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

Selçuk Kavut*, Subhamoy Maitra† and Melek D. Yücel†

Abstract

For the first time we find Boolean functions on 9 variables having nonlinearity 241, that remained as an open question in literature for almost three decades. Such functions are discovered using a suitably modified steepest-descent based iterative heuristic search in the class 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 the same search method, we also find several other important functions and we study the autocorrelation, propagation characteristics and resiliency of the RSBFs (using proper affine transformations, if required). The results show that it is possible to get balanced Boolean functions on $n = 10$ variables having autocorrelation spectra with maximum absolute value $< 2^{\frac{n}{2}}$, which was not known earlier. In certain cases the functions can be affinely transformed to get first order propagation characteristics. We also obtain 10-variable functions having first order resiliency and nonlinearity 492 which was posed as an open question in Crypto 2000.

Keywords. Autocorrelation, Boolean Functions, Combinatorial Problems, Cryptography, Heuristic Search, Nonlinearity, Rotational Symmetry.

1 Introduction

Boolean functions with very high nonlinearity is one of the most challenging problems in the area of cryptography and combinatorics. The problem is also related to covering radius of first order Reed-Muller code. On even number of variables n, there 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 are available since 1972 as follows.

*Department of Electrical Engineering and Institute of Applied Mathematics, Middle East Technical University (METU – ODTÜ), 06531 Ankara, Türkiye. Email: kavut@metu.edu.tr, melekdy@metu.edu.tr

†Applied Statistics Unit, Indian Statistical Institute, 203 B T Road, Kolkata 700 108, India. Email: subho@isical.ac.in

1. **Negative results.** In 1972 [1], it has been shown that the maximum nonlinearity of 5-variable Boolean functions is 12 and in 1980 [28] it has been shown that the maximum nonlinearity of 7-variable Boolean functions is 56. Thus for odd $n \leq 7$, 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 $2^{n-1} - 2^{\frac{n-1}{2}} + 20 \cdot 2^{\frac{n-15}{2}}$.

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 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 also for $n = 9, 11$ variables by efficient search in the RSBF class [16].

Here we concentrate on the balanced functions over even number of variables. In [19], a construction has been proposed having $\Delta_f \leq 2^{\frac{n}{2}} + \Delta_g$, 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, 14, 15] for 8-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 the similar idea corresponding to the odd number of variables, the question for 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 a 10-variable function ϕ with $\Delta_\phi = 24 < 2^{\frac{10}{2}}$.

Next we 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 [22] the best known nonlinearity of

10-variable 1-resilient function was 488, a suboptimal one.

1.1 Background

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].

A lot of hard optimization problems have been attacked in various other domains using general purpose heuristic strategies like simulated annealing, genetic algorithms, tabu search and various forms of hill-climbing. For Boolean functions such attempts were initially made in [25, 26, 27]. These attempts provided good but suboptimal results. Subsequently, simulated annealing [17] was used to provide competitive results [2, 14] in terms of nonlinearity and autocorrelation values together for small functions ($n \leq 8$). 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 trade-offs). Supplementing optimization with theory allows the best possible trade-offs between nonlinearity, algebraic degree and correlation immunity for balanced functions on $n \leq 8$ variables. Very recently, an interesting result showing the existence of 9-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 suitable heuristic search. The set of Rotational 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 9 variables and found encouraging results. Note that the search in [8, 9] for 9-variables was not exhaustive and it could achieve the nonlinearity till 240. This study has been extended in [38, 39, 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 has appeared in [15, 16] so that it can be applied for a search in the class of rotational symmetric Boolean functions and have found functions which are very good in terms of their Walsh and autocorrelation spectra. The strategy presented in [15] has been applied

for the complete space of Boolean functions and it performs much better when applied to a much smaller (but rich) space of RSBFs. In [16], the search was on RSBFs, but it was constrained to produce the balanced functions only. We have relaxed this requirement and found much better results.

In the following section we present basic definitions related to Boolean functions. In Section 3, we present our search strategy. The results are presented in Section 4.

2 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, $f = [f(0,0,\cdots,0),\ f(1,0,\cdots,0),\ f(0,1,\cdots,0),\ \ldots, f(1,1,\cdots,1)]$. The *Hamming weight* of a binary string S is the number of 1's in S denoted by $wt(S)$. 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., $wt(f) = 2^{n-1}$. Also, the *Hamming distance* between equidimensional binary strings S_1 and S_2 is defined by $d(S_1, S_2) = wt(S_1 \oplus S_2)$, 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 k-th order products ($0 \leq k \leq n$) of the variables. More precisely, $f(x_1, \ldots, x_n)$ can be written as

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

where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \{0,1\}$. 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 $x \cdot \omega = x_1\omega_1 \oplus \ldots \oplus x_n\omega_n$. 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 m-th order correlation immune (respectively m-resilient) iff its Walsh transform satisfies

$$W_f(\omega) = 0, \text{ for } 1 \leq wt(\omega) \leq m \text{ (respectively } 0 \leq wt(\omega) \leq m).$$

Propagation Characteristics (PC) and Strict Avalanche Criteria (SAC) [33] are important properties of Boolean functions to be used in S-boxes. Further, Zhang and Zheng [42] identified related cryptographic measures called Global Avalanche Characteristics (GAC).

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

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

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

$$\Delta_f(\alpha) = 0 \; for \; 1 \leq wt(\alpha) \leq k.$$

2.1 Rotation Symmetric Boolean Functions

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

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

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

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

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 $1 \leq k \leq n$.*

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

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

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 $2^{g_n} << 2^{2^n}$, 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* $\Lambda_{n,i}$, which is the lexicographically first element belonging to the orbit [40]. *The rotation symmetric truth table* (RSTT) is defined as the g_n-bit string

$$[f(\Lambda_{n,0}), f(\Lambda_{n,1}), \ldots, f(\Lambda_{n,g_n-1})],$$

where the representative elements are again arranged lexicographically.

The Walsh transform of a rotation symmetric Boolean function 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 ${}_n\mathcal{A}_{i,j} = \sum_{x \in G_n(\Lambda_{n,i})} (-1)^{x \cdot \Lambda_{n,j}}$, for an n-variable RSBF. The Walsh spectrum for an RSBF can then be calculated from the RSTT as $W_f(\Lambda_{n,j}) = \sum_{i=0}^{g_n-1} (-1)^{f(\Lambda_{n,i})}\, {}_n\mathcal{A}_{i,j}$.

3 Search Strategy

The search strategy of [16] uses a steepest-descent like iterative algorithm, where each iteration step has the balanced Boolean functions f and f_{min} as input and output respectively. 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}. The sum of squared errors [14, 41] is used as the cost function, which is given as

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

The cost function defined above is the sum of squared errors between the Walsh spectrum of f and that of a bent function. In [41], it is shown that this cost is equal to $\sum_{\alpha \neq 0} \Delta_f^2(\alpha)$. Hence, the cost function used in [16] is a simultaneous measure of the sum of squared errors both in the Walsh and the autocorrelation spectra of f with respect to the corresponding spectra of bent functions.

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 differentiates it from the steepest-descent algorithm. This search technique minimizes the cost until a local minimum is attained, then it takes a step in the direction of non-decreasing 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 also makes it possible to escape from the local minima.

The closest balanced neighbors of a balanced f are obtained by swapping any two dissimilar values of its truth table. When the search space is restricted to balanced RSBFs as in the algorithm of [16], if two dissimilar bits in the truth table are swapped, then all entries of the corresponding orbits should be changed to obtain another RSBF. So, at each

step of the algorithm, the neighborhood of f is constituted by swapping RSTT entries corresponding to possible pairs of equal-size orbits having dissimilar values. The main disadvantage of this algorithm is that it makes a search in the set of balanced RSBFs only, which is a very small fraction of the whole set. This restriction prevents the algorithm to reach some unbalanced RSBFs with very good profiles, which may be affinely transformable to resilient or balanced functions. Hence, we modify the algorithm in [16] by extending the search space to all RSBFs.

Our modified 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 $cost_{flipped}$ in $COST$, and the corresponding Boolean function itself in SET_f. Among the stored cost values, the minimum one, $cost_{min}$, 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

$f = f_{initial}$;
for(*int* $k = 0$; $k < N$; $k++$){
    for(*int* $i = 0$; $i < g_n$; $i++$){
        Flip one orbit of f
        $SET_f[\ i\ ] = f_{flipped}$
        $COST[\ i\ ] = cost_{flipped}$
    }
    Find $cost_{min}$ *(minimum* $cost_{flipped}$ *in* $COST$*), and* f_{min} *(respective* $f_{flipped}$ *in* SET_f*)*
    while(f_{min} *is already in* $STORE$){
        Remove $cost_{min}$ *from* $COST$*, and* f_{min} *from* SET_f
        Find $cost_{min}$ *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, instead of swapping two bits as in the algorithm of [16], our modified algorithm reduces the number of neighbors from ${g_n}^2$ to g_n. Notice that, this is a remarkable reduction, which makes an iteration step of our algorithm much faster than that of the algorithm in [16].

Using our algorithm, we obtain some unbalanced RSBFs with very good cryptographic properties that are unattainable by the algorithm in [16].

4 Results

We present our results in three parts: functions having
i) nonlinearity $> 2^{n-1} - 2^{\frac{n-1}{2}}$ for $n = 9, 11, 13$;
ii) absolute indicator $< 2^{\frac{n}{2}}$ for $n = 10$;
iii) resiliency 1 and nonlinearity 492 for $n = 10$.

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

```
977F3FFA0EFAAEC955F8FACDCCA9A0837666EBC0FA88E0B3F4E08983C845915E
7F7C2C29FCCBA101EA98C085E8118B5EFE21E9118483851EE1952136971676E9
```

Thus it is clear that the function $g(y_1, y_2) \oplus f(x_1, \ldots, x_9)$ is an 11-variable function with nonlinearity $2^{11-1} - 2^{\frac{11-1}{2}} + 2 = 994$ where $g(y_1, y_2)$ is a 2-variable bent function. Similarly $h(y_1, y_2, y_3, y_4) \oplus f(x_1, \ldots, x_9)$ is a 13-variable function with nonlinearity $2^{13-1} - 2^{\frac{13-1}{2}} + 4 = 4036$ where $h(y_1, y_2, y_3, y_4)$ is a 4-variable bent function. Thus there exist Boolean functions having nonlinearity $> 2^{n-1} - 2^{\frac{n-1}{2}}$ for $n = 9, 11, 13$. Keeping this in mind, and adding the results of [1, 28, 31], 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 $n > 7$.*

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 $n > 7$.

ii) Now we concentrate on balanced functions on even number of variables with absolute indicator $< 2^{\frac{n}{2}}$. We answer this question positively for a 10-variable function.

- We find the following unbalanced RSBF ϕ on 10-variables such that $\Delta_\phi = 24 < 2^{\frac{10}{2}}$.

  ```
  FA8CD4B4F675CA70FA7C2B27E0C82E45AFCD6FA14DDE5D7EE811E1840DAD3467
  9DFAB1A77CFF895761F3A6E866E37BA9BDC00742ED42817404F6D9F64B70682E
  C2E6EF8CCE13882B3BB1BEFE8592336B7C53EF1F9D28A9D17838B81E2EDE9C82
  8AB2A501556E3459EDB7701DC4462E600431FA6DB7C7AA2825CB7B0039D05CE8
  ```

  We find 20 zeros in the Walsh spectrum of ϕ. Choose an $\omega = (0, 0, 0, 0, 0, 1, 0, 0, 1, 1)$ such that $W_\phi(\omega) = 0$. Thus the function $f(x) = \phi(x) \oplus \omega \cdot x$ is balanced. hence we get a balanced 10-variable function f such that $\Delta_f = 24 < 2^{\frac{10}{2}}$. The nonlinearity and algebraic degree of f as presented below are 488 and 7 respectively.

  ```
  9CEA4D2D901353E99C1AB2BE86AEB7DCC9ABF6382BB8C4E78E77781D6BCBADFE
  FB9C283E1A9910CE07953F710085E230DBA69EDB8B2418ED6290406F2D16F1B7
  A4807615A87511B25DD72767E3F4AAF21A357686FB4E30481E5E218748B8051B
  ECD43C983308ADC08BD1E984A220B7F9625763F4D1A133B143ADE2995FB6C571
  ```

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 $wt(\alpha) = 1$. This ensures that f' is PC(1). This technique has been used in [20].

We have checked that by linear transformation on f one can get the PC(1) property and the function with the PC(1) property is as follows.

```
C0EC6696A657BDF973FC366AC2B753360945A191C1E959F7DD551B2664373874
0E0F44A382CA7FB24FD08C00C05B8736A6930A4054F0C8E99047FECFB61F42A7
0DC6223F6BB884DB90FC55E52BD084594CEF8FF55F09219DA5A1C72C975ADE30
D1D54D00D27B8E646ED42284E5EDC38DE63417156A4D8CB73E759D3A364BEB49
```

- We also find an unbalanced RSBF ϕ with $nl(\phi) = 488$, $\Delta_\phi = 24$, and $deg(\phi) = 9$ as given below.

```
FFFEEBF9E8CAAFD2E8C5A4899CFFB20CFDC4F162992580C283E5FAAA8F1C51B5
FAA6B471FA12385996824D379154A55DD10EA827BF9D8D98D0EB07B43606CE27
FE9D883C8B216F42FAD853081BC036D7C26DC44D60B75E3FD2037734C93662A3
E70611B8CCD0586F8BAB87E7C1F69681B254ACCB113B9E614E295569A1F91D7F
```

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.

```
96687D907EA3C6447EACCD1FF56924656BAD98F4F0B316ABEA736CC319753823
6CCFDDE79384AE30FF14DB5E073DCCCBB8983E4E29F4E40E46826E225F90584E
68F4E1AAE2B7F92B934EC5618DA95F41ABFB5224F6DE37A9446A1EA2A0A0F4CA
8E9087D15AB931F91DC2EE71A86000E8243DC55D78AD080827BFC300379074E9
```

We then obtain the following PC(1) function by linear transformation.

```
E268057177B22ACE3F3F44CB6D3B93674A9579E2DB90E916F107A69B9666C8A2
3161C81F185FD09F4060259DE418A0931ED23193024E7AE76C4FD9C35D73520A
B7CEDFBC389E34B7B2146DA01B6F5307BBD802DFAC85919197FEBC0A68B04232
C4E37E5BF7DAA2D3A26CAF8BF15800BDC5D142459CDDC8B8AA51AF58F8B2B428
```

iii) Next we present a 10-variable 1-resilient function having nonlinearity 492 and absolute indicator 56. We start with the unbalanced RSBF ϕ as follows.

```
E9C6B17C9F136FE496BA574B7CEEA820D33C8E9D776F709B6EB1A8E9CCD01941
B34F4EF095F8C2E23E6A68AA6B40C2DA3CE8DB469C81A883F4A1A24146877153
9A5E75BA64F9EA00D627FBC5A509AC595BAC7C886880988C68DA6101E109A3DD
4EF4AD80E3DB312DD2E080428C91911FAE309D53C8082557247D803F2F07335E
```

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 10 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.

```
8180CDED6C1C0302AA32E761B2079F0C37D8393E5B8DF2934B2AACEA7EB40BF0
AF6694BAF19E415E4580C0D679DB9BEB982963591185C33FEC2F67987D121D3B
C4E281F3D071957A74DF8A99FF258E9EC3D3AE6BE39415B0F4E5DA104DFC0125
24AD19CBA965D3768C525AD75C5316AA0F77F1A49E4AFD4223D40756C8388886
```

As for the statistical information, 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 many 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 just a few dozens being transformable to 1-resilient functions. 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. This statistical information clearly demonstrates what our algorithm achieves over the algorithm in [16] by not restricting the search space to the set of balanced functions.

Using a computer system with Pentium IV 2.8 GHz processor and 248 MB RAM, and setting the iteration number $N = 100,000$, a typical run of our algorithm takes 1 minute and 29 seconds for $n = 9$. For $n = 10$, a typical run takes 57 minutes with iteration number N equal to 400,000.

5 Conclusion

Functions, which were not known for a long time, could be achieved with our steepest-descent based iterative heuristic search in the class of rotation symmetric Boolean functions. As a major result, we could show the existence of Boolean functions having nonlinearity $> 2^{n-1} - 2^{\frac{n-1}{2}}$ for $n = 9, 11, 13$. In the process, by applying affine transformations, we could find balanced PC(1) Boolean functions on 10 variables with maximum absolute value in the autocorrelation spectrum $< 2^{\frac{n}{2}}$ along with other cryptographic properties like good nonlinearity and algebraic degree. Further, we discovered several 10-variable 1-resilient functions with nonlinearity 492, which was posed as an open question in Crypto 2000.

References

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

[2] J. A. Clark and J. L. Jacob. Two-stage optimization in the design of Boolean functions. In *ACISP 2000*, number 1841 in Lecture Notes in Computer Science, pages 242–254. Springer-Verlag, 2000.

[3] J. Clark, J. Jacob, S. Stepney, S. Maitra and W. Millan. Evolving Boolean functions satisfying multiple criteria. In *INDOCRYPT 2002*, Volume 2551 in Lecture Notes in Computer Science, pages 246–259, Springer Verlag, 2002.

[4] J. Clark, J. Jacob, S. Maitra and P. Stănică. Almost Boolean functions: The design of Boolean functions by spectral inversion. *Computational Intelligence*, pages 450–462, Volume 20, Number 3, 2004.

[5] T. W. Cusick and P. Stănică. Fast evaluation, weights and nonlinearity of rotation-symmetric functions. *Discrete Mathematics*, pages 289-301, vol 258, no 1-3, 2002.

[6] D. K. Dalai, K. C. Gupta and S. Maitra. Results on algebraic immunity for cryptographically significant Boolean functions. In *INDOCRYPT 2004*, number 3348 in Lecture Notes in Computer Science, pages 92–106, Springer Verlag, December 2004.

[7] J. F. Dillon. Elementary Hadamard Difference sets. PhD Thesis, University of Maryland, 1974.

[8] E. Filiol and C. Fontaine. Highly nonlinear balanced Boolean functions with a good correlation-immunity. In *Advances in Cryptology - EUROCRYPT'98*, Springer-Verlag, 1998.

[9] C. Fontaine. On Some Cosets of the First-Order Reed-Muller Code with High Minimum Weight. In *IEEE Transactions on Information Theory*, 45(4):1237–1243, 1999.

[10] S. Gangopadhyay, P. H. Keskar and S. Maitra. Patterson-Wiedemann functions revisited. Accepted in *Discrete Mathematics*, (a special issue containing selected papers from R. C. Bose Centenary Symposium on Discrete Mathematics and Applications, December 2002).

[11] X. Guo-Zhen and J. Massey. A spectral characterization of correlation immune combining functions. *IEEE Transactions on Information Theory*, 34(3):569–571, May 1988.

[12] M. Hell, A. Maximov and S. Maitra. On efficient implementation of search strategy for rotation symmetric Boolean functions. In *Ninth International Workshop on Algebraic and Combinatoral Coding Theory, ACCT 2004*, Black Sea Coast, Bulgaria, June 19–25, 2004.

[13] T. Johansson and E. Pasalic. A construction of resilient functions with high nonlinearity. *IEEE International Symposium on Information Theory, ISIT 2000*, Sorrento, Italy, June 2000.

[14] S. Kavut and M. D. Yücel. Improved cost function in the design of Boolean functions satisfying multiple criteria. In *Indocrypt 2003*, pages 121–134, Lecture Notes in Computer Science, Volume 2904, Springer Verlag, 2003.

[15] S. Kavut and M. D. Yücel. A new algorithm for the design of strong Boolean functions (in Turkish). In *First National Cryptology Symposium*, pages 95–105, METU, Ankara, Türkiye, November 18-20, 2005.

[16] S. Kavut, S. Maitra and M. D. Yücel. Autocorrelation spectra of balanced Boolean functions on odd number input variables with maximum absolute value $< 2^{\frac{n+1}{2}}$. In *Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA 06*, March 13–15, 2006, LIFAR, University of Rouen, France.

[17] S. Kirkpatrick, Jr. C. D. Gelatt, and M. P. Vecchi. Optimization by simulated annealing. *Science*, 220(4598):671–680, May 1983.

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

[19] S. Maitra. Highly nonlinear balanced Boolean functions with very good autocorrelation property. In *Workshop on Coding and Cryptography - WCC 2001*, Electronic Notes in Discrete Mathematics, Volume 6. Elsevier, January 2001.

[20] S. Maitra and P. Sarkar. Modifications of Patterson-Wiedemann functions for cryptographic applications. *IEEE Transactions on Information Theory*, 48(1):278–284, January 2002.

[21] S. Maitra and P. Sarkar. Cryptographically significant Boolean functions with five valued Walsh spectra. *Theoretical Computer Science*, Volume 276, Number 1–2, pages 133-146, 2002.

[22] S. Maitra and E. Pasalic. Further constructions of resilient Boolean functions with very high nonlinearity. *IEEE Transactions on Information Theory*, 48(7):1825–1834, July 2002.

[23] A. Maximov, M. Hell and S. Maitra. Plateaued rotation symmetric Boolean functions on odd number of variables. In *First Workshop on Boolean Functions: Cryptography and Applications, BFCA 05*, LIFAR, University of Rouen, France, March 7–9, 2005.

[24] A. Maximov. Classes of plateaued rotation symmetric Boolean functions under transformation of Walsh spectra. In *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 *First International Conference on Information and Communications Security*, number 1334 in Lecture Notes in Computer Science, pages 149–158. Springer Verlag, 1997.

[26] W. Millan, A. Clark and E. Dawson. Heuristic design of cryptographically strong balanced Boolean functions. In *Advances in Cryptology EUROCRYPT'98*, pages 489–499. Springer Verlag LNCS 1403, 1998.

[27] W. Millan, A. Clark and E. Dawson. Boolean function design using hill climbing methods. In *4th Australasian Conference on Information, Security and Privacy*, number 1587 in Lecture Notes in Computer Science, pages 1–11. Springer Verlag, April 1999.

[28] J. J. Mykkeltveit. The covering radius of the $(128, 8)$ Reed-Muller code is 56. *IEEE Transactions on Information Theory*, IT-26(3):359–362, 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 *Workshop on Coding and Cryptography - WCC 2001*, Paris, January 8–12, 2001. Electronic Notes in Discrete Mathematics, Volume 6, Elsevier Science, 2001.

[30] E. Pasalic and T. Johansson. Further results on the relation between nonlinearity and resiliency of Boolean functions. In *IMA Conference on Cryptography and Coding*, number 1746 in Lecture Notes in Computer Science, pages 35–45. Springer-Verlag, 1999.

[31] N. J. Patterson and D. H. Wiedemann. The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, IT-29(3):354–356, 1983. See correction in IT-36(2):443, 1990.

[32] J. Pieprzyk and C. X. Qu. Fast hashing and rotation-symmetric functions. *Journal of Universal Computer Science*, pages 20-31, vol 5, no 1 (1999).

[33] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of Boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, Lecture Notes in Computer Science, pages 161–173. Springer-Verlag, 1991.

[34] O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, 20:300–305, 1976.

[35] Z. Saber, M. Faisal Uddin and A. Youssef. On the existence of $(9, 3, 5, 240)$ resilient functions. Preprint 2006.

[36] P. Sarkar and S. Maitra. Nonlinearity bounds and constuction of resilient Boolean functions. In *Advances in Cryptology - Crypto 2000*, pages 515–532, Berlin, 2000. Springer-Verlag. Lecture Notes in Computer Science Volume 1880.

[37] Special Issue on Particle Swarm Optimization. *IEEE Transactions on Evolutionary Computation*, Volume 8, number 3, June 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, Electronics Notes in Discrete Mathematics, volume 15, pages 178-183, Elsevier, December 2002. Available at: 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. *Information Processing Letters*, 88:299–304, 2003.

[40] P. Stănică, S. Maitra and J. Clark. Results on rotation symmetric bent and correlation immune Boolean functions. *Fast Software Encryption Workshop (FSE 2004)*, New Delhi, INDIA, LNCS 3017, Springer Verlag, pages 161–177, 2004.

[41] M. D. Yücel. Alternative Nonlinearity Criteria for Boolean Functions. *Electrical and Electronics Engineering Depertmental Memorandum*, Middle East Technical University, Türkiye, No. 2001-1, January 2001.

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