Search for Boolean Functions With Excellent Profiles in the Rotation Symmetric Class

Selçuk Kavut, Subhamoy Maitra, and Melek D. Yücel

***Abstract*—For the first time Boolean functions on 9 variables having nonlinearity 241 are discovered, that remained as an open question in literature for almost three decades. Such functions are found by heuristic search in the space of rotation symmetric Boolean functions (RSBFs). This shows that there exist Boolean functions on n (odd) variables having nonlinearity $> 2^{n-1} - 2^{\frac{n-1}{2}}$ if and only if $n > 7$. Using similar search technique, balanced Boolean functions on 9, 10, and 11 variables are attained having autocorrelation spectra with maximum absolute value $< 2^{\lfloor \frac{n}{2} \rfloor}$. On odd number of variables, earlier such functions were known for 15, 21 variables; there was no evidence of such functions at all on even number of variables. In certain cases, our functions can be affinely transformed to obtain first-order resiliency or first-order propagation characteristics. Moreover, 10 variable functions having first-order resiliency and nonlinearity 492 are presented that had been posed as an open question at Crypto 2000. The functions reported in this paper are discovered using a suitably modified steepest descent based iterative heuristic search in the RSBF class along with proper affine transformations. It seems elusive to get a construction technique to match such functions.**

***Index Terms*—Autocorrelation, Boolean functions, combinatorial problems, cryptography, heuristic search, nonlinearity, rotational symmetry.**

I. Introduction

BOOLEAN functions with very high nonlinearity pose some of the most challenging problems in the area of symmetric cryptography and combinatorics. The problem is also related to the covering radius of the first-order Reed–Muller code. On even number of variables n, the maximum possible nonlinearity $2^{n-1} - 2^{\frac{n}{2}-1}$ is attained for the well-known bent functions [7], [34]. However, for the case when n is odd, the situation is more complicated and very few results have been available since 1972 as follows.

1) **Negative results.** In 1972 [1], it has been shown that the maximum nonlinearity of five-variable Boolean functions is 12 and in 1980 [28] it has been shown that the maximum nonlinearity of seven-variable Boolean functions is 56. Thus, for odd $n < 7$, the maximum nonlinearity of n-variable functions is $2^{n-1} - 2^{\frac{n-1}{2}}$.
2) **Positive results.** In 1983 [31], it has been shown that one can get Boolean functions on 15 variables having nonlinearity 16276 and using this result one can show that for odd $n \geq 15$, it is possible to get Boolean functions having nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 20 \cdot 2^{\frac{n-7}{2}}$.

The question for $n = 9, 11, 13$ stayed completely open; the maximum nonlinearity known for these cases was $2^{n-1} - 2^{\frac{n-1}{2}}$ and there was no proof or evidence (before this work) whether there are functions having nonlinearity strictly greater than that. In this paper, we show the existence of such functions. Our result shows that the covering radius of the $(2^9, 10)$ Reed–Muller code [18] is at least 241.

In the process of searching, we also find functions with very good autocorrelation properties. Boolean functions with very high nonlinearity and very low autocorrelation (for better confusion and diffusion) are important building blocks in both stream- and block-cipher implementations. This means that one needs Boolean functions such that the maximum absolute value in both the Walsh and autocorrelation spectra are low. The maximum absolute value in the autocorrelation spectrum of a Boolean function f is denoted by Δ_f. It has been conjectured in [42] that for any balanced function f on an odd number of variables n, $\Delta_f \geq 2^{\frac{n+1}{2}}$. However, the conjecture has been disproved for $n = 15$ in [20] and $n = 21$ in [10] by modifying the Patterson–Wiedemann type functions [31] and so far there has been no evidence of such functions for odd $n < 15$, which we present here.

For the first time, we make a systematic study for these functions and could discover 9-, 10-, and 11-variable balanced Boolean functions with maximum absolute value in the autocorrelation spectrum $< 2^{\lfloor \frac{n}{2} \rfloor}$. In particular, the Δ_f values are 24 for the 9-, 10-variable cases and 56 for the 11-variable case.

1) We find nine-variable functions f with nonlinearity 240, algebraic degree 7 and $\Delta_f = 24$. Further, some of these functions can be transformed to 1-resilient or PC(1) functions. This is the first time 1-resilient functions with maximum absolute value in the autocorrelation spectrum $< 2^{\frac{n-1}{2}}$ are demonstrated for any variable.
2) We find an 11-variable function f having nonlinearity 990, algebraic degree 10, and $\Delta_f = 56$; which can be transformed to a PC(1) function. Moreover, we find functions g with algebraic degree 9, nonlinearity 988, and $\Delta_g = 56$. Some of these functions can be transformed to 1-resilient functions or to PC(1)functions. Similar to the 9-variable case, for the 11-variable case we get 1-resilient functions with maximum absolute value in the autocorrelation spectrum $< 2^{\frac{n+1}{2}}$.

Manuscript received August 16, 2006; revised February 20, 2007. The material in this paper was presented in part at the Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA 06, LIFAR, University of Rouen, France, March 2006.

S. Kavut and M. D. Yücel are with the Department of Electrical and Electronics Engineering, Middle East Technical University–ODTÜ, 06531 Ankara, Turkey (e-mail: kavut@metu.edu.tr; melekdy@metu.edu.tr).

S. Maitra is with the Applied Statistics Unit, Indian Statistical Institute, Kolkata, PIN 700 108, India (e-mail: subho@isical.ac.in).

Communicated by A. Canteaut, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2007.894696

Let us concentrate on the balanced functions over even number of variables. In [19], a construction has been proposed having $\Delta_f < 2^{\frac{n}{2}} + \Delta_g$, where f is an n-variable (n even) balanced function and g is an $\frac{n}{2}$-variable one. Experimental results are available in [2], [13], [14] for eight-variable balanced functions having maximum absolute value in the autocorrelation spectrum as low as 16 which are better than the construction of [19]. Thus, one can see that for $n = 8$, functions f are available with $\Delta_f = 2^{\frac{n}{2}}$. Following a similar idea corresponding to the odd number of variables, the question for an even number of variables is whether there are balanced functions f on even number of variables such that $\Delta_f < 2^{\frac{n}{2}}$. We answer this question positively for 10-variable functions. We find 10-variable functions f with nonlinearity 488, algebraic degree 9, and $\Delta_f = 24$; some of them can be transformed to PC(1) functions. Balanced Boolean functions having maximum absolute value in the autocorrelation spectrum $< 2^{\frac{n}{2}}$ on even number of variables n have not been demonstrated earlier.

Here we also present a 10-variable 1-resilient function having nonlinearity 492, which is theoretically the maximum possible nonlinearity for such functions [36]. In [36], a tight upper bound on nonlinearity of resilient Boolean functions has been proposed and a list of functions on 7 to 10 variables have been presented in [36, Table 3] which were not known at that time. After that it becomes a challenging question to discover such functions and the papers [29], [22], [40], [35] present some of them. The 10-variable 1-resilient function having nonlinearity 492 was in the list which remained unknown till date and we present the function for the first time in this paper. Earlier, the best known nonlinearity of 10-variable 1-resilient function was 488 [22], a suboptimal one.

Construction of important Boolean functions has for some time used combinatorial techniques and search methods together. Patterson and Wiedemann [31] proposed a construction of highly nonlinear Boolean functions on n variables (n odd) using such a hybrid approach. These functions were later modified using heuristic search once again [20], to get balanced functions with very high nonlinearity and very low autocorrelation. Recent results on highly nonlinear, balanced, correlation immune functions show that computer search is very effective after some initial pruning on the search domain. In fact, most of the best functions on small number of variables (7–10) are available in this way [22], [36], [29].

Think of any Boolean function as a mapping from GF$(2^n) \rightarrow$ GF(2). Then the functions for which $f(\alpha^2) = f(\alpha)$, for any $\alpha \in$ GF(2^n) are referred as idempotents [8], [9] as it follows from $f^2 = f$ in multiplicative algebra. In [31], for $n = 15$, the functions having nonlinearity $16276 = 2^{n-1} - 2^{\frac{n-1}{2}} + 20$ could be identified in the idempotent class. From this motivation, in [8], [9] the idempotents were studied for $n = 9$. However, in [8], [9] the search was not exhaustive and mostly toward studying the balanced functions; that is the reason why the functions with nonlinearity 241 could not be discovered. One should note that the idempotents can be seen as RSBFs as pointed out in [8], [9]. This motivates us to study the nine-variable RSBF class for Boolean functions with high nonlinearity and we identify the functions with nonlinearity 241.

A lot of hard optimization problems have been attacked in various other domains using general-purpose heuristic strategies such as simulated annealing, genetic algorithms, tabu search, and various forms of hill-climbing. For Boolean functions such attempts were initially made in [25]–[27]. These attempts provided good but suboptimal results. Subsequently, simulated annealing [17] was used to provide competitive results [2], [13] in terms of nonlinearity and autocorrelation values together for small functions ($n < 8$). In [3], it was observed that some of the functions obtained by annealing could be transformed using simple linear change of basis to obtain resilient functions with excellent profiles (i.e., the best possible tradeoffs). Supplementing optimization with theory allows the best possible tradeoffs between nonlinearity, algebraic degree, and correlation immunity for balanced functions on $n \leq 8$ variables. Very recently, an interesting result showing the existence of nine-variable, 3-resilient functions having nonlinearity 240 has been presented in [35]. This question was open since Crypto 2000 [36]. These functions could be discovered by a heuristic search that exploits "Particle Swarm Optimization" [37].

In general, for $n \geq 9$, optimization based techniques are not competitive since the search space increases super-exponentially as n increases. Thus, we need some initial pruning before attempting a suitable heuristic search. The set of rotation symmetric Boolean functions (RSBFs) is interesting to look into as the space is much smaller ($\approx 2^{\frac{2^n}{n}}$) than the total space of Boolean functions (2^{2^n}) and the set contains functions with very good cryptographic properties. These functions have been analyzed in [8], [9], where the authors studied the nonlinearity of these Boolean functions up to nine variables and found encouraging results. This study has been extended in [38]–[40], [6], [4], [12], [23], [24], where it has been justified theoretically and experimentally that the RSBF class is extremely important in terms of Boolean functions with good cryptographic properties. On the other hand, in [32], Pieprzyk and Qu studied these functions as components in the rounds of a hashing algorithm and research in this direction was later continued in [5].

In this paper, we suitably modify the steepest descent like iterative algorithm that appeared in [14] so that it can be applied for a search in the class of rotational symmetric Boolean functions and find functions which are very good in terms of their Walsh and autocorrelation spectra. The strategy presented in [14] has been applied to the complete space of Boolean functions that resulted in discovery of eight-variable balanced Boolean functions f having nonlinearity 116 and Δ_f 16. It performs much better when applied to the much smaller (but rich) space of RSBFs. To have a quick feel of how efficient our strategy is, one may refer to Remark 1.

In the following section we present basic definitions related to Boolean functions. In Section III, we present our search strategy. The results are presented in Section IV.

II. Preliminaries on Boolean Functions

A Boolean function on n variables may be viewed as a mapping from V_n $\{0,1\}^n$ into $\{0,1\}$. The *truth table* of a Boolean function $f(x_1, \ldots, x_n)$ is a binary string of length 2^n

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

The *Hamming weight* of a binary string S is the number of 1's in S denoted by $\mathrm{wt}(S)$. An n-variable function f is said to be *balanced* if its truth table contains an equal number of 0's and 1's, i.e., $\mathrm{wt}(f) = 2^{n-1}$. Also, the *Hamming distance* between equidimensional binary strings S_1 and S_2 is defined by $d(S_1, S_2) = \mathrm{wt}(S_1 \oplus S_2)$, where $\oplus$ denotes the addition over GF(2).

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

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

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

Functions of degree at most one are called *affine* functions. An affine function with constant term equal to zero is called a *linear* function. The set of all n-variable affine (respectively, linear) functions is denoted by $A(n)$ (respectively, $L(n)$). The nonlinearity of an n-variable function f is

$$nl(f) = \min_{g \in A(n)} (d(f, g))$$

i.e., the minimum distance from the set of all n-variable affine functions.

Let $x = (x_1, \ldots, x_n)$ and $\omega = (\omega_1, \ldots, \omega_n)$ both belonging to $\{0, 1\}^n$ and $x \cdot \omega = x_1\omega_1 \oplus \cdots \oplus x_n\omega_n$. Let $f(x)$ be a Boolean function on n variables. Then the *Walsh transform* of $f(x)$ is a real-valued function over $\{0, 1\}^n$ which is defined as

$$W_f(\omega) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus x \cdot \omega}.$$

In terms of Walsh spectrum, the nonlinearity of f is given by

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

In [11], an important characterization of correlation-immune functions has been presented, which we use as the definition here. A function $f(x_1, \ldots, x_n)$ is mth-order correlation immune (respectively, m-resilient) iff its Walsh transform satisfies $W_f(\omega) = 0$, for $1 \le \mathrm{wt}(\omega) \le m$ (respectively, $0 \le \mathrm{wt}(\omega) \le m$).

Propagation characteristics (PC) and strict avalanche criteria (SAC) [33] are important properties of Boolean functions to be used in S-boxes.

Let $\alpha \in \{0, 1\}^n$ and f be an n-variable Boolean function. The autocorrelation value of the Boolean function f with respect to the vector α is

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

and the absolute indicator is

$$\Delta_f = \max_{\alpha \in \{0,1\}^n} |\Delta_f(\alpha)|.$$

A function is said to satisfy PC(k), if

$$\Delta_f(\alpha) = 0, \qquad \text{for } 1 \le \mathrm{wt}(\alpha) \le k.$$

Adding the last entry Δ to the notation used in [36], by an $(n, m, d, \sigma, \Delta)$ function we denote an n-variable, m-resilient function with degree d, nonlinearity σ, and absolute indicator Δ. By $(n, -1, d, \sigma, \Delta)$ we mean unbalanced functions and by $(n, 0, d, \sigma, \Delta)$ we mean balanced functions.

A. Rotation Symmetric Boolean Functions

Let $x_i \in \{0, 1\}$ for $1 \le i \le n$. For $1 \le k \le n$, we define

$$\rho_n^k(x_i) = \begin{cases} x_{i-k}, & \text{if } i + k \le n \text{ and} \\ x_{i-k-n}, & \text{if } i + k > n. \end{cases}$$

Let $(x_1, x_2, \ldots, x_{n-1}, x_n) \in V_n$. We can extend the definition of ρ_n^k to n-tuples as

$$\rho_n^k(x_1, x_2, \ldots, x_n) \quad (\rho_n^k(x_1), \rho_n^k(x_2), \ldots, \rho_n^k(x_n)).$$

Definition 1: A Boolean function f is called *rotation symmetric* if for each input $(x_1, \ldots, x_n) \in \{0, 1\}^n$, $f(\rho_n^k(x_1, \ldots, x_n)) = f(x_1, \ldots, x_n)$ for $1 \le k \le n$.

Following [38], let us consider the set of vectors

$$G_n(x_1, \ldots, x_n) = \{\rho_n^k(x_1, \ldots, x_n), \text{ for } 1 < k < n\}.$$

Note that $G_n(x_1, \ldots, x_n)$ generates an orbit in the set V_n. Let g_n be the number of such orbits. Using Burnside's lemma, it can be shown (see also [38]) that

$$g_n = \frac{1}{n} \sum_{k|n} \phi(k)\, 2^{\frac{n}{k}}$$

ϕ being Euler's *phi*–function. It can be easily checked that $g_n \approx \frac{2^n}{n}$. Since $2^{g_n} \ll 2^{2^n}$, the number of n-variable RSBFs is much smaller than the total space of Boolean functions.

An *orbit* is completely determined by its *representative element* $\mathrm{A}_{n,i}$, which is the lexicographically first element belonging to the ith orbit [40]. The rotation-symmetric truth table (RSTT) is defined as the g_n-bit string

$$|f(\mathrm{A}_{n,0}), f(\mathrm{A}_{n,1}), \ldots, f(\mathrm{A}_{n,g_n-1})|$$

where the representative elements are again arranged lexicographically.

The Walsh transform of an RSBF takes the same value for all elements belonging to the same orbit, i.e., $W_f(u) = W_f(v)$ if $u \in G_n(v)$. In analyzing the Walsh spectrum of RSBFs, the ${}_n\mathcal{A}$ matrix of size $g_n \times g_n$ has been introduced [40]. The (i, j)th entry of the matrix ${}_n\mathcal{A}$ is defined as

$${}_n\mathcal{A}_{i,j} = \sum_{x \in G_n(\mathrm{A}_{n,j})} (-1)^{x \cdot \mathrm{A}_{n,i}}$$

for an n-variable RSBF. The Walsh spectrum for an RSBF can then be calculated from the RSTT as

$$W_f(\mathrm{A}_{n,j}) = \sum_{i=0}^{g_n-1} (-1)^{f(\mathrm{A}_{n,i})} {}_nA_{i,j}.$$

III. Search Strategy

Our search strategy uses a steepest descent like iterative algorithm, where each iteration step has the input Boolean function f and the output Boolean function $f_{\min}$. At each iteration step, a cost function is calculated within a predefined neighborhood of f and the Boolean function having the smallest cost is chosen as the iteration output $f_{\min}$. We use the sum of squared errors [13], [41] as the cost function, which is defined as

$$\mathrm{Cost} = \sum_{\omega} (W_f^2(\omega) - 2^n)^2.$$

In some rare cases, the cost of $f_{\min}$ may be larger than or equal to the cost of f. This is the crucial part of the search strategy, which provides the ability to escape from local minima and its distinction from the steepest descent algorithm.

The 1-neighborhood of f is obtained by flipping a single element of its truth table. For an n-variable balanced Boolean function, the 1-neighborhood consists of 2^n many distinct Boolean functions, each being at the Hamming distance 1 to the original Boolean function. However, when the search space is restricted to RSBFs, the situation is different. If a bit in the truth table of an RSBF is changed, all entries corresponding to an orbit (a rotationally symmetric partition, which is composed of vectors that are equivalent under rotational shifts) should be changed to obtain another RSBF. The closest rotationally symmetric neighbors of RSBFs can be found by complementing the truth table entries corresponding to a complete orbit. So, at each step of the algorithm, we constitute the neighborhood of f by complementing each RSTT entry (i.e., changing all the values in a truth table corresponding to an orbit).

Our steepest descent based search technique minimizes the cost until a local minimum is attained, then it takes a step in the direction of nondecreasing cost. That is, whenever possible, the cost is minimized; otherwise, a step in the reverse direction is taken. The deterministic step in the reverse direction corresponds to the smallest possible cost increase within the predefined neighborhood of the preceding Boolean function, which makes it possible to escape from the local minima.

Our algorithm given below starts with an arbitrary RSBF, f_{initial}, and stops after a fixed number of iterations, N. At each iteration, g_n distinct Boolean functions within the predefined neighborhood, each of which is shown by f_{flipped}, are visited by storing the cost value $\mathrm{cost}_{\mathrm{flipped}}$ in $COST$, and the corresponding Boolean function itself in SET_f. Among the stored cost values, the minimum one, $\mathrm{cost}_{\min}$, is chosen, and the respective Boolean function, $f_{\min}$, is obtained from SET_f as the candidate of the step output. If the candidate $f_{\min}$ is already in $STORE$, which contains all previous iteration outputs, then this candidate $f_{\min}$ and its cost are removed from SET_f and $COST$, respectively. The minimum cost value is searched again in $COST$ among the remaining cost values to find the respective new candidate for $f_{\min}$.

Algorithm 1:

$f = f_{\mathrm{initial}}$;
for(*int* $k = 0$; $k < N$; k 1){
  for(*int* $i = 0$; $i < g_n$; i +){
    Flip one orbit of f
    $SET_f[i] = f_{\mathrm{flipped}}$
    $COST[i]$ $cost_{\mathrm{flipped}}$
  }
  Find $\mathrm{cost}_{\min}$ (minimum $\mathrm{cost}_{\mathrm{flipped}}$ in $COST$), and $f_{\min}$ (respectively, f_{flipped} in SET_f)
  while($f_{\min}$ is already in $STORE$){
    Remove $\mathrm{cost}_{\min}$ from $COST$, and $f_{\min}$ from SET_f
    Find $\mathrm{cost}_{\min}$ in $COST$, and $f_{\min}$ in SET_f
  }
  $STORE[k]$ $f_{\min}$
  f $f_{\min}$
}

Since the neighbors of f are obtained simply by flipping a bit in its RSTT, the number of neighbors is equal to g_n.

IV. Results

We start this section with the most important result of this paper.

A. Nine-Variable Function With Nonlinearity 241

The following is the truth table of a nine-variable function $f(x_1, \ldots, x_9)$ having nonlinearity $2^{9-1} - 2^{\frac{9+1}{2}} + 1 = 241$.

```
977F3FFA0EFAAEC955F8FACDCCA9A083
7666EBC0FA88E0B3F4E08983C845915E
7F7C2C29FCCBA101EA98C085E8118B5E
FE21E91184838351EE1952136971676E9.
```

Given an integer $m > 0$ and even, it is clear that the function $g(y_1, y_2, \ldots, y_m) \oplus f(x_1, \ldots, x_9)$ is an n-variable $(n \quad m+9)$ function with nonlinearity $2^{n-1} - 2^{\frac{n}{2}-1} - 2^{\frac{m}{2}}$, where $g(y_1, y_2, \ldots, y_m)$ is an m-variable bent function. Thus, there exist Boolean functions having nonlinearity $> 2^{n} \quad 2^{\frac{n-1}{2}}$ for odd $n \geq 9$. Keeping this in mind, and adding the results of [1], [28] that the maximum nonlinearity of Boolean functions on odd number of variables for odd $n \leq 7$ is $2^{n-1} - 2^{\frac{n-1}{2}}$, we get the following.

Theorem 1: There exist Boolean functions on n (odd) variables having nonlinearity $> 2^{n-1} - 2^{\frac{n-1}{2}}$ if and only if $n > 7$.

TABLE I
SUMMARY OF THE RESULTS

RSBF No	Initially Attained RSBF	Affinely Transformed Results
1	(9, 0, 7, 240, 24)	(9, 0, 7, 240, 24)*, (9, 1, 7, 240, 24)
2	(11, -1, 10, 990, 56)*	(11, 0, 10, 990, 56)*
3	(11, 0, 9, 988, 56)	(11, 0, 9, 988, 56)*, (11, 1, 9, 988, 56)
4	(10, -1, 9, 488, 24)*	(10, 0, 9, 488, 24)*
5	(10, -1, 8, 492, 56)	(10, 1, 8, 492, 56)

In other words, for odd n, the covering radius of the $(2^n, n+1)$ Reed–Muller code is $> 2^{n-1} - 2^{\frac{n-1}{2}}$ if and only if $n > 7$.

We have announced the result first in [15].

Remark 1: At this point, we want to highlight the efficiency of the search method. In [16] (our work later than that for this paper), it has been noted that there are 1512 many nine-variable RSBFs having nonlinearity 241 and this is the maximum nonlinearity in the nine-variable RSBF class. Note that the nine-variable RSBF class is of size 2^{60}. Thus, in a random search, the probability of getting a nine-variable RSBF with nonlinearity 241 is $1-(1-\frac{1512}{2^{60}})^i$ in i many attempts. Note that $\lim_{i\to\infty}(1-\frac{1}{i})^i = \frac{1}{e}$. Thus, in approximately $\frac{2^{60}}{1512}(> 2^{49})$ many attempts one may get such a function with probability $1-\frac{1}{e} > \frac{1}{2}$ in a random search. Our search method performs much better than that. We found five RSBFs having nonlinearity 241 in $2 \cdot 10^8$ $(< 2^{28})$ many generation of functions using Algorithm 1; which shows that the efficiency of our search strategy plays an important role to discover such functions.

Next we concentrate on other important functions in the RSBF class.

B. Important RSBF's on 9, 10, and 11 Variables

In Table I, we summarize the profiles of the some other important RSBFs that we obtain by Algorithm 1. We use the notation (number of variables, resiliency, degree, nonlinearity, absolute indicator) for each profile; resiliency $= -1$ (respectively, 0) denotes unbalanced (respectively, balanced) functions. If the given profile $(n, m, d, \sigma, \Delta)$ can be transformed into a function having the property of PC(1), then we denote it by $(n, m, d, \sigma, \Delta)^*$.

1) Algorithm 1 outputs the following function ϕ, which is a nine-variable balanced RSBF having $nl(\phi) = 240$ and $\Delta_\phi = 24 < 32 = 2^{\frac{9-1}{2}}$ and algebraic degree 7.

   005473257A0E49676BDD10E864D3287F
   399BB2E30214BC916865E70B58853BBE
   0ED3C29B9F48AD0F55490665BBB1C356
   2D857833F92B159E33C5D1765BDEDEE9.

   Given an n-variable Boolean function f, let us define

   $$S_f = \{\omega \in \{0,1\}^n \mid W_f(\omega) = 0\}.$$

   If there exist n linearly independent vectors in S_f, then one can construct a nonsingular $n \times n$ matrix B_f whose rows are linearly independent vectors from S_f. Let, $C_f = B_f^{-1}$. Now one can define $f'(x) = f(C_f x)$. Both f' and f have the same weight, nonlinearity and algebraic degree [18]. Moreover, $W_{f'}(\omega) = 0$ for $\mathrm{wt}(\omega) = 1$. This ensures that f' is correlation immune of order 1. Further, if f is balanced then f' is 1-resilient. This technique has been used in [30], [21], [3]. The following function is obtained by a linear transformation on the input variables of ϕ above, which is 1-resilient:

   1C969EEC0B5B87307EB530AD3C365AD3
   2A677C130CBA71435798C8B6A9DE615
   ECF9D05D64E8987F8414D1018621E7EE
   E05FD4E1AF403F05BF2226AEE2B36D0E.

   A similar technique can be used to construct PC(1) functions. Given an n-variable Boolean function f, let us define $T_f = \{\alpha \mid \Delta_f(\alpha) = 0\}$. If there exist n linearly independent vectors in T_f, then one can construct a nonsingular $n \times n$ matrix D_f whose rows are linearly independent vectors from T_f. Now one can define $f'(x) = f(xD_f)$. Both f' and f have the same weight, nonlinearity, and algebraic degree [18]. Moreover, $\Delta_{f'}(\alpha) = 0$ for $\mathrm{wt}(\alpha) = 1$. This ensures that f' is PC(1). This technique has been used in [20]. The following function is obtained by a linear transformation on the input variables of ϕ above, which is PC(1):

   2C317F8130464E9D30EA0A95556F8EAA
   E108188979AC18E9F23AA6793CBBE526
   F0DA686073CFD3D6ABE78F641FEB34DD
   64ED3721BCE0C6CA0CB8E5FCA6655004.

   It would be interesting to get a transformation on input variables such that 1-resiliency and PC(1) can both be achieved at the same time.

2) Using Algorithm 1, we find the following function ϕ, which is an 11-variable unbalanced RSBF having $nl(\phi) = 990$, $\Delta_\phi = 56$, and $\deg(\phi) = 10$. Note that this function is by itself a PC(1) function which is not balanced, but soon we will provide a balanced PC(1) function as well.

   FEEDB8A7CA94D83AF4C88330F7C04EC8
   BB64F4C5C05B0F41BB6AF41130BCB595
   CACF7D60FF75F163B01473DB00FE2553
   DACF7CDDAE6517161A40DAA08A32D263
   F198E0EE3FA62C15BEFE3A36BF75280A
   8B5571703A1EE7CA4551BEEC4C2372SA
   A798A1BF2EB5B3A6C9FC7C63566A5628
   06996510A2D8984484CC1B49B60D684B
   EB4386C4E814F8A85AEB8D3958E54677
   8BF8FFE94ADD0E3DCBEF2B7648C004C9
   D18A72276E167F001FDC16B8BD6AA1CC
   342727529EE9E8E025B40C4A2A596389

992A86C0C935CBAF1CF98F279B1E8829
E0C3AAF07EA4781A633C698836280D91
502897936D335601890CE2C496906035
C075B5E1128A64878F7940A33D8171DE.

We transform ϕ to a balanced one, f, by using $\omega = (0,0,0,0,1,1,0,0,1,1,1)$ for which $W_\phi(\omega) = 0$. Thus, the function $f(x) = \phi(x) \oplus \omega \cdot x$ is balanced as given below with the same $nl(\phi)$, Δ_ϕ, and $\deg(\phi)$.

9784D1CE5C024EAC625E15A69EA927A1
D20D9DAC56CD99D72DFC628759D5DCFC
A3A6140969E362F526D2E54D69974C3A
B3A615B438F381808CD64C36E35BBB0A
98F18987A930BA832868ACA0D61C4163
E23C1819AC88715CD3C7287A251A1B33
CEF1CDD6B82325305F6AEAF53F033F41
6FF00C79344E0ED2125A8DDFDF640122
822AEFAD7E826E3ECC7D1BAF318C2F1E
E2919680DC1B98AB5D79BDE021A96DA0
BDE31B4EF8D0E996894AD02ED403C8A5
5D4E4E3B087F7E76B3229ADC43300AE0
F043EFA95FA35D398A6F19B1F277E140
89AAC399E832EE8CF5AAFF1E5F4164F8
3941FEFAFBA5C0971F9A7452FFF9095C
A91CDC88841CF21119EFD63554E818B7.

Note that this balanced function f is by itself a PC(1) function. Since the preceding function is of nonlinearity 990, which is not divisible by 4, it cannot be made 1-resilient by affine transformation.

3) Next we present such a function of nonlinearity 988 having degree 9, so that we may get 1-resiliency by linear transformation on input variables. By Algorithm 1, we get a balanced RSBF f having nonlinearity 988, $\Delta_f = 56$, and algebraic degree 9.

ECB4DE71F3FD6B13FB1ABAB7688A075E
FA9F17D89B9DCA3E6D80D0CC542B63ED
BE8992BB076FE6C083CAD2A7E0CD4AE9
6CE6C411A244F4B166600D9F281AB8B6
DEB881879619CBCB407E29BAFC3CE501
C14AB0DCA31CCD2BEC01F4A621C8E8D7
7DF1FD28B0201317CC5C3421EB618F53
3969280455E2D3BB4DD04299CF859F7C
A6EDDF95D417803EC77C5786B0CAE19B
61453BA818C38B89AAA50AE5A8370446
E41365998E14E6B1984E16B1A1E2188F
FDF04057AE61993D5902F4D5BC85B37E
2BF7EB06BEF248959B504911030B072A
A5B526A54A651843FC8F2957D0EF635E
1F926C875C95113037238B49F31FCB9F
74A3E7547119979GE1BED57696FE6EA0.

The function is then transformed to 1-resilient function as follows:

975D2EFDA7C9D97E96B58F09B0569601
88614907BACF4617219BF147E6B34314
410C9E8BB000FE87E8A7A3590CF4B1A6
6D11818429EC3F0F61EF89CB9E898BE0
B208B29527E8404F871B756693944C39
72D242039F3017FD34E2973C2B2567A5
C2FFF57B3783DD747993E8346E5DE671
ADE80D1D3E98FA461ACAA93A2FF87622
D0BCA271ABDD139C66ED2D8C75ED7DD3
B22968E85BC520361B31DD9F09FF1162
974F19DD09251C16C56CDC7C3AE920EA
DBC08BFC51B3F300DE3C7B6CC668D504
01EC68AC1D3AB7525BEEE63D0C208D35
8F88DFD59DD59B4433B80016AF5DA8BD
D8E2B053C0E67A16241122E8E4A4C158
CB654ABAFDA03E73A05A75DA610B99BF.

Further, we can also transform f to a PC(1) function as follows:

850EC14AF195F38DD59EB29E7CD758C7
6122F20FCE9E83DE393F53757954269F
44C0EC07E6724883E726A750939EE1DB
5475F56C1D3933F585C6DB9719D8BA35
58041ABEF105914D59F02FFB8CED823D
982469B85F3287465488B8CBAEB4A110E
F2381C97099C58E1A0FD724A35D28129
D9F61CA877BE0109BD67A3B62EA4BA5F
0DA4AE0E2D84AA64301635E183CE33D1
9B7D50C9230D027BBB22443BF5765A34
F3AF2B9F0AB2DE85ABDF1367526B9123
51D91F43EB123B9CE5B164E6DFB95E81
60D537FB9FD65A0AD8674BC3443C8380
4D5D3169CD0E5B22E723184D144D0918
00332B98CF8E2E39F53C6BAEF24402F1
9B9B703616B1C860AE538705DEEAF0B7

4) Using Algorithm 1, we first find an unbalanced RSBF ϕ with $nl(\phi) = 488$, $\Delta_\phi = 24$, and $\deg(\phi) = 9$ as given below. This is an unbalanced PC(1) function.

FFFEEBF9E8CAAFD2E8C5A4899CFFB20C
FDC4F162992580C283E5FAAA8F1C51B5
FAA6B171FA12385996824D379154A55D
D10EA827BF9D8D98D0EB07B43606CE27

FE9D883C8B216F42FAD853081BC036D7
C26DC44D60B75E3FD2037734C93662A3
E70611B8CCD0586F8BAB87E7C1F69681
B254ACCB113B9E614E295569A1F91D7F.

We find only one zero at $\omega = (1,1,1,1,1,1,1,1,1,1)$ in the Walsh spectrum of ϕ, which is used to get a balanced function as follows. One may note that this function is by itself a PC(1) function.

96687D907EA3C6447EACCD1FF5692465
6BAD98F4F0B316ABEA736CC319753823
6CCFDDE79384AE30FF14DB5E073DCCCB
B8983E4E29F4E40E46826E225F90584E
68F4E1AAE2B7F92B934EC5618DA95F41
ABFB5224F6DE37A9446A1EA2A0A0F4CA
8E9087D15AB931F91DC2EE71A86000E8
243DC55D78AD080827BFC300379074E9.

5) We first identify unbalanced RSBF ϕ having nonlinearity 492 and algebraic degree 8. The function ϕ is as follows:

F9C6B17C9F136FF496BA574B7CEEA820
D33C8E9D776F709B6EB1A8E9CCD01941
B34F4EF095F8C2E23E6A68AA6B40C2DA
3CE8DB469C81A883F4A1A24146877153
9A5E75BA64F9EA00D627FBC5A509AC59
5BAC7C886880988C68DA6101E109A3DD
4EF4AD80E3DB312DD2E080428C91911F
AE309D53C8082557247D803F2F07335E.

To make it balanced we take

$$\omega = (0,0,0,0,0,0,0,1,0,1)$$

where $W_\phi(\omega) = 0$. Thus, $f = \phi \oplus \omega \cdot x$ is a balanced function. Then we consider the set

$$S_f = \{\omega \in \{0,1\}^n \mid W_f(\omega) = 0\}$$

having $|S_f| = 40$. There exist ten linearly independent vectors in S_f, and one can construct a nonsingular 10×10 matrix B_f whose rows are linearly independent vectors from S_f. We have considered the following matrix:

$$B_f = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let $C_f = B_f^{-1}$ and then $f'(x) = f(C_f x)$ is a 10-variable 1-resilient function with algebraic degree 8 and nonlinearity 492. The function f' is as follows:

8180CDED6C1C0302AA32E761B2079F0C
37D8393E5B8DF2934B2AACEA7EB40BF0
AF6694BAF19E415E4580C0D679DB9BEB
982963591185C33FEC2F67987D121D3B
C4E281F3D071957A74DF8A99FF258E9F
C3D3AE6BE39415B0F4E5DA104DFC0125
24AD19CBA965D3768C525AD75C5316AA
0F77F1A49E4AFD4223D40756C8388886.

C. Search Effort

In Remark 1, we have quantified how efficient our search method is in terms of finding nine-variable RSBFs having nonlinearity 241. Since it is not possible to completely enumerate the other important functions we have achieved, the efficiency of the search method cannot be quantified. However, the following search efforts related to Algorithm 1 show that it is indeed possible to achieve good functions in nominal time.

For $n = 9$, we have carried out 2000 runs each with $N = 100\,000$ iterations. Among these 200 million RSBFs, five have the nonlinearity 241, and 580 more RSBFs have the nonlinearity 240 and absolute indicator 24. For $n = 10$, 250 runs have been performed each with $N = 400\,000$ iterations. Among the total of 100 million RSBFs, 11 have the nonlinearity 488 and absolute indicator 24, all transformable to balanced functions. In the same experiment, we have found 67 479 RSBFs with nonlinearity 492, all transformable to balanced functions and among them we could obtain several 1-resilient functions using linear change of basis. Besides, we have noticed that only four of the 67 479 RSBFs are balanced, and none of these balanced functions can be transformed into a 1-resilient function. For $n = 11$, there are seven successes with nonlinearity 988 and absolute indicator 56 in 500 runs. Moreover, we have encountered an unbalanced RSBF having nonlinearity 990 and absolute indicator 56, which is transformable to a balanced function.

Using a computer system with Pentium IV 2.8-GHz processor and 256-MB RAM, and setting the iteration number $N = 100\,000$, a typical run of our algorithm takes 1 min and 29 s for $n = 9$. With the same computer system, a typical run takes 57 min for $n = 10$, and 69 min for $n = 11$, by setting the iteration numbers to $N = 400\,000$ and $N = 500\,000$, respectively.

V. Conclusion

Functions which have not been known for a long time could be achieved with our steepest descent based iterative heuristic search in the class of RSBFs. As a major result, we find nine-variable RSBFs with nonlinearity 241 and thus, we could show the existence of Boolean functions having nonlinearity $> 2^{n-1} - 2^{\frac{n+1}{2}}$ for $n = 9, 11, 13$. We could find balanced Boolean functions on 9, 10, and 11 variables with maximum absolute value in the autocorrelation spectrum $< 2^{\lceil \frac{n+2}{2} \rceil}$ with

other cryptographic properties such as good nonlinearity and algebraic degree. Some of these functions on each of the 9, 10, and 11 variables cases can be affinely transformed to balanced PC(1) functions. Some of these functions on 9 and 11 variables can be transformed to 1-resilient functions as well. Further, we discovered several 10-variable 1-resilient functions with nonlinearity 492, which was posed as an open question at Crypto 2000.

Acknowledgment

We deeply appreciate and thank the Institute of Applied Mathematics at Middle East Technical University for the computational facilities provided. We also like to thank the anonymous reviewers for their suggestions that improved the presentation of this paper.

References

[1] E. R. Berlekamp and L. R. Welch, "Weight distributions of the cosets of the (32, 6) Reed-Muller code," *IEEE Trans. Inf. Theory*, vol. IT-18, no. 1, pp. 203–207, Jan. 1972.

[2] J. A. Clark and J. L. Jacob, "Two-stage optimization in the design of Boolean functions," in *Proc. ACISP 2000 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 1841, pp. 242–254.

[3] J. Clark, J. Jacob, S. Stepney, S. Maitra, and W. Millan, "Evolving Boolean functions satisfying multiple criteria," in *Proc. INDOCRYPT 2002 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2002, vol. 2551, pp. 246–259.

[4] J. Clark, J. Jacob, S. Maitra, and P. Stănică, "Almost Boolean functions: The design of Boolean functions by spectral inversion," *Comput. Intell.*, vol. 20, no. 3, pp. 450–462, 2004.

[5] T. W. Cusick and P. Stănică, "Fast evaluation, weights and nonlinearity of rotation-symmetric functions," *Discr. Math.*, vol. 258, no. 1-3, pp. 289–301, 2002.

[6] D. K. Dalai, K. C. Gupta, and S. Maitra, "Results on algebraic immunity for cryptographically significant Boolean functions," in *Proc. INDOCRYPT 2004 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2004, vol. 3348, pp. 92–106.

[7] J. F. Dillon, "Elementary Hadamard difference sets," Ph.D. dissertation, Univ. Maryland, College Park, 1974.

[8] E. Filiol and C. Fontaine, "Highly nonlinear balanced Boolean functions with a good correlation-immunity," in *Advances in Cryptology – EUROCRYPT'98 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1998, vol. 1403, pp. 475–488.

[9] C. Fontaine, "On some cosets of the first-order Reed–Muller code with high minimum weight," *IEEE Trans. Information Theory*, vol. 45, no. 4, pp. 1237–1243, May 1999.

[10] S. Gangopadhyay, P. H. Keskar, and S. Maitra, "Patterson-Wiedemann functions revisited," *Discr. Math*, vol. 306, pp. 1540–1556, 2002, A special issue containing selected papers from "R.C. Bose Centennial Symposium on Discrete Mathemematics and Applications".

[11] X. Guo-Zhen and J. Massey, "A spectral characterization of correlation immune combining functions," *IEEE Trans. Inf. Theory*, vol. 34, no. 3, pp. 569–571, May 1988.

[12] M. Hell, A. Maximov, and S. Maitra, "On efficient implementation of search strategy for rotation symmetric Boolean functions," in *Proc. 9th Int. Workshop on Algebraic and Combinatoral Coding Theory, ACCT 2004*, Black Sea Coast, Bulgaria, Jun. 2004.

[13] S. Kavut and M. D. Yücel, "Improved cost function in the design of Boolean functions satisfying multiple criteria," in *Indocrypt 2003 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2003, vol. 2904, pp. 121–134.

[14] S. Kavut and M. D. Yücel, "A new algorithm for the design of strong Boolean functions ," in *Proc. 1st Nat. Cryptology Symp.* (in Turkish), Ankara, Turkey, Nov. 2005, pp. 95–105.

[15] S. Kavut, S. Maitra, and M. D. Yücel, There Exist Boolean Functions on n (Odd) Variables Having Nonlinearity $> 2^{n-1} - 2^{\frac{n-1}{2}}$ if and Only if $n > 7$, IACR eprint server, 2006 [Online]. Available: http://eprint.iacr.org/2006/181

[16] S. Kavut, S. Maitra, S. Sarkar, and M. D. Yücel, "Enumeration of 9-variable rotation symmetric Boolean functions having nonlinearity > 240," in *INDOCRYPT – 2006 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2006, vol. 4329, pp. 266–279.

[17] S. Kirkpatrick, C. D. Gelatt Jr., and M. P. Vecchi, "Optimization by simulated annealing," *Science*, vol. 220, no. 4598, pp. 671–680, May 1983.

[18] F. J. MacWillams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[19] S. Maitra, "Highly nonlinear balanced Boolean functions with very good autocorrelation property," in *Proc. Workshop on Coding and Cryptography – WCC 2001*. Amsterdam, The Netherlands: Elsevier, 2001, vol. 6, Electronic Notes in Discrete Mathematics.

[20] S. Maitra and P. Sarkar, "Modifications of Patterson-Wiedemann functions for cryptographic applications," *IEEE Trans. Inf. Theory*, vol. 48, no. 1, pp. 278–284, Jan. 2002.

[21] S. Maitra and P. Sarkar, "Cryptographically significant Boolean functions with five valued Walsh spectra," *Theor. Comp. Sci.*, vol. 276, no. 1–2, pp. 133–146, 2002.

[22] S. Maitra and E. Pasalic, "Further constructions of resilient Boolean functions with very high nonlinearity," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1825–1834, Jul. 2002.

[23] A. Maximov, M. Hell, and S. Maitra, "Plateaued rotation symmetric Boolean functions on odd number of variables," in *Proc. 1st Workshop on Boolean Functions: Cryptography and Applications, BFCA 05*, LIFAR, Univ. Rouen, France, Mar. 2005, pp. 83–104.

[24] A. Maximov, "Classes of plateaued rotation symmetric Boolean functions under transformation of Walsh spectra," in *Proc. Workshop on Coding and Cryptography, WCC 2005*, IACR eprint server, no. 2004/354.

[25] W. Millan, A. Clark, and E. Dawson, "An effective genetic algorithm for finding highly nonlinear Boolean functions," in *Proc. 1st Int. Conf. Information and Communications Security (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1997, vol. 1334, pp. 149–158.

[26] W. Millan, A. Clark, and E. Dawson, "Heuristic design of cryptographically strong balanced Boolean functions," in *Adv. Cryptology EUROCRYPT'98 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1998, vol. 1403, pp. 489–499.

[27] W. Millan, A. Clark, and E. Dawson, "Boolean function design using hill climbing methods," in *Proc. 4th Australasian Conf. Information, Security and Privacy (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1999, vol. 1587, pp. 1–11.

[28] J. J. Mykkeltveit, "The covering radius of the (128, 8) Reed-Muller code is 56," *IEEE Trans. Inf. Theory*, vol. IT-26, no. 3, pp. 359–362, May 1980.

[29] E. Pasalic, S. Maitra, T. Johansson, and P. Sarkar, "New constructions of resilient and correlation immune Boolean functions achieving upper bound on nonlinearity," in *Proc. Workshop on Coding and Cryptography – WCC 2001, Paris, France, Jan. 8–12, 2001 (Electronic Notes in Discrete Mathematics)*. Amsterdam, The Netherlands: Elsevier, 2001, vol. 6, pp. 158–167.

[30] E. Pasalic and T. Johansson, "Further results on the relation between nonlinearity and resiliency of Boolean functions," in *Proc. IMA Conf. Cryptography and Coding (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1999, vol. 1746, pp. 35–45.

[31] N. J. Patterson and D. H. Wiedemann, "The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 3, pp. 354–356, May 1983.

[32] J. Pieprzyk and C. X. Qu, "Fast hashing and rotation-symmetric functions," *J. Universal Comp. Sci.*, vol. 5, no. 1, pp. 20–31, 1999.

[33] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle, "Propagation characteristics of Boolean functions," in *Adv. Cryptology – EUROCRYPT'90 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1991, pp. 161–173.

[34] O. S. Rothaus, "On bent functions," *J, Comb. Theory, Ser. A*, vol. 20, pp. 300–305, 1976.

[35] Z. Saber, M. F. Uddin, and A. Youssef, "On the existence of $(9, 3, 5, 240)$ resilient functions," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2269–2270, May 2006.

[36] P. Sarkar and S. Maitra, "Nonlinearity bounds and constuction of resilient Boolean functionsf," in *Adv. Cryptology – Crypto 2000 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 1880, pp. 515–532.

[37] "Special issue on particle swarm optimization," *IEEE Trans. Evol. Comput.*, vol. 8, Jun. 2004.

[38] P. Stănică and S. Maitra, "Rotation symmetric Boolean functions—Count and cryptographic properties," in *R. C. Bose Centenary Symposium on Discrete Mathematics and Applications (Electronic Notes in Discrete Mathematics)*. Amsterdam, The Netherlands: Elsevier, 2002, vol. 15, pp. 178–183 [Online]. Available: http://www1.elsevier.com/gej-ng/31/29/24/75/23/show/Products/notes/index.htt.

[39] P. Stănică and S. Maitra, "A constructive count of rotation symmetric functions," *Inf. Process. Lett.*, vol. 88, pp. 299–304, 2003.

[40] P. Stănică, S. Maitra, and J. Clark, "Results on rotation symmetric bent and correlation immune Boolean functions," in *Proc. Fast Software Encryption Workshop (FSE 2004), New Delhi, India (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2004, vol. 3017, pp. 161–177.

[41] M. D. Yücel, Alternative Nonlinearity Criteria for Boolean Functions, Electrical and Electronics Engineering Depertment, Middle East Technical University, Ankara, Turkey, 2001, Memorandum no. 2001-1.

[42] X. M. Zhang and Y. Zheng, "GAC – The criterion for global avalanche characteristics of cryptographic functions," *J. Universal Comp. Sci.*, vol. 1, no. 5, pp. 316–333, 1995.