

On Nonlinearity and Autocorrelation Properties of Correlation Immune Boolean Functions*

SUBHAMOY MAITRA

*Applied Statistics Unit
Indian Statistical Institute
Calcutta 700 108, India
E-mail: subho@isical.ac.in*

In this paper we discuss the nonlinearity and autocorrelation properties of correlation immune Boolean functions. First we provide a construction method for unbalanced, first order correlation immune Boolean functions on even an number of variables $n \geq 6$. These functions achieve the currently best known nonlinearity of $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$. Then we provide a simple modification of these functions to get unbalanced correlation immune Boolean functions on an even number of variables n , with a nonlinearity of $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} - 2$ and a maximum possible algebraic degree of $n - 1$. Moreover, we present a detailed study on the Walsh spectra of these functions. Next we study the autocorrelation values of correlation immune and resilient Boolean functions. We provide new lower bounds and related results on the absolute indicator and sum of square indicator of autocorrelation values for low orders of correlation immunity. Recently it has been show that the nonlinearity and algebraic degree of correlation immune and resilient functions can be optimized simultaneously. Our analysis shows that under such a scenario, the sum of square indicator also attains its minimum value. We also point out the weakness of two recursive construction techniques for resilient functions in terms of autocorrelation values.

Keywords: algebraic degree, autocorrelation, Boolean function, correlation immunity, cryptography, global avalanche characteristics, nonlinearity, resiliency, Walsh spectra

1. INTRODUCTION

Nonlinearity, correlation immunity and autocorrelation are three cryptographically important properties of Boolean functions. The concept of correlation immune Boolean functions was introduced by Siegenthaler [26], and these functions are now used in stream cipher systems to resist cryptanalytic attacks [25].

Nonlinearity is one of the most challenging combinatorial properties of Boolean functions. It is also related to the 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. The

Received May 13, 2002; accepted April 24, 2003.

Communicated by Shih-Ping Shieh.

*This paper is a combined and revised version of the papers "Correlation Immune Boolean Functions with Very High Nonlinearity," IACR ePrint Server, <http://eprint.iacr.org>, No: 2000/054, Date: October 27, 2000 and "Autocorrelation Properties of correlation immune Boolean functions," INDOCRYPT 2001, number 2247, LNCS, pp. 242-253, Springer Verlag, December 2001.

construction of balanced Boolean functions on an even number of variables with very high nonlinearity has been considered in [6, 20, 24]. Dobbertin [6] 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 an odd number of variables. It is known [1, 14] that 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 $n = 9, 11$, and 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 $2^{n-1} - 2^{\frac{n-1}{2}}$ [16, 17, 20].

Recently, weight divisibility results for resilient and correlation immune functions have been presented [3, 21, 29, 33]. These results have direct consequence towards non-trivial upper bounds on the nonlinearity of such functions. The construction of resilient and correlation immune Boolean functions achieving these upper bounds has been discussed in [15, 21, 29]. Thus, it is very clear that a lot of interest have been generated in this area.

The construction of resilient (balanced correlation immune) functions has direct application to combine functions in certain models of stream ciphers, and the works on this subject have been published [2, 9, 15, 20, 21, 23, 29]. However, few construction results related to unbalanced correlation immune functions are available (though some results have been published in recent papers [15, 29]). In this paper, we examine the construction of unbalanced correlation immune Boolean functions on even number of input variables with very high nonlinearity. The basic input for construction is a 6-variable correlation immune function with a nonlinearity of 26 and an algebraic degree of 5, which were very recently studied [15]. Using this 6-variable function, for the first time, we show the existence of an 8-variable correlation immune function with a nonlinearity of 116 and an algebraic degree of 5. We extend our result to the construction of correlation immune functions with a nonlinearity of $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$ and an algebraic degree of 5. Moreover, we present a simple modification of these functions to get correlation immune functions with a nonlinearity of $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} - 2$ and an algebraic degree of $n - 1$. This represents the currently best known result in this direction. Moreover, using the technique presented in this paper, the authors in [12] obtained 1-resilient functions with the currently best known parameters.

Recent results [21] show that the Walsh spectra of m th order correlation immune Boolean functions on n variables with the maximum possible nonlinearity are three valued for $m > \frac{n}{2} - 1$, and that 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 of $m = 1$. Thus it is important to examine the Walsh spectra of such functions, which we will employ here.

Next we will focus on autocorrelation values for correlation immune and resilient (balanced correlation immune) Boolean functions. We will provide the currently best known lower bounds on Δ_f (the absolute indicator) and σ_f (the sum of square indicator) for low orders of correlation immunity (see section 2 for definitions). Very recently, the autocorrelation properties of correlation immune and resilient Boolean functions were presented in [34], and we will provide even better results here. The autocorrelation property of higher order correlation immune functions has been considered in [30]. It has

been shown in [30] that for an n -variable, m -resilient function, $\Delta_f \geq 2^n \frac{2m-n+3}{n+1}$. However, this result is not applicable under low orders of correlation immunity.

For high orders of correlation immunity, we will provide better results for an important subclass of correlation immune and resilient functions which attain the maximum possible nonlinearity. It has recently been found that given a certain order of correlation immunity, the nonlinearity and algebraic degree of correlation immune and resilient functions can be optimized simultaneously [3, 29]. Here, we will extend this analysis to the sum of square indicator of autocorrelation values. We will show that when the nonlinearity and algebraic degree are maximized, the sum of square indicator attains its minimum value.

In [35], it was noted that the propagation property works against correlation immunity. We here explicitly show that Δ_f values work against the order of correlation immunity. Here, we will also point out the limitations of two recursive construction methods for resilient Boolean functions with respect to autocorrelation values.

2. DEFINITIONS AND NOTATIONS

In this section, we will introduce a few definitions and notations. Let s, s_1, s_2 be binary strings of the 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 and s_2 is denoted by $d(s_1, s_2)$, i.e., $d(s_1, s_2) = \#(s_1 \neq s_2)$. Another measure $wd(s_1, s_2)$ 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 $wd(s_1, s_2) = \lambda - 2d(s_1, s_2)$. The Hamming weight or, simply, the weight of s is equal to the number of ones in s and is denoted by $wt(s)$.

By Ω_n , we mean the set of all n -variable Boolean functions. We define an n -variable Boolean function as a bit string of length 2^n , which is the output column of its truth table. An n -variable function f is said to be balanced if its output column in the truth table contains equal numbers of 0's and 1's (i.e., $wt(f) = 2^{n-1}$).

We denote the addition operator over $GF(2)$ using \oplus . An n -variable Boolean function can be uniquely represented by a multivariate polynomial over $GF(2)$. We can write $f(X_n, \dots, X_1)$ as

$$a_0 \oplus \left(\bigoplus_{i=1}^{i=n} a_i X_i \right) \oplus \left(\bigoplus_{1 \leq i \neq j \leq n} a_{ij} X_i X_j \right) \oplus \dots \oplus a_{12\dots n} X_1 X_2 \dots X_n,$$

where the coefficients $a_0, a_i, a_{ij}, \dots, a_{12\dots n} \in \{0, 1\}$. This representation of f is called the algebraic normal form (ANF) of f . The number of variables in the highest order product term with a nonzero coefficient is called the algebraic degree, or simply the degree of f . Functions of degree at most one are called affine functions. An affine function with a 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 f from the set of all n -variable affine functions.

Here, we will use the 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 are 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_1f_2 . Thus, $f = f_1f_2$ means that in algebraic normal form, $f = (1 \oplus X_n)f_1 \oplus X_nf_2$.

Now we will define an important tool for analysing Boolean functions. Let $\bar{X} = (X_n, \dots, X_1)$ and $\bar{w} = (w_n, \dots, w_1)$ be n -tuples on $GF(2)$ and $\bar{X} \cdot \bar{w} = X_nw_n \oplus \dots \oplus X_1w_1$. Let $f(\bar{X})$ be a Boolean function whose domain is the vector space over $GF(2)^n$. Then the Walsh transform of $f(\bar{X})$ is a real valued function over $GF(2)^n$ that can be defined as

$$W_f(\bar{w}) = \sum_{\bar{X}} (-1)^{f(\bar{X}) \oplus \bar{X} \cdot \bar{w}},$$

where the sum is over all \bar{X} in $GF(2)^n$. For a function f , we define $F_f = |\{\bar{w} \in \{0, 1\}^n | W_f(\bar{w}) \neq 0\}|$. This is the number of nonzero coefficients in the Walsh spectra. Note that $W_f(\bar{w}) = wd(f, \bigoplus_{i=1}^n w_i X_i)$.

In [7], the following characterization of correlation immunity was provided. A function $f(X_n, \dots, X_1)$ is m -th order correlation immune (CI) iff its Walsh transform W_f satisfies $W_f(\bar{w}) = 0$, for $1 \leq wt(\bar{w}) \leq m$. If f is balanced then $W_f(\bar{0}) = 0$. Balanced m -th order correlation immune functions are called m -resilient functions. Thus, a function $f(X_n, \dots, X_1)$ is m -resilient iff its Walsh transform W_f satisfies

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

By the $[n, m, d, x]$ function, we mean an unbalanced n -variable m th order correlation function having a nonlinearity of x and a degree of d . By (n, m, d, x) , we denote an n -variable m -resilient function with a nonlinearity of x and a degree of d .

The Propagation Characteristic (PC) and Strict Avalanche Criteria (SAC) [18] are important properties of Boolean functions used in S-boxes. However, Zhang and Zheng [31] showed that SAC and PC have some limitations when it comes to identify certain desirable cryptographic properties of a Boolean function. In this respect, they proposed the idea of Global Avalanche Characteristics (GAC). Here, we state two important indicators of GAC.

Let $\bar{X} \in \{0, 1\}^n$ be an n tuple X_n, \dots, X_1 , and let $\bar{\alpha} \in \{0, 1\}^n$ be an n tuple $\alpha_n, \dots, \alpha_1$. Let $f \in \Omega_n$ and $\Delta_f(\bar{\alpha}) = wd(f(\bar{X}), f(\bar{X} \oplus \bar{\alpha}))$, the autocorrelation value of f with respect to the vector $\bar{\alpha}$. The sum-of-square indicator

$$\sigma_f = \sum_{\bar{\alpha} \in \{0,1\}^n} \Delta_f^2(\bar{\alpha}) \text{ and the absolute indicator } \Delta_f = \max_{\bar{\alpha} \in \{0,1\}^n, \bar{\alpha} \neq \bar{0}} |\Delta_f(\bar{\alpha})|.$$

It may very well happen that correlation immune or resilient functions, which are good in terms of the order of correlation immunity, algebraic degree and nonlinearity, may not be good in terms of their SAC or PC properties. Also, achieving 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 where $f(\bar{X}) \oplus f(\bar{X} \oplus \bar{\alpha})$ is constant

for some nonzero $\bar{\alpha}$ which is a weakness. It is important to get good autocorrelation properties for such functions. This is why we will examine the autocorrelation properties of correlation immune and resilient functions.

For a linear function f , $\Delta_f = 2^n$, and $\sigma_f = 2^{3n}$. For functions f , on an even number of variables, we have $\Delta_f = 0$ ($\sigma_f = 2^{2n}$) iff f is a bent function [13, 31]. However, bent functions are not balanced. In fact, for a function f of even weight, $\Delta_f \equiv 0 \pmod{8}$, and for a function f of odd weight, $\Delta_f \equiv 4 \pmod{8}$. For a balanced function f , $\sigma_f \geq 2^{2n} + 2^{n+3}$ [27] for both odd and even number of variables. A comparatively sharper result in this direction was proposed in [28], which we will discuss in subsection 4.

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 reported in [27, 28] are valid for any Boolean function f whose Walsh spectrum contains at least one zero.

3. CONSTRUCTION OF HIGHLY NONLINEAR CORRELATION IMMUNE FUNCTIONS

First, we will consider the basic construction method.

Construction 3.1 [19] Let $h \in \Omega_n$ be an $[n, 1, d, x]$ function, where n is even. Consider the function $g(X_{n+2}, \dots, X_1) = X_{n+2}X_{n+1} \oplus h(X_n, \dots, X_1)$; i.e., the truth table of g is of the form $hhhh^c$.

Then we have the following result.

Proposition 3.1 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 3.1. Then

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

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

Note that g is of the form $hhhh^c$, and that X_i is of the form $llll$, for $1 \leq i \leq n$. Here by X_i , we mean the output column of a truth table considering the function X_i , where X_i is considered to be an $(n+2)$ -variable function. (Here, X_i is an output column of length 2^{n+2} , and l is an 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 (an 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, $g(X_{n+2}, \dots, X_1) = X_{n+2}X_{n+1} \oplus h(X_n, \dots, X_1)$ and the degree of h is $d > 2$, we get item 4. \square

The construction of resilient Boolean functions using linear transformation was used in [11]. Here, we will use a similar method for correlation immune functions. The method is as follows.

Given a function $f \in \Omega_n$, we define $S_f = \{\bar{w} \in \{0, 1\}^n | W_f(\bar{w}) = 0\}$, where W_f is the Walsh transform of f . If there exist 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 $f'(\bar{X}) = f(C_f \bar{X})$, then both f', f have the same nonlinearity and algebraic degree. Moreover, $W_{f'}(\bar{w}) = 0$ for $wt(\bar{w}) = 1$, where $W_{f'}$ is the Walsh Transform of f' . This ensures that f' is 1st order correlation immune.

Let ϵ_i^k be a k -bit vector with an i th ($1 \leq i \leq k$) entry of 1 and let all the other entries be 0. For example $\epsilon_k^k = (1, 0, \dots, 0)$ and $\epsilon_1^k = (0, \dots, 0, 1)$.

Now, we will 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, \oplus means the bitwise XOR of two binary vectors. Note that each vector corresponds to a linear function. The vectors r_i for $1 \leq i \leq n$ correspond to the linear functions X_i , and the vectors r_i for $i = n + 1, n + 2$ correspond 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 3.1, then B_g is of the following form. Note that B_g is a nonsingular (invertible) matrix. Let us consider the binary matrix $C_g = B_g^{-1}$.

Then we have the following theorem.

Theorem 3.1 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 3.1 and the result of Proposition 3.1 here. From h , it is possible to get a function $g \in \Omega_{n+2}$, such that $nl(g) = 2^n + 2x$ and the 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 $\bar{X} = (X_{n+2}, \dots, X_1)$, which we interpret as a column vector here. Hence, the function $g'(\bar{X}) = g(C_g \bar{X})$ is an $[n + 2, 1, d, 2^n + 2x]$ function. \square

Next, we will consider the initial function for this construction. The construction of a $[6, 1, 5, 26]$ Boolean function was proposed in [15]. 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 3.1. Note that this is the first time that a correlation immune function with nonlinearity greater than 112 has been reported. Also in [3], it was 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 even n . With $n = 8, m = 1$, and $d = 5$, we get that the maximum possible nonlinearity of an $[8, 1, 5, 116]$ function is $2^{8-1} -$

$2^{\frac{8}{2}-1} - 2^{1+\lfloor \frac{8-1}{5} \rfloor} = 116$. Thus, this function achieves the maximum possible nonlinearity and, in turn, shows the tightness of the bound [3] in this case.

In general, we have the following theorem.

Theorem 3.2 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 be 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 3.1 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. \square

Now, we will examine the Walsh spectra of the function g' . Since $g'(\bar{X}) = g(C_g \bar{X})$, the Walsh spectra of g, g' are the permutations of each other. Note that any linear function λ of $n + 2$ variables can be written in any of the following four forms: $llll, ll^c ll^c, ll^c l^c, ll^c l^c l$, where l is a linear function of n variables. Note that, $wd(g, \lambda) = wd(hhhh^c, llll)$ or $wd(hhhh^c, ll^c ll^c)$ or $wd(hhhh^c, ll^c l^c)$ or $wd(hhhh^c, ll^c l^c l)$. Thus, $wd(g, \lambda) = \pm 2wd(h, l)$. The Walsh spectrum 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 3.1 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 will examine some more interesting results for 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, $wd(f, l) = 0, \pm 8$, 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 the $[8, 1, 5, 116]$ function F , constructed using the function f , gives the following Walsh spectra: $wd(F, \lambda) = 0, \pm 16$, when $ndg(\lambda)$ is odd and $wd(f, \lambda) = \pm 8, \pm 24$, when $ndg(\lambda)$ is even for $\lambda \in L(8)$. We will generalize this result. First, we will update Construction 3.1.

Construction 3.2 Let $h \in \Omega_n$ be an $[n, 1, d, x]$ function, where n is even. Also, let $wd(h, l) = 0, \pm x$, when $ndg(l)$ is odd, and let $wd(h, l) = \pm y, \pm z$, when $ndg(l)$ is even for $l \in L(n)$. Then, consider the function $g(X_{n+2}, \dots, X_1) = X_{n+2}X_{n+1} \oplus h(X_n, \dots, X_1)$; i.e., the truth table of g is of the form $hhhh^c$. Consider the binary matrix C_g shown in Table 1. Let $\bar{X} = (X_{n+2}, \dots, X_1)$. Interpret \bar{X} as a column vector. Construct the function $g'(\bar{X}) = g(C_g \bar{X})$.

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

Table 1. The B_g and C_g matrices.

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

Lemma 3.1 Let $g' \in \Omega_{n+2}$ be as mentioned in Construction 3.2. 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 takes 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, $wd(g(X_{n+2}, \dots, X_1), \lambda) = 0$, or $\pm 2x$ when $ndg(l)$ is odd and $wd(g(X_{n+2}, \dots, X_1), \lambda) = \pm 2y$, 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 $g'(\bar{X}) = g(C_g \bar{X})$ and from the form of the matrix C_g . □

Theorem 3.3 It is possible to construct $[n, 1, 5, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}]$ functions f with

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

Proof: The proof follows from Construction 3.2, Lemma 3.1 and the Walsh spectra of the initial $[6, 1, 5, 26]$ function mentioned above. □

3.1 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 [26] 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 will achieve using the following technique, which has earlier been used in [9].

Definition 3.1 Let $f, g \in \Omega_n$, and let there exist 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 the values of just a specific pair of positions are complementary and the positions are the same distances from the top and bottom of the function. The following result shows the importance of Definition 3.1.

Proposition 3.2 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 the algebraic degree of f is less than $n - 1$, then g is of algebraic degree $n - 1$.

Proof: Items 1 and 2 were proven in and in [9] and [10], respectively. Now we will prove item 3. Consider $f = f_1f_2$, where $f_1, f_2 \in \Omega_{n-1}$; that is, the truth table of f can be seen as the concatenation of the truth tables of the functions f_1 and f_2 . Similarly, consider $g = g_1g_2$, 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, the degree of g is $n - 1$. □

Theorem 3.4 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 3.2 that it is possible to construct an $[n, 1, 5, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}]$ function. We will consider such a function f . Now, this function is unbalanced; 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 can construct a palindromically related function $g \in \Omega_n$. From Proposition 3.2, 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 will 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 3.1, 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 3.3 Let $f, g \in \Omega_n$ be palindromically related, and let $l \in L(n)$. Then,

1. $wd(f, l) = wd(g, l)$, if l is nondegenerate on an 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 the $wd(\cdot)$ value for both functions f, g will be the 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, $f[i] = f[2^n - 1 - i]$, and $g[i] = g[2^n - 1 - i]$. Also, $f[i] \neq g[i]$. Thus, the contribution to the $wd(\cdot)$ value 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 3.5 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. $W_f(\bar{w}) = 0, \pm 8 \cdot 2^{\frac{n}{2}-3}$, for $wt(\bar{w})$ odd, and
2. $W_f(\bar{w}) = \pm 4 \cdot 2^{\frac{n}{2}-3} \pm 4, \pm 12 \cdot 2^{\frac{n}{2}-3} \pm 4$, for $wt(\bar{w})$ 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 3.3. $W_f(\bar{w}) = 0, \pm 8 \cdot 2^{\frac{n}{2}-3}$, for $wt(\bar{w})$ odd, and $W_f(\bar{w}) = \pm 4 \cdot 2^{\frac{n}{2}-3}, \pm 12 \cdot 2^{\frac{n}{2}-3}$, for $wt(\bar{w})$ even. Then, the result follows from Proposition 3.3. \square

4. AUTOCORRELATION OF CORRELATION IMMUNE FUNCTIONS

The autocorrelation properties of correlation immune Boolean functions have received a lot of attention recently [30, 34, 35]. Here, we will discuss these properties.

4.1 Lower Bound on Sum-of-Square Indicator

We will begin this section with a result from [32, Theorem 3].

Theorem 4.1 Let $f \in \Omega_n$. Then, $\sigma_f = \frac{2^{3n}}{F_f}$. Moreover, if f has a three valued Walsh spectra $0, \pm 2^x$, then $\sigma_f = \frac{2^{3n}}{F_f}$.

Next, we have the following result, which follows directly from the definition of correlation immunity and F_f .

Proposition 4.1 Let $f \in \Omega_n$ be an m -th order correlation immune function. Then, $F_f \leq 2^n - \sum_{i=1}^m \binom{n}{i}$. Moreover, if f is m -resilient, then $F_f \leq 2^n - \sum_{i=1}^m \binom{n}{i}$.

The next result follows from Theorem 4.1 and Proposition 4.1

Lemma 4.1 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 $\sigma_f \geq \frac{2^{3n}}{2^n - \sum_{i=1}^m \binom{n}{i}}$.

To identify the 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 .

Theorem 4.2 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 $\sigma_f > 2^{2n} + 2^{n+\log_2 \sum_{i=1}^m \binom{n}{i}}$.

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. A similar result follows for resilient functions. \square

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

Currently, no results are available from the lower bound of σ_f values for correlation immune and resilient functions. The only known results are for balanced functions, which are given in [27, 28]. The lower bound for balanced functions given in [27] is $2^{2n} + 2^{n+3}$. The result given in [28] is as follows. For a balanced function f ,

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

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

Now, we will present 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 $m > \frac{n}{2}$, $\sigma_f > 2^{2n} + 2^{2n-1}$. This result is also true for m -resilient functions. This provides a strong lower bound on the 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 chosen m .

4.2 Lower Bound on the Absolute Indicator

Now, we will concentrate on the absolute indicator of GAC. We already have a result for the sum-of-square indicator for correlation immune and resilient functions. We will use this result here.

Lemma 4.2 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, $\Delta_f \geq \sqrt{\frac{1}{2^n - 1} \frac{2^{2n} \sum_{i=0}^m \binom{n}{i}}{2^n - \sum_{i=0}^m \binom{n}{i}}}$ or an n -variable m -resilient function f .

Proof: We know that $\sigma_f = \sum_{\bar{\alpha} \in \{0,1\}^n} \Delta_f^2(\bar{\alpha})$. Thus, the absolute value of each $\Delta_f(\bar{\alpha})$ will be the minimum value only when each $\Delta_f(\bar{\alpha})$, for $\bar{\alpha} \in \{0, 1\}^n$ (except the all zero

case), possess equal values. Hence, the minimum value of Δ_f will be $\sqrt{\frac{\sigma_f - 2^{2^n}}{2^n - 1}}$. This gives the result when the value of σ_f from Lemma 4.1 is used. \square

In [34], it was 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 $\Delta_f \geq 2^{m-1} \sum_{i=0}^{+\infty} 2^{i(m-1-n)} = 2^{m-1} \frac{1}{1-2^{m-1-n}}$. 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, $\Delta_f \geq 2^m \sum_{i=0}^{+\infty} 2^{i(m-n)} = 2^m \frac{1}{1-2^{m-n}}$.

For lower orders of correlation immunity ($m \leq \frac{n}{2} - 1$), and lower orders of resiliency ($m \leq \frac{n}{2} - 2$), our result in Lemma 4.2 is better than the result in [34]. Since the expressions are too complicated to compare, we provide a table below to substantiate our claim. We will present a comparison for n -variable, m -resilient functions. Note that the Δ_f values for balanced functions are divisible by 8. Thus, after calculating the expressions, we increase the values to the closest integers divisible by 8. In each row, we first provide the Δ_f values from Lemma 4.2, and then under that we provide the result from [34]. It is clear that our result provide a considerable improvement over that in [34] as both n, m increase.

Using simplification in Lemma 4.2, we get the following result.

Theorem 4.3 For an n -variable m -th order correlation immune function f ,

$$\Delta_f > 2^{\frac{n}{2}} \sqrt{\frac{\sum_{i=1}^m \binom{n}{i}}{2^n - \sum_{i=1}^m \binom{n}{i}}}. \text{ Similarly, } \Delta_f > 2^{\frac{n}{2}} \sqrt{\frac{\sum_{i=0}^m \binom{n}{i}}{2^n - \sum_{i=0}^m \binom{n}{i}}} \text{ for an } n\text{-variable } m\text{-resilient function } f.$$

Proof: The result follows from overestimating $2^n - 1$ by 2^n . \square

It is known that for a function f of even weight, $\Delta_f \equiv 0 \pmod 8$. Since the correlation immune functions and resilient functions are all of even weight, the Δ_f values will be the values that are greater than the values given in Theorem 4.3, which are divisible by 8. Our result has the following consequences.

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

4.3 Lower Bounds Using Weight Divisibility Results

Here, we will use the weight divisibility results of correlation immune and resilient Boolean functions [21]. It is known that the values in the Walsh spectrum of an m -th order correlation immune function are divisible by 2^{m+1} . Similarly for m -resilient functions, the Walsh spectrum values are divisible by 2^{m+2} .

Table 2. Comparison of our results with those presented in [34].

n^m	1	2	3	4	5	6	7	8	9	10	11	12	13	14
8	8	8												
8	8	8												
9	8	8												
8	8	8												
10	8	8	16											
8	8	16												
11	8	16	24											
8	8	16												
12	8	16	24	32										
8	8	16	24											
13	8	16	24	40										
8	8	16	24											
14	8	16	24	48	72									
8	8	16	24	40										
15	8	16	32	78	80									
8	8	16	24	40										
16	8	16	32	56	88	144								
8	8	16	24	40	72									
17	8	16	32	64	104	168								
8	8	16	24	40	72									
18	8	16	32	72	120	192	288							
8	8	16	24	40	72	136								
19	8	16	40	72	136	224	344							
8	8	16	24	40	72	136								
20	8	16	40	80	152	256	400	600						
8	8	16	24	40	72	136	264							
21	8	16	40	88	176	296	472	712						
8	8	16	24	40	72	136	264							
22	8	16	48	96	192	344	552	840	1224					
8	8	16	24	40	72	136	264	520						
23	8	24	48	112	216	392	648	1000	1464					
8	8	16	24	40	72	136	264	520						
24	8	24	56	120	240	440	752	1176	1752	2496				
8	8	16	24	40	72	136	264	520	1032					
25	8	24	56	128	264	504	864	1384	2088	3008				
8	8	16	24	40	72	136	264	520	1032					
26	8	24	56	136	296	568	1000	1624	2488	3624	5096			
8	8	16	24	40	72	136	264	520	1032	2056				
27	8	24	64	152	320	632	1144	1904	2960	4360	6176			
8	8	16	24	40	72	136	264	520	1032	2056				
28	8	24	64	160	352	712	1304	2216	3504	5232	7480	10368		
8	8	16	24	40	72	136	264	520	1032	2056	4104			
29	8	24	64	168	384	792	1488	2560	4128	6264	9056	12640		
8	8	16	24	40	72	136	264	520	1032	2056	4104			
30	8	24	72	184	424	880	1680	2960	4848	7472	10944	15400	21064	
8	8	16	24	40	72	136	264	520	1032	2056	4104	8200		
31	8	24	72	192	456	976	1896	3400	5672	8880	13184	18744	25800	
8	8	16	24	40	72	136	264	520	1032	2056	4104	8200		
32	8	24	80	208	496	1080	2128	3888	6600	10512	15832	22768	31592	42736
8	8	16	24	40	72	136	264	520	1032	2056	4104	8200	16392	

We will now obtain the sum of square indicators of such functions. We will once again refer to Theorem 4.1. For $f \in \Omega_n$, $\sigma_f \geq \frac{2^{2n}}{F_f}$.

- For an n -variable, m -th order correlation immune function, the values in the Walsh spectra are $0, \pm i^{2^{m+1}}$, $i = 1, 2, \dots$. From Parseval's relation [5] we get $\sum_{\bar{w} \in \{0,1\}^n} W_f^2(\bar{w}) = 2^{2n}$. Hence, we get that for such a function f , $F_f \leq 2^{2n-2m-2}$.

- For an n -variable, m -resilient Boolean function, the Walsh spectra contain the values $0, \pm i2^{m+2}, i = 1, 2, \dots$. Using Parseval's relation, we get that for such a function f , $F_f \leq 2^{2n-2m-4}$.

Theorem 4.4 For an n -variable, m -th order correlation immune function f , $\sigma_f \geq 2^{n+2m+2}$, and for an n -variable, m -resilient function f , $\sigma_f \geq 2^{n+2m+4}$.

Proof: It is known from [21] that for m -th order correlation immune (respectively, m -resilient) functions, the nonzero values of the Walsh spectra will always be divisible by 2^{m+1} (respectively, 2^{m+2}). Thus, using Parseval's relation, we get that for correlation immune (respectively, resilient) functions, $F_f \leq 2^{2n-2m-2}$ (respectively, $F_f \leq 2^{2n-2m-4}$). Hence, the result follows from Theorem 4.1. \square

Note that the trivial lower bound on the sum of the 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 $m > \frac{n}{2} - 2$.

The weight divisibility results obtained using the algebraic degree of the functions have been presented in [3]. These results can be used to provide a sharper lower bound on σ_f involving the algebraic degree. From [3], it is clear that for an n -variable, m -th order correlation immune function with algebraic degree of 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 an algebraic degree of 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 4.4 to include the algebraic degree as follows.

Theorem 4.5 For an n -variable, m -th order ($m > \frac{n}{2} - 1$) correlation immune (respectively resilient) function f with an algebraic degree of d , $\sigma_f \geq 2^{2n+2m+2+2\lfloor \frac{n-m-1}{d} \rfloor}$ (respectively, $\sigma_f \geq 2^{n+2m+4+2\lfloor \frac{n-m-2}{d} \rfloor}$).

Next, we will focus on a very important subset of correlation immune and resilient functions which possess maximum possible nonlinearity. Importantly, resilient functions have direct application in stream cipher systems. Now, the clear benchmark for selecting resilient functions is the present of the functions which possess the best possible trade-off among the parameters nonlinearity, algebraic degree, and the order of resiliency. However, we should consider one more important criterion in the selection process. It is a fact that we can find functions with the best possible trade-off and having the 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 will show shortly. For this purpose, we will concentrate on defining of plateaued functions [32, Definition 9]. Apart from the bent and linear functions, the other plateaued functions have three-valued Walsh spectra: $0, \pm 2^x$. We can once again employ Theorem 4.1 (the result from [32, Theorem 3]). Let $f \in \Omega_n$ and let f have a three-valued Walsh spectra $0, \pm 2^x$. Then, $\sigma_f = \frac{2^{2n}}{F_f}$. We present the following known

[21] results.

- For n -variable, m -th order correlation immune functions 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 [5], $\sum_{\bar{w} \in \{0,1\}^n} W_f^2(\bar{w}) = 2^{2n}$. Hence, we get that for such a function f , $F_f = 2^{2n-2m-2}$.
- For n -variable, m -resilient functions 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 , $F_f = 2^{2n-2m-4}$.

Hence we get the following result.

Theorem 4.6 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 (respectively resilient) functions follows from Theorem 4.1 and $F_f = 2^{2n-2m-2}$ (respectively, $F_f = 2^{2n-2m-4}$) [21]. \square

Recently reported results [3, 29] clearly show that the nonlinearity and algebraic degree of correlation immune and resilient functions are optimized simultaneously. Theorem 4.6 provides the result when the nonlinearity is maximized. Thus, the algebraic degree is also maximized in this case. Here, we can show that at this situation, the sum of square indicator attains its minimum value, too. This indicates that for an n -variable, m -resilient function the nonlinearity, algebraic degree, and sum of square indicator of autocorrelation values are optimized simultaneously.

4.4 Construction Results

Resilient Boolean functions, which are provably optimized in terms of the order of resiliency, algebraic degree and nonlinearity [21], have immediate applications in stream cipher systems. Unfortunately, the general construction techniques does not provide good autocorrelation properties. First, we will discuss 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 will initially consider such a function f constructed using linear concatenation, 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, using search techniques, we can get a (5, 1, 3, 12) function g , such that $\Delta_g = 8$. The truth table of the function is 0000101111011001110010100111000. *This function achieves the best possible trade-off among order of resiliency, nonlinearity, algebraic degree, and autocorrelation.* Recently, (7, 2, 4, 56) [15] and (8, 1, 6, 116) [12] functions have been found by means of computer search. It has been reported in [4] that the minimum Δ_f values for these two cases (so far found by computer search) are 32, and 80, re-

spectively. Moreover, it has been shown in [4] that the (10, 1, 8, 488) function provided in [12] has Δ_f value of 320, and the (10, 1, 8, 484) function provided in [20] has a Δ_f value of 192. In [4], the simulated annealing technique was applied to find resilient functions with very good autocorrelation properties. The functions (7, 1, 5, 56), (7, 2, 4, 56), (8, 1, 6, 116), and (10, 1, 8, 484) with Δ_f values of 16, 24, 24, and 64, respectively, have been reported in [4].

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

4.4.1 Recursive construction I

Here, we will consider the recursive construction which has been discussed in [2, 11] based on different forms. We will use the notation in [11] here to construct an $(n + 1)$ -variable function F from two n -variable functions f, g :

$$Q_i(f(X_n, \dots, X_1), g(X_n, \dots, X_1)) = F(X_{n+1}, \dots, X_1) = (1 \oplus X_i) f(X_n, \dots, X_{i+1}, X_{i-1}, X_1) \oplus X_i g(X_n, \dots, X_{i+1}, X_{i-1}, X_1)$$

Let f be an n -variable, m -resilient degree d Boolean function having a nonlinearity of x . Define $F(X_{n+1}, \dots, X_1)$ as an $(n + 1)$ -variable Boolean function as follows: $F(X_{n+1}, \dots, X_1) = Q_i(f(X_n, \dots, X_1), a \oplus f(b \oplus X_n, \dots, b \oplus X_1))$. Here, $a, b \in \{0, 1\}$ and if m is even, then $a \neq b$, and if m is odd, then $a = 1$ and b can be either 0 or 1. Then, $F(X_{n+1}, X_n, \dots, X_1)$ is an $(m + 1)$ -resilient, degree d function having a nonlinearity of $2x$ [11].

Note that any of the operators Q_i can be expressed as a combination of Q_{n+1} and a suitable permutation of the input variables. The permutation of the input variables preserves the autocorrelation property, resiliency, algebraic degree, and nonlinearity. So it is enough to look into the construction function as $F(X_{n+1}, \dots, X_1) = Q_{n+1}(f(X_n, \dots, X_1), a \oplus f(b \oplus X_n, \dots, b \oplus X_1))$, i.e., $F(X_{n+1}, \dots, X_1) = (1 \oplus X_{n+1}) f(X_n, \dots, X_1) \oplus X_{n+1}(a \oplus f(b \oplus X_n, \dots, b \oplus X_1))$.

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

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

Similarly, it can be shown that for the case in which m is 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 .

4.4.2 Recursive construction II

Now, we will consider the construction reported in [29] that was later modified to obtain that reported in [15]. An (n, m, d, x) function f is said to be in the *desired* form [15] 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 $W_{f_1}(\bar{w}) \neq 0$, then $W_{f_2}(\bar{w}) = 0$, 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 following the language in [29], 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 in which $\alpha_{n+3} = 0$, $\alpha_{n+2} = \alpha_{n+1} = 1$ and any pattern for $\alpha_n, \dots, \alpha_1$. In this case, $F(X_{n+2}, \dots, X_1) = F(X_{n+2} \oplus \alpha_{n+2}, \dots, X_1 \oplus \alpha_1)$; hence we get $\Delta_F(\alpha_{n+2}, \dots, \alpha_1) = 2^{n+2}$. On the other hand, $G(X_{n+2}, \dots, X_1) \oplus G(X_{n+2} \oplus \alpha_{n+2}, \dots, X_1 \oplus \alpha_1) = f_1 \oplus f_2 \oplus 1$. 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 [22]; i.e., $f_1 \oplus f_2 \oplus 1$ is also balanced. Hence, $\Delta_G(\alpha_{n+2}, \dots, \alpha_1) = 0$. This gives that $\Delta_{F_1}(\alpha_{n+3}, \dots, \alpha_1) = \Delta_F(\alpha_{n+2}, \dots, \alpha_1) + \Delta_G(\alpha_{n+2}, \dots, \alpha_1) = 2^{n+2} + 0 = 2^{n+2}$. Therefore, $\Delta_{F_1} \geq 2^{n+2}$.

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

It would be interesting to find a construction which provides good Δ_f values for resilient functions f with the best possible nonlinearity, algebraic degree and σ_f values.

5. CONCLUSIONS

In this paper, we have considered nonlinearity and autocorrelation of correlation immune Boolean functions. We have presented a generalized construction method for highly nonlinear first order correlation immune functions. We have also discussed in detail the algebraic degree and Walsh spectra of these functions. In addition, we have discussed the autocorrelation properties of correlation immune Boolean functions and provide the currently best known lower bound in this direction for low orders of correlation immunity. We have also shown that some of the recently reported methods for constructing resilient functions have weaknesses in terms of the autocorrelation properties. It would be interesting to develop a generalized method for constructing resilient Boolean functions with a very good autocorrelation property.

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*, Vol. 18, 1972, pp. 203-207.
2. P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On correlation immune functions," *Advances in Cryptology - CRYPTO '91*, LNCS, No. 576, Springer Verlag, 1992, pp. 86-100.
3. C. Carlet and P. Sarkar, "Spectral domain analysis of correlation immune and resilient Boolean functions," *Finite Fields and its Applications*, Vol. 8, 2002, pp. 120-130.
4. J. A. Clark, J. L. Jacob, S. Stepney, S. Maitra, and W. Millan, "Evolving Boolean functions satisfying multiple criteria," *Progress in Cryptology - INDOCRYPT 2002: Third International Cryptology Conference in India, Hyderabad, December 2002*, LNCS, No. 2551, Springer Verlag, 2002, pp. 246-259.

5. C. Ding, G. Xiao, and W. Shan, "The stability theory of stream ciphers," LNCS, No. 561, Springer Verlag, 1991.
6. H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity," in *Fast Software Encryption*, LNCS, No. 1008, Springer Verlag, 1994, pp. 61-74.
7. X. Guo-Zhen and J. Massey, "A spectral characterization of correlation immune combining functions," *IEEE Transactions on Information Theory*, Vol. 34, 1988, pp. 569-571.
8. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North Holland, 1977.
9. S. Maitra and P. Sarkar, "Hamming weights of correlation immune Boolean functions," *Information Processing Letters*, Vol. 71, 1999, pp. 149-153.
10. S. Maitra and P. Sarkar, "Highly nonlinear resilient functions optimizing Siegenthaler's inequality," *Advances in Cryptology – CRYPTO '99*, LNCS, No. 1666, 1999, Springer Verlag, pp. 198-215.
11. S. Maitra and P. Sarkar, "Cryptographically significant Boolean functions with five valued Walsh spectra," *Theoretical Computer Science*, Vol. 276, 2002, pp. 133-146.
12. S. Maitra and E. Pasalic, "Further constructions of resilient Boolean functions with very high nonlinearity," *IEEE Transactions on Information Theory*, Vol. 48, 2002, pp. 1825-1834.
13. W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," *Advances in Cryptology – EUROCRYPT '89*, Springer Verlag, 1990, pp. 549-562.
14. J. J. Mykkeltveit, "The covering radius of the (128, 8) Reed-Muller code is 56," *IEEE Transactions on Information Theory*, Vol. 26, 1983, pp. 358-362.
15. E. Pasalic, T. Johansson, S. Maitra, and P. Sarkar, "New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity," *Workshop on Coding and Cryptography, Electronic Notes in Discrete Mathematics*, Vol. 6, 2001.
16. 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*, Vol. 29, 1983, pp. 354-356.
17. 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*, Vol. 36, 1990, pp. 43.
18. B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle, "Propagation characteristics of Boolean functions," *Advances in Cryptology – EUROCRYPT '90*, LNCS, 1991, pp. 161-173.
19. O. S. Rothaus, "On bent functions," *Journal of Combinatorial Theory – Series A*, 1976, pp. 300-305.
20. P. Sarkar and S. Maitra, "Construction of nonlinear Boolean functions with important cryptographic properties," *Advances in Cryptology – EUROCRYPT 2000*, 2000, pp. 485-506.
21. P. Sarkar and S. Maitra, "Nonlinearity bounds and constructions of resilient Boolean functions," *Advances in Cryptology – CRYPTO 2000*, 2000, pp. 515-532.
22. P. Sarkar and S. Maitra, "Cross-correlation analysis of cryptographically useful Boolean functions and S-boxes," *Theory of Computing Systems*, Vol. 35, 2002, pp. 39-57.

23. J. Seberry, X. M. Zhang, and Y. Zheng, "On constructions and nonlinearity of correlation immune Boolean functions," *Advances in Cryptology – EUROCRYPT '93*, 1994, pp. 181-199.
24. J. Seberry, X. M. Zhang, and Y. Zheng, "Nonlinearly balanced Boolean functions and their propagation characteristics," *Advances in Cryptology – CRYPTO '93*, 1994, pp. 49-60.
25. T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," *IEEE Transactions on Computers*, Vol. 34, 1985, pp. 81-85.
26. T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *IEEE Transactions on Information Theory*, Vol. 30, 1984, pp. 776-780.
27. J. J. Son, J. I. Lim, S. Chee, and S. H. Sung, "Global avalanche characteristics and nonlinearity of balanced Boolean functions," *Information Processing Letters*, Vol. 65, 1998, pp. 139-144.
28. S. H. Sung, S. Chee, and C. Park, "Global avalanche characteristics and propagation criterion of balanced Boolean functions," *Information Processing Letters*, Vol. 69, 1999, pp. 21-24.
29. Y. V. Tarannikov, "On resilient Boolean functions with maximum possible nonlinearity," in *Progress in Cryptology – INDOCRYPT 2000*, 2000 pp. 19-30.
30. Y. V. Tarannikov, P. Korolev, and A. Botev, "Autocorrelation coefficients and correlation immunity of Boolean functions," *Autocorrelation Coefficients and Correlation Immunity of Boolean Functions (ASIACRYPT 2001)*, 2001, pp. 460-479.
31. X. M. Zhang and Y. Zheng, "GAC – the criterion for global avalanche characteristics of cryptographic functions," *Journal of Universal Computer Science*, Vol. 1, 1995, pp. 316-333.
32. Y. Zheng and X. M. Zhang, "Plateaued functions," *Computer Science*, 1999, pp. 284-300.
33. Y. Zheng and X. M. Zhang, "Improving upper bound on nonlinearity of high order correlation immune functions," in *Proceedings of Selected Areas in Cryptography (SAC 2000)*, LNCS, No. 2012, Springer Verlag, 2001, pp. 264-274.
34. Y. Zheng and X. M. Zhang, "New results on correlation immunity," in *Proceedings of 3rd International Conference on Information Security and Cryptography (ICISC 2000)*, LNCS, No. 2015, Springer Verlag, 2000, pp. 49-63.
35. Y. Zheng and X. M. Zhang, "On relationships among propagation degree, nonlinearity and correlation immunity," *Advances in Cryptology – ASIACRYPT '00*, LNCS, No. 1979, Springer Verlag, 2000, pp. 470-482.



Subhamoy Maitra received his Bachelor of Electronics and Telecommunication Engineering degree in the year 1992 from Jadavpur University, Calcutta and Master of Technology in Computer Science in the year 1996 from Indian Statistical Institute, Calcutta. He has completed Ph.D. from Indian Statistical Institute in 2001. Currently he is a faculty at Indian Statistical Institute, Calcutta. His research interest is in Cryptology and Digital Watermarking.