Highly Nonlinear Balanced Boolean Functions with very good Autocorrelation Property

Subhamoy Maitra

Indian Statistical Institute, 203, B.T. Road, Calcutta 700 035, INDIA
Email : subho@isical.ac.in

Abstract

Constructing highly nonlinear balanced Boolean functions with very good autocorrelation property is an interesting open question. In this direction we use the measure Δ_f, the highest magnitude of all autocorrelation coefficients for a function f. We provide balanced functions f with currently best known nonlinearity and Δ_f values together. We extend the result of Maitra and Sarkar (2000) for 15-variable functions which experimentally disprove the conjecture proposed by Zhang and Zheng (1995). We prove it theoretically for different ranges of nonlinearity, where our constructions are based on modifications of Patterson-Wiedemann (1983) functions. Also we propose a simple bent based construction technique to get functions with very good Δ_f values for odd number of variables. This construction has a root in Kerdock Codes. Moreover, our construction on even number of variables is a recursive one and we conjecture (similar to Dobbertin's conjecture (1994) with respect to nonlinearity) that this provides the minimum possible value of Δ_f for a balanced function f on even number of variables. Next we discuss about the autocorrelation values of correlation immune and resilient Boolean functions. We provide new lower bounds and related results on absolute indicator and sum of square indicator (of autocorrelation) for certain orders of correlation immunity and resiliency and clearly show that autocorrelation goes against order of correlation immunity. We also point out the weakness of two recursive construction techniques for resilient functions in terms of autocorrelation values.

Key words: Boolean Function, Nonlinearity, Balancedness, Correlation Immunity, Autocorrelation, Propagation Characteristics, Global Avalanche Characteristics.

[1] Extended version of the paper "Highly Nonlinear Balanced Boolean Functions with Very Good Autocorrelation Property" presented in WCC, Paris, January 2001.

1 Introduction

Nonlinearity and autocorrelation values are two fundamental properties for cryptographically significant Boolean functions. It is well known (26; 21; 10; 8) that bent functions possess the best possible nonlinearity and autocorrelation values. However, bent functions are available for even number of variables only and they are not balanced. For nonlinear balanced functions the relationship between nonlinearity and autocorrelation values is not explicit. In this paper we construct balanced Boolean functions with currently best known trade-off between nonlinearity and autocorrelation values. For a function F, we use the parameter $nl(F)$ (see Definition 2) for nonlinearity and Δ_F (see Definition 6) for absolute indicator of autocorrelation values. A good balanced function F must have high $nl(F)$ and low Δ_F.

We provide balanced functions F on n variables (n even) with nonlinearity $nl(F) = 2^{n-1} - 2^{\frac{n}{2}} + nl(f)$ and $\Delta_F = 2^{\frac{n}{2}} + \Delta_f$, where f is an $\frac{n}{2}$ variable balanced function. This result is superior to the result proposed in (37), where $nl(F) = 2^{n-1} - 2^{\frac{n}{2}}$ and $\Delta_F = 2^{\frac{n}{2}+1}$. Also we conjecture from our recursive result that this construction provides the minimum possible value of Δ_f for a balanced function f on even number of variables.

In case of odd number of variables we use a bent based construction which is motivated from synthesis of Kerdock codes. The parameters we achieve are same as the parameters that appeared in (37, Section 5.2). However, our construction is easy to understand. In (37) it was conjectured that for a balanced function F on n variables (n odd), $\Delta_F \geq 2^{\frac{n+1}{2}}$. The conjecture has been experimentally disproved by running a computer program in (19). Experimental results (19) show that the conjecture is not true for functions with nonlinearity strictly greater than $2^{n-1} - 2^{\frac{n-1}{2}}$. However, we show here that the conjecture can be disproved directly from Patterson-Wiedemann functions and without running a computer experiment. We here extend the analysis of (19) by theoretically showing that the conjecture (37) is not true for different ranges of nonlinearity. We disprove the conjecture showing that for $n = 15$, there are functions with $\Delta_F < 2^{\frac{n+1}{2}}$ and this happens for functions with nonlinearity strictly less than, equal to and strictly greater than (three different cases) the bent concatenation nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$.

Next we concentrate on the autocorrelation values for correlation immune and resilient (balanced correlation immune) Boolean functions (see Definition 7). We provide the currently best known lower bounds on Δ_f, σ_f (see Definition 6) for these classes. Very recently autocorrelation properties of correlation immune and resilient Boolean functions were presented in (40) and we provide better results here. Also we provide sharper result for the class of correlation immune and resilient functions which attain the maximum possible

nonlinearity. In (41), it has been discussed that the propagation property goes against correlation immunity. We here explicitly show that the Δ_f values goes against the order of correlation immunity. We also point out the limitation of two recursive construction methods of resilient Boolean functions in terms of autocorrelation values.

2 Preliminaries

Here we introduce a few definitions and notations.

Definition 1 *Let s, s_1, s_2 be binary strings of same length λ. The bitwise complement of s is denoted by s^c. 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, $wd(s_1, s_2) = \lambda - 2\, d(s_1, s_2)$. The Hamming weight or simply the weight of s is the number of ones in s and 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. $wt(f) = 2^{n-1}$).

By Ω_n we mean the set of all n-variable Boolean functions. Note that we denote the addition operator over $GF(2)$ by $\oplus$. An n-variable Boolean function can be uniquely represented by a multivariate polynomial over $GF(2)$.

Definition 2 *Let $f(X_n, \ldots, X_1)$ be an n-variable function. We can write f 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 $a_0, a_i, a_{ij}, \ldots, a_{12\ldots n} \in \{0, 1\}$. 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. The set of all n-variable affine (respectively linear) functions is denoted by $A(n)$ (respectively $L(n)$). The nonlinearity $nl(f)$ of an n-variable function f is defined as

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

i.e. $nl(f)$ is the distance of f from the set of all n-variable affine functions. We also define

$$\tau_f = \max_{g \in A(n)} \mid wd(f,g) \mid = 2^n - 2nl(f).$$

Lower value of τ_f implies better nonlinearity of f.

In this document we will use concatenation of Boolean functions. Consider $f_1, f_2 \in \Omega_{n-1}$ and $f \in \Omega_n$. Then by concatenation of f_1 and f_2, we mean that the output columns of truth table of f_1, f_2 will be concatenated to provide the output column of the truth table of an n-variable function. We denote the concatenation of f_1, f_2 by $f_1 f_2$. Thus, $f = f_1 f_2$ means that in algebraic normal form, $f = (1 \oplus X_n) f_1 \oplus X_n f_2$.

Proposition 3 *Let $l_1, l_2 \in L(k)$. Then, $d(l_1, l_2) = 0, 2^{k-1}, 2^k$ ($wd(l_1, l_2) = 2^k, 0, -2^k$) according as $l_1 = l_2$ (are same), $l_1 \neq l_2$ or l_2^c (are distinct), $l_1 = l_2^c$ (are complement to each other).*

Definition 4 *Let $\overline{X} = (X_n, \ldots, X_1)$ and $\overline{\omega} = (\omega_n, \ldots, \omega_1)$ be n-tuples on GF(2) and $\overline{X}.\overline{\omega} = X_n\omega_n \oplus \ldots \oplus X_1\omega_1$. Let $f(\overline{X})$ be a Boolean function whose domain is the vector space over GF(2)^n. Then the Walsh transform of $f(\overline{X})$ is a real valued function over GF(2)^n that can be defined as*

$$W_f(\overline{\omega}) = \sum_{\overline{X}} (-1)^{f(\overline{X}) \oplus \overline{X}.\overline{\omega}},$$

where the sum is over all $\overline{X}$ in GF(2)^n. The relationship between Walsh distance and Walsh transform is

$$W_f(\overline{\omega}) = wd(f, \bigoplus_{i=1}^{i=n} \omega_i X_i).$$

For a function f, we define

$$\mathbf{F}_f = \mid \{\overline{\omega} \in \{0,1\}^n \mid W_f(\overline{\omega}) \neq 0\} \mid .$$

This is the number of nonzero coefficients in the Walsh spectra.

Propagation Characteristic (PC) and Strict Avalanche Criteria (SAC) (36; 25) are important properties of Boolean functions to be used in S-boxes.

Definition 5 *Let $\overline{X}$ be an n tuple $X_1, \ldots, X_n$ and $\overline{\alpha} \in \{0,1\}^n$. A function $f \in \Omega_n$ is said to satisfy*

(1) SAC if $f(\overline{X}) \oplus f(\overline{X} \oplus \overline{\alpha})$ is balanced for any $\overline{\alpha}$ such that $wt(\overline{\alpha}) = 1$.
(2) SAC(k) if any function obtained from f by keeping any k input bits constant satisfies SAC.
(3) PC(l) if $f(\overline{X}) \oplus f(\overline{X} \oplus \overline{\alpha})$ is balanced for any $\overline{\alpha}$ such that $1 \leq wt(\overline{\alpha}) \leq l$.

(4) PC(l) of order k if any function obtained from f by keeping any k input bits constant satisfies PC(l).

However, Zhang and Zheng (37) justified that SAC and PC have some limitations in identifying certain desirable cryptographic properties of a Boolean function. In this direction they have proposed the idea of Global Avalanche Characteristics (GAC). The following definition states two important indicators of GAC. Note that, the absolute indicator of GAC is a stronger property than the sum-of-square indicator.

Definition 6 *Let* $\overline{X} \in \{0,1\}^n$ *be an n tuple* $X_n, \ldots, X_1$ *and* $\overline{\alpha} \in \{0,1\}^n$ *be an n tuple* $\alpha_n, \ldots, \alpha_1$. *Let* $f \in \Omega_n$ *and*

$$\Delta_f(\overline{\alpha}) = wd(f(\overline{X}), f(\overline{X} \oplus \overline{\alpha})),$$

the autocorrelation value of f with respect to the vector $\overline{\alpha}$. *The sum-of-square indicator*

$$\sigma_f = \sum_{\overline{\alpha} \in \{0,1\}^n} \Delta_f^2(\overline{\alpha}).$$

The absolute indicator

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

Note that $\Delta_f(\overline{\alpha}) = 0$ iff $f(\overline{X}) \oplus f(\overline{X} \oplus \overline{\alpha})$ is balanced. Also $\mid \Delta_f(\overline{\alpha}) \mid = 2^n$ iff $f(\overline{X}) \oplus f(\overline{X} \oplus \overline{\alpha})$ is constant and $\overline{\alpha}$ is called a linear structure of f. Note that $\overline{0}$ is always a linear structure for a Boolean function. However, existence of any nonzero linear structure is cryptographically undesirable.

For functions f, on even number of variables, we have $\Delta_f = 0$, iff f is a bent function. However, bent functions are not balanced. In fact, for balanced functions f, $\Delta_f \geq 8$ (see (34)) for both odd and even number of variables. In the next two sections (Section 3, 4) we will propose several construction methods to provide balanced functions f with very high $nl(f)$ and very low Δ_f.

Then we concentrate on the autocorrelation spectra of correlation immune and resilient Boolean functions (Section 5). In (13), the following characterization of correlation immunity is provided.

Definition 7 *A function* $f(X_n, \ldots, X_1)$ *is m-th order correlation immune (CI) iff its Walsh transform* W_f *satisfies*

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

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

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

By (n, m, d, x) we denote an n-variable resilient function of order m, nonlinearity x and degree d.

It may very well happen that correlation immune or resilient functions, which are good in terms of order of correlation immunity, algebraic degree and nonlinearity, may not be good in terms of SAC or PC properties. Also getting good SAC or PC properties may not be sufficient for cryptographic purposes. There may be a function f which possesses good SAC or PC properties, but $f(\overline{X}) \oplus f(\overline{X} \oplus \overline{\alpha})$ is constant for some nonzero $\overline{\alpha}$, which is a weakness. It is important to get good autocorrelation properties for such functions. That is why, we here look into the autocorrelation properties of correlation immune and resilient functions in Section 5.

3 Construction for any odd n

First we need the following important result. The motivation of choosing two bent functions with the property used in the following lemma comes from the use of bent functions in Kerdock code.

Lemma 8 *Let n be odd and $f_1, f_2 \in \Omega_{n-1}$ are two bent functions such that $f_1(X_{n-1}, \ldots, X_1) \oplus f_2(X_{n-1} \oplus \alpha_{n-1}, \ldots, X_1 \oplus \alpha_1)$ is also bent for any vector $(\alpha_{n-1}, \ldots, \alpha_1) \in \{0,1\}^{n-1}$. Construct $F \in \Omega_n$ such that $F = f_1 f_2$, i.e. $F = (1 \oplus X_n) f_1(X_{n-1}, \ldots, X_1) \oplus X_n f_2(X_{n-1}, \ldots, X_1)$. Then $\Delta_F = 2^{\frac{n+1}{2}}$. Also it is possible to get such a balanced F.*

PROOF. We have to calculate $wd(F(X_n, \ldots, X_1), F(X_n \oplus \alpha_n, \ldots, X_1 \oplus \alpha_1))$ for nonzero $(\alpha_n, \ldots, \alpha_1) \in \{0,1\}^n$. We have two cases.
When $\alpha_n = 0$, then $wd(F(X_n, \ldots, X_1), F(X_n \oplus \alpha_n, \ldots, X_1 \oplus \alpha_1))$
$= wd(f_1(X_{n-1}, \ldots, X_1), f_1(X_{n-1} \oplus \alpha_{n-1}, \ldots, X_1 \oplus \alpha_1))$
$+ wd(f_2(X_{n-1}, \ldots, X_1), f_2(X_{n-1} \oplus \alpha_{n-1}, \ldots, X_1 \oplus \alpha_1))$
$= 0 + 0 = 0$, since both f_1, f_2 are bent.
When $\alpha_n = 1$, then $\mid wd(F(X_n, \ldots, X_1), F(X_n \oplus \alpha_n, \ldots, X_1 \oplus \alpha_1)) \mid$
$\leq \mid wd(f_1(X_{n-1}, \ldots, X_1), f_2(X_{n-1} \oplus \alpha_{n-1}, \ldots, X_1 \oplus \alpha_1)) \mid$
$+ \mid wd(f_2(X_{n-1}, \ldots, X_1), f_1(X_{n-1} \oplus \alpha_{n-1}, \ldots, X_1 \oplus \alpha_1)) \mid$
$= 2^{\frac{n-1}{2}} + 2^{\frac{n-1}{2}} = 2^{\frac{n+1}{2}}$, since $f_1(X_{n-1}, \ldots, X_1) \oplus f_2(X_{n-1} \oplus \alpha_{n-1}, \ldots, X_1 \oplus \alpha_1)$ is also bent. It is also easy to see that $\Delta_F(\overline{\alpha})$ can have the values $0, \pm 2^{\frac{n+1}{2}}$. Since F is on odd number of variables, all the $\Delta_F(\overline{\alpha})$ values cannot be zero. Hence, $\Delta_F = 2^{\frac{n+1}{2}}$. If $F = f_1 f_2$ is not balanced, use $F = f_1 f_2^c$, which is balanced. ■

Next we propose the following construction.

Construction 0 *Let $g_1, g_2 \in \Omega_m$ and $h_1, h_2 \in \Omega_k$ are all bent functions for m, k even and take $n = m+k$. Also, $g_1(Y_m, \ldots, Y_1) \oplus g_2(Y_m \oplus \beta_m, \ldots, X_1 \oplus \beta_1)$ is bent for any $(\beta_m, \ldots, \beta_1) \in \{0,1\}^m$ and $h_1(Z_k, \ldots, Z_1) \oplus h_2(Z_k \oplus \gamma_k, \ldots, Z_1 \oplus \gamma_1)$ is bent for any $(\gamma_k, \ldots, \gamma_1) \in \{0,1\}^k$. Let $f_1, f_2 \in \Omega_n$ such that $f_1 = g_1 \oplus h_1$ and $f_2 = g_2 \oplus h_2$, where $X_n = Y_m, \ldots, X_{n-m+1} = Y_1, X_{n-m} = Z_k, \ldots, X_1 = Z_1$. If $wt(f_1) = wt(f_2)$, then replace f_2 by f_2^c. This is required to make the function $f_1 f_2$ balanced.*

Lemma 9 *Let f_1, f_2 are as in Construction 0. Then $f_1(X_n, \ldots, X_1) \oplus f_2(X_n \oplus \alpha_n, \ldots, X_1 \oplus \alpha_1)$ is bent for any $(\alpha_n, \ldots, \alpha_1) \in \{0,1\}^n$.*

PROOF. We have f_1, f_2 as in Construction 0. Let $\alpha_n = \beta_m, \ldots, \alpha_{n-m+1} = \beta_1, \alpha_{n-m} = \gamma_k, \ldots, \alpha_1 = \gamma_1$. Thus, $f_1(X_n, \ldots, X_1) \oplus f_2(X_n \oplus \alpha_n, \ldots, X_1 \oplus \alpha_1)$ $= (g_1(Y_m, \ldots, Y_1) \oplus h_1(Z_k, \ldots, Z_1)) \oplus (g_2(Y_m \oplus \beta_m, \ldots, Y_1 \oplus \beta_1) \oplus h_2(Z_k \oplus \gamma_k, \ldots, Z_1 \oplus \gamma_1)) = (g_1(Y_m, \ldots, Y_1) \oplus g_2(Y_m \oplus \beta_m, \ldots, Y_1 \oplus \beta_1))$
$\oplus (h_1(Z_k, \ldots, Z_1) \oplus h_2(Z_k \oplus \gamma_k, \ldots, Z_1 \oplus \gamma_1))$, which is bent (16, Theorem 10, Page 428) as $g_1(Y_m, \ldots, Y_1) \oplus g_2(Y_m \oplus \beta_m, \ldots, Y_1 \oplus \beta_1)$ and $h_1(Z_k, \ldots, Z_1) \oplus h_2(Z_k \oplus \gamma_k, \ldots, Z_1 \oplus \gamma_1)$ are both bent. ■

Lemma 10 *For even $n \geq 4$, it is possible to find bent functions $f_1, f_2 \in \Omega_n$ where $f_1(X_n, \ldots, X_1) \oplus f_2(X_n \oplus \alpha_n, \ldots, X_1 \oplus \alpha_1)$ is bent for any $(\alpha_n, \ldots, \alpha_1) \in \{0,1\}^n$.*

PROOF. We have checked by running computer program that there exists $g_1, g_2 \in \Omega_4$ such that $g_1(X_4, \ldots, X_1) \oplus g_2(X_4 \oplus \alpha_4, \ldots, X_1 \oplus \alpha_1)$ is bent for any $(\alpha_4, \ldots, \alpha_1) \in \{0,1\}^4$.

First we consider n of the form 0 mod 4. Thus, taking $f_1 = g_1, f_2 = g_2$ we prove the base case for $n = 4$. Let there exists such $f_1, f_2 \in \Omega_{4a}$, $a > 1$ integer. Now, we will prove such pair of functions will be available for $n = 4a + 4$. From induction hypothesis, we have such $h_1, h_2 \in \Omega_{4a}$. Hence, if we take, $f_1 = g_1 \oplus h_1$ and $f_2 = g_2 \oplus h_2$, where $f_1, f_2 \in \Omega_n$, then from Lemma 9, $f_1(X_n, \ldots, X_1) \oplus f_2(X_n \oplus \alpha_n, \ldots, X_1 \oplus \alpha_1)$ is bent for any $(\alpha_n, \ldots, \alpha_1) \in \{0,1\}^n$.

Next we consider n of the form 2 mod 4. For the base case, we run computer program to find bent functions $h_1, h_2 \in \Omega_6$, such that $h_1(X_6, \ldots, X_1) \oplus h_2(X_6 \oplus \alpha_6, \ldots, X_1 \oplus \alpha_1)$ is bent for any $(\alpha_6, \ldots, \alpha_1) \in \{0,1\}^6$. We take $f_1 = h_1, f_2 = h_2$ as base case. Let there exists such $f_1, f_2 \in \Omega_{4a+2}$, $a > 1$ integer. Now, we will prove such pair of functions will be available for $n = 4a + 6$. From induction hypothesis, we have such $h_1, h_2 \in \Omega_{4a+2}$. Hence, if we take, $f_1 = g_1 \oplus h_1$ and $f_2 = g_2 \oplus h_2$, where $f_1, f_2 \in \Omega_n$, then from Lemma 9, $f_1(X_n, \ldots, X_1) \oplus f_2(X_n \oplus \alpha_n, \ldots, X_1 \oplus \alpha_1)$ is bent for any $(\alpha_n, \ldots, \alpha_1) \in \{0,1\}^n$. ■

Theorem 11 *Consider the balanced function $F \in \Omega_n$, $n > 3$ odd, as in Construction 0. Then $\Delta_F = 2^{\frac{n+1}{2}}$ and $nl(F) = 2^{n-1} - 2^{\frac{n-1}{2}}$. For $n = 3$, $\Delta_F = 8$, $nl(F) = 2$.*

PROOF. The proof for Δ_F follows from Lemma 8, Lemma 9 and Lemma 10. According to Construction 0, F is a concatenation of two bent functions. Hence, $nl(F) = 2^{n-1} - 2^{\frac{n-1}{2}}$. ■

Thus, we provide functions F on odd number of variables which are of similar quality as in (37) in terms of $nl(F)$ and Δ_F. However, our construction is much simpler. Now it is important to refer to the paper (1). Following (1, Theorem 4), the concatenation of any two bent functions of $(n-1)$ variables provides a function F of n variables with nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$. Since the sum-of-square indicator (see Definition 6) of the obtained function F equals 2^{2n+1} (see (1, Theorem 1)), the absolute indicator of F equals $2^{\frac{n+1}{2}}$ iff the magnitudes of all autocorrelation coefficients with respect to $\overline{\alpha} = (\alpha_n, \ldots, \alpha_1)$ with $\alpha_n = 1$ are equal to $2^{\frac{n+1}{2}}$ (because all autocorrelation coefficients with respect to $\alpha_n = 0$ are equal to 0). We could provide construction of such functions here.

3.1 Construction for odd $n = 15$

In (37), construction of balanced function f on odd number of variables with $\Delta_f = 2^{\frac{n+1}{2}}$ and nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$ has been proposed. It has also been conjectured in (37) that for balanced Boolean functions on odd number of variables, this is the minimum possible value of Δ_f.

Here we consider the functions provided in (27) and provide simple mathematical argument towards disproving the conjecture. The conjecture was first disproved in (19), which we extend here. In fact we prove that, it is possible to construct 15 variable balanced functions f with nonlinearity less that, equal to and greater than $2^{14} - 2^7$ (the bent concatenation nonlinearity) with $\Delta_f < 2^{\frac{15+1}{2}} = 256$. Thus, the conjecture is disproved for three different ranges of nonlinearity.

Consider a Boolean function of n-variables as its truth table which is a binary string of length 2^n. It is then easy to see the following result.

Proposition 12 *Let $f \in \Omega_n$. If x bits of the output column of f is complemented to get g, then (1) $nl(g) \geq nl(f) - x$ and (2) $\Delta_g \leq \Delta_f + 4x$.*

Proposition 13 *It is possible to construct $f \in \Omega_{15}$ with $nl(f) = 16276$, $wt(f) = 16364$ and $\Delta_f = 160$.*

PROOF. Consider a function $f_1 \in \Omega_{15}$ with $nl(f_1) = 16276$, $wt(f_1) = 16492$ and $\Delta_{f_1} = 160$ (we found such a function by running the same experiment as done by Patterson and Wiedemann (23)). From (23), we know that there are 3255 linear functions in $L(15)$ at a distance 16364 from f_1. Let l be one of these 3255 linear functions. Define $f = f_1 \oplus l$. Then $f \in \Omega_{15}$, $nl(f) = nl(f_1) = 16276$ and $wt(f) = wt(f_1 \oplus l) = d(f_1, l) = 16364$ (see also (27)). Also it is clear that $\Delta_f = \Delta_{f_1}$ and hence the result. ■

Lemma 14 *It is possible to construct a balanced function $g \in \Omega_{15}$ such that $nl(g) = 16256 = 2^{14} - 2^7$ and $\Delta_g \leq 240 < 256 = 2^{\frac{15+1}{2}}$.*

PROOF. Take the function f as in Proposition 13. Since $nl(f) = 16276$, there is one affine function $\lambda \in A(15)$ such that $d(f, \lambda) = 16276$. Now consider the truth table of f, λ, which are binary strings of length 2^{15}. For a string S, denote $S[i]$ as the ith location of the string S, where $0 \leq i \leq 2^{15}-1$. Now let us identify 20 locations $i_1, \ldots, i_{20}$ such that $\lambda[i_k] = 1$ and $f[i_k] = 0$. We construct g from f such that $g[j] = f[j]$ for the $2^{15} - 20$ positions, where $j \neq i_k$ for $1 \leq k \leq 20$. For $j = i_k$, $1 \leq k \leq 20$ we take $g[j] = 1$. Thus, $wt(g) = 16364 + 20 = 16384 = 2^{14}$ and from item 1 of Proposition 12, $nl(g) \geq 16276 - 20$. Since, $d(g, \lambda) = 16276 - 20 = 16256 = 2^{14} - 2^7$, we have $nl(g) = 16256$. Now from Proposition 12, item 2 we get, $\Delta_g \leq \Delta_f + 4 \times 20 = 240$. ■

Lemma 15 *It is possible to construct a balanced function $h \in \Omega_{15}$ such that $nl(h) = 16254 = 2^{14} - 2^7 - 2 < 2^{14} - 2^7$ and $\Delta_h \leq 248 < 256 = 2^{\frac{15+1}{2}}$.*

PROOF. Take the function g as in Lemma 14. We have $nl(g) = 16256$, and there is one linear function $\lambda \in L(15)$ (the same one as in the proof of Lemma 14) such that $d(g, \lambda) = 16256$. Now consider the truth table of g, λ, which are binary strings of length 2^{15}. Now let us identify 2 locations i_1, i_2 such that $\lambda[i_1] = 1, g[i_1] = 0, \lambda[i_2] = 0, g[i_2] = 1$. We construct h from g such that $h[j] = g[j]$ for the $2^{15} - 2$ positions, where $j \neq i_k$ for $1 \leq k \leq 2$. For $j = i_k$, $1 \leq k \leq 2$ we take $h[j] = 1 - g[j]$. Note that $wt(h) = wt(g) + 1 - 1 = wt(g)$. Also, $d(h, \lambda) = 16256 - 2 = 16254 < 2^{14} - 2^7$. Hence, $nl(h) = 16254$. Now from Proposition 12, item 2 we get, $\Delta_h \leq \Delta_g + 4 \times 2 = 248$. ■

The following case provides a construction for $n = 15$ variable functions h with nonlinearity strictly greater than bent concatenation nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$ and $\Delta_g < 2^{\frac{n+1}{2}}$. In (19), a balanced functions f on 15 variables constructed in (27) with nonlinearity $2^{14} - 2^7 + 6$ has been examined by running computer program and it has been found that Δ_f for such a function is $216 < 256 = 2^{\frac{15+1}{2}}$. Thus the conjecture of (37) for this specific range of nonlinearity (greater than bent concatenation nonlinearity) has been disproved in (19) by experiment. The function f, as described in (27), is a modification of Patterson-

Wiedemann function (23). We provide the mathematical justification here.

Lemma 16 *It is possible to construct a balanced function $H \in \Omega_{15}$ such that $nl(H) = 16262 = 2^{14} - 2^7 + 6 > 2^{14} - 2^7$ and $\Delta_H \leq 240 < 256 = 2^{\frac{15+1}{2}}$.*

PROOF. From Proposition 13, we can construct $f \in \Omega_{15}$ with $nl(f) = 16276, wt(f) = 16364$ and $\Delta_f = 160$. As described in (27), select 20 bits in the truth table of f uniformly at random which contain the value 0 and complement them to 1. In process we get a function H. Note that $wt(H) = 16364 + 20 = 16384 = 2^{14}$ and from item 1 of Proposition 12, $nl(H) \geq 16276 - 20$. The random experiment shows that it is possible to get H with $nl(H) = 16262$ (see also (27)). Now from Proposition 12, item 2 we get, $\Delta_H \leq \Delta_f + 4 \times 20 = 240$. Further, the random experiment shows that it is possible to find $\Delta_H = 216$ at minimum (see also (19)). ■

Note that we are interested in three different ranges of nonlinearity. The functions constructed by Patterson and Wiedemann (23; 24) are important since the construction provides better nonlinearity than bent concatenation nonlinearity. Also the balanced functions (27) constructed from the Patterson-Wiedemann functions provide the nonlinearity greater than the bent concatenation one. The Δ_f values of these functions is less than 256. We like to point out that we can modify the Patterson-Wiedemann functions in such a manner such that the nonlinearity falls below (also equal to) the bent concatenation nonlinearity, and even then the Δ_f value is less than 256. However, there are other construction methods for balanced functions with nonlinearity equal to and less than the bent concatenation nonlinearity (27; 20), which can not provide the Δ_f value less than $2^{\frac{n+1}{2}}$ for any odd n.

Now consider the other side. Let us use the function H, with $\Delta_H = 216$ as in the proof of Lemma 16, to construct a balanced function $H_{2i+15} = b(Y_{2i}, \ldots, Y_1) \oplus H(X_{15}, \ldots, X_1)$, where b is a bent function. Note that H_{2i+15} has nonlinearity greater than the bent concatenation nonlinearity, but $\Delta_{H_{2i+15}} = 2^{2i} \cdot \Delta_H = 2^{2i} \cdot 216 > 2^{\frac{2i+15}{2}}$. That is, even if the nonlinearity is greater than the bent concatenation nonlinearity, we are not getting good autocorrelation value. It is an interesting open problem in this area to disprove the conjecture of (37) for odd $n \neq 15$.

4 Construction for even n

In this section we modify the Maiorana-McFarland type bent functions to get balanced Boolean functions with very small value of Δ_f. Similar kinds of constructions have earlier been considered in (11; 29; 27). This construction

provides high nonlinearity and high algebraic degree which are cryptographically important. However, there the Δ_f parameter has not been considered before, which is the main thrust in this section. Let us first describe the construction.

Construction 1 *Let G be a bent function on n variables, which is the concatenation of $q = 2^{\frac{n}{2}}$ distinct linear functions on $k = \frac{n}{2}$ variables. Thus we can write, $G = l_0 l_1 \ldots l_{q-1}$, where $l_i \in L(\frac{n}{2})$ and $l_i \neq l_j$ for $i \neq j$. Basically, $l_i = a_k X_k \oplus \ldots \oplus a_1 X_1$, where $(a_k, \ldots, a_1)$ is k bit binary representation of i. Here, l_0 means the constant zero function. Let $F = f l_1 \ldots l_{q-1}$, where $f \in \Omega_{\frac{n}{2}}$ is a balanced function. That is in G we replace l_0 by f to get F.*

Theorem 17 (29; 11; 27) *For even n, let $F \in \Omega_n$ as described in Construction 1. Then we have the following. (1) F is balanced. (2) $nl(F) = 2^{n-1} - 2^{\frac{n}{2}} + nl(f)$. (3) $deg(F) = \frac{n}{2} + deg(f)$.*

Now we will prove some results to get an upper bound on Δ_F. First let us consider $\overline{\alpha} \in \{0,1\}^n$, where $\overline{\alpha} = (\alpha_n, \ldots, \alpha_{\frac{n}{2}+1}, \alpha_{\frac{n}{2}}, \ldots, \alpha_1)$ and we write $\overline{\beta} = (\alpha_n, \ldots, \alpha_{\frac{n}{2}+1})$ and $\overline{\gamma} = (\alpha_{\frac{n}{2}}, \ldots, \alpha_1)$. That is $\overline{\alpha} = (\overline{\beta}, \overline{\gamma})$. Note that $\overline{\alpha} \neq (0, 0, \ldots, 0)$, i.e. $\overline{\alpha}$ is not an all zero vector. Moreover, we denote $\overline{X} = (X, \ldots, X_{\frac{n}{2}+1}, X_{\frac{n}{2}}, \ldots, X_1)$, $\overline{U} = (X_n, \ldots, X_{\frac{n}{2}+1})$ and $\overline{V} = (X_{\frac{n}{2}}, \ldots, X_1)$. That is $\overline{X} = (\overline{U}, \overline{V})$.

Lemma 18 *Consider $F \in \Omega_n$ as in Construction 1. Let us consider $\overline{\alpha} = (\alpha_n = 0, \ldots, \alpha_{\frac{n}{2}+1} = 0, \alpha_{\frac{n}{2}}, \ldots, \alpha_1)$ and $\overline{\gamma} = (\alpha_{\frac{n}{2}}, \ldots, \alpha_1)$. Then $\mid \Delta_F(\overline{\alpha}) \mid \leq 2^{\frac{n}{2}} + \mid \Delta_f(\overline{\gamma}) \mid$.*

PROOF. For the bent function $G \in \Omega_n$, $\Delta_G(\overline{\alpha}) = 0$ for all nonzero $\overline{\alpha}$. That means, $wd(G(\overline{X}), G(\overline{X} \oplus \overline{\alpha})) = 0$. This gives that

$wd(l_0, l_0(\overline{V} \oplus \overline{\gamma})) + wd(l_1, l_1(\overline{V} \oplus \overline{\gamma})) + \ldots + wd(l_{q-2}, l_{q-2}(\overline{V} \oplus \overline{\gamma})) + wd(l_{q-1}, l_{q-1}(\overline{V} \oplus \overline{\gamma})) = 0$.

We have, $wd(l_i, l_i(\overline{V} \oplus \overline{\gamma}))$ can take the values $\pm q = \pm 2^{\frac{n}{2}}$. In particular, $wd(l_0, l_0(\overline{V} \oplus \overline{\gamma}))$ takes the value $q = 2^{\frac{n}{2}}$. Thus,

$wd(l_1, l_1(\overline{V} \oplus \overline{\gamma})) + \ldots + wd(l_{q-2}, l_{q-2}(\overline{V} \oplus \overline{\gamma})) + wd(l_{q-1}, l_{q-1}(\overline{V} \oplus \overline{\gamma})) = -q$.
Hence,

$wd(F(\overline{X}), F(\overline{X} \oplus \overline{\alpha})) = wd(f, f(\overline{V} \oplus \overline{\gamma})) + wd(l_1, l_1(\overline{V} \oplus \overline{\gamma})) + \ldots + wd(l_{q-2}, l_{q-2}(\overline{V} \oplus \overline{\gamma})) + wd(l_{q-1}, l_{q-1}(\overline{V} \oplus \overline{\gamma})) = \Delta_f(\overline{\gamma}) - q = -2^{\frac{n}{2}} + \Delta_f(\overline{\gamma})$.

Thus $\mid \Delta_F(\overline{\alpha}) \mid \leq 2^{\frac{n}{2}} + \mid \Delta_f(\overline{\gamma}) \mid$. ■

Lemma 19 *Consider $F \in \Omega_n$ as in Construction 1.*

Let us consider $\overline{\alpha} = (\alpha_n, \ldots, \alpha_{\frac{n}{2}+1}, \alpha_{\frac{n}{2}}, \ldots, \alpha_1)$ *where* $\overline{U} = (\alpha_n, \ldots, \alpha_{\frac{n}{2}+1})$ *is a nonzero vector and* $\overline{V} = (\alpha_{\frac{n}{2}}, \ldots, \alpha_1)$. *Then* $\mid \Delta_F(\overline{\alpha}) \mid \leq 2 \mid W_f(\overline{U}) \mid$.

PROOF. From Construction 1, it is clear that the function F can be seen as concatenation of q functions. Since $(\alpha_n, \ldots, \alpha_{\frac{n}{2}+1})$ is a nonzero vector, if we write the truth tables of $F(\overline{X})$ and $F(\overline{X} \oplus \overline{\alpha})$, then for the small functions of $\frac{n}{2}$ variables, the truth tables of $f(\overline{V})$ and $f(\overline{V} \oplus \overline{\gamma})$ or any of the $l_i(\overline{V})$ and $l_i(\overline{V} \oplus \overline{\gamma})$ cannot occur at the corresponding positions in the truth tables of $F(\overline{X})$ and $F(\overline{X} \oplus \overline{\alpha})$.

The functions f and l_r will correspond in the truth tables, where r has a binary representation $(\alpha_n, \ldots, \alpha_{\frac{n}{2}+1})$. Hence, from Definition 4, $wd(f, l_r) = W_f(\overline{U})$, the Walsh transform value. Also let $i = i_n, \ldots, i_{k+1}$ and $j = j_n, \ldots, j_{k+1}$ in binary representation. If $(i_n, \ldots, i_{k+1})$ and $(j_n, \ldots, j_{k+1})$ are related by $i_n = \alpha_n \oplus j_n, \ldots, i_k = \alpha_k \oplus j_k$, then the smaller truth tables of l_i, l_j will come at the corresponding positions in the truth tables of $F(\overline{X})$ and $F(\overline{X} \oplus \overline{\alpha})$.

Thus, $wd(F(\overline{X}), F(\overline{X} \oplus \overline{\alpha})) = 2wd(f(\overline{V}), l_r(\overline{V} \oplus \overline{\gamma})) + 2 \sum_{i=r \oplus j} wd(l_i(\overline{V}), l_j(\overline{V} \oplus \overline{\gamma})) = 2wd(f(\overline{V}), l_r(\overline{V} \oplus \overline{\gamma}))$. This is because, $l_i(\overline{V}), l_j(\overline{V} \oplus \overline{\gamma})$ are two distinct affine functions and hence by Proposition 3, $wd(l_i(\overline{V}), l_j(\overline{V} \oplus \overline{\gamma})) = 0$. ■

In the next lemma we need the parameter τ_f (see Definition 2).

Lemma 20 *Let us consider the function* $F \in \Omega_n$ *as in Construction 1. Then* $\Delta_F = \max(2^{\frac{n}{2}} + \Delta_f, 2\tau_f)$.

PROOF. From Lemma 18, we get that the maximum value of $\mid \Delta_f(\overline{\gamma}) \mid$ is Δ_f and from Lemma 19, we have that maximum value of $\mid W_f(\overline{U}) \mid$ is τ_f. ■

Now we provide an updated version of Construction 1.

Construction 2 *We construct a balanced function* F *as in Construction 1, with a restriction on the balanced function* f. *We construct* f *such that,* $nl(f) \geq 2^{\frac{n}{2}-2}$.

Theorem 21 *Let us consider* F *as in Construction 2. Then,* $\Delta_F \leq 2^{\frac{n}{2}} + \Delta_f$.

PROOF. Here, $2\tau_f = 2 \times 2^{\frac{n}{2}} - 4nl(f) \leq 2^{\frac{n}{2}}$. Thus, $2^{\frac{n}{2}} + \Delta_f \geq 2\tau_f$. ■

In the above theorem, we provide an upper bound on Δ_F. However, for all the functions those have been checked, we get the strict equality $\Delta_F = 2^{\frac{n}{2}} + \Delta_f$. Let us denote $\Delta^b(n) = \min_{h \in \Omega_n, h \ balanced} \Delta_h$. Theorem 21 provides the bound $\Delta^b(n) \leq 2^{\frac{n}{2}} + \Delta^b(\frac{n}{2})$. However, we could not devise any method such that

the strict inequality $\Delta^b(n) < 2^{\frac{n}{2}} + \Delta^b(\frac{n}{2})$ occurs. Thus we make the following conjecture.

Conjecture 1 *Let n be an even integer. Then $\Delta^b(n) = 2^{\frac{n}{2}} + \Delta^b(\frac{n}{2})$.*

This conjecture is similar to Dobbertin's conjecture (11) on nonlinearity of balanced Boolean functions on even number of variables. Let $nlb(n)$ is the maximum nonlinearity for balanced functions on n variables. Then the conjecture states that, for even n, $nlb(n) = 2^{n-1} - 2^{\frac{n}{2}} + nlb(\frac{n}{2})$. Presently this conjecture is still open. Thus the balanced functions we have described here possess currently best known nonlinearity and autocorrelation values together.

Our result provides a recursive construction. Now we have to consider different cases to provide some compact nonrecursive formulae. First we consider the case where, $n = 2^i \times j$, for $i \geq 1$ and $j \geq 3$, odd. We can extend the Construction 2 in the following way. Let $F \in \Omega_n$. Now, $\Delta_F = 2^{\frac{n}{2}} + \Delta_f$. Here $f \in \Omega_{\frac{n}{2}}$, i.e., $f \in \Omega_{2^{i-1} \times j}$. Then we can use Construction 2 once again since $\frac{n}{2}$ is still even if $i > 1$. If $i = 1$, then we use a balanced function on odd number of variables as described in previous section. Hence we get the following result.

Theorem 22 *It is possible to construct $F \in \Omega_n$, where $n = 2^i \times j$ with $\Delta_F = \sum_{x=1}^{i} 2^{\frac{n}{2^x}} + \sigma$ where $\sigma = 2^{\frac{n}{2^{i+1}} + \frac{1}{2}}$ if $j \geq 5$ and $\sigma = 8$ for $j = 3$. Also, $nl(F) = 2^{n-1} - \sum_{x=1}^{i} 2^{\frac{n}{2^x} - 1} - 2^{\frac{n}{2^{i+1}} - \frac{1}{2}}$.*

PROOF. $\Delta_F = 2^{\frac{n}{2}} + \Delta_f = 2^{\frac{n}{2}} + 2^{\frac{n}{4}} + \Delta_g = 2^{\frac{n}{2}} + 2^{\frac{n}{4}} + \ldots + 2^{\frac{n}{2^i}} + \Delta_h$. Now $\frac{n}{2^i} = j = 2y + 1$ and by construction of Theorem 11 for Boolean functions on odd number of variables, $\Delta_h = 2^{y+1} = 2^{\frac{n}{2^{i+1}} + \frac{1}{2}}$ for $j \geq 5$. Also $\Delta_h = 8$ for $j = 3$. The nonlinearity result follows from recursive use of Theorem 17, item 2 and the result that it is possible to construct a balanced function on j variables with nonlinearity $2^{j-1} - 2^{\frac{j-1}{2}}$. ■

We also like to point out that the results for a 30 variable function is already an interesting one. Note that we have got a balanced function $f \in \Omega_{15}$ with $nl(f) = 16262 > 2^{15-1} - 2^{\frac{15-1}{2}}$ and $\Delta_f = 216 < 2^{\frac{n+1}{2}}$ (see proof of Lemma 16). Thus we get a balanced function $F \in \Omega_{30}$ with $nl(F) = 2^{29} - 2^{15} + 16262$ and $\Delta_F = 2^{15} + 216$. This is clearly a better result than what we have presented in Theorem 22. In Theorem 22 we consider $\Delta_h = 2^{y+1}$ and $nl(h) = 2^{j-1} - 2^{\frac{j-1}{2}}$. Here, for a 15-variable function h, $\Delta_h < 2^{y+1}$ and $nl(h) > 2^{j-1} - 2^{\frac{j-1}{2}}$.

Next we consider the case $n = 2^i$. Here we use the recursive construction and come down to a 4 variable function ultimately.

Theorem 23 *It is possible to construct $F \in \Omega_n$, where $n = 2^i$ with $\Delta_F = \sum_{x=1}^{i-2} 2^{\frac{n}{2^x}} + 8$. Also, $nl(F) = 2^{n-1} - \sum_{x=1}^{i-2} 2^{\frac{n}{2^x} - 1} - 4$.*

PROOF. We use the construction recursively until we get a 4 variable Boolean function. For balanced 4 variable function h, by computer search it has been checked that the minimum value of Δ_h is 8. The nonlinearity result follows from recursive use of Theorem 17, item 2. ■

It should be noted that in (37), construction of balanced Boolean functions f on even number of variables have been proposed with $\Delta_f = 2^{\frac{n}{2}+1}$ and $nl(f) = 2^{n-1} - 2^{\frac{n}{2}}$. Our results are clearly superior. It will be an interesting research direction either to prove that this is the best possible parameters or to construct a balanced function with better results than this.

5 Correlation Immune and Resilient Boolean Functions

Correlation immunity is a very significant cryptographic property of Boolean functions and it has received a lot of attention in literature (see (31; 32; 13; 3; 30; 4; 12; 28) and the references in these papers). On the other hand, two fundamental properties for cryptographically significant Boolean functions are nonlinearity and autocorrelation. Nonlinearity is one of the most challenging combinatorial properties of Boolean functions and is related to the covering radius of first order Reed-Muller code (see (26; 23; 24; 11; 14; 15; 5; 27) and the references in these papers). Very recently weight divisibility results of correlation immune and resilient (balanced correlation immune) Boolean functions have been proved (28; 35; 39; 1) and these results have direct consequences towards nontrivial upper bounds on nonlinearity of these subclasses of Boolean functions. Also these results show that if we increase the order of correlation immunity then the nonlinearity decreases. Currently it has been noted in (41) that propagation property also goes against correlation property, and some lower bounds on Δ_f values of m-th order correlation immune and resilient functions have been presented (40).

Here we provide better results which directly relate the autocorrelation measures with order of correlation immunity. For a linear function f, $\Delta_f = 2^n$, and $\sigma_f = 2^{3n}$. For functions f, on even number of variables, we have $\Delta_f = 0$ ($\sigma_f = 2^{2n}$) iff f is a bent function (21; 37). However, bent functions are not balanced. In fact, for a function f of even weight $\Delta_f \equiv 0 \bmod 8$ and for a function f of odd weight $\Delta_f \equiv 4 \bmod 8$ (9). For balanced function f, $\sigma_f \geq 2^{2n} + 2^{n+3}$ (33) for both odd and even number of variables. A comparatively sharper result in this direction has been proposed in (34) which we will discuss shortly.

Note that the properties Δ_f, σ_f are invariant under nonsingular linear transformation on input variables of the function f. Thus, it is easy to see that the σ_f results of the papers (33; 34) are valid for any Boolean function f whose

Walsh spectrum contains at least one zero.

5.1 Lower Bound on sum-of-square Indicator

We start this section with a result from (38, Theorem 3).

Theorem 24 *Let $f \in \Omega_n$. Then $\sigma_f \geq \frac{2^{3n}}{\mathbf{F}_f}$.*

Next we have the following result, which follows directly from Definition 7.

Proposition 25 *Let $f \in \Omega_n$ be an m-th order correlation immune function. Then $\mathbf{F}_f \leq 2^n - \sum_{i=1}^{m} \binom{n}{i}$. Moreover, if f is m-resilient, then $\mathbf{F}_f \leq 2^n - \sum_{i=0}^{m} \binom{n}{i}$.*

The sum-of-square indicator of GAC has been introduced in (37) (see also Definition 6). We start with the following result which uses Theorem 24 and Proposition 25.

Lemma 26 *Let $f \in \Omega_n$ be an m-th order correlation immune function. Then, $\sigma_f \geq \frac{2^{3n}}{2^n - \sum_{i=1}^{m} \binom{n}{i}}$. Moreover, if f is m-resilient, then $\sigma_f \geq \frac{2^{3n}}{2^n - \sum_{i=0}^{m} \binom{n}{i}}$.*

To identify important consequences of this result we need to get an approximate result which will provide a σ_f value of the form $2^{2n} + 2^{n+q}$, where q is a function of n, m. This we provide in the following result.

Theorem 27 *Let $f \in \Omega_n$ be an m-th order correlation immune function. Then, $\sigma_f > 2^{2n} + 2^{n+\log_2 \sum_{i=1}^{m} \binom{n}{i}}$. Similarly, if f is m-resilient, then $\sigma_f > 2^{2n} + 2^{n+\log_2 \sum_{i=0}^{m} \binom{n}{i}}$.*

PROOF. Note that $\frac{2^{3n}}{2^n - \sum_{i=1}^{m} \binom{n}{i}} > 2^{2n} + 2^n \sum_{i=1}^{m} \binom{n}{i}$. Thus the result follows for correlation immune functions. The result is similar for resilient functions also. ■

Note that, in our analysis, there is no significant difference in the result of correlation immune and resilient functions in terms of numerical values.

Currently there is no result on lower bound of σ_f values for correlation immune and resilient functions. The only known results are for balanced functions which are given in (33; 34). The lower bound for balanced functions given in (33) is $2^{2n} + 2^{n+3}$. The result in (34) is as follows. For a balanced function f,

$$\sigma_f \geq \quad 2^{2n} + 2^6(2^n - t - 1), \text{ if } 0 \leq t \leq 2^n - 2^{n-3} - 1, t \text{ odd}, \quad \text{(i)}$$
$$2^{2n} + 2^6(2^n - t + 2), \text{ if } 0 \leq t \leq 2^n - 2^{n-3} - 1, t \text{ even}, \quad \text{(ii)}$$
$$(1 + \tfrac{1}{2^n - 1 - t})2^{2n}, \text{ if } 2^n - 2^{n-3} - 1 < t \leq 2^n - 2, \quad \text{(iii)}$$

if f satisfies propagation characteristics with respect to t vectors. Note that for case (i) and (ii), even if we overestimate this lower bound, it is $2^{2n} + 2^{n+6}$. For the case (iii) the lower bound varies from $2^{2n} + 2^{n+3}$ to 2^{2n+1} and also this depends on the propagation characteristics of the function.

Now we enumerate the consequences of our result.

- In our result the lower bound depends directly on the order m of correlation immunity and this is the first nontrivial result in this direction.
- Note that for $m > \frac{n}{2}$, $\log_2 \sum_{i=1}^{m} \binom{n}{i} > n - 1$. Thus for all m-th order correlation immune functions with $m > \frac{n}{2}$, $\sigma_f > 2^{2n} + 2^{2n-1}$. The result is true for m-resilient functions also. This provides a strong lower bound on sum-of-square indicator for m-th order correlation immune and m-resilient functions.
- Given any value r $(1 \leq r < n)$, it is possible to find an m-th order correlation immune or m-resilient function f such that $\sigma_f > 2^{2n} + 2^{n+r}$ by properly choosing m.

5.2 Lower Bound on Absolute Indicator

Now we concentrate on the absolute indicator of GAC. We have the result on sum-of-square indicator for correlation immune and resilient functions. We use the result in this direction.

Lemma 28 *For an n-variable m-th order correlation immune function f, $\Delta_f \geq \sqrt{\frac{1}{2^n-1} \frac{2^{2n} \sum_{i=1}^{m} \binom{n}{i}}{2^n - \sum_{i=1}^{m} \binom{n}{i}}}$. Similarly, $\Delta_f \geq \sqrt{\frac{1}{2^n-1} \frac{2^{2n} \sum_{i=0}^{m} \binom{n}{i}}{2^n - \sum_{i=0}^{m} \binom{n}{i}}}$ for an n-variable m-resilient function f.*

PROOF. We know, $\sigma_f = \sum_{\overline{\alpha} \in \{0,1\}^n} \Delta_f^2(\overline{\alpha})$. Thus, the absolute value of each $\Delta_f(\overline{\alpha})$ will be minimum only when they all possess equal values. Hence, the minimum value of Δ_f will be $\sqrt{\frac{\sigma_f - 2^{2n}}{2^n - 1}}$. This gives the result using the value of σ_f from Lemma 26. ■

Thus, using simplification we get the following result.

Theorem 29 *For an n-variable m-th order correlation immune function f, $\Delta_f > 2^{\frac{n}{2}} \sqrt{\frac{\sum_{i=1}^{m} \binom{n}{i}}{2^n - \sum_{i=1}^{m} \binom{n}{i}}}$. Similarly, $\Delta_f > 2^{\frac{n}{2}} \sqrt{\frac{\sum_{i=0}^{m} \binom{n}{i}}{2^n - \sum_{i=0}^{m} \binom{n}{i}}}$ for an n-variable m-resilient function f.*

PROOF. The result follows from overestimating $2^n - 1$ by 2^n. ■

It is known that, for a function f of even weight, $\Delta_f \equiv 0 \bmod 8$ (9). Since the correlation immune functions and resilient functions are all of even weight, the Δ_f values will be the value greater than the values given in Theorem 29, which are divisible by 8. The only published result on the lower bound on Δ_f for a balanced function f is $\Delta_f \geq 8$ (33). Our result has the following consequences.

- The value Δ_f is a function of n, m.
- For $m > \frac{n}{2}$, $\Delta_f > 2^{\frac{n}{2}}$.
- For small values of m, $\Delta_f > \sqrt{\sum_{i=1}^{m} \binom{n}{i}} > \sqrt{\binom{n}{m}}$.
- For $m = 1$, $\Delta_f > \sqrt{n}$.

5.3 Lower Bounds using Weight Divisibility Results

Here we use the weight divisibility results of correlation immune and resilient Boolean functions (28). It is known that the values in the Walsh spectrum of an m-th order correlation immune function is divisible by 2^{m+1}. Similarly for m-resilient functions, the Walsh spectrum values are divisible by 2^{m+2}.

Let us now find out the sum of square indicators of such functions. We once again refer to Theorem 24. For $f \in \Omega_n$, $\sigma_f \geq \frac{2^{3n}}{\mathbf{F}_f}$.

- For an n-variable, m-th order correlation immune function the values in Walsh spectra are $0, \pm i 2^{m+1}, i = 1, 2, \ldots$. From Parseval's relation (10) $\sum_{\overline{\omega} \in \{0,1\}^n} W_f(\overline{\omega}) = 2^{2n}$. Hence, we get that for such a function f, $\mathbf{F}_f \leq 2^{2n-2m-2}$.
- For an n-variable, m-resilient function the values in Walsh spectra are $0, \pm i 2^{m+2}, i = 1, 2, \ldots$. Using Parseval's relation, we get that for such a function f, $\mathbf{F}_f \leq 2^{2n-2m-4}$.

Theorem 30 *For an n-variable, m-th order correlation immune function f, $\sigma_f \geq 2^{n+2m+2}$. Similarly, for an n-variable, m-resilient function f, $\sigma_f \geq 2^{n+2m+4}$.*

PROOF. The result for correlation immune function follows from Theorem 24 and $\mathbf{F}_f \leq 2^{2n-2m-2}$. The result for resilient function follows from Theorem 24 and $\mathbf{F}_f \leq 2^{2n-2m-4}$. ■

Note that the trivial lower bound on the sum of square indicator is 2^{2n}. Hence, for correlation immune functions, this bound is nontrivial, when $n+2m+2 > 2n$, i.e, $m > \frac{n}{2} - 1$. Similarly for resilient functions, this bound is nontrivial for $m > \frac{n}{2} - 2$. Using these results, we immediately get the result on the Δ_f values of these functions.

Theorem 31 *For an n-variable, m-th ($m > \frac{n}{2} - 1$) order correlation immune function f, $\Delta_f > 2^{\frac{2m+1}{2}}$. Similarly, for an n-variable, m-resilient ($m > \frac{n}{2} - 2$) function f, $\Delta_f > 2^{\frac{2m+3}{2}}$.*

PROOF. For the correlation immune function f, we have, $\Delta_f \geq \sqrt{\frac{2^{n+2m+2}-2^{2n}}{2^n-1}}$. Thus, overestimating $2^n - 1$ as 2^n, $\Delta_f > \sqrt{2^{2m+2} - 2^n} \geq \sqrt{2^{2m+1}}$ (since $m > \frac{n}{2} - 1) = 2^{\frac{2m+1}{2}}$. Similarly for the resilient function f, we have, $\Delta_f \geq \sqrt{\frac{2^{n+2m+4}-2^{2n}}{2^n-1}}$. Thus, overestimating $2^n - 1$ as 2^n, $\Delta_f > \sqrt{2^{2m+4} - 2^n} \geq \sqrt{2^{2m+3}} = 2^{\frac{2m+3}{2}}$. ■

Note that the weight divisibility results using algebraic degree of the functions have been presented in (6; 7). These results can be used to provide sharper lower bounds on σ_f, Δ_f involving algebraic degree. From (6; 7), it is clear that for an n-variable, m-th order correlation immune function with algebraic degree d, the values of the Walsh spectra will be divisible by $2^{m+1+\lfloor\frac{n-m-1}{d}\rfloor}$. Similarly for an n-variable, m-resilient function with algebraic degree d, the values of the Walsh spectra will be divisible by $2^{m+2+\lfloor\frac{n-m-2}{d}\rfloor}$. Using these results we can update Theorem 30, Theorem 31 involving algebraic degree as follows.

Theorem 32 *For an n-variable, m-th order ($m > \frac{n}{2} - 1$) correlation immune function f with algebraic degree d, $\sigma_f \geq 2^{n+2m+2+2\lfloor\frac{n-m-1}{d}\rfloor}$, and $\Delta_f > 2^{\frac{2m+1+\lfloor\frac{n-m-1}{d}\rfloor}{2}}$. Similarly, for an n-variable, m-resilient ($m > \frac{n}{2} - 2$) function f with algebraic degree d, $\sigma_f \geq 2^{n+2m+4+2\lfloor\frac{n-m-2}{d}\rfloor}$, and $\Delta_f > 2^{\frac{2m+3+\lfloor\frac{n-m-2}{d}\rfloor}{2}}$.*

In (40), it has been shown that $\Delta_f \geq 2^{m-1}\sum_{i=0}^{+\infty} 2^{i(m-1-n)}$ for an unbalanced n-variable m-th order correlation immune function for the range $2 \leq m \leq n$. Note that, $\Delta_f \geq 2^{m-1}\sum_{i=0}^{+\infty} 2^{i(m-1-n)} = 2^{m-1}\frac{1}{1-2^{m-1-n}}$. Thus even if we overestimate the lower bound, it can be at most 2^m as the maximum value of $2^{m-1-n}i$ is $\frac{1}{2}$. Also $\Delta_f \geq 2^m\sum_{i=0}^{+\infty} 2^{i(m-n)}$ for an n-variable m-resilient function for the range $1 \leq m \leq n-1$. This gives, $\Delta_f \geq 2^m\sum_{i=0}^{+\infty} 2^{i(m-n)} = 2^m\frac{1}{1-2^{m-n}}$. Overestimating this we will get 2^{m+1}.

For higher orders ($m > \frac{n}{2} - 1$ for correlation immunity and $m > \frac{n}{2} - 2$ for resiliency) Theorem 31 provides better result than (40). For lower order of correlation immunity ($m \leq \frac{n}{2} - 1$), we use our result in Theorem 29. Note that our result is better than that of (40) when $(2^n + 2^{2m}) \sum_{i=1}^{m} \binom{n}{i} > 2^{n+2m}$. For the case of resiliency ($m \leq \frac{n}{2} - 2$), our result is better when $(2^n + 2^{2m}) \sum_{i=0}^{m} \binom{n}{i} > 2^{n+2m}$.

Next we concentrate on a very important subset of correlation immune and resilient functions which possess maximum possible nonlinearity. Importantly the resilient functions have direct application in stream cipher systems. Now the clear benchmark in selecting the resilient functions is the functions which possess the best possible trade-off among the parameters nonlinearity, algebraic degree and the order of resiliency. However, we point out that we should consider one more important criteria in the selection process. In fact we find functions with best possible trade-off having same values of nonlinearity, algebraic degree and order of resiliency but having different autocorrelation properties. Thus, it is important to select the one with better Δ_f values. It is also interesting to note that any two functions with this best possible trade-off must possess the same σ_f values, which we prove here.

Now we concentrate on Definition of plateaued functions (38, Definition 9). Apart from the bent and linear functions, the other plateaued functions have the property that they have three valued Walsh spectra $0, \pm 2^x$. We call that these functions possess three valued Walsh spectra with the values $0, \pm 2^x$. Next we have the following result from (38, Theorem 3).

Theorem 33 *Let $f \in \Omega_n$ and f has a three valued Walsh spectra $0, \pm 2^x$. Then $\sigma_f = \frac{2^{3n}}{\mathbf{F}_f}$.*

Now we concentrate on two special subsets of correlation immune and resilient Boolean functions respectively. We present the following known (28) results.

- For an n-variable, m-th order correlation immune function with $m > \frac{n}{2} - 1$, the maximum possible nonlinearity that can be achieved is $2^{n-1} - 2^m$ and these functions possess three valued Walsh spectra $0, \pm 2^{m+1}$. Thus from Parseval's relation (10) $\sum_{\overline{\omega} \in \{0,1\}^n} W_f(\overline{\omega}) = 2^{2n}$. Hence, we get that for such a function f, $\mathbf{F}_f = 2^{2n-2m-2}$.
- For an n-variable, m-resilient function with $m > \frac{n}{2} - 2$, the maximum possible nonlinearity that can be achieved is $2^{n-1} - 2^{m+1}$ and these functions possess three valued Walsh spectra $0, \pm 2^{m+2}$. Using Parseval's relation, we get that for such a function f, $\mathbf{F}_f = 2^{2n-2m-4}$.

Hence we get the following result.

Theorem 34 *For an n-variable, m-th ($m > \frac{n}{2} - 1$) order correlation immune*

function f with maximum possible nonlinearity, $\sigma_f = 2^{n+2m+2}$. Similarly, for an n-variable, m-resilient $(m > \frac{n}{2} - 2)$ function f with maximum possible nonlinearity, $\sigma_f = 2^{n+2m+4}$.

PROOF. The result for correlation immune function follows from Theorem 33 and $\mathbf{F}_f = 2^{2n-2m-2}$. The result for resilient function follows from Theorem 33 and $\mathbf{F}_f = 2^{2n-2m-4}$. ■

Current results (35; 6; 7) clearly identify that the nonlinearity and algebraic degree of the correlation immune and resilient functions are optimized simultaneously. Here we show that at this situation, the sum of square indicator attains its minimum value too.

5.4 Construction Results

Resilient Boolean functions, which are provably optimized in terms of order of resiliency, algebraic degree and nonlinearity (28), have immediate applications in stream cipher systems. Unfortunately, the general construction techniques does not provide good autocorrelation properties. First we will talk about some specific resilient functions and their Δ_f values. Then we will analyze some of the well known constructions and calculate the autocorrelation values.

Let us consider the $(5, 1, 3, 12)$ functions. We initially consider such a function f constructed using linear concatenation (27), which is $(1 \oplus X_5)(1 \oplus X_4)(X_1 \oplus X_2) \oplus (1 \oplus X_5)X_4(X_1 \oplus X_3) \oplus X_5(1 \oplus X_4)(X_2 \oplus X_3) \oplus X_5X_4(X_1 \oplus X_2 \oplus X_3)$. This function has $\Delta_f = 16$. However, by studying the equivalence classes in (2) and then using linear transformation, it is possible to get a $(5, 1, 3, 12)$ function g, such that $\Delta_g = 8$. The truth table of the function is 00001011110110011110010100111000. *This function achieves the best possible trade-off among order of resiliency, nonlinearity, algebraic degree and autocorrelation.*

Also, recently (7, 2, 4, 56) (22) and (8, 1, 6, 116) (17) functions have been found by computer search. It is very interesting to note Δ_f values for these two cases are same for all the functions those are found by computer search, which are respectively 32, 80.

However, the existing recursive construction results are not very good in terms of the autocorrelation values. We now discuss the absolute indicator values of autocorrelation of some of these constructions.

5.4.1 Recursive Construction I

Here we consider the recursive construction which has been discussed in (3; 18; 20) in different forms. We consider the notation in (20) here for constructing an $(n+1)$-variable function F from two n-variable functions f, g.

$$\begin{aligned} Q_i(f(X_n,\ldots,X_1),g(X_n,\ldots,X_1)) &= F(X_{n+1},\ldots,X_1) \\ &= (1\oplus X_i)f(X_n,\ldots,X_{i+1},X_{i-1},\ldots,X_1) \\ &\quad \oplus X_i g(X_n,\ldots,X_{i+1},X_{i-1},\ldots,X_1). \end{aligned}$$

Let f be an n-variable, m-resilient degree d function having nonlinearity x. Define $F(X_{n+1},\ldots,X_1)$ to be an $(n+1)$-variable function as

$$F(X_{n+1},\ldots,X_1) = Q_i(f(X_n,\ldots,X_1), a\oplus f(b\oplus X_n,\ldots,b\oplus X_1)).$$

Here $a,b\in\{0,1\}$ and if m is even $a\neq b$ and if m is odd, $a=1$ and b can be either 0 or 1. Then $F(X_{n+1},X_n,\ldots,X_1)$ is an $(m+1)$-resilient, degree d function having nonlinearity $2x$ (20).

Note that, any of the operators Q_i can be expressed as a composition of Q_{n+1} and a suitable permutation of the input variables. The permutation of input variables preserves the autocorrelation property, resiliency, algebraic degree and nonlinearity. So it is enough to look into the construction function as

$$F(X_{n+1},\ldots,X_1) = Q_{n+1}(f(X_n,\ldots,X_1), a\oplus f(b\oplus X_n,\ldots,b\oplus X_1)), \textit{i.e.},$$

$$F(X_{n+1},\ldots,X_1) = (1\oplus X_{n+1})f(X_n,\ldots,X_1)\oplus X_{n+1}(a\oplus f(b\oplus X_n,\ldots,b\oplus X_1)).$$

First consider the case when m is even. Then $a\neq b$. Let us consider, $a=1, b=0$, then $F(X_{n+1},\ldots,X_1) = (1\oplus X_{n+1})f(X_n,\ldots,X_1)\oplus X_{n+1}(1\oplus f(X_n,\ldots,X_1)) = X_{n+1}\oplus f(X_n,\ldots,X_1)$. It is clear that $\Delta_f(1,0,\ldots,0) = -2^{n+1}$.

If we consider $a=0, b=1$, then $F(X_{n+1},\ldots,X_1) = (1\oplus X_{n+1})f(X_n,\ldots,X_1)\oplus X_{n+1}f(1\oplus X_n,\ldots,1\oplus X_1)$. Then, $\Delta_f(1,1,\ldots,1) = 2^{n+1}$.

Similarly it can be shown that for the case m odd, there will be linear structures in this construction. Thus, for this recursive construction, for an n variable function, the absolute indicator value is 2^n.

5.4.2 Recursive Construction II

Now we consider an elegant construction (35) which was later modified in (22). An (n,m,d,x) function f (see Definition 7) is said to be in *desired* form (22) if it is of the form $(1\oplus X_n)f_1\oplus X_n f_2$, where f_1, f_2 are $(n-1, m, d-1, x-2^{n-2})$ functions. This means that the nonzero values of the Walsh spectra

of f_1, f_2 do not intersect, i.e., if $W_{f_1}(\overline{\omega}) \neq 0$, then $W_{f_2}(\overline{\omega}) = 0$, and vice versa. Let f be an (n, m, d, x) function in the *desired* form, where f_1, f_2 are both $(n-1, m, d-1, x-2^{n-2})$ functions. Let $F = X_{n+2} \oplus X_{n+1} \oplus f$ and $G = (1 \oplus X_{n+2} \oplus X_{n+1})f_1 \oplus (X_{n+2} \oplus X_{n+1})f_2 \oplus X_{n+2} \oplus X_n$. Note that in the language of (35), the function G above is said to depend quasilinearly on the pair of variables (X_{n+2}, X_{n+1}). Also, $F_1 = (1 \oplus X_{n+3})F \oplus X_{n+3}G$. The function F_1 constructed from f above is an $(n+3, m+2, d+1, 2^{n+1}+4x)$ function in the **desired** form.

Consider the case $\alpha_{n+3} = 0, \alpha_{n+2} = \alpha_{n+1} = 1$ and any pattern for $\alpha_n, \ldots, \alpha_1$. In this case, $F(X_{n+2}, \ldots, X_1) = F(X_{n+2} \oplus \alpha_{n+2}, \ldots, X_1 \oplus \alpha_1)$ and hence $\Delta_F(\alpha_{n+2}, \ldots, \alpha_1) = 2^{n+2}$. On the other hand, $G(X_{n+2}, \ldots, X_1) \oplus G(X_{n+2} \oplus \alpha_{n+2}, \ldots, X_1 \oplus \alpha_1) = f_1 \oplus f_2 \oplus 1$. Note that, if the nonzero values of the Walsh spectra of f_1, f_2 do not intersect, then $f_1 \oplus f_2$ is balanced, i.e. $f_1 \oplus f_2 \oplus 1$ is also balanced. Hence, $\Delta_G(\alpha_{n+2}, \ldots, \alpha_1) = 0$. This gives that $\Delta_{F_1}(\alpha_{n+3}, \ldots, \alpha_1) = \Delta_F(\alpha_{n+2}, \ldots, \alpha_1) + \Delta_G(\alpha_{n+2}, \ldots, \alpha_1) = 2^{n+2} + 0 = 2^{n+2}$. So, $\Delta_{F_1} \geq 2^{n+2}$.

Thus, for this recursive construction, for an n variable function the absolute indicator value is greater than or equal to 2^{n-1}.

Note that different kinds of constructions of resilient Boolean functions has been proposed in (27). The main technique used there is concatenation of small affine functions. It will be of interest to analyze the absolute indicator values of such constructions.

6 Conclusion

Here we have discussed about the autocorrelation values of different classes of cryptographically significant Boolean functions. We present constructions of balanced functions which provide currently best known autocorrelation values. We also discuss the autocorrelation properties of correlation immune and resilient Boolean functions.

References

[1] P. Charpin A. Canteaut, C. Carlet and C. Fontaine. Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions. In *Advances in Cryptology - EUROCRYPT 2000*, number 1807 in Lecture Notes in Computer Science, pages 507–522. Springer Verlag, 2000.

[2] 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.

[3] 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.

[4] C. Carlet. More correlation immune and resilient functions over Galois fields and Galois rings. In *Advances in Cryptology - EUROCRYPT'97*, pages 422–433. Springer-Verlag, May 1997.

[5] C. Carlet. Recent results on binary bent functions. In *International Conference on Combinatorics, Information Theory and Statistics*, 1997.

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

[7] C. Carlet and P. Sarkar. Spectral domain analysis of correlation immune and resilient Boolean functions. *Preprint*, 2001.

[8] C. Carlet and P. Guillot. A characterization of bent functions. *Journal of Combinatorial Theory, Series A*, 76(2):328–335, September 1996.

[9] C. Ding and P. Sarkar. *Personal Communication.* 2000.

[10] C. Ding, G. Xiao, and W. Shan. *The Stability Theory of Stream Ciphers.* Number 561 in Lecture Notes in Computer Science. Springer-Verlag, 1991.

[11] 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.

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

[13] 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.

[14] 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.

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

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

[17] S. Maitra and E. Pasalic. Further constructions of resilient Boolean functions with very high nonlinearity. Accepted in SETA, May, 2001, Norway.

[18] 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.

[19] S. Maitra and P. Sarkar. Modifications of Patterson-Wiedemann functions for cryptographic applications. Preprint 2000, available at http://www.isical.ac.in/~ subho.

[20] S. Maitra and P. Sarkar. Cryptographically significant Boolean functions with five valued Walsh spectra. *To be Published in Theoretical Computer Science*, 2001.

[21] W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic

functions. In *Advances in Cryptology - EUROCRYPT'89*, pages 549–562. Springer-Verlag, 1990.

[22] E. Pasalic, T. Johansson, S. Maitra, and P. Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity. In *Workshop on Coding and Cryptography*, Electronic Notes in Discrete Mathematics. Elsevier, January 2001.

[23] 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.

[24] 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.

[25] 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.

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

[27] 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.

[28] 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.

[29] 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.

[30] 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.

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

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

[33] J. J. Son, J. I. Lim, S. Chee, and S. H. Sung. Global avalanche characteristics and nonlinearity of balanced Boolean functions. *Information Processing Letters*, 65:139–144, 1998.

[34] S. H. Sung, S. Chee, and C. Park. Global avalanche characteristics and propagation criterion of balanced Boolean functions. *Information Processing Letters*, 69:21–24, 1999.

[35] Y. V. Tarannikov. On resilient Boolean functions with maximum possible nonlinearity. In *Progress in Cryptology - INDOCRYPT 2000*, number

1977 in Lecture Notes in Computer Science, pages 19–30. Springer Verlag, 2000.

[36] A. F. Webster and S. E. Tavares. On the design of S-boxes. In *Advances in Cryptology - CRYPTO'85*, Lecture Notes in Computer Science, pages 523–534. Springer-Verlag, 1986.

[37] 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.

[38] Y. Zheng and X. M. Zhang. Plateaued functions. In *ICICS'99*, number 1726 in Lecture Notes in Computer Science, pages 284–300. Springer Verlag, 1999.

[39] 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. Springer Verlag, 2000.

[40] Y. Zheng and X. M. Zhang. New results on correlation immunity. In *ICISC 2000*, Lecture Notes in Computer Science. Springer Verlag, 2000.

[41] Y. Zheng and X. M. Zhang. On relationships among propagation degree, nonlinearity and correlation immunity. In *Advances in Cryptology - ASIACRYPT'00*, Lecture Notes in Computer Science. Springer Verlag, 2000.