Correlation Immune Boolean Functions with Very High Nonlinearity

Subhamoy Maitra
Computer & Statistical Service Center
Indian Statistical Institute
203, B.T. Road, Calcutta 700 035, INDIA
e-mail: subho@isical.ac.in

Abstract

Here we provide a construction method for unbalanced, first order correlation immune Boolean functions on even number of variables $n \geq 6$. These functions achieve the currently best known nonlinearity $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$. Then we provide a simple modification of these functions to get unbalanced correlation immune Boolean functions on even number of variables n, with nonlinearity $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} - 2$ and maximum possible algebraic degree $n - 1$. Moreover, we present a detailed study on the Walsh spectra of these functions.

Keywords : *Cryptography, Correlation Immunity, Nonlinearity, Algebraic Degree, Boolean Function, Walsh Spectra.*

1 Introduction

Nonlinearity and correlation immunity are two challenging combinatorial properties of Boolean functions. These properties are also important for cryptographic purposes. The concept of correlation immune Boolean functions was introduced by Siegenthaler [25] and these functions are used in stream cipher systems for resisting cryptanalytic attacks [26]. Construction and enumeration of correlation immune Boolean functions have received a lot of attention as evident from [12, 28, 13, 9].

Nonlinearity is also an important cryptographic criteria for Boolean functions. This is also related to covering radius of first order Reed-Muller codes [8, Chapter 13]. It was shown by Rothaus [19], that for even n, the maximum nonlinearity achievable for any Boolean function is $2^{n-1} - 2^{\frac{n}{2}-1}$ and the functions having this nonlinearity are called bent functions. However, bent functions are not balanced. Construction of balanced Boolean functions on even number of variables with very high nonlinearity has been considered in [24, 4, 21]. Dobbertin [4] has conjectured that, for even n, $nlb(n) = 2^{n-1} + 2^{\frac{n}{2}} + nlb(\frac{n}{2})$, where $nlb(n)$ is the maximum possible nonlinearity for an n-variable balanced function.

The nonlinearity question is open for functions on odd number of variables. It is known that [1, 14, 7] for odd $n \leq 7$, the maximum possible nonlinearity is $2^{n-1} - 2^{\frac{n-1}{2}}$. The question of maximum nonlinearity is open for $n = 9, 11, 13$ and the maximum possible nonlinearity that can be achieved is $2^{n-1} - 2^{\frac{n-1}{2}}$. For odd $n \geq 15$, it is possible to construct (both unbalanced and balanced) functions with nonlinearity strictly greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ [17, 18, 21].

Recently, weight divisibility results on resilient and correlation immune functions have been presented [22]. These results have direct consequence towards nontrivial upper bounds on nonlinearity of such functions. Almost at the same time Tarannikov [27] and Zheng and Zhang [29] independently got similar kinds of results. Very recently, Carlet [3] and Sarkar [20] have proved weight divisibility results for correlation immune and resilient (balanced correlation immune) Boolean functions involving algebraic degree of the functions and these results have sharpened the upper bounds. The works [3] and [20] are independent and use different kinds of techniques. Also, construction of resilient and correlation immune Boolean functions achieving these upper bounds have been discussed in [22, 27, 16]. Thus, it is very clear that a lot of interest have been generated in this direction.

Construction of resilient (balanced correlation immune) functions have direct application as combining functions in certain models of stream ciphers and there are lot of results available in this direction [2, 23, 5, 10, 21, 22, 27, 16]. However, construction results related to unbalanced correlation immune functions has not yet received a lot of attention (though there are some results available in recent papers [27, 16]). In this paper we provide a construction of unbalanced correlation immune Boolean functions on even number of input variables with very high nonlinearity. Unless otherwise mentioned, we will use n as an even integer. The basic input to the construction is a 6-variable correlation immune function with nonlinearity 26 and algebraic degree 5, which could be constructed very recently [16]. Using this 6-variable function, for the first time we show the existence of an 8-variable correlation immune function with nonlinearity 116 and algebraic degree 5. We extend our result to construct correlation immune functions with nonlinearity $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$ and algebraic degree 5. Moreover, we present a simple modification of these functions to get correlation immune functions with nonlinearity $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} - 2$ and algebraic degree $n-1$. Since construction of unbalanced correlation immune functions with very high nonlinearity is not known we will compare our results with the maximum possible nonlinearity achieved by resilient Boolean functions [21] on even number of variables. This is given in Section 4.

Recent results show [22] that the Walsh spectra of mth order correlation immune Boolean functions on n variables with maximum possible nonlinearity is three valued for $m > \frac{n}{2} - 1$ and the spectral values are $0, \pm 2^{m+1}$. However, the situation is not so clear for $m \leq \frac{n}{2} - 1$ and here we consider the case $m = 1$. Thus it is important to talk about the Walsh spectra of such functions, which we take up in this initiative.

1.1 Definitions and Notations

By Ω_n we mean the set of all Boolean functions. The addition operator over $GF(2)$ is denoted by $\oplus$. We sometimes interpret a Boolean function on n input variables by the output column of its truth table, which is a binary string of length 2^n. For binary strings S_1, S_2 of same length s, we denote by $\#(S_1 = S_2)$ (respectively $\#(S_1 \neq S_2)$), the number of places where S_1 and S_2 are equal (respectively unequal). The Hamming distance between S_1, S_2 is denoted by $d(S_1, S_2)$, i.e. $d(S_1, S_2) = \#(S_1 \neq S_2)$. The Walsh distance $wd(S_1, S_2)$, between S_1 and S_2, is defined as, $wd(S_1, S_2) = \#(S_1 = S_2) - \#(S_1 \neq S_2)$. Note that, $wd(S_1, S_2) = s - 2\, d(S_1, S_2)$. Also the Hamming weight or simply the weight of a binary string S is the number of ones in S. This is denoted by $wt(S)$. An n-variable function f is said to be balanced if its output column in the truth table contains equal number of 0's and 1's (i.e. $wt(f) = 2^{n-1}$). The ith location of a binary string S is denoted by $S[i]$.

An n-variable Boolean function $f(X_n, \ldots, X_1)$ 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, $f(X_n, \ldots, X_1)$ can be written as $a_0 \oplus (\bigoplus_{i=1}^{i=n} a_i X_i) \oplus (\bigoplus_{1 \leq i \neq j \leq n} a_{ij} X_i X_j) \oplus \ldots \oplus a_{12\ldots n} X_1 X_2 \ldots X_n$ 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 degree of 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. For a linear function l, by $ndg(l)$ we denote the number of input variables on which l is nondegenerate.

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 distance from the set of all n-variable affine functions.

Walsh transform is an important tool in analysis of Boolean functions. Let $\overline{X} = (X_n, \ldots, X_1)$ and $\overline{\omega} = (\omega_n, \ldots, \omega_1)$ both belong to $\{0, 1\}^n$ and $\overline{X}.\overline{\omega} = X_n \omega_n \oplus \ldots \oplus X_1 \omega_1$. Let $f(\overline{X})$ be a Boolean function on n variables. Then the Walsh transform of $f(\overline{X})$ is a real valued function over $\{0, 1\}^n$ that can be defined as $W_f(\overline{\omega}) = \sum_{\overline{X} \in \{0,1\}^n} (-1)^{f(\overline{X}) \oplus \overline{X}.\overline{\omega}}$. The relationship between Walsh transform and Walsh distance is [11] $W_f(\overline{\omega}) = wd(f, \bigoplus_{i=1}^{i=n} \omega_i X_i)$.

In [6], the following characterization of correlation immunity is provided. A function $f(X_n, \ldots, X_1)$ is m-th order correlation immune (CI) iff its Walsh transform W_f satisfies $W_f(\overline{\omega}) = 0$, for $1 \leq wt(\overline{\omega}) \leq m$. If f is balanced then $W_f(\overline{0}) = 0$. Balanced m-th order correlation immune functions are called m-resilient functions. Thus, a function $f(X_n, \ldots, X_1)$ is m-resilient iff its Walsh transform W_f satisfies $W_f(\overline{\omega}) = 0$, for $0 \leq wt(\overline{\omega}) \leq m$.

By $[[n, m, d, x]]$ we denote an n-variable unbalanced correlation immune function of order m, nonlinearity x and degree d.

2 Basic Construction

First we consider the generalized construction method.

Construction 2.1 *Let $h \in \Omega_n$ be an $[[n, 1, d, x]]$ function, where n is even. Consider the* *function $g(X_{n+2}, \ldots, X_1) = X_{n+2}X_{n+1} \oplus h(X_n, \ldots, X_1)$, i.e. the truth table of g is of the form $hhhh^c$.*

Then we have the following result.

Proposition 2.1 *Let $h \in \Omega_n$ be an $[[n, 1, d, x]]$ function, where n is even and $d > 2$. Let $g \in \Omega_{n+2}$ be generated from h as in Construction 2.1. Then*

1. *$nl(g) = 2^n + 2x$,*
2. *$wd(g, X_i) = 0$ for $1 \leq i \leq n$ and*
3. *$wd(g, X_{n+2} \oplus X_1) = wd(g, X_{n+1} \oplus X_1) = 0$.*
4. *The function g has algebraic degree d.*

Proof : Note that for any affine function $\lambda \in A(n+2)$, we can write λ in any one of the forms $llll, ll^cll^c, lll^cl^c, ll^cl^cl$, where $l \in A(n)$. Now consider $\lambda = llll$. Then, $d(g, \lambda) = d(hhhh^c, llll) = d(h, l) + d(h, l) + d(h, l) + d(h^c, l) = 2d(h, l) + d(h, l) + d(h^c, l) = 2x + 2^n$. The result is similar for λ of other forms also. This gives the nonlinearity result.

Note that g is of the form $hhhh^c$ and X_i is the form $llll$, for $1 \leq i \leq n$. Here by X_i we mean output column of a truth table considering the function X_i, where X_i is considered as an $(n+2)$-variable function (Here X_i is the output column of length 2^{n+2} and l is the output column of length 2^n). Since h is correlation immune, $wd(h, l) = 0$ and hence, $wd(g, X_i) = wd(h, l) + wd(h, l) + wd(h, l) + wd(h^c, l) = 0$ for $1 \leq i \leq n$.

Since, h is 1st order correlation immune, we have $wd(h, X_1) = wd(h, X_1^c) = 0$. Note that here by X_1 we mean the output column of a truth table considering the function X_1, where X_1 is considered as an n-variable function (output column of length 2^n). Now, $wd(g, X_{n+2} \oplus X_1) = wd(hhhh^c, X_1X_1X_1^cX_1^c) = wd(h, X_1) + wd(h, X_1) + wd(h, X_1^c) + wd(h^c, X_1^c) = 0$. Similarly, it can be seen that $wd(g, X_{n+1} \oplus X_1) = 0$.

Since, $g(X_{n+2}, \ldots, X_1) = X_{n+2}X_{n+1} \oplus h(X_n, \ldots, X_1)$, and degree of h is $d > 2$, we get the item 4. ∎

Construction of resilient Boolean functions using linear transformation has been used in [15]. We use here a similar method for correlation immune functions. The method is as follows.

Given a function $f \in \Omega_n$, we define $S_f = \{\overline{\omega} \in \{0, 1\}^n \mid W_f(\overline{\omega}) = 0\}$, where W_f is the Walsh transform of f. If there exists n linearly independent vectors in S_f, then we 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 if we construct a function $f'(\overline{X}) = f(C_f\overline{X})$, then both f', f *have the same nonlinearity and algebraic degree*. Moreover, $W_{f'}(\overline{\omega}) = 0$ for $wt(\overline{\omega}) = 1$, where $W_{f'}$ is the Walsh Transform of f'. This ensures that f' is 1st order correlation immune.

Let ϵ_i^k be an k-bit vector with ith $(1 \leq i \leq k)$ entry 1 and all other entries 0. For example $\epsilon_k^k = (1, 0, \ldots, 0)$ and $\epsilon_1^k = (0, \ldots, 0, 1)$.

Now we concentrate on $(n+2)$-bit vectors. We define, $r_i = \epsilon_i^{n+2}$, $1 \leq i \leq n$ and $r_i = \epsilon_i^{n+2} \oplus \epsilon_1^{n+2}$ for $i = n+1, n+2$. Here, the $\oplus$ means bitwise XOR of two binary vectors. Note that each vector corresponds to a linear function. The vectors r_i for $1 \leq i \leq n$ corresponds to the linear functions X_i and the vectors r_i for $i = n+1, n+2$ corresponds to $X_{n+1} \oplus X_1$ and $X_{n+2} \oplus X_1$. It is important to note that the $(n+2)$ vectors r_i are linearly independent. Thus, if we consider the function g as in Construction 2.1, then B_g is of the following form. Note that B_g is a nonsingular (invertible) matrix. Let us consider the binary matrix $C_g = B_g^{-1}$.

$$B_g = \begin{bmatrix} 0 & 0 & 0 & . & . & 0 & 0 & 1 \\ 0 & 0 & 0 & . & . & 0 & 1 & 0 \\ 0 & 0 & 0 & . & . & 1 & 0 & 0 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ 0 & 0 & 1 & . & . & 0 & 0 & 0 \\ 0 & 1 & 0 & . & . & 0 & 0 & 1 \\ 1 & 0 & 0 & . & . & 0 & 0 & 1 \end{bmatrix}, \quad C_g = \begin{bmatrix} 1 & 0 & 0 & . & . & 0 & 0 & 1 \\ 1 & 0 & 0 & . & . & 0 & 1 & 0 \\ 0 & 0 & 0 & . & . & 1 & 0 & 0 \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ 0 & 0 & 1 & . & . & 0 & 0 & 0 \\ 0 & 1 & 0 & . & . & 0 & 0 & 0 \\ 1 & 0 & 0 & . & . & 0 & 0 & 0 \end{bmatrix}$$

Table 1.

Then we have the following theorem.

Theorem 2.1 *Let $h \in \Omega_n$ be an $[[n, 1, d, x]]$ function, where n is even. Then it is possible to construct a function g', which is $[[n+2, 1, d, 2^n + 2x]]$.*

Proof : We use Construction 2.1 and the result of Proposition 2.1 here. From h, it is possible to get a function $g \in \Omega_{n+2}$, such that $nl(g) = 2^n + 2x$ and degree of g is d. Now it is possible to get a nonsingular matrix B_g. Thus we can get a binary matrix $C_g = B_g^{-1}$. Consider $\overline{X} = (X_{n+2}, \ldots, X_1)$ and we interpret it as a column vector here. Hence, the function $g'(\overline{X}) = g(C_g \overline{X})$ is an $[[n+2, 1, d, 2^n + 2x]]$ function. ■

Next we consider the initial function for this construction. Construction of $[[6, 1, 5, 26]]$ Boolean function has been proposed in [16]. The following is a 64 bit truth table of the $[[6, 1, 5, 26]]$ Boolean function that we use here 0000010110101001010100111111000110101111110000101100010000101001. From this we can construct an $[[8, 1, 5, 116]]$ function using Theorem 2.1. Note that this is the first time when a correlation immune function with nonlinearity greater than 112 gets reported. Also in [3, 20], it has been reported that the maximum possible nonlinearity of an $[[n, m, d, x]]$ function is $2^{n-1} - 2^{\frac{n}{2}-1} - 2^{m+\lfloor\frac{n-m-1}{d}\rfloor}$ for n even. Putting $n = 8, m = 1, d = 5$, we get that the maximum possible nonlinearity of an $[[8, 1, 5, 116]]$ function is $2^{8-1} - 2^{\frac{8}{2}-1} - 2^{1+\lfloor\frac{8-1-1}{5}\rfloor} = 116$. Thus this function achieves the maximum possible nonlinearity and in turn shows the tightness of the bound [3, 20] in this case.

In general we have the following theorem.

Theorem 2.2 *It is possible to construct $[[n, 1, 5, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}]]$ functions.*

Proof : Note that it is possible to construct a $[[6, 1, 5, 26]]$ function. Now $26 = 2^{6-1} - 2^{\frac{6}{2}} + 2^{\frac{6}{2}-2}$, which is the base case of induction. Let it is possible to construct an $[[m, 1, 5, 2^{m-1} -$

$2^{\frac{m}{2}} + 2^{\frac{m}{2}-2}]]$ function for even $m > 6$. From this, using Theorem 2.1 we can construct an $[[m+2, 1, 5, 2^m + 2(2^{m-1} - 2^{\frac{m}{2}} + 2^{\frac{m}{2}-2})]]$ function. Now, $2^m + 2(2^{m-1} - 2^{\frac{m}{2}} + 2^{\frac{m}{2}-2}) = 2^{(m+2)-1} - 2^{\frac{m+2}{2}} + 2^{\frac{m+2}{2}-2}$. Thus the proof. ■

Now we talk about the Walsh spectra of the function g'. Since $g'(\overline{X}) = g(C_g\overline{X})$, the Walsh spectra of g, g' are same. Note that any linear function λ of $n+2$ variables can be written as any of the following four forms, $llll, ll^cll^c, lll^cl^c, ll^cl^cl$, where l is a linear function of n variables. Note that, $wd(g, \lambda) = wd(hhhh^c, llll)$ *or* $wd(hhhh^c, ll^cll^c)$ *or* $wd(hhhh^c, lll^cl^c)$ *or* $wd(hhhh^c, ll^cl^cl)$. Thus, $wd(g, \lambda) = \pm 2wd(h, l)$. The Walsh spectra of the $[[6, 1, 5, 26]]$ function
0000010110101001010100111111000110101111110000101100010000101001 contains 7 different values $0, \pm 4, \pm 8, \pm 12$. Thus, the $[[n = 6 + 2i, 1, 5, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}]]$ functions have the Walsh spectra $0, \pm 4 \cdot 2^i, \pm 8 \cdot 2^i, \pm 12 \cdot 2^i$. Hence we have the following results.

Corollary 2.1 *It is possible to construct* $[[n, 1, 5, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}]]$ *functions with seven valued Walsh spectra* $0, \pm 4 \cdot 2^{\frac{n}{2}-3}, \pm 8 \cdot 2^{\frac{n}{2}-3}, \pm 12 \cdot 2^{\frac{n}{2}-3}$.

Now we talk some more interesting results on the Walsh spectra of these functions. We have earlier mentioned that for a linear function l, by $ndg(l)$ we denote the number of input variables on which l is nondegenerate. It can be checked that for the $[[6, 1, 5, 26]]$ function f mentioned above, we find $wd(f, l) = 0, \pm 8$, when $ndg(l)$ is odd and $wd(f, l) = \pm 4, \pm 12$, when $ndg(l)$ is even for $l \in L(6)$. It can also be observed that $[[8, 1, 5, 116]]$ function F, constructed by using the function f, gives the Walsh spectra as follows : $wd(F, \lambda) = 0, \pm 16$, when $ndg(\lambda)$ is odd and $wd(f, \lambda) = \pm 8, \pm 24$, when $ndg(\lambda)$ is even for $\lambda \in L(8)$. We generalize this result. First we update the Construction 2.1.

Construction 2.2 *Let* $h \in \Omega_n$ *be an* $[[n, 1, d, x]]$ *function, where* n *is even. Also,* $wd(h, l) = 0, \pm x$, *when* $ndg(l)$ *is odd and* $wd(h, l) = \pm y, \pm z$, *when* $ndg(l)$ *is even for* $l \in L(n)$. *Then Consider the function* $g(X_{n+2}, \ldots, X_1) = X_{n+2}X_{n+1} \oplus h(X_n, \ldots, X_1)$, *i.e. the truth table of* g *is of the form* $hhhh^c$. *Consider the binary matrix* C_g *mentioned in Table 1. Let* $\overline{X} = (X_{n+2}, \ldots, X_1)$. *Interpret* $\overline{X}$ *as a column vector. Construct the function* $g'(\overline{X}) = g(C_g\overline{X})$.

We have already proved that the function $g'(\overline{X})$ is an $[[n+2, 1, d, 2^n + 2x]]$ one. Now we prove the result on Walsh spectra of the function g'.

Lemma 2.1 *Let* $g' \in \Omega_{n+2}$ *be the function as mentioned in Construction 2.2. Then* $wd(g', \lambda) = 0, \pm 2 \cdot x$, *when* $ndg(\lambda)$ *is odd and* $wd(g', \lambda) = \pm 2 \cdot y, \pm 2 \cdot z$, *when* $ndg(\lambda)$ *is even for* $\lambda \in L(n+2)$.

Proof : Note that λ is any of the following four forms : $X_{n+2} \oplus X_{n+1} \oplus l$, $X_{n+2} \oplus l$, $X_{n+1} \oplus l$, l, where $l \in L(n)$. Now, $wd(g(X_{n+2}, \ldots, X_1), \lambda) = 0$, *or* $\pm 2x$ when $ndg(l)$ is odd and $wd(g(X_{n+2}, \ldots, X_1), \lambda) = \pm 2y$, *or* $\pm 2z$ when $ndg(l)$ is even. It is important to see that $ndg(\lambda)$ is odd when (i) λ is of the form $X_{n+2} \oplus X_{n+1} \oplus l$, or l and $ndg(l)$ is odd, (ii) λ is of the form $X_{n+2} \oplus l$, or $X_{n+1} \oplus l$ and $ndg(l)$ is even. Similarly, $ndg(\lambda)$ is even when (i) λ is of the form $X_{n+2} \oplus X_{n+1} \oplus l$, or l and $ndg(l)$ is even, (ii) λ is of the form $X_{n+2} \oplus l$, or $X_{n+1} \oplus l$ and $ndg(l)$ is odd. Then the proof follows from the result that $g'(\overline{X}) = g(C_g\overline{X})$ and the form of the matrix C_g. ■

Theorem 2.3 *It is possible to construct* $[[n, 1, 5, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}]]$ *functions* f *with*

1. $W_f(\overline{\omega}) = 0, \pm 8 \cdot 2^{\frac{n}{2}-3}$, *for* $wt(\overline{\omega})$ *odd and*
2. $W_f(\overline{\omega}) = \pm 4 \cdot 2^{\frac{n}{2}-3}, \pm 12 \cdot 2^{\frac{n}{2}-3}$, *for* $wt(\overline{\omega})$ *even.*

Proof : The proof follows from Construction 2.2, Lemma 2.1 and the Walsh spectra of the initial $[[6, 1, 5, 26]]$ function mentioned above. ■

3 Modified Construction for Maximum Possible Algebraic Degree

Note that all the functions we have constructed so far are of algebraic degree 5. However, it is known [25], that the maximum possible algebraic degree of an $[[n, m, d, x]]$ function is $d = n - m$. Thus, here for $m = 1$, we need to achieve the algebraic degree $n - 1$. This we achieve using the following technique which has earlier been used in [10].

Definition 3.1 *Let* $f, g \in \Omega_n$ *and there exists* i_0, i_1 *with* $i_0 + i_1 = 2^n - 1$, *such that*

1. $f[i_0] = f[i_1] = a$, $a \in \{0, 1\}$,
2. $g[i_0] = g[i_1] = 1 - a$ *and*
3. $f[j] = g[j]$ *if* $j \neq i_0, i_1$.

Then we say that f, g *are palindromically related.*

Note that values of just a specific pair of positions are complemented and the positions are at the same distances from top and bottom of the function. The following result shows the importance of Definition 3.1.

Proposition 3.1 *Let* $f, g \in \Omega_n$ *be palindromically related. Then*

1. f *is correlation immune of order 1 iff* g *is correlation immune of order 1.*
2. $nl(g) \geq nl(f) - 2$.
3. *If algebraic degree of* f *is less than* $n - 1$, *then* g *is of algebraic degree* $n - 1$.

Proof : Item 1 and 2 are proved in [10] and in [11] respectively. Now we prove item 3. Consider $f = f_1 f_2$, where $f_1, f_2 \in \Omega_{n-1}$, that is, the truth table of f can be seen as concatenation of truth tables of the functions f_1 and f_2. Similarly, consider $g = g_1 g_2$, where $g_1, g_2 \in \Omega_{n-1}$. Since, f is of algebraic degree less than $n - 1$, we have $wt(f_1)$ and $wt(f_2)$ are both even. Thus, $wt(g_1)$ and $wt(g_2)$ are both odd. Hence degree of g is $n - 1$. ■

Theorem 3.1 *It is possible to construct* $[[n, 1, n-1, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} - 2]]$ *functions.*

Proof : We know from Theorem 2.2, that it is possible to construct an $[[n, 1, 5, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}]]$ function. We consider such a function f. Now this function is unbalanced and hence it cannot be of the form hh^c, for $h \in \Omega_{n-1}$. Thus, there will be at least one location i such that $f[i] = f[2^n - 1 - i]$. From f we construct a palindromically related function $g \in \Omega_n$. From Proposition 3.1, it is clear that g is an $[[n, 1, n-1, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} - 2]]$ function. ■

Thus from an $[[8, 1, 5, 116]]$ function we can construct an $[[8, 1, 7, 114]]$ function.

Now we analyze the Walsh spectra of $[[n, 1, n-1, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} - 2]]$ functions. From Corollary 2.1 we get that the Walsh spectra of the $[[n, 1, 5, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}]]$ functions have seven valued Walsh spectra $0, \pm 4 \cdot 2^{\frac{n}{2}-3}, \pm 8 \cdot 2^{\frac{n}{2}-3}, \pm 12 \cdot 2^{\frac{n}{2}-3}$.

Proposition 3.2 *Let* $f, g \in \Omega_n$ *be palindromically related and* $l \in L(n)$. *Then*

1. $wd(f, l) = wd(g, l)$, *if* l *is nondegenerate on odd number of variables.*

2. $wd(f, l) = wd(g, l) \pm 4$, *if* l *is nondegenerate on even number of variables.*

Proof : Let $ndg(l)$ be odd. If we consider the truth table of l, then $l[i] \neq l[2^n - 1 - i]$. Note that, $f[i] = f[2^n - 1 - i]$ and $g[i] = g[2^n - 1 - i]$. Thus, though $f[i] \neq g[i]$, the contribution to Walsh distance for both the functions f, g will be same for the points $i, 2^n - 1 - i$, which is 0.

On the other hand, if $ndg(l)$ is even, the truth table of l has the property $l[i] = l[2^n - 1 - i]$. Here $f[i] = f[2^n - 1 - i]$, $g[i] = g[2^n - 1 - i]$. Also $f[i] \neq g[i]$. Thus the contribution to Walsh distance for both the functions f, g will differ for the points $i, 2^n - 1 - i$, which is ± 4. ■

Hence we get the following result related to the Walsh spectra of the functions which are optimized with respect to the algebraic degree.

Theorem 3.2 *It is possible to construct* $[[n, 1, n-1, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} - 2]]$ *functions* f *with the 11-valued Walsh spectra as follows.*

1. $W_f(\overline{\omega}) = 0, \pm 8 \cdot 2^{\frac{n}{2}-3}$, *for* $wt(\overline{\omega})$ *odd and*

2. $W_f(\overline{\omega}) = \pm 4 \cdot 2^{\frac{n}{2}-3} \pm 4, \pm 12 \cdot 2^{\frac{n}{2}-3} \pm 4$, *for* $wt(\overline{\omega})$ *even.*

Proof : Consider the Walsh spectra of the $[[n, 1, 5, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}]]$ function f as in Theorem 2.3. $W_f(\overline{\omega}) = 0, \pm 8 \cdot 2^{\frac{n}{2}-3}$, for $wt(\overline{\omega})$ odd and $W_f(\overline{\omega}) = \pm 4 \cdot 2^{\frac{n}{2}-3}, \pm 12 \cdot 2^{\frac{n}{2}-3}$, for $wt(\overline{\omega})$ even. Then the result follows from Proposition 3.2. ■

4 Comparison with Existing Results

Currently there is no construction which can provide unbalanced correlation immune functions with as good nonlinearity as ours. In fact, as far as we know, there is no existing construction which can discuss about a generalized construction of first order correlation immune functions with very high nonlinearity. That is the reason we compare our result with the maximum known nonlinearity of 1-resilient functions [21].

First we provide a table for functions on small number of variables. Column A presents the nonlinearity achieved by 1st order correlation immune functions with algebraic degree 5 and column B presents the nonlinearity achieved by 1st order correlation immune functions with maximum possible algebraic degree $(n-1)$. Column C provides the currently best known nonlinearity achieved by 1st order balanced correlation immune functions [21] with maximum possible algebraic degree $(n-2)$ and column D provides the currently best known nonlinearity achieved by 1st order balanced correlation immune functions [21] with maximum possible algebraic degree less than $(n-2)$. For comparison we also present the currently best known nonlinearity for balanced Boolean functions in column E.

n	A	B	C [21]	D [21]	E
6	26	26	24	24	26
8	116	114	112	112	116
10	488	486	484	480	492

Table 2.

It should be noted that for $n \geq 12$, the currently best known nonlinearity achieved by 1st order balanced correlation immune functions [21, Theorem 7] with algebraic degree $\frac{n}{2}+2$ is $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$. However, the maximum possible algebraic degree of n-variable, 1-resilient function is $n-2$. For $n \geq 12$, the currently best known nonlinearity achieved by 1st order balanced correlation immune functions [21, Theorem 8] with maximum possible algebraic degree $(n-2)$ is $2^{n-1} - 2^{\frac{n}{2}} + y$, where y is the maximum possible nonlinearity of an $(\frac{n}{2}-1)$-variable balanced 1st order correlation immune function with algebraic degree $(\frac{n}{2}-3)$. We estimate y as $2^{\frac{n}{2}-2} - 2^{\frac{n}{4}-2} - 4$ [22], the upper bound of nonlinearity for an $(\frac{n}{2}-1)$-variable function which is balanced and 1st order correlation immune. So, the currently best known nonlinearity achieved by 1st order balanced correlation immune functions [21] with maximum possible algebraic degree $(n-2)$ is $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} - 2^{\frac{n}{4}-2} - 4$.

We here achieve the nonlinearity $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$ for 1st order unbalanced correlation immune functions with algebraic degree 5. Moreover, we achieve the nonlinearity $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} - 2$ for 1st order correlation immune functions with maximum possible algebraic degree $(n-1)$.

Hence, considering the functions with maximum possible algebraic degree, we find that for $n \geq 12$ the nonlinearity achieved in this paper for 1st order correlation immune Boolean function (algebraic degree $n-1$) is $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} - 2$, which is greater than the nonlinearity $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} - 2^{\frac{n}{4}-2} - 4$ achieved in [21] for 1st order resilient (balanced correlation immune) Boolean function (algebraic degree $n-2$).

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] P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation immune functions. In *Advances in Cryptology - CRYPTO'91*, pages 86–100. Springer-Verlag, 1992.

[3] C. Carlet. On the coset weight divisibility and nonlinearity of resilient and correlation immune functions. *Preprint*, 2000.

[4] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. In *Fast Software Encryption*, number 1008 in Lecture Notes in Computer Science, pages 61–74. Springer-Verlag, 1994.

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

[6] 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.

[7] X. Hou. Covering radius of the Reed-Muller code $R(1, 7)$ - a simpler proof. *Journal of Combinatorial Theory, Series A*, 74(3):337–341, 1996.

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

[9] S. Maitra and P. Sarkar. Enumeration of correlation immune Boolean functions. In *4th Australasian Conference on Information, Security and Privacy*, number 1587 in Lecture Notes in Computer Science, pages 12–25. Springer Verlag, April 1999.

[10] S. Maitra and P. Sarkar. Hamming weights of correlation immune Boolean functions. *Information Processing Letters*, 71(3-4):149–153, 1999.

[11] S. Maitra and P. Sarkar. Highly nonlinear resilient functions optimizing Siegenthaler's inequality. In *Advances in Cryptology - CRYPTO'99*, number 1666 in Lecture Notes in Computer Science, pages 198–215. Springer Verlag, August 1999.

[12] C. J. Mitchell. Enumerating Boolean functions of cryptographic significance. *Journal of Cryptology*, 2(3):155–170, 1990.

[13] P. Sung Mo, L. Sangjin, S. Soo Hak, and K. Kwangjo. Improving bounds for the number of correlation immune Boolean functions. *Information Processing Letters*, 61(4):209–212, 1997.

[14] J. J. Mykkeltveit. The covering radius of the $(128, 8)$ Reed-Muller code is 56. *IEEE Transactions on Information Theory*, IT-26(3):358–362, 1983.

[15] 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.

[16] E. Pasalic, T. Johansson, S. Maitra, and P. Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity. *Cryptology ePrint Archive, eprint.iacr.org, No. 2000/048*, September 26, 2000.

[17] 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.

[18] N. J. Patterson and D. H. Wiedemann. Correction to - the covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, IT-36(2):443, 1990.

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

[20] P. Sarkar. Spectral domain analysis of correlation immune and resilient boolean functions. *Cryptology ePrint Archive, eprint.iacr.org, No. 2000/049*, September 26, 2000.

[21] P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. In *Advances in Cryptology - EUROCRYPT 2000*, number 1807 in Lecture Notes in Computer Science, pages 485–506. Springer Verlag, 2000.

[22] P. Sarkar and S. Maitra. Nonlinearity bounds and constructions of resilient boolean functions. In *Advances in Cryptology - CRYPTO 2000*, number 1880 in Lecture Notes in Computer Science, pages 515–532. Springer Verlag, 2000.

[23] J. Seberry, X. M. Zhang, and Y. Zheng. On constructions and nonlinearity of correlation immune Boolean functions. In *Advances in Cryptology - EUROCRYPT'93*, pages 181–199. Springer-Verlag, 1994.

[24] J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearly balanced Boolean Functions and their propagation characteristics. In *Advances in Cryptology - CRYPTO'93*, pages 49–60. Springer-Verlag, 1994.

[25] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776–780, September 1984.

[26] T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Transactions on Computers*, C-34(1):81–85, January 1985.

[27] Y. V. Tarannikov. On resilient Boolean functions with maximum possible nonlinearity. *Cryptology ePrint Archive, eprint.iacr.org, No. 2000/005*, March 10, 2000.

[28] Y. X. Yang and B. Guo. Further enumerating Boolean functions of cryptographic significance. *Journal of Cryptology*, 8(3):115–122, 1995.

[29] Y. Zheng and X. M. Zhang. Improving upper bound on nonlinearity of high order correlation immune functions. In *SAC 2000*, Lecture Notes in Computer Science (to be published). Springer Verlag, 2000.