(2^{n-1} - 2^{\frac{n-1}{2}} + 20 \times 2^{\frac{n-15}{2}}\right)$ for odd $n \geqslant 15$. Astoundingly, for the cases of $n = 9, 11, 13$, the maximum nonlinearity known until 2006 was still equal to the bent concatenation bound.

☆ This work is partially presented in [1,2].

* Corresponding author.
E-mail addresses: skavut@gyte.edu.tr (S. Kavut), melekdy@metu.edu.tr (M. Diker Yücel).

0890-5401/$ - see front matter © 2009 Elsevier Inc. All rights reserved.
doi:10.1016/j.ic.2009.12.002

Table 1
Summary of nonlinearity results for $n = 7, 9, 11, 13, 15$.

n	7	9	11	13	15
Bent concatenation bound: $2^{n-1} - 2^{\frac{n-1}{2}}$	56	240	992	4032	16,256
Nonlinearity results in [6]	–	241	994	4036	16,264
Balanced function nonlinearities in [7,8]	–	–	–	4036	16,272
Our nonlinearity results	–	242	996	4040	16,272
Patterson–Wiedemann construction [9]	–	–	–	–	16,276
Upper bound [4]	56	244	1000	4050	16,292

In 2006, 9-variable Rotation Symmetric Boolean Functions (RSBFs) with nonlinearity 241 $\left(= 2^{9-1} - 2^{\frac{9-1}{2}} + 1\right)$ were discovered [6], which led to the construction of functions with nonlinearity exceeding the bent concatenation bound by $2^{\frac{n-9}{2}}$, for odd $n \geqslant 9$. Such functions were attained utilizing the steepest-descent like iterative algorithm that first appeared in [12] and then was suitably modified in [6] for a search in the class of RSBFs.

RSBFs seem to be *rich* in terms of highly nonlinear functions and there is a close relation between RSBFs and idempotents [13,14]. Considering a Boolean function f as a mapping from $GF(2^n) \to GF(2)$, the functions for which $f(\alpha^2) = f(\alpha)$ for any $\alpha \in GF(2^n)$, are referred to as idempotents. As pointed out in [13,14], the idempotents can be regarded as RSBFs with proper choice of basis. In [9], 15-variable Patterson–Wiedemann functions having nonlinearity 16,276 are also identified in the idempotent class.

As the size of the RSBF class is much smaller $\left(\approx 2^{\frac{2^n}{n}}\right)$ than the total size of n-variable Boolean functions $\left(2^{2^n}\right)$, an exhaustive search is possible for 9-variable RSBFs. In [15], such a search has shown that there is no 9-variable RSBF having nonlinearity greater than 241. So, we feel like increasing the search space of the heuristic in order to find functions with higher nonlinearity.

Motivated by this fact, we firstly propose the generalized k-RSBFs, as functions which satisfy $f(\alpha^{2^k}) = f(\alpha)$, where $1 \leqslant k|n$. Note that if $k = 1$, the resulting class corresponds to conventional RSBFs, and for $k = n$, generalized k-RSBFs cover the entire space. In the space of k-RSBFs, we also define the generalized class of k-DSBFs (k-Dihedral Symmetric Boolean Functions) as a subset of k-RSBFs by imposing the condition of invariance under the action of dihedral group.

Secondly, we have used the steepest-descent like iterative algorithm in [6] for a search in the generalized 3-RSBF and 3-DSBF classes. This search has successfully ended up with 9-variable functions in both of these classes, having nonlinearity 242, and absolute indicator values of 32, 40 and 56. This result shows that the covering radius of the first order Reed–Muller code $RM(1, 9)$ is at least 242. This result is also important for $n = 11$ and $n = 13$, since the bent concatenation of 9-variable functions with nonlinearity 242 leads to the construction of 11-variable and 13-variable functions with nonlinearities exceeding the bent concatenation bound by $2 \times 2^{\frac{n-9}{2}}$.

Thirdly, knowing the fact that k-RSBFs and k-DSBFs are invariant under some special types of permutations on input vectors, we have considered the possibility of other rich classes that are invariant under some permutations. Linearly equivalent Boolean functions [16] f and g, where $f = g(Ax)$ and A is an invertible matrix, have the same nonlinearity; therefore, while searching for highly nonlinear functions, it is quite logical to classify all $n!$ permutations up to the linear equivalence of Boolean functions that are invariant under them. More specifically, for 9-variable Boolean functions, we classify 9! many permutations into 30 classes, which are different up to the linear equivalence of Boolean functions that are invariant under them. Then for each class, by picking up a representative permutation arbitrarily, we have searched the corresponding set of Boolean functions. In some of these sets, we have consequently obtained 9-variable Boolean functions with nonlinearity 242 and absolute indicator values of 40, 48 and 56. So, our aim of defining other rich classes is accomplished. We note, however, that the presented functions do not contain any zero in their Walsh spectra; therefore, they cannot be linearly transformed to balanced functions.

In the following section, after reviewing some basic definitions related to Boolean functions, we present preliminaries of permutation group actions. In Section 3, we introduce the generalized rotation symmetric and dihedral symmetric Boolean functions. Classification of permutations on inputs of 9-variable Boolean functions, with respect to the linear equivalence of Boolean functions that are invariant under them, is presented in Section 4. Different results related to 9-variable Boolean functions with nonlinearity 242 are presented in Sections 3 and 4.

2. Preliminaries

2.1. Boolean functions

An n-variable Boolean function $f(x)$ produces a single-bit result for each n-bit input vector $x = (x_0, \ldots, x_{n-1})$, which may be considered as a mapping from $\{0, 1\}^n$ into $\{0, 1\}$. $f(x)$ is basically represented by its *truth table*, that is, a binary vector of length 2^n,

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

We represent the set of all n-variable Boolean functions by $\mathcal{B}_n$; clearly $|\mathcal{B}_n| = 2^{2^n}$. A binary vector g has the *Hamming weight* $wt(g)$ equal to the number of its nonzero elements. The *Hamming distance* between two binary vectors g and h, both having the same length, is defined as the number of places for which g and h differ, i.e., $d(g,h) = wt(g \oplus h)$, where $\oplus$ denotes the addition over $GF(2)$. An n-variable Boolean function f is called *balanced* if $wt(f) = 2^{n-1}$.

The *algebraic normal form* (ANF) of a Boolean function is defined as its unique representation in the form of a multivariate polynomial over $GF(2)$,

$$f(x_0,\ldots,x_{n-1}) = c \oplus \bigoplus_{0 \leqslant i \leqslant n-1} a_i x_i \oplus \bigoplus_{0 \leqslant i < j \leqslant n-1} a_{ij} x_i x_j \oplus \ldots \oplus a_{01\ldots n-1} x_0 x_1 \ldots x_{n-1},$$

where the coefficients $c, a_i, a_{ij}, \ldots, a_{01\ldots n-1} \in \{0,1\}$. The *algebraic degree*, or simply the degree of f, is the number of variables in the highest order product term with nonzero coefficient, which is denoted by $deg(f)$.

A Boolean function is called *affine* if its degree is at most one. The set of all n-variable affine functions is represented by A_n. The nonlinearity of an n-variable Boolean function f is defined as its minimum distance to any affine function, i.e.,

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

Boolean functions used in cryptographic systems must be highly nonlinear to resist best affine approximation and correlation attacks [17,18].

The *Walsh transform* of an n-variable Boolean function $f(x)$ is an integer valued function over $\{0,1\}^n$ defined as

$$W_f(w) = \sum_{x \in \{0,1\}^n} (-1)^{f(x)} (-1)^{\langle x,w \rangle},$$

where $x = (x_0,\ldots,x_{n-1})$, $w = (w_0,\ldots,w_{n-1}) \in \{0,1\}^n$ and $\langle x,w \rangle = x_0 w_0 \oplus \ldots \oplus x_{n-1} w_{n-1}$.

The nonlinearity of an n-variable Boolean function $f(x)$ can be alternatively expressed by means of its Walsh spectrum, i.e.,

$$nl(f) = \frac{1}{2}\left(2^n - \max_{w \in \{0,1\}^n} |W_f(w)|\right).$$

The autocorrelation function of $f(x)$ is given by

$$r_f(d) = \sum_{x \in \{0,1\}^n} (-1)^{f(x)} (-1)^{f(x \oplus d)},$$

where $d = (d_0,\ldots,d_{n-1}) \in \{0,1\}^n$. The autocorrelation value having the maximum magnitude, excluding $r_f(0,\ldots,0)$, is also known as the absolute indicator [19] and denoted as

$$\Delta_f = \max_{d \neq (0,\ldots,0) \in \{0,1\}^n} |r_f(d)|.$$

A Boolean function is balanced if and only if its Walsh spectrum value is zero at the origin. On the other hand, if an unbalanced Boolean function $g(x)$ contains a zero in its Walsh spectrum except the origin, say $W_g(u) = 0$ and $u \neq (0,\ldots,0)$, it can be linearly transformed into a balanced function $f(x) = g(x) \oplus \langle x,u \rangle$, which has the same nonlinearity and absolute indicator; i.e., $nl(f) = nl(g)$ and $\Delta_f = \Delta_g$. Bent functions are not balanced but they have the largest possible nonlinearity $\left(2^{n-1} - 2^{\frac{n}{2}-1}\right)$ and the smallest possible absolute indicator (0) values.

2.2. Group action by permutation groups

A group G is said to act on a set X if there is a mapping $\phi : G \times X \to X$ denoted as $g \cdot x$, which satisfies the following two axioms for all elements $x \in X$.

1. $e \cdot x = x$ where e stands for the identity element of G.
2. $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G$.

The mapping ϕ is called the *group action* and the set X is called a G-set. The *orbit* of x is defined as the set $G(x) = \{g \cdot x | g \in G\}$, i.e., the group action moves x to its orbit. As the set of orbits of X under the action of G, denoted by $\mathcal{G}$, constitutes a partition of X, the corresponding equivalence relation is defined by $x \sim y$ iff there exists a $g \in G$ such that $g \cdot x = y$. Hence, the orbits form the equivalence classes under this relation.

Let G be a permutation group acting on $\{0,1\}^n$, and consider the class of n-variable Boolean functions which are invariant under the action of G, i.e., any Boolean function f in the class satisfies the condition for each $x \in \{0,1\}^n, f(x) = f(y)$, for all $y \in G(x)$. As a consequence of the invariance property, the class composes a subclass of $\mathcal{B}_n$, and knowing the number of orbits, i.e., $|\mathcal{G}|$, it contains $2^{|\mathcal{G}|}$ many n-variable Boolean functions, each satisfying the given condition. The value of $|\mathcal{G}|$ can be determined using Burnside's Lemma.

Lemma 1 (Burnside's Lemma). *Let G be a group of permutations acting on a set X, and $fix_X(g) = \{x \in X | g \cdot x = x\}$ for each $g \in G$. Then the number of orbits induced on X is given by*

$$\frac{1}{|G|}\sum_{g\in G}|fix_X(g)|.$$

Let us represent an orbit by its lexicographically first element denoted by Λ_i. The Boolean function f which is invariant under the action of G, can be represented by $(f(\Lambda_0),\ldots,f(\Lambda_{|\mathcal{G}|-1}))$, where $\Lambda_0,\ldots,\Lambda_{|\mathcal{G}|-1}$ are again arranged lexicographically. Clearly, this representation is shorter than the truth table of f. Further, it can be shown [20] that $W_f(u) = W_f(v)$ if $u \in G(v)$, implying that the Walsh spectrum of f can be at most $|\mathcal{G}|$ valued. Then, defining a $|\mathcal{G}| \times |\mathcal{G}|$ matrix $\mathcal{M}$ as $\mathcal{M}_{i,j} = \sum_{x\in G(\Lambda_i)}(-1)^{\langle x,\Lambda_j\rangle}$, the Walsh spectrum of f can be calculated as [20]

$$W_f(\Lambda_j) = \sum_{i=0}^{|\mathcal{G}|-1}(-1)^{f(\Lambda_i)}\mathcal{M}_{i,j}.$$

3. Generalized rotation and dihedral symmetric Boolean functions

In the following, we firstly propose the generalized class of "k-rotation symmetric Boolean functions (k-RSBFs)" in Definition 1, after recalling the conventional RSBFs. Secondly, we describe "k-Dihedral Symmetric Boolean Functions (k-DSBFs)" in Definition 2, by generalizing the usual DSBFs.

Letting $(x_0,x_1,\ldots,x_{n-1}) \in \{0,1\}^n$, the (left) i-cyclic shift operator ${\rho^i}_n$ on n-tuples is defined as

$${\rho^i}_n(x_0,x_1,\ldots,x_{n-1}) = (x_{(0+i) \bmod n},\ldots,x_{(n-1+i) \bmod n}),$$

for $1 \leqslant i \leqslant n$. A Boolean function f is called *rotation symmetric* if for each input $(x_0,\ldots,x_{n-1}) \in \{0,1\}^n, f\left({\rho^1}_n(x_0,\ldots,x_{n-1})\right) = f(x_0,\ldots,x_{n-1})$. That is, RSBFs are invariant under all cyclic rotations of the inputs. The inputs of a rotation symmetric Boolean function can be divided into orbits so that each orbit consists of all cyclic shifts of one input. An orbit generated by $(x_0,x_1,\ldots,x_{n-1})$ is denoted by $G_n(x_0,x_1,\ldots,x_{n-1}) = \{{\rho^i}_n(x_0,x_1,\ldots,x_{n-1}) |\ 1 \leqslant i \leqslant n\}$ and the number of such orbits is represented by $g_n\left(\approx 2^{\frac{2^n}{n}}\right)$. More specifically, using Lemma 1 g_n can be shown [21] to be equal to $\frac{1}{n}\sum_{t|n}\phi(t)2^{\frac{n}{t}}$, where $\phi(t)$ is the Euler's phi-function. The total number of n-variable RSBFs is 2^{g_n}.

Definition 1. Let $1 \leqslant k \leqslant n, k|n$. An n-variable Boolean function f is called k-rotation symmetric if f is invariant under ${\rho^k}_n$, i.e., for each input $(x_0,\ldots,x_{n-1}) \in \{0,1\}^n, f\left({\rho^k}_n(x_0,\ldots,x_{n-1})\right) = f(x_0,\ldots,x_{n-1})$.

So, the k-rotation symmetric Boolean functions are invariant under k-cyclic rotations of inputs by definition. An orbit of $(x_0,x_1,\ldots,x_{n-1})$ under the action of ${\rho^k}_n$ is ${G^k}_n(x_0,x_1,\ldots,x_{n-1}) = \left\{{\rho^i}_n(x_0,x_1,\ldots,x_{n-1}) \,|\, i = k, 2k, 3k,\ldots,n\right\}$. For example, ${G^3}_9(101\ 001\ 111) = \{(001\ 111\ 101), (111\ 101\ 001), (101\ 001\ 111)\}$.

If $g_{n,k}$ is the number of distinct orbits in the k-RSBF class of n-variable functions, one can show that $g_{n,k} = \frac{k}{n}\sum_{t|\frac{n}{k}}\phi(t)2^{\frac{n}{t}}$, where $\phi(t)$ is the Euler's phi function. $g_{n,k}$ is approximately equal to $2^{k\frac{2^n}{n}}$.

Before defining the generalized class of "k-Dihedral Symmetric Boolean Functions", we recall the conventional DSBF definition. The class of DSBFs [22], a subset of the RSBF class, is invariant under the action of the dihedral group denoted by D_n. In addition to the (left) i-cyclic shift operator ${\rho^i}_n$ on n-tuples, which is defined previously, the dihedral group D_n also includes the reflection operator $\tau_n(x_0,x_1,\ldots,x_{n-1}) = (x_{n-1},\ldots,x_1,x_0)$. The $2n$ permutations of D_n are then defined as $\left\{{\rho^1}_n, {\rho^2}_n,\ldots,{\rho^{n-1}}_n, {\rho^n}_n, \tau_n{\rho^1}_n, \tau_n{\rho^2}_n,\ldots,\tau_n{\rho^{n-1}}_n, \tau_n{\rho^n}_n\right\}$. The dihedral group D_n generates [23] equivalence classes in the set $\{0,1\}^n$. Let d_n be the number of such partitions. The following proposition gives the exact count of d_n [22], [24, p.184].

Proposition 1. *Let d_n be the total number of orbits induced by the dihedral group D_n acting on $\{0,1\}^n$. Then $d_n = g_n/2 + l$, where, $g_n = \frac{1}{n}\sum_{t|n}\phi(t)2^{\frac{n}{t}}$ is the number of rotation symmetric classes [21], $\phi(t)$ is the Euler's phi-function and*

$$l = \begin{cases} \frac{3}{4}2^{\frac{n}{2}}, & \text{if } n \text{ is even,} \\ 2^{\frac{n-1}{2}}, & \text{if } n \text{ is odd.} \end{cases}$$

Since there are 2^{d_n} many n-variable DSBFs and $d_n \approx 2^{\frac{2^n}{2n}}$, a reduction in the size of the search space over the size of RSBFs is provided.

Table 2
Comparison of the orbit counts g_n, d_n, $g_{n,k}$ and $d_{n,k}$ (for $n = 4, 6, \ldots, 15$, and all integers k, which divide n).

n		k	2	3	4	5	6	7
4	$g_4 = 6$	$g_{4,k}$	10	–	–	–	–	–
	$d_4 = 6$	$d_{4,k}$	7	–	–	–	–	–
6	$g_6 = 14$	$g_{6,k}$	24	36	–	–	–	–
	$d_6 = 13$	$d_{6,k}$	16	24	–	–	–	–
8	$g_8 = 36$	$g_{8,k}$	70	–	136	–	–	–
	$d_8 = 30$	$d_{8,k}$	43	–	76	–	–	–
9	$g_9 = 60$	$g_{9,k}$	–	176	–	–	–	–
	$d_9 = 46$	$d_{9,k}$	–	104	–	–	–	–
10	$g_{10} = 108$	$g_{10,k}$	208	–	–	528	–	–
	$d_{10} = 78$	$d_{10,k}$	120	–	–	288	–	–
12	$g_{12} = 352$	$g_{12,k}$	700	1044	1376	–	2080	–
	$d_{12} = 224$	$d_{12,k}$	382	570	720	–	1072	–
14	$g_{14} = 1182$	$g_{14,k}$	2344	–	–	–	–	8256
	$d_{14} = 687$	$d_{14,k}$	1236	–	–	–	–	4224
15	$g_{15} = 2192$	$g_{15,k}$	–	6560	–	10,944	–	–
	$d_{15} = 1224$	$d_{15,k}$	–	3408	–	5600	–	–

Definition 2. Let $1 \leqslant k \leqslant n, k|n$. An n-variable Boolean function f is called k-dihedral symmetric if f is invariant under both ${\rho^k}_n$ and τ_n.

As the class of DSBFs is a subspace of RSBFs, the generalized class of k-DSBFs is a subspace of k-RSBFs. When Proposition 1 is applied to k-dihedral symmetric functions, we obtain the following corollary.

Corollary 1. *Let $d_{n,k}$ be the number of distinct orbits, in the class of k-DSBFs of n variables. Then, $d_{n,k} = g_{n,k}/2 + l$, where, $g_{n,k} = \frac{k}{n}\sum_{t|\frac{n}{k}} \phi(t)2^{\frac{n}{t}}$ is the number of k-rotation symmetric classes, $\phi(t)$ is the Euler's phi-function and*

$$l = \begin{cases} 2^{\frac{n}{2}-1}, & \text{if } n \text{ is even, } k \text{ is even,} \\ \frac{3}{4}2^{\frac{n}{2}}, & \text{if } n \text{ is even, } k \text{ is odd,} \\ 2^{\frac{n-1}{2}}, & \text{if } n \text{ is odd.} \end{cases}$$

Table 2 compares the orbit counts of RSBFs, DSBFs, k-rotational classes and k-dihedral classes for $k|n$, $n \leqslant 15$.

3.1. 9-variable 3-DSBFs and 3-RSBFs

We have made a search for a highly nonlinear 9-variable function in the generalized 3-RSBF and 3-DSBF classes. This search has successfully ended up with functions having nonlinearity 242, presented in Appendix A, in both of these classes. As mentioned previously, we have utilized the steepest-descent like iterative search algorithm, which was used in [6] to discover 9-variable RSBFs having nonlinearity 241. The details, which can be found in the related literature, are extraneous for present purposes. We only note that it is an efficient search technique with an outstanding ability to escape from local optima.

It is clear that using one of these 9-variable functions (say f) and a 2-variable bent function (say g), the 11-variable function $g(y_0, y_1) \oplus f(x_0, \ldots, x_8)$ with the highest known nonlinearity of $2^{11-1} - 2^{\frac{11-1}{2}} + 4 = 996$, can be obtained. This technique is called *bent-concatenation*. Similarly $h(y_0, y_1, y_2, y_3) \oplus f(x_0, \ldots, x_8)$ is the most nonlinear 13-variable function known to date, with nonlinearity $2^{13-1} - 2^{\frac{13-1}{2}} + 8 = 4040$, where h is a 4-variable bent function and f is one of the 9-variable functions with nonlinearity 242. We think this is a significant improvement on the results of [6], which can be summarized as in the following theorem:

Theorem 1. *Let n be an odd integer greater than 7. There exist n-variable Boolean functions having nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 2 \times 2^{\frac{n-9}{2}}$.*

Since for odd $n \geqslant 15$, the nonlinearity given by Theorem 1 is less than the nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 20 \times 2^{\frac{n-15}{2}}$ obtained in [9], this result is significant for odd $9 \leqslant n \leqslant 13$.

Our search applied to the space of 9-variable 3-DSBFs having size 2^{104} (see Table 2) leads to several unbalanced 9-variable functions with nonlinearity 242. Two examples of such functions (f_1 and f_2) with absolute indicator values 32 and 40 are given in Appendix A.

Using a computer system with Pentium IV 2.8 GHz processor and 256 MB RAM, a typical run of the search algorithm takes 1 min and 17 s. We have carried out 100 runs, each starting with a randomly chosen Boolean function in the space of 9-variable 3-DSBFs. The algorithm has produced 152 functions with the nonlinearity 241, and 36 many 3-DSBFs having nonlinearity 242.

Additionally, we have applied the search strategy to 9-variable 3-RSBFs (the size of the search space is now 2^{176} as can be seen from Table 2), for which we initiate the search algorithm with a 9-variable 3-DSBF having nonlinearity 242. Then we have obtained some 9-variable 3-RSBFs (which are not in 3-DSBFs) having nonlinearity 242, absolute indicator 56, and algebraic degree 7. An example of such a function is f_3, presented in Appendix A.

3.2. 11 and 13-variable DSBFs

We now present our computer search results for 11 and 13-variable DSBFs, with nonlinearities 994 and 4036, respectively. It should be noticed that those functions have exactly the same nonlinearities, as those would be obtained by bent-concatenating 9-variable functions with nonlinearity 241.

In [22], the class of Dihedral Symmetric Boolean Functions (DSBFs), a subset of the RSBF class, which is invariant under the action of the dihedral group, is introduced. It has been shown that some of the 9-variable RSBFs having nonlinearity 241 also belong to this subset, demonstrating the richness of DSBFs in terms of high nonlinearity. Motivated by this, we have carried out a systematic search in the DSBF class for $n = 11, 13$, and found Boolean functions having nonlinearity $> 2^{n-1} - 2^{\frac{n-1}{2}}$. More specifically, for 11-variable DSBFs, we have attained an 11-variable DSBF with nonlinearity 994 within the space of size 2^{126}.

For 13-variable DSBFs, in order to reduce the search space $\left(2^{380}\right)$, we have applied some additional permutations on input vectors, and obtained a subset of size 2^{74}, in which we have found several 13-variable DSBFs with nonlinearity 4036 using the steepest-descent like search algorithm. To decrease the size $\left(2^{380}\right)$ of the search space, we apply the following permutation in addition to the permutations of dihedral group on input vectors

$$\pi(x_0, x_1, \ldots, x_{12}) = (x_0, x_2, x_4, x_6, x_8, x_{10}, x_{12}, x_1, x_3, x_5, x_7, x_9, x_{11})$$

such that for each input $(x_0, \ldots, x_{12}) \in \{0,1\}^{13}$,

$$f\left(\rho^1{}_n(x_0, \ldots, x_{12})\right) = f(\tau_n(x_0, \ldots, x_{12})) = f(\pi(x_0, \ldots, x_{12})) = f(x_0, \ldots, x_{12}),$$

and the search space of 13-variable DSBFs is reduced from 2^{380} to 2^{74}. f_5 given in Appendix A is a function found in this set with nonlinearity 4036, absolute indicator value 208, and algebraic degree 10.

A typical run takes 1 min using the computer system with Pentium IV 2.8 GHz processor and 256 MB RAM; and we have encountered two functions of nonlinearity 4036 in 500 runs. Then, exploiting the combinatorial search techniques similar to those used in [15], we have performed an efficient exhaustive search to enumerate 13-variable Boolean functions having nonlinearity $\geqslant 4036$ in this subset of size 2^{74}. The exhaustive search yields only 8 many Boolean functions having nonlinearity 4036 and there is no Boolean function with nonlinearity > 4036 in the subset. In addition, we note that among these functions, there is only one which is different up to the affine equivalence (given by Proposition 2 in [15]). The exhaustive search takes 22 days using the same computer system. Consequently, keeping in mind that some of 9-variable RSBFs with nonlinearity 241 also belong to the class of DSBFs [22], we get the following result:

Theorem 2. *Let n be odd and $9 \leqslant n \leqslant 13$. There exist Dihedral Symmetric Boolean Functions (DSBFs) on n variables having nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 2^{\frac{n-9}{2}}$.*

For the 11-variable DSBF case for which the size of search space is 2^{126}, we have carried out 8000 runs of the search algorithm, and found the 11-variable DSBF f_4, having nonlinearity 994, absolute indicator value 200, and algebraic degree 9 (see Appendix A for the truth table). A typical run of the search algorithm takes 1 min and 16 s using the same computer system.

4. Permutations on input vectors of 9-variable Boolean functions

As it is deduced from the discussion in the preceding section, RSBFs are invariant under a special type of permutation. To search for better cryptographic characteristics, we consider the possibility of other classes of Boolean functions that are invariant under some permutations. Since linearly equivalent functions have the same nonlinearity, it makes sense to classify all $n!$ permutations up to the linear equivalence of Boolean functions that are invariant under them. The classification is based on the following proposition, which is easy to prove.

Proposition 2. *Let f and g be Boolean functions which are invariant under arbitrary permutations π_f and π_g, respectively. If there exists a bijective linear mapping $L : \{0,1\}^n \to \{0,1\}^n$ such that $f(x) = g(L(x))$, i.e., $f = g \circ L$, then $\pi_f = (L^{-1} \circ \pi_g \circ L)$.*

Table 3 Classification of all possible 362,880 many permutations for 9-variable Boolean functions, and the best achieved nonlinearity result for each class.

Representative permutation	Number of permutations	Maximum number of input vectors in an orbit	Total number of distinct orbits	Best achieved nonlinearity result
(0,1,2,3,4,5,6,7,8)				
(*identity*)	1	1	512	240
(5,7,4,8,2,0,6,1,3)	945	2	272	240[6]
(3,1,7,0,5,4,6,2,8)	1260	2	288	240
(7,1,2,3,5,4,6,0,8)	378	2	320	240
(0,8,2,3,4,5,6,7,1)	36	2	384	240
(4,6,7,2,8,1,5,3,0)	**2240**	**3**	**176**	**242**[3,4]
(5,1,2,4,7,8,6,3,0)	3360	3	192	240
(0,1,2,8,4,5,6,3,7)	168	3	256	240
(1,4,7,5,6,2,0,3,8)	**11,340**	**4**	**140**	**242**[2]
(4,7,5,6,0,1,3,2,8)	11,340	4	168	240
(0,2,1,7,4,3,5,6,8)	7560	4	176	240
(0,8,2,3,4,1,6,5,7)	756	4	192	240
(0,7,2,5,4,1,3,6,8)	3024	5	128	239
(8,7,3,0,1,6,2,4,5)	**20,160**	**6**	**100**	**242**[1]
(0,2,1,4,5,6,7,8,3)	**30,240**	**6**	**104**	**242**
(7,1,0,3,4,2,8,6,5)	10,080	6	112	240
(7,4,0,5,1,8,6,2,3)	10,080	6	144	240
(8,4,3,2,1,7,5,6,0)	2520	6	144	240
(0,6,2,7,8,1,5,3,4)	7560	6	160	240
(8,1,3,2,4,5,0,7,6)	2520	6	192	240
(2,0,6,1,4,5,7,8,3)	25,920	7	80	240
(0,3,5,8,1,4,7,2,6)	45,360	8	72	240
(1,6,7,4,8,2,5,3,0)	**40,320**	**9**	**60**	**241**[5,7]
(5,8,6,7,2,0,1,3,4)	9072	10	80	240
(1,3,8,7,4,0,6,5,2)	18,144	10	96	240
(3,5,7,1,6,0,8,2,4)	15,120	12	88	240
(0,2,7,8,4,6,3,1,5)	15,120	12	96	240
(4,5,7,1,0,8,3,6,2)	25,920	14	60	240[7]
(6,5,1,4,7,2,3,0,8)	24,192	15	64	238
(4,8,1,2,6,7,5,0,3)	18,144	20	48	240[7]

[1] Nonlinearity result of 242 is attained in the subset of size 2^{74} in the set of size 2^{100}.
[2] Nonlinearity result of 242 is attained in the subset of size 2^{86} in the set of size 2^{140}.
[3] Nonlinearity result of 242 is attained in the subset of size 2^{104} in the set of size 2^{176}.
[4] The class contains the permutation corresponding to 3-RSBFs.
[5] The class contains the permutation corresponding to RSBFs.
[6] The class contains the permutation corresponding to 9-DSBFs.
[7] Nonlinearity result is obtained by exhaustive search.

Proof. Our hypotheses are $f = f \circ \pi_f, g = g \circ \pi_g, f = g \circ L$, and $g = f \circ L^{-1}$. Then,

$$f = g \circ L = g \circ \pi_g \circ L = f \circ L^{-1} \circ \pi_g \circ L = f \circ \pi_f.$$

Hence, $\pi_f = (L^{-1} \circ \pi_g \circ L)$.

Thus, we classify all possible permutations up to the equivalence

$$\pi_f \sim \pi_g \Leftrightarrow \exists L \text{ such that } \pi_f = (L^{-1} \circ \pi_g \circ L).$$

The classification can be accomplished through a computer program by exploiting the Jordan Normal Form for matrices. Specifically for 9-variable Boolean functions, in 9! (=362,880) permutations of the identity matrix, there are only 30 classes (see Table 3), which are different up to the equivalence defined above. Then, we apply the search algorithm for each class using its representative permutation and determine the corresponding nonlinearity. The algorithm identifies some of these classes as rich classes that yield new Boolean functions with nonlinearity 242 as emphasized in four rows of Table 3. As in the case of RSBFs, the maximum nonlinearity that can be found in the class of functions that are invariant under the representative permutation (1, 6, 7, 4, 8, 2, 5, 3, 0) with total number of distinct orbits 60 is 241, since this class is linearly equivalent to the class of RSBFs.

We have also carried out exhaustive searches in the spaces of sizes 2^{60} and 2^{48}, exploiting the combinatorial search techniques similar to those used in [15]. We have found that there is no Boolean function having nonlinearity greater than the bent concatenation bound of 240 in the classes of Boolean functions that are invariant under the representative permutations (4, 5, 7, 1, 0, 8, 3, 6, 2) and (4, 8, 1, 2, 6, 7, 5, 0, 3). The exhaustive search takes 38 h for the former (of size 2^{60}) and 1 min for the latter (of size 2^{48}) cases using the computer system described above.

From Table 3, it is seen that we have attained several 9-variable Boolean functions with nonlinearity 242, which we initially found in 3-DSBFs and 3-RSBFs, in the classes of sizes 2^{100}, 2^{104}, 2^{140}. In Appendix A, we present 9-variable Boolean

functions having nonlinearity 242 and different autocorrelation spectra from those of the functions found in 3-DSBFs and 3-RSBFs.

We have applied 100 runs of the search algorithm [6] to the space of size 2^{104} and found two 9-variable Boolean functions with nonlinearity 242, absolute indicator value 48, and algebraic degree 7. f_6 is one of these functions whose truth table is given in Appendix A. A typical run takes the same amount of time as for the case of 3-DSBFs (since the sizes of both spaces are the same).

Then, in order to reduce the search space, we have considered some subclasses. For this purpose, we have applied the reflection operator, which is defined as $\tau_n(x_0, x_1, \ldots, x_8) = (x_8, \ldots, x_1, x_0)$ for 9-variable Boolean functions, in addition to the representative permutation. As a result of this method, we have identified a subset of size 2^{74} in the set of size 2^{100}. In this subset, we have attained several 9-variable Boolean functions with nonlinearity 242, absolute indicators 40 and 64, and algebraic degree 7. We provide one of them, f_7, having absolute indicator 64 in Appendix A. We have carried out 100 runs of the search algorithm resulting in 9 many Boolean functions with nonlinearity 242 such that seven of them with absolute indicator value of 64, and the remaining with that of 40. A typical run takes 1 min and 4 s using the same computer system. Next, we have performed an exhaustive search, exploiting the combinatorial search techniques similar to those used in [15]; and we have found that there is no 9-variable Boolean function with nonlinearity greater than 242 in this subset of size 2^{74}. The exhaustive search takes four days using the computer system with Pentium IV 2.8 GHz processor and 256 MB RAM.

5. Conclusions

By suitably generalizing the class of RSBFs, we have introduced k-RSBFs, as functions which satisfy $f\left(\alpha^{2^k}\right) = f(\alpha)$, where the nonzero positive integer k divides n, and $\alpha \in GF(2^n)$. We have also defined the class of k-DSBFs as a subset of k-RSBFs imposing the condition of invariance under the action of dihedral group. Using the steepest-descent like iterative algorithm in [6,25] for a search in the generalized 3-DSBF and 3-RSBF classes, we have attained 9-variable 3-RSBFs and 3-DSBFs with nonlinearity 242. This result shows the existence of n-variable Boolean functions having nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 2 \times 2^{\frac{n-9}{2}}$ for $n = 9, 11, 13$. In [26], it is conjectured that the covering radius of $RM(1, n)$ is even and our nonlinearity result for $n = 9$ shows that the covering radius is at least 242. The upper bound given in [3] for the covering radius of $RM(1, 9)$ is 244.

Further, we have classified all possible permutations up to the linear equivalence of Boolean functions that are invariant under them. Specifically for $n = 9$, there are 30 such classes. Exploiting the same search algorithm [6], we have attained 9-variable Boolean functions having nonlinearity 242 in the class of size 2^{104}. We have then considered some subclasses by inserting permutation of the reflection operator τ_n to the representative permutation and found many functions with nonlinearity 242 as shown in Table 3. As an example, we have identified a subset of size as small as 2^{74}, in the set of size 2^{100}, having 9-variable Boolean functions with nonlinearity 242. Moreover, we have obtained an 11-variable DSBF having nonlinearity 994 and a 13-variable DSBF having nonlinearity 4036, which confirm the richness of DSBFs [22] in terms of high nonlinearity for $n = 11$ and 13.

We think that the results that we present contain significant information on the existence of maximum nonlinearity-Boolean functions with odd number of input variables, within the classes that are invariant under some permutations.

Acknowledgments

We acknowledge Dr. Gregor Leander's discussion on the linear equivalence of Boolean functions that are invariant under random permutations, which has helped us finding one missing class in Table 3.

Appendix A. Examples of functions with high nonlinearity

f_1 – The following is the truth table of f_1, which is a 9-variable, 3-DSBF having nonlinearity 242, absolute indicator value 32, and algebraic degree 7:

```
125425D30A398F36508C06817BEE122E250D973314F976AED58A3EA9120DA4FE
0E4D4575C42DD0426365EBA7FC5F45BE9B2F336981B5E1863618F49474F6FE00
```

f_2 – The function f_2 below is another 9-variable 3-DSBF having nonlinearity 242, absolute indicator value 40, and algebraic degree 7:

```
68B7EF2DA03B0D3EA00DB6A96DD99AEAFDB9C842B6D5DC8C4526CE0DD29020DB
B75FE3314568344E73688FF0CB2482E065231869E1AA4583765CC491F8A8DB12
```

f_3 – The truth table of f_3, a 9-variable 3-RSBF (which is not in 3-DSBFs) having nonlinearity 242, absolute indicator value 56, and algebraic degree 7 is:

3740B6A118A1E19642A85E2B7E2F3C3CB65FA0D95EC9DB1EA92BDB3666185AE0
087F5FE6E0757106A12FC918754C40E8A1BCCB7A714032A8961456E066E8A801

f_4 – The 11-variable DSBF f_4 having nonlinearity 994, absolute indicator value 200, and algebraic degree 9 has the truth table:

68C1F052AA14260999DD0365487844C6C397A7B6114A787724957BC46471F12D
F05F873ECC6E8A29034265887BD17A2A483583367B8FF1312C347E12FA1708F3
AA1433AF952B5BE9B5F02CA891985C92114A640C2D6380C57B9BB3027E991D8D
34C45B66D00E5B7D6ACF80EEAB021A430CE54E707AAD520DAB9D472F4081FF1F
89CC06215F1B8CAA973658CF27DAADD3CF36AA0118B0DDC08716D3D526E4C70D
065371D97C2054E458A2390BD550E5736ADAC2DF8B0A10492BACC3C317B381F7
1A21F52076CB3C3DB60144F836DF2AB32DDDE0EAC051FCBD8C8F10491299751F
41F0E96761AC6F053F888DE7234945F79C9B92B3703B19BF6545C557BBBF57FF

f_5 – The truth table of the 13-variable DSBF f_5 found in the reduced space of size (from 2^{380} to 2^{74}) with nonlinearity 4036, absolute indicator value 208, and algebraic degree 10 is:

177E7EF97EFCFF937FF8EBA0FAFBC71A7EFBEAD0EC8B8815EA99FADEA12A568D
7EE8EA8BF889B215FDB1848F80950677EDC883D3AE9DB2ED9D031888277CD4F7
7FEDE881ECDC948AFF90D0968B0C0676EFE3CE028524D4FAC114C666116C2A6B
F8E2A195815AF71A89FCD3A29B48BDE3C7F6155F139090904C2B2AA1F321AA3F
7EEEF8B2E881D107ECA1E3B5C665D088EAAE9354A710C37C81CB04E4156C3A28
ECAFEC0AB5ED504C85361D75B325AA88F4560730A4386C7C13537CF04CCD299B
FA85B81D9C129772D143368CFE2A43C88096AEB4B35E8809D3DE64959BE7A90E
A12BBF7D077227FA034FC601D340931535A159CF4C88CC17BB0B4D13C8990BAE
7EFCE8ACEAC18B0DE881C517E253407FF8F4C917EC5E9F32A12C3826F700C081
F889C9F8934B2770DC7B5710F44F2EF09146A5CA1530BD3107663CA14BCD0C81
F9A18DABB9F411C88A26ECF6364474B484321F7D47E33B779B5E58679CCD85D5
FA35626C042E4E419C244A902CF12EF5420E660B6EA0EE0570A0A4B64D86979E
FFCDD1728BC516A786F10348976A7F09B212350A0A78D5F1BFA85CD8350BA194
C015D72899F98F208E1B73E9C0950093B24AE7B96C65933782CAFC7BCCD715BC
9D0208CA8AAA7FE2147A2E49192BFBCD145A74FAF0790003E75B7451930B1736
1E76880372D3A1AB70F18590E1F5177A8E8B449F61B2075AF08597D6519ECCE9
7EEDEEF5FC90CDB4ED8CA10785CE10E3E881C147F523072FB81D274B71403EEF
FB81AE60F4C6122EB9A032EC96AA5A09C8171CF41ED05879BE7F5444A101D107
EAC481D3A197ABC0825E349E192A7A40A3A07BCA367F5300EE3424AE5DECAB15
C347647CD962E09806265E01DEA75B12117F3C3C1BA1D85771DBA0A751B58512
EE82891381B78D8FCE97AE741242F081C19C593CEDF4EB2C5A3874753A619B21
D1315E5802AE6AE6247FB95F5ECB6B3FC78A22A962842D2F82A1A0A3C026B276
FBDC1B632D1878F144700CFD70EC711687F05D3025D9870548B5AB5708EDAF76
700800F86C2951DB6CECCD01BDED51766E01CD11CD349F7C21A7943CC37ED6A9
EBAFE4B6B2133A49819BF1334739D86BD128EA42504A60C1876E6CCD6FEA11D3
8A1D17180E6650C810D86FD0A622FA179BAED88422E1E3D45F6651CFDD03D734
A0151733A72E48C196D6BE92C4EF4951D5EC028A2F5FE997B00182330101824E
DE5934CDAC2FCAD63CF43D33871F0B3EC00CA1DDAAB17BDEA1B5B67E13669EE1
93A6454915D5B5C9D088C8893AABB85D07742AC84CBC20C752C2099EFADBF1F6
077532896E64AB9DFA003F974105110AED6B238E6E753716821F05DE176E5A69
52B97F79C081414F3E08A60BC816CDDE3F41AA17C0779350B912AF76073E7AC9
C5FD819B602186BE79078F5C543E36C9BF158126D33EE6697712D6A9F4E1E997

f_6 – The 9-variable Boolean function f_6 (found in the space of size 2^{104}) of nonlinearity 242, absolute indicator value 48, and algebraic degree 7 is:

7B8F94BAD364DAC9931906F9465FF33E921E13D7552DAFD684757B662FDA3C68
FA8D94B3C3659B5FCC46FD1518050F97A1E02039AAF74337134F30AB5B41D9DE

f_7 – The 9-variable Boolean function f_7 (found in a subset of size 2^{74} obtained from the set of size 2^{100}) with nonlinearity 242, absolute indicator value 64, and algebraic degree 7 has the following truth table:

0331786B34D878855663A2E961F1CB4F779EBBF6881ABB24AC033E6C2B32E049
3D0891DB1888EA5E6F910310311532FC68D5F2A4B5BE6445E41F64299F0CC99A

References

[1] S. Kavut, M.D. Yücel, Generalized rotation symmetric and dihedral symmetric Boolean functions – 9 variable Boolean functions with nonlinearity 242, in: Proceedings of the 17th International Applied Algebra, Algebraic Algorithms, and Error Correcting Codes Symposium, Lecture Notes in Computer Science, vol. 4851, Bangalore, India, 2007, pp. 321–329.

[2] S. Kavut, M.D. Yücel, Random permutations on input vectors of Boolean functions, in: Proceedings of the Fourth International Workshop on Boolean Functions: Cryptography and Applications, BFCA'08, Copenhagen, Denmark, 2008, pp. 97–108.

[3] T. Helleseth, T. Kløve, J. Mykkeltveit, On the covering radius of binary codes, IEEE Transactions on Information Theory 24 (1978) 627–628.

[4] X.d. Hou, On the norm and covering radius of the first order Reed–Muller codes, IEEE Transactions on Information Theory 43 (3) (1997) 1025–1027.

[5] O.S. Rothaus, On bent functions, Journal of Combinatorial Theory, Series A 20 (1976) 300–305.

[6] S. Kavut, S. Maitra, M.D. Yücel, Search for Boolean functions with excellent profiles in the rotation symmetric class, IEEE Transactions on Information Theory 53 (5) (2007) 1743–1751, an earlier version of this paper is available under the title "There exist Boolean functions on n (odd) variables having nonlinearity $> 2^{n-1} - 2^{\frac{n-1}{2}}$ if and only if $n > 7$" at IACR eprint server, http://eprint.iacr.org/2006/181, May 28, 2006

[7] S. Maitra, S. Kavut, M.D. Yücel, Balanced Boolean function on 13-variables having nonlinearity greater than the bent concatenation bound, in: Proceedings of the Fourth International Workshop on Boolean Functions: Cryptography and Applications, BFCA'08, Copenhagen, Denmark, 2008, pp. 109–118.

[8] S. Sarkar, S. Maitra, Idempotents in the neighbourhood of Patterson–Wiedemann functions having Walsh spectra zeros, Designs, Codes and Cryptography, Special issue: Coding and Cryptography 9 (1–3) (2008) 95–103

[9] N.J. Patterson, D.H. Wiedemann, The covering radius of the $(2^{15}, 16)$ Reed–Muller code is at least 16,276, IEEE Transactions on Information Theory 29 (3) (1983) 354–356, see also the correction in IEEE Transactions on Information Theory, 36 (2) (1990) 443.

[10] E.R. Berlekamp, L.R. Welch, Weight distributions of the cosets of the (32, 6) Reed–Muller code, IEEE Transactions on Information Theory 18 (1) (1972) 203–207

[11] J.J. Mykkeltveit, The covering radius of the (128, 8) Reed–Muller code is 56, IEEE Transactions on Information Theory 26 (3) (1980) 359–362

[12] S. Kavut, M.D. Yücel, A new algorithm for the design of strong Boolean functions (in Turkish), in: Proceedings of the First National Cryptology Symposium, METU, Ankara, Türkiye, 2005, pp. 95–105.

[13] E. Filiol, C. Fontaine, Highly nonlinear balanced Boolean functions with a good correlation-immunity, in: Eurocrypt 1998, Lecture Notes in Computer Science, vol. 1403, 1998, pp. 475–488.

[14] C. Fontaine, On some cosets of the first-order Reed–Muller code with high minimum weight, IEEE Transactions on Information Theory 45 (4) (1999) 1237–1243

[15] S. Kavut, S. Maitra, S. Sarkar, M.D. Yücel, Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity >240, in: Proceedings of Indocrypt 2006, Lecture Notes in Computer Science, vol. 4329, Kolkata, India, 2006, pp. 266–279.

[16] F.J. MacWillams, N.J.A. Sloane, The Theory of Error Correcting Codes, North-Holland, Amsterdam, 1977.

[17] A. Canteaut, M. Trabbia, Improved fast correlation attacks using parity-check equations of weight 4 and 5, in: Proceedings of Eurocrypt 2000, Lecture Notes in Computer Science, vol. 1807, 2000, pp. 573–588.

[18] C. Ding, G. Xiao, W. Shan, The stability theory of stream ciphers, Lecture Notes in Computer Science, vol. 561, Springer, Berlin, 1991.

[19] X.M. Zhang, Y. Zheng, GAC – the criterion for global avalanche characteristics of cryptographic functions, Journal of Universal Computer Science 1 (5) (1995) 316–333

[20] P. Stănică, S. Maitra, J. Clark, Results on rotation symmetric bent and correlation immune Boolean functions, in: Proceedings of the Fast Software Encryption Workshop, FSE 2004, Lecture Notes in Computer Science, vol. 3017, New Delhi, India, 2004, pp. 161–177.

[21] P. Stănică, S. Maitra, Rotation symmetric Boolean functions – count and cryptographic properties, Discrete Applied Mathematics 156 (10) (2008) 1567–1580

[22] S. Maitra, S. Sarkar, D.K. Dalai, On dihedral group invariant Boolean functions, in: Proceedings of the Third International Workshop on Boolean Functions: Cryptography and Applications, BFCA'07, Paris, France, 2007, pp. 43–56.

[23] F.S. Roberts, Applied Combinatorics, Prentice-Hall, Englewood Cliffs, NJ, 1984.

[24] F. Harary, Graph Theory, Addison-Wesley, Reading, MA, 1972.

[25] S. Kavut, S. Maitra, M.D. Yücel, Autocorrelation spectra of balanced Boolean functions on odd number input variables with maximum absolute value $< 2^{\frac{n+1}{2}}$, in: Proceedings of the Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA'06, Rouen, France, 2006, pp. 73–86.

[26] R.A. Brualdi, N. Cai, V. Pless, Orphan structure of the first order Reed–Muller codes, Discrete Mathematics 102 (1992) 239–247.