New Results on Correlation Immunity

Yuliang Zheng[1] and Xian-Mo Zhang[2]

[1] Monash University, Frankston, Melbourne, VIC 3199, Australia
yuliang.zheng@monash.edu.au, www.netcomp.monash.edu.au/links/
[2] The University of Wollongong, Wollongong, NSW 2522, Australia
xianmo@cs.uow.edu.au

Abstract. The absolute indicator for GAC forecasts the overall avalanche characteristics of a cryptographic Boolean function. From a security point of view, it is desirable that the absolute indicator of a function takes as small a value as possible. The first contribution of this paper is to prove a tight lower bound on the absolute indicator of an mth-order correlation immune function with n variables, and to show that a function achieves the lower bound if and only if it is affine. The absolute indicator for GAC achieves the upper bound when the underlying function has a non-zero linear structure. Our second contribution is about a relationship between correlation immunity and non-zero linear structures. The third contribution of this paper is to address an open problem related to the upper bound on the nonlinearity of a correlation immune function. More specifically, we prove that given any odd mth-order correlation immune function f with n variables, the nonlinearity of f, denoted by N_f, must satisfy $N_f \leq 2^{n-1} - 2^{m+1}$ for $\frac{1}{2}n - 1 \leq m < 0.6n - 0.4$ or f has a non-zero linear structure. This extends a known result that is stated for $0.6n - 0.4 \leq m \leq n - 2$.

Key Words:

Correlation Immunity, Absolute Indicator, Nonlinearity, Linear Structures, Stream Ciphers

1 Introduction

Correlation immunity has long been recognized as one of the critical indicators of nonlinear combining functions of shift registers in stream generators (see [10]). A high correlation immunity is generally a very desirable property, in view of various successful correlation attacks against a number of stream ciphers (see for instance [5]).

Another class of cryptanalytic attacks against stream ciphers, called best approximation attacks, were advocated in [3]. Success of these attacks in breaking a stream cipher is made possible by exploiting the low nonlinearity of functions employed by the cipher, and it highlights the significance of nonlinearity in the analysis and design of encryption algorithms.

However it should be pointed out that correlation immunity is not harmonious with some other cryptographic requirements. In particular, high correlation immunity may introduce weaknesses in terms of a low algebraic degree, a small avalanche degree and a low nonlinearity and so on. This can be seen, for instance, from recent work in [14, 15].

GAC is a nonlinearity indicator introduced in [11] to study the global or overall avalanche characteristics of a cryptographic function. Two different indicators were proposed to measure numerically the GAC of a functions, namely, the sum-of-squares indicator and the absolute indicator. A small value for the absolute indicator of a function is generally more desirable.

In the first part of this paper we show that functions with a high order correlation immunity necessarily has weaknesses in its avalanche characteristics. More specifically, we prove that if f is a balanced mth-order correlation immune function with n variables, then the absolute indicator for GAC of f, denoted by Δ_f, satisfies $\Delta_f \geq 2^m \sum_{i=0}^{+\infty} 2^{i(m-n)}$. For an unbalanced function f, we show that $\Delta_f \geq 2^{m-1} \sum_{i=0}^{+\infty} 2^{i(m-1-n)}$. We further investigate the tightness of the lower bounds and identify a necessary and sufficient condition on when the two lower bounds are achieved.

When $\Delta_f = 2^n$, f must have a non-zero linear structure, which is considered cryptographically undesirable. In the second part of this paper, we employ correlation immunity to characterize Boolean functions having non-zero linear structures.

Recently, Zheng and Zhang [14] have proved that if f is an mth-order correlation immune function f with n variables, then its nonlinearity satisfies $N_f \leq 2^{n-1} - 2^{m+1}$, when $0.6n - 0.4 \leq m \leq n-2$, regardless of the balance of the function. Note that the inequality $N_f \leq 2^{n-1} - 2^{m+1}$ does not hold for $m = n-1$. Fortunately, this is a trivial case, as an $(n-1)$th-order correlation immune function f with n variables must be affine. In the same paper, Zheng and Zhang have also shown that the equality holds if and only if f is a plateaued function. The authors leave as an open problem for the case of $\frac{1}{2}n - 1 \leq m < 0.6n - 0.4$. This open problem is addressed in the third part of this paper. In particular, we prove that the inequality $N_f \leq 2^{n-1} - 2^{m+1}$ does hold for odd m with $\frac{1}{2}n - 1 \leq m < 0.6n - 0.4$ otherwise f has a non-zero linear structure. This brings us a step closer to finally solving the open problem.

2 Boolean Functions

We consider functions from V_n to $GF(2)$ (or simply functions on V_n), where V_n is the vector space of n tuples of elements from $GF(2)$. The *truth table* of a function f on V_n is a $(0,1)$-sequence defined by $(f(\alpha_0),\ f(\alpha_1), \ldots,\ f(\alpha_{2^n-1}))$, and the *sequence* of f is a $(1,-1)$-sequence defined by $((-1)^{f(\alpha_0)},\ (-1)^{f(\alpha_1)},\ \ldots,\ (-1)^{f(\alpha_{2^n-1})})$, where $\alpha_0 = (0,\ldots,0,0)$, $\alpha_1 = (0,\ldots,0,1)$, $\ldots$, $\alpha_{2^{n-1}-1} = (1,\ldots,1,1)$. The *matrix* of f is a $(1,-1)$-matrix of order 2^n defined by $M = ((-1)^{f(\alpha_i \oplus \alpha_j)})$ where $\oplus$ denotes the addition in $GF(2)$.

Given two sequences $\tilde{a} = (a_1, \cdots, a_m)$ and $\tilde{b} = (b_1, \cdots, b_m)$, their *component-wise product* is defined by $\tilde{a} * \tilde{b} = (a_1 b_1, \cdots, a_m b_m)$. In particular, if $m = 2^n$ and $\tilde{a}$, $\tilde{b}$ are the sequences of functions f and g on V_n respectively, then $\tilde{a} * \tilde{b}$ is the sequence of $f \oplus g$ where $\oplus$ denotes the addition in $GF(2)$.

Let $\tilde{a} = (a_1, \cdots, a_m)$ and $\tilde{b} = (b_1, \cdots, b_m)$ be two sequences or vectors, the *scalar product* of $\tilde{a}$ and $\tilde{b}$, denoted by $\langle \tilde{a}, \tilde{b} \rangle$, is defined as the sum of the component-wise multiplications. In particular, when $\tilde{a}$ and $\tilde{b}$ are from V_m, $\langle \tilde{a}, \tilde{b} \rangle = a_1 b_1 \oplus \cdots \oplus a_m b_m$, where the addition and multiplication are over $GF(2)$, and when $\tilde{a}$ and $\tilde{b}$ are $(1, -1)$-sequences, $\langle \tilde{a}, \tilde{b} \rangle = \sum_{i=1}^{m} a_i b_i$, where the addition and multiplication are over the reals.

An *affine* function f on V_n is a function that takes the form of $f(x_1, \ldots, x_n) = a_1 x_1 \oplus \cdots \oplus a_n x_n \oplus c$, where $a_j, c \in GF(2)$, $j = 1, 2, \ldots, n$. Furthermore f is called a *linear* function if $c = 0$.

A $(1, -1)$-matrix N of order n is called a *Hadamard* matrix if $NN^T = nI_n$, where N^T is the transpose of N and I_n is the identity matrix of order n. A Sylvester-Hadamard matrix of order 2^n, denoted by H_n, is generated by the following recursive relation

$$H_0 = 1, \; H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}, \; n = 1, 2, \ldots.$$

Obviously H_n is symmetric. Let $\ell_i, 0 \leq i \leq 2^n - 1$, be the i row of H_n. It is known that ℓ_i is the sequence of a linear function $\varphi_i(x)$ defined by the scalar product $\varphi_i(x) = \langle \alpha_i, x \rangle$, where α_i is the ith vector in V_n according to the ascending alphabetical order.

The *Hamming weight* of a $(0, 1)$-sequence ξ, denoted by $HW(\xi)$, is the number of ones in the sequence. Given two functions f and g on V_n, the *Hamming distance* $d(f, g)$ between them is defined as the Hamming weight of the truth table of $f(x) \oplus g(x)$, where $x = (x_1, \ldots, x_n)$.

A function f is said to be *balanced* if its truth table contains an equal number of ones and zeros.

3 Cryptographic Criteria of Boolean Functions

The following criteria for cryptographic Boolean functions are often considered: balance, nonlinearity, avalanche criterion, correlation immunity, algebraic degree and non-zero linear structures. In this paper we focus mainly on nonlinearity and correlation immunity.

The so-called Parseval's equation (Page 416 [6]) is a useful tool in this work: Let f be a function on V_n and ξ denote the sequence of f. Then $\sum_{i=0}^{2^n-1} \langle \xi, \ell_i \rangle^2 = 2^{2n}$ where ℓ_i is the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$.

The *nonlinearity* of a function f on V_n, denoted by N_f, is the minimal Hamming distance between f and all affine functions on V_n, i.e.,

$$N_f = \min_{i=1,2,\ldots,2^{n+1}} d(f, \varphi_i)$$

where φ_1, φ_2, ..., $\varphi_{2^{n+1}}$ are all the affine functions on V_n. High nonlinearity is useful in resisting a linear attack and a best approximation attack. The following characterization of nonlinearity will be useful (for a proof see for instance [7]).

Lemma 1. *The nonlinearity of f on V_n can be expressed by*

$$N_f = 2^{n-1} - \frac{1}{2}\max\{|\langle \xi, \ell_i \rangle|, 0 \le i \le 2^n - 1\}$$

where ξ is the sequence of f and ℓ_0, ..., ℓ_{2^n-1} are the rows of H_n, namely, the sequences of linear functions on V_n.

From Lemma 1 and Parseval's equation, it is easy to verify that $N_f \le 2^{n-1} - 2^{\frac{1}{2}n-1}$ for any function f on V_n. If $N_f = 2^{n-1} - 2^{\frac{1}{2}n-1}$, then f is called a *bent function* [8]. It is known that a bent function on V_n exists only when n is even.

Let f be a function on V_n. For a vector $\alpha \in V_n$, denote by $\xi(\alpha)$ the sequence of $f(x \oplus \alpha)$. Thus $\xi(0)$ is the sequence of f itself and $\xi(0) * \xi(\alpha)$ is the sequence of $f(x) \oplus f(x \oplus \alpha)$. Set $\Delta_f(\alpha) = \langle \xi(0), \xi(\alpha) \rangle$, the scalar product of $\xi(0)$ and $\xi(\alpha)$. $\Delta(\alpha)$ is called the auto-correlation of f with a shift α. We omit the subscript of $\Delta_f(\alpha)$ if no confusion occurs. Obviously, $\Delta(\alpha) = 0$ if and only if $f(x) \oplus f(x \oplus \alpha)$ is balanced, i.e., f satisfies the avalanche criterion with respect to α. In the case that f does not satisfy the avalanche criterion with respect to a vector α, it may be desirable for $f(x) \oplus f(x \oplus \alpha)$ to be almost balanced. That is, one may require $|\Delta(\alpha)|$ to be a small value. In an extreme case, $\alpha \in V_n$ is called a *linear structure* of f if $|\Delta(\alpha)| = 2^n$ (i.e., $f(x) \oplus f(x \oplus \alpha)$ is a constant). For any function f, $\Delta(\alpha_0) = 2^n$, where α_0 is the zero vector on V_n. It is easy to verify that the set of all linear structures of a function f form a linear subspace of V_n, whose dimension is called the *linearity of f*, denoted by L_f. A non-zero linear structure is cryptographically undesirable hence we should avoid non-zero linear structures in the design of cryptographic functions as possible as we can. It is also well-known that if f has non-zero linear structures, then there exists a nonsingular $n \times n$ matrix B over $GF(2)$ such that $f(xB) = g(y) \oplus \psi(z)$, where $x = (y, z)$, $y \in V_p$, $z \in V_q$, g is a function on V_p that has no non-zero linear structures, and ψ is a linear function on V_q.

The concept of correlation immune functions was introduced by Siegenthaler [10]. Xiao and Massey gave an equivalent definition [1, 4]: A function f on V_n is called a *mth-order correlation immune function* if

$$\sum_{x \in V_n} f(x)(-1)^{\langle \beta, x \rangle} = 0$$

for all $\beta \in V_n$ with $1 \le HW(\beta) \le m$, where in the the sum, $f(x)$ and $\langle \beta, x \rangle$ are regarded as real-valued functions. From the first equality in Section 4.2 of [1], a correlation immune function can also be equivalently restated as follows: Let f be a function on V_n and let ξ be its sequence. Then f is called a *mth-order correlation immune function* if $\langle \xi, \ell \rangle = 0$ for every ℓ, where ℓ is the sequence of a linear function $\varphi(x) = \langle \alpha, x \rangle$ on V_n constrained by $1 \le HW(\alpha) \le m$. In fact, $\langle \xi, \ell_i \rangle = 0$, where ℓ_i is the ith row of H_n, if and only if $f(x) \oplus \langle \alpha_i, x \rangle$ is

balanced, where α_i is the binary representation of an integer i, $0 \le i \le 2^n - 1$. Correlation immune functions are used in the design of running-key generators in stream ciphers to resist a correlation attack and the design of hash functions. Relevant discussions on correlation immune functions, more generally on resilient functions, can be found in [12].

4 A Tight Lower Bound on the Absolute Indicators of Correlation Immune Functions

Let f be a function on V_n and ξ denote the sequence of f. We introduce two new notations:

1. Set $\Im_f = \{i \mid \langle \xi, \ell_i \rangle \neq 0,\ 0 \le i \le 2^n - 1\}$ where ℓ_i is the ith row of H_n,
2. set $\Im_f^* = \{\alpha_i \mid \langle \xi, \ell_{\alpha_i} \rangle \neq 0,\ 0 \le i \le 2^n - 1\}$ where α_i is the binary representation of an integer i, $0 \le i \le 2^n - 1$ and ℓ_{α_i} is identified with ℓ_i.

$\Im_f^*$ is essentially the same as $\Im_f$ with the only difference being that its elements are represented by a binary vector in V_n. We will simply write $\Im_f$ as $\Im$ and $\Im_f^*$ as $\Im^*$ when no confusion arises. It is easy to verify that $\#\Im_f$ and $\#\Im_f^*$ are invariant under any nonsingular linear transformation on the variables of the function f. $\#\Im_f$ ($\#\Im_f^*$) together with the distribution of $\Im_f$ ($\Im_f^*$) determines the correlation immunity and other cryptographic properties of a function.

Lemma 2. *Let f be a function on V_n, β be a vector in V_n and B be a nonsingular $n \times n$ matrix over $GF(2)$. Then the following statements hold:*

(i) *Set $g(x) = f(xB \oplus \beta)$. Then $\#\Im_g^* = \#\Im_f^*$.*
(ii) *Set $g(x) = f(x \oplus \beta)$. Then $\Im_g^* = \Im_f^*$.*
(iii) *Set $g(x) = f(xB)$. Then $\Im_g^* = \Im_f^* B^T$ where $XB^T = \{\alpha B^T | \alpha \in X\}$.*
(iv) *Set $g(x) = f(x) \oplus \varphi(x)$, where $\varphi(x) = \langle \beta, x \rangle$. Then $\Im_g^* = \beta \oplus \Im_f^*$ where $X = \{\beta \oplus \gamma | \gamma \in X\}$.*

Proof. Since (ii), (iii) and (iv) together imply (i), we prove (ii), (iii) and (iv) only.

(ii) $\alpha \in \Im_g^* \iff g(x) \oplus \langle \alpha, x \rangle$ is unbalanced, i.e., $f(x \oplus \beta) \oplus \langle \alpha, x \rangle$ is unbalanced $\iff f(x \oplus \beta) \oplus \langle \alpha, x \oplus \beta \rangle$ is unbalanced $\iff f(u) \oplus \langle \alpha, u \rangle$ is unbalanced where $u = x \oplus \beta \iff \alpha \in \Im_f^*$. This proves $\Im_g^* = \Im_f^*$.

(iii) $\alpha \in \Im_g^* \iff g(x) \oplus \langle \alpha, x \rangle$ is unbalanced, i.e., $f(xB) \oplus \langle \alpha, x \rangle$ is unbalanced $\iff f(u) \oplus \langle \alpha, uB^{-1} \rangle$ is unbalanced where $xB = u$. Note that $\langle \alpha, uB^{-1} \rangle = (uB^{-1})\alpha^T = u(B^{-1}\alpha^T) = (B^{-1}\alpha^T)^T u^T = \alpha (B^T)^{-1} u^T = \langle \alpha (B^T)^{-1}, u \rangle$. Therefore $f(u) \oplus \langle \alpha, uB^{-1} \rangle$ is unbalanced $\iff f(u) \oplus \langle \alpha (B^T)^{-1}, u \rangle$ is unbalanced $\iff \alpha (B^T)^{-1} \in \Im_f^* \iff \alpha \in \Im_f^* B^T$. This proves $\Im_g^* = \Im_f^* B^T$.

(iv) $\alpha \in \Im_g^* \iff g(x) \oplus \langle \alpha, x \rangle$ is unbalanced, i.e., $f(x) \oplus \langle \beta, x \rangle \oplus \langle \alpha, x \rangle$ is unbalanced $\iff f(x) \oplus \langle \beta \oplus \alpha, x \rangle$ is unbalanced $\iff \beta \oplus \alpha \in \Im_f^* \iff \alpha \in \beta \oplus \Im_f^*$. This proves $\Im_g^* = \beta \oplus \Im_f^*$.

The following definition is from [11].

Definition 1. *For a function f on V_n, the* absolute indicator *for GAC of f is defined as*

$$\Delta_f = \max_{\alpha \in V_n, \alpha \neq 0} |\Delta(\alpha)|$$

Obviously $\Delta_f = 2^n$ if and only if f has a non-zero linear structure, while $\Delta_f = 0$ if and only if f is bent. Since balanced functions are not bent, we have $\Delta_f > 0$ where f is balanced. In designing cryptographic algorithms, we are concerned with a balanced nonlinear function f that shows a small Δ_f, as was discussed in [11] where it was argued that a smaller Δ_f is cryptographically more desirable. This section shows that a high order of correlation immunity may result in weaknesses in avalanche characteristics.

The following lemma is the re-statement of a relation proved in Section 2 of [2].

Lemma 3. *For every function f on V_n, we have*

$$(\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1}))H_n = (\langle \xi, \ell_0 \rangle^2, \langle \xi, \ell_1 \rangle^2, \ldots, \langle \xi, \ell_{2^n-1} \rangle^2).$$

where ξ denotes the sequence of f and ℓ_i is the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$.

From [14], we have the following statement.

Lemma 4. *Consider a function f on V_n. Let $\xi = (a_0, a_1, \ldots, a_{2^n-1})$, where $a_j = \pm 1$ denote the sequence of f and ℓ_i denote the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$. Let p be an integer with $1 \leq p \leq n-1$. Write $\xi = (\xi_0, \xi_1, \ldots, \xi_{2^p-1})$ where each ξ_i is of length 2^{n-p}. Let e_i denote the ith row of H_{n-p}, $i = 0, 1, \ldots, 2^{n-p} - 1$.*

$$\begin{aligned} &2^p(\langle \xi_0, e_j \rangle, \langle \xi_1, e_j \rangle, \langle \xi_2, e_j \rangle, \ldots, \langle \xi_{2^p-1}, e_j \rangle) \\ &= (\langle \xi, \ell_j \rangle, \langle \xi, \ell_{j+2^{n-p}} \rangle, \langle \xi, \ell_{j+2 \cdot 2^{n-p}} \rangle, \ldots, \langle \xi, \ell_{j+(2^p-1)2^{n-p}} \rangle) H_p \end{aligned}$$

where $j = 0, 1, \ldots, 2^{n-p} - 1$.

The following lemma is useful in proving one of our main theorems.

Lemma 5. *Let $(k_0, k_1, \ldots, k_{2^n-1})H_n = (r_0, r_1, \ldots, r_{2^n-1})$, where $k_0 = 0$ and each k_j and each r_j are both real numbers. Then*

$$\max\{|r_1|, \ldots, |r_{2^n-1}|\} \geq \max\{|k_1|, \ldots, |k_{2^n-1}|\}$$

Proof. Without loss of generality, we assume that $|k_{2^{n-1}}| = \max\{|k_1|, \ldots, |k_{2^n-1}|\}$. Let $H_n = [P \ Q]$ where both P and Q are $2^n \times 2^{n-1}$ matrices. Hence we have $(k_0, k_1, \ldots, k_{2^n-1})Q = (r_{2^{n-1}}, r_{2^{n-1}+1}, \ldots, r_{2^n-1})$. Let e_0 denote the all-one sequence of length 2^{n-1}. It is obvious that

$$(k_0, k_1, \ldots, k_{2^n-1})Qe_0^T = (r_{2^{n-1}}, r_{2^{n-1}+1}, \ldots, r_{2^n-1})e_0^T \tag{1}$$

Note that $Q = \begin{bmatrix} H_{n-1} \\ -H_{n-1} \end{bmatrix}$ and hence we have $Qe_0^T = 2^{n-1}(b_0, b_1, \ldots, b_{2^n-1})^T$ where $(b_0, b_1, \ldots, b_{2^n-1})$ satisfies $b_0 = 1$, $b_{2^{n-1}} = -1$ and other $b_j = 0$. Due to (1), we have $2^{n-1}(k_0 - k_{2^{n-1}}) = \sum_{j=2^{n-1}}^{2^n-1} r_j$, where $k_0 = 0$. This proves that there exits some i_0, $2^{n-1} \leq i_0 \leq 2^n - 1$, such that $|r_{i_0}| \geq |k_{2^{n-1}}|$. Thus the lemma holds. □

We notice that $\max\{|r_0|, |r_1|, \ldots, |r_{2^n-1}|\} \geq \max\{|k_0|, |k_1|, \ldots, |k_{2^n-1}|\}$ is still true. However this inequality is less useful in this paper as $\Delta(\alpha_0) = 2^n$ holds for every function on V_n, and we are concerned with Δ_f where $\Delta_f = \max_{\alpha \in V_n, \alpha \neq 0} |\Delta(\alpha)|$.

Theorem 1. *Let f be a function on V_n. Then the following statements hold:*

(i) If there exist an m-dimensional linear subspace W, $1 \leq m \leq n-1$, and a vector α^* in V_n such that $\Im_f^* \cap (\alpha^* \oplus W) = \emptyset$ where $\emptyset$ denotes the empty set, then

$$\Delta_f \geq 2^m \sum_{i=0}^{+\infty} 2^{i(m-n)} \tag{2}$$

(ii) Under the assumption of (i), the following three statements are equivalent:
(a) $\Delta_f = 2^m \sum_{i=0}^{+\infty} 2^{i(m-n)}$,
(b) $m = n-1$,
(c) f has a non-zero linear structure.

Proof. First we prove (i). Due to Lemma 2, we can assume, without loss of generality, that $\alpha^* = \alpha_0$, where α_0 denotes the zero vector in V_n, and $W = \{\alpha_0, \alpha_1, \ldots, \alpha_{2^m-1}\}$. Let ξ denote the sequence of f and ℓ_i be the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$. Since $\Im_f^* \cap W = \emptyset$, we have $\langle \xi, \ell_i \rangle = 0$, $i = 0, 1, \ldots, 2^m - 1$. Due to Lemma 3, we have

$$(\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1}))H_n = (0, \ldots, 0, \langle \xi, \ell_{2^m} \rangle^2, \ldots, \langle \xi, \ell_{2^n-1} \rangle^2)$$

or

$$(0, \ldots, 0, \langle \xi, \ell_{2^m} \rangle^2, \ldots, \langle \xi, \ell_{2^n-1} \rangle^2)H_n = 2^n(\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1})) \tag{3}$$

Applying Lemma (4) (with $p = n - m$ and $j = 0$) to Equation (3), we obtain

$$\begin{aligned}(0, &\sum_{j=2^m}^{2\cdot 2^m-1} \langle \xi, \ell_j \rangle^2, \ldots, \sum_{j=2^n-2^m}^{2^n-1} \langle \xi, \ell_j \rangle^2)H_{n-m} \\ &= 2^n(\Delta(\alpha_0), \Delta(\alpha_{2^m}), \Delta(\alpha_{2\cdot 2^m}), \ldots, \Delta(\alpha_{(2^{n-m}-1)\cdot 2^m})\end{aligned} \tag{4}$$

Applying Parseval's equation to f, we have $\sum_{i=1}^{2^{n-m}-1} \sum_{j=i\cdot 2^m}^{(i+1)\cdot 2^m-1} \langle \xi, \ell_j \rangle^2 = 2^{2n}$. It is easy to see that there exists some i_0, $1 \leq i_0 \leq 2^{n-m} - 1$, such that

$$\sum_{j=i_0\cdot 2^m}^{(i_0+1)\cdot 2^m-1} \langle \xi, \ell_j \rangle^2 \geq \frac{2^{2n}}{2^{n-m}-1} = 2^{n+m} \sum_{i=0}^{+\infty} 2^{i(m-n)}$$

Applying Lemma 5 to (4), we conclude that there exists some j_0, $1 \leq j_0 \leq 2^{n-m} - 1$, such that

$$2^n |\Delta(\alpha_{j_0\cdot 2^m})| \geq 2^{n+m} \sum_{i=0}^{+\infty} 2^{i(m-n)}$$

This proves that $\Delta_f \geq 2^m \sum_{i=0}^{+\infty} 2^{i(m-n)}$ and hence (i) holds. Next we prove (ii).

First we prove (a) $\Longleftrightarrow$ (b). Assume that (a) holds, i.e., $\Delta_f = 2^m \sum_{i=0}^{+\infty} 2^{i(m-n)}$, or equivalently, $\Delta_f = 2^m \sum_{i=0}^{+\infty} 2^{i(m-n)} = \frac{2^n}{2^{n-m}-1}$. Therefore $\frac{2^n}{2^{n-m}-1}$ must be an integer. Since 2^n is not divisible by $2^{n-m}-1$ if $n-m \geq 2$, we conclude that $m = n-1$, i.e., (b) holds. Conversely, assume that (b) holds, i.e., $m = n-1$. In this case, by using (i) of the theorem, we have $\Delta_f \geq 2^m \sum_{i=0}^{+\infty} 2^{i(m-n)} = \frac{2^n}{2^{n-m}-1} = 2^n$. Hence $\Delta_f = 2^n$, i.e., (a) holds.

We now prove (b) $\Longleftrightarrow$ (c). Assume that (b) holds, i.e., $m = n-1$. In this case, by using (i) of the theorem, we have $\Delta_f \geq 2^m \sum_{i=0}^{+\infty} 2^{i(m-n)} = \frac{2^n}{2^{n-m}-1} = 2^n$. Hence $\Delta_f = 2^n$. This means that f has a non-zero linear structure and hence (c) holds. Conversely, assume that (c) holds, i.e., f has a non-zero linear structure. Due to Lemma 2, without loss of generality, assume that $\alpha_{2^{n-1}}$ is a non-zero linear structure. Hence we can write f as $f(x) = cx_1 \oplus g(y)$ where g is a function on V_{n-1}, $x = (x_1, \ldots, x_n)$, $y = (x_2, \ldots, x_n)$ and c is a constant in $GF(2)$. Once again, due to Lemma 2, without loss of generality, assume that $c = 0$. Let η denote the sequence of g. Then the sequence ξ of f can be denoted as $\xi = (\eta, \eta)$. It is easy to verify that $\langle \xi, \ell_i \rangle = 0$ where ℓ_i is the ith row of H_n, $i = 0, 1, \ldots, 2^{n-1}-1$. This proves that $\Im_f^* \cap W = \emptyset$ where W is specialized as an $(n-1)$-dimensional subspace, that is, $W = \{\alpha_0, \alpha_1, \ldots, 2^{n-1}-1\}$. This proves that $m = n-1$ and hence (b) holds. □

From the definition of correlation immune functions [1, 4], if f is a balanced mth-order correlation immune functions, then $m \leq n-1$, and a function on V_n is $(n-1)$th-order correlation immune if and only if $f(x) = x_1 \oplus \cdots \oplus x_n \oplus c$ where $x = (x_1, \ldots, x_n)$ and c is a constant in $GF(2)$. Using Theorem 1, we obtain

Theorem 2. *Let f be a balanced mth-order correlation immune function on V_n $(1 \leq m \leq n-1)$. Then*

$$\Delta_f \geq 2^m \sum_{i=0}^{+\infty} 2^{i(m-n)}$$

where the equality holds if and only if $f(x) = x_1 \oplus \cdots \oplus x_n \oplus c$ where $x = (x_1, \ldots, x_n)$ and c is a constant in $GF(2)$.

Let f be a function on V_n whose sequence is ξ. Assume that f satisfies $\langle \xi, \ell_i \rangle = 0$ for every $i = 1, \ldots, 2^n - 1$, or equivalently, $f(x) \oplus \langle \alpha, x \rangle$ is balanced for every non-zero vector in V_n. It is easy to verify that f must be a constant in $GF(2)$. For this reason, we define the zero function on V_n and the non-zero constant function on V_n as an *nth-order correlation immune function* on V_n.

Theorem 3. *Let f be an unbalanced mth-order correlation immune function on V_n $(2 \leq m \leq n)$. Then*

$$\Delta_f \geq 2^{m-1} \sum_{i=0}^{+\infty} 2^{i(m-1-n)}$$

where the equality holds if and only if f is a constant. (Note that an nth-order correlation immune function is defined as a constant).

Proof. Let $\beta \in V_n$ and $HW(\beta) = m$. Set $\psi(x) = \langle \beta, x \rangle$ and $g = f \oplus \psi$. It is easy to see that g is a balanced $(m-1)$th-order correlation immune function on V_n. Due to Theorem 2, the statement holds. □

Theorems 2 and 3 indicate that correlation immunity is not harmonious with avalanche characteristics.

5 A Relationship between Correlation Immunity and Linear Structures

In this section, we consider the case when the absolute indicator for SAC achieves the maximum value i.e., $\Delta_f = 2^n$.

Theorem 4. *Let f be a function on V_n. If there exist a p-dimensional linear subspace W with $1 \le p \le n-1$ and a vector α in V_n such that $\Im_f^* \subseteq \alpha \oplus W$ if and only if f has a non-zero linear structure.*

Proof. We first prove the necessity. Since the existence of non-zero linear structures is invariant under a nonsingular linear transformation on the variables, without loss of generality, we can assume $W = \{(a_1, \ldots, a_p, 0, \ldots, 0) | (a_1, \ldots, a_p, 0, \ldots, 0) \in V_n\}$. In other words, $W = \{\alpha_0, \alpha_{2^{n-p}}, \alpha_{2 \cdot 2^{n-p}}, \ldots, \alpha_{(2^p-1) \cdot 2^{n-p}}\}$, where each $\alpha_j \in V_n$ and α_j is the binary representation of an integer j. Let $W^* = \{(0, \ldots, 0, c_1, \ldots, c_{n-p}) \ | (0, \ldots, 0, c_1, \ldots, c_{n-p}) \in V_n\}$. In other words, $W^* = \{\alpha_0, \alpha_1, \ldots, \alpha_{2^{n-p}-1}\}$, where each $\alpha_j \in V_n$ is the binary representation of an integer j, $j = 0, 1, \ldots, 2^{n-p}$, and

$$V_n = (\alpha_0 \oplus W) \cup (\alpha_1 \oplus W) \cup \cdots \cup (\alpha_{2^{n-s}-1} \oplus W)$$

where $(\alpha_j \oplus W) \cap (\alpha_i \oplus W) = \emptyset$ whenever $j \neq i$.

Since $\Im_f^* \subseteq \alpha_{j_0} \oplus W$ for some j_0, $0 \le j_0 \le 2^{n-p} - 1$, $\langle \xi, \ell_i \rangle = 0$ if $\alpha_i \in \alpha_j \oplus W$ with $j \neq \jmath_0$, where α_i is the representation of an integer i. Note that $\alpha_i \in \alpha_j \oplus W$ if and only if $i \in \{j, \ j + 2^{n-p}, \ldots, j + (2^p - 1)2^{n-p}\}$. By using Lemma 4, we have

$$\begin{aligned} &(\langle \xi_0, e_i \rangle), \langle \xi_1, e_i \rangle), \ldots, \langle \xi_{2^p-1}, e_i \rangle) H_p \\ &= (\langle \xi, \ell_i \rangle, \langle \xi, \ell_{i+2^{n-p}} \rangle, \ldots, \langle \xi, \ell_{i+(2^p-1)2^{n-p}} \rangle) = (0, 0, \ldots, 0) \end{aligned}$$

whenever $i \neq j_0$. Therefore

$$(\langle \xi_0, e_i \rangle, \langle \xi_1, e_i \rangle, \ldots, \langle \xi_{2^p-1}, e_i \rangle) = (0, 0, \ldots, 0) \tag{5}$$

whenever $i \neq j_0$. Since $\langle \xi_0, e_i \rangle = 0$, whenever $i \neq j_0$, we conclude $\xi_0 = b_0 e_{j_0}$ where $b_0 = \pm 1$. Similarly $\xi_1 = b_1 e_{j_0}$ where $b_1 = \pm 1$, ..., $\xi_{2^p-1} = b_{2^p-1} e_{j_0}$ where $b_{2^p-1} = \pm 1$. Therefore the sequence of f, ξ, satisfies

$$\xi = (b_0 e_{j_0}, b_1 e_{j_0}, \ldots, b_{2^p-1} e_{j_0}) \tag{6}$$

Since e_{j_0} is a row of H_{n-p}, e_{j_0} is the sequence of a linear function on V_{n-p}, denoted by ψ. Let $(b_0, b_1, \ldots, b_{2^p-1})$ be the sequence of a function on V_p, denoted by g. Due to (6), f can be expressed as $f(x) = g(y) \oplus \psi(z)$ where $x = (y, z)$, $y \in V_p$, $z \in V_{n-p}$. This proves that f has a non-zero linear structure.

Conversely, assume that f has a non-zero linear structure. Then f is equivalent to $g(x) = cx_1 \oplus h(y)$ under a nonsingular linear transformation on the variables, where h is a function on V_{n-1}, $x = (x_1, \ldots, x_n)$ and $y = (x_2, \ldots, x_n)$. Without loss of generality, assume that $c = 0$. Let ξ' denote the sequence of g and η denote the sequence of h. Then $\xi' = (\eta, \eta)$. Obviously, if ℓ_i satisfies $\ell_i = (e, -e)$, where ℓ_i denotes the ith row of H_n and e is a row of H_{n-1}, we have $\langle \xi', \ell_i \rangle = 0$. Therefore if $\langle \xi', \ell_j \rangle \neq 0$ then ℓ_j must take the form of $\ell_j = (e, e)$. Due to the structure of H_n, j satisfies $0 \leq j \leq 2^{n-1} - 1$. This proves that $\Im_g \subseteq \{0, 1, \ldots, 2^{n-1} - 1\}$, equivalently, $\Im_g^* \subseteq W = \{\alpha_0, \alpha_1, \ldots, \alpha_{2^{n-1}-1}\}$, where W obviously is an $(n-1)$-dimensional subspace of V_n. Since the linearity is invariant under any nonsingular linear transformation on the variables, we have the same conclusion on $\Im_f^*$. Thus we have proved the sufficiency. □

Theorem 4 can be viewed as a way of characterizing Boolean functions having non-zero linear structures by the use of correlation immunity. This result will be used in the next section.

6 A New Result on Upper Bound on Nonlinearity of Correlation Immune Functions

6.1 Previously Known Results

Recently Zheng and Zhang proved that when $0.6n - 0.4 \leq m \leq n - 2$, the nonlinearity N_f of an mth-order correlation immune function f with n variables satisfies the condition of $N_f \leq 2^{n-1} - 2^{m+1}$. In the same paper they also showed that if a correlation immune function achieves the maximum nonlinearity for such a function, then it is a *plateaued function*.

The concept of plateaued functions was introduced in [13]. Let f be a function on V_n and ξ denote the sequence of f. If there exists an even number r, $0 \leq r \leq n$, such that $\#\Im = 2^r$ and each $\langle \xi, \ell_j \rangle^2$ takes the value of 2^{2n-r} or 0 only, where ℓ_j denotes the jth row of H_n, $j = 0, 1, \ldots, 2^n - 1$, then f is called a *rth-order plateaued function* on V_n. f is also simply called a *plateaued function* on V_n if we ignore the particular order r. Some facts about plateaued functions follow: if f is a rth-order plateaued function, then r must be even; f is an nth-order plateaued function if and only if f is bent: and f is a 0th-order plateaued function if and only if f is affine. Plateaued functions are interesting as they have a number of cryptographically useful properties [13]. For instance: $\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) \geq \frac{2^{3n}}{\#\Im}$ where the equality holds if and only if f is a plateaued function.

We now introduce a main result in [14].

Theorem 5. *Let f be an mth-order correlation immune function on V_n. If m and n satisfy the condition of $0.6n - 0.4 \leq m \leq n - 2$, then $N_f \leq 2^{n-1} - 2^{m+1}$,*

where the equality holds if and only if f is also a $2(n-m-2)$th-order plateaued function.

Note that Theorem 5 is an improvement on Sarkar and Maitra's upper bound [9], $N_f \leq 2^{n-1} - 2^m$ when $m > \frac{1}{2}n - 1$.

The following result was given by Sarkar and Maitra [9].

Theorem 6. *Let f be an mth-order correlation immune function on V_n, where $m \leq n-2$. Then $\langle \xi, \ell \rangle \equiv 0 \pmod{2^{m+1}}$ where ℓ is any row of H_n. In particular, if f is balanced mth-order correlation immune, then $\langle \xi, \ell \rangle \equiv 0 \pmod{2^{m+2}}$.*

The following two Lemmas can be found from [14].

6.2 A New Result

Lemma 4 can be generalized. Let f be a function on V_n and W be a p-dimensional subspace of V_n. Let $U = \{0, \alpha_{2^{n-p}}, \alpha_{2 \cdot 2^{n-p}}, \ldots, \alpha_{(2^p-1)2^{n-p}}\}$. Since both W and U are p-dimensional subspaces of V_n, we can find an $n \times n$ matrix B over $GF(2)$ satisfying $WB^T = U$, where $WB^T = \{\alpha B^T | \alpha \in W\}$. Set $x = uB$ and $g(u) = f(uB)$. Consider $f(x) \oplus \langle \alpha, x \rangle$ where $\alpha \in W$. Note that $\langle \alpha, x \rangle = x\alpha^T = uB\alpha^T = u(\alpha B^T)^T = \langle \alpha B^T, u \rangle$. Therefore $f(x) \oplus \langle \alpha, x \rangle = g(u) \oplus \langle \alpha B^T, u \rangle$ where $\alpha \in W$ and $\alpha B^T \in U$. Let η denote the sequence of g. Equivalently, we have $\langle \xi, \ell_j \rangle = \langle \eta, \ell_i \rangle$ where j is the binary representation of $\alpha \in W$, and i is the binary representation of $\alpha B^T \in U$.

Define a permutation π on $\{0, 1, \ldots, 2^n - 1\}$ as follows: $\pi(j) = i$ if $\alpha_j B^T = \alpha_i$, where i and j are the the binary representations of α_i and α_j respectively. Therefore

$$\langle \xi, \ell_j \rangle = \langle \eta, \ell_{\pi(j)} \rangle \text{ or } \langle \xi, \ell_{\pi^{-1}(j)} \rangle = \langle \eta, \ell_j \rangle \tag{7}$$

Rewrite $\eta = (\eta_0, \eta_1, \ldots, \eta_{2^p-1})$ where each η_i is of length 2^{n-p}. Applying Lemma 4 to the function g and the subspace U, we have

$$\begin{aligned} &2^p(\langle \eta_0, e_j \rangle, \langle \eta_1, e_j \rangle, \langle \eta_2, e_j \rangle, \ldots, \langle \eta_{2^p-1}, e_j \rangle) \\ &= (\langle \eta, \ell_j \rangle, \langle \eta, \ell_{j+2^{n-p}} \rangle, \ldots, \langle \eta, \ell_{j+(2^p-1)2^{n-p}} \rangle) H_p \end{aligned}$$

where e_j denotes the jth row of H_p, $j = 0, 1, \ldots, 2^{n-p} - 1$. Due to (7), we obtain

$$\begin{aligned} &2^p(\langle \eta_0, e_j \rangle, \langle \eta_1, e_j \rangle, \langle \eta_2, e_j \rangle, \ldots, \langle \eta_{2^p-1}, e_j \rangle) \\ &= (\langle \xi, \ell_{\pi^{-1}(j)} \rangle, \langle \xi, \ell_{\pi^{-1}(j+2^{n-p})} \rangle, \ldots, \langle \xi, \ell_{\pi^{-1}(j+(2^p-1)2^{n-p})} \rangle) H_p \end{aligned} \tag{8}$$

where e_j denotes the jth row of H_p, $j = 0, 1, \ldots, 2^{n-p} - 1$.

Lemma 6. *Let f be a function on V_n and ξ denote the sequence of f. Let q be an odd number with $1 \leq q \leq n-2$, such that*

$$\langle \xi, \ell_j \rangle = 0 \text{ for all } j \text{ such that } HW(\alpha_j) \leq q \text{ and } HW(\alpha_j) \text{ is odd}$$

where $\alpha_j \in V_n$ is the binary representation of integer j. Then $\langle \xi, \ell_j \rangle \equiv 0 \pmod{2^{q+2}}$ holds for all j with $HW(\alpha_j) = q + 2$ where $\alpha_j \in V_n$ is the binary representation of an integer j.

Proof. Let $U = \{0, \alpha_{2^{n-q-1}}, \alpha_{2.2^{n-q-1}}, \ldots, \alpha_{(2^{q+1}-1)2^{n-q-1}}\}$. Obviously U can be rewritten as $U = \{(a_1, a_2, \ldots, a_{q+1}, 0, \ldots, 0) | (a_1, a_2 \ldots, a_{q+1}, 0, \ldots, 0) \in V_n\}$.

Set

$$W = \{(a_1, a_2, \ldots, a_{q+2}, 0, \ldots, 0) | (a_1, a_2 \ldots, a_{q+2}, 0, \ldots, 0) \in V_n, \\ HW(a_1, a_2, \ldots, a_{q+2}) \text{ is even}\}$$

Since both U and W are $(q+1)$-dimensional subspaces of V_n, there exists an $n \times n$ matrix B over $GF(2)$ satisfying

(i) $WB^T = U$, where $WB^T = \{\alpha B^T | \alpha \in W\}$, in particular, we require $\alpha_{(2^{q+1}-1)2^{n-q-1}} B^T = \alpha_{(2^{q+1}-1)2^{n-q-1}}$,
(ii) $\alpha_j B^T = \alpha_j$, $j = 1, \ldots, 2^{n-q-1} - 1$.

Set $x = uB$ and $g(u) = f(uB)$. Let $\eta = (\eta_0, \eta_1, \ldots, \eta_{2^{n-q-1}-1})$ denote the sequence of g, where each η_i is of length 2^{n-q-1}. Obviously $HW(\alpha)$ is even for any $\alpha \in W$, i.e., $HW(\alpha)$ takes the values, $0, 2, 4, \ldots, q-1, q+1$. Therefore $HW(\alpha_{2^{n-q-2}} \oplus \alpha)$ must be odd, i.e., $HW(\alpha)$ takes the values, $1, 3, 5, \ldots, q, q+2$. Note that $\alpha_{(2^{q+1}-1)2^{n-q-1}} = (1, \ldots, 1, 0, \ldots, 0)$ and $HW(\alpha_{2^n - 2^{n-q-1}}) = q+1$. Obviously, $\alpha_{2^{n-q-2}} \oplus \alpha_{(2^{q+1}-1)2^{n-q-1}} = (1, \ldots, 1, 1, 0, \ldots, 0) = \alpha_{(2^{q+2}-1)2^{n-q-2}}$. Note that $HW(\alpha_{(2^{q+2}-1)2^{n-q-2}}) = q+2$, and for any other $\alpha \in W$ with $\alpha \neq \alpha_{(2^{q+1}-1)2^{n-q-1}}$, we have $1 \leq HW(\alpha_{2^{n-q-2}} \oplus \alpha) \leq q$. Due to the property of f, $\langle \xi, \ell_j \rangle = 0$ for all j, where j is the integer representation of $\alpha_{2^{n-q-2}} \oplus \alpha$, if $\alpha \in W$ and $\alpha \neq \alpha_{(2^{q+1}-1)2^{n-q-1}}$, From the properties of B, $(\alpha_{2^{n-q-2}} \oplus \alpha_j)B^T = \alpha_{2^{n-q-2}} \oplus \alpha_j B^T$ for all $\alpha_j \in W$. In particular, $(\alpha_{2^{n-q-2}} \oplus \alpha_{(2^{q+1}-1)2^{n-q-1}})B^T = \alpha_{2^{n-q-2}} \oplus \alpha_{(2^{q+1}-1)2^{n-q-1}}$.

Using (8) with $j = 1$, we have

$$2^{q+1}(\langle \eta_0, e_1 \rangle, \langle \eta_1, e_1 \rangle, \langle \eta_2, e_1 \rangle, \ldots, \langle \eta_{2^{q+1}-1}, e_1 \rangle) \\ = (0, \ldots, 0, \langle \xi, \ell_{(2^{q+1}-1)2^{n-q-1}} \rangle) H_{q+1} \qquad (9)$$

Since $2^{n-q-1} \geq 2$, $\langle \eta_{2^{q+1}-1}, e_1 \rangle$ is even. Comparing the rightmost term in both sides of (9), we conclude that $\langle \xi, \ell_{(2^{q+1}-1)2^{n-q-1}} \rangle \equiv 0 \pmod{2^{q+2}}$. By the same reasoning, we can prove that $\langle \xi, \ell_j \rangle \equiv 0 \pmod{2^{q+2}}$ holds for all j with $HW(\alpha_j) = q+2$. □

Lemma 7. *Let f be a function on V_n and ξ denote the sequence of f. Let q be an odd number with $1 \leq q \leq n-2$, such that*

$$\langle \xi, \ell_j \rangle = 0 \text{ for all } j \text{ such that } HW(\alpha_j) \text{ is odd and } HW(\alpha_j) \leq q$$

where $\alpha_j \in V_n$ is the binary representation of integer j. Then either there exists some j_0 such that $|\langle \xi, \ell_{j_0} \rangle| \geq 2^{q+2}$, or $\langle \xi, \ell_j \rangle = 0$ for all j where $HW(\alpha_j)$ is odd.

Proof. By using Lemma 6, $\langle \xi, \ell_j \rangle \equiv 0 \pmod{2^{q+2}}$ holds for all j with $HW(\alpha_j) = q+2$ where $\alpha_j \in V_n$. There exist two cases to be considered.

Case 1: there exists some j_0 with $HW(\alpha_{j_0}) = q+2$ satisfying $\langle \xi, \ell_{j_0} \rangle \neq 0$. In this case we have $|\langle \xi, \ell_{j_0} \rangle| \geq 2^{q+2}$. Thus the lemma holds.

Case 2: $\langle \xi, \ell_j \rangle = 0$ holds for all j with $HW(\alpha_j) = q+2$ where $\alpha_j \in V_n$. In this case, we conclude that $\langle \xi, \ell_j \rangle = 0$ holds for all j such that $HW(\alpha_j) \leq q+2$ and $HW(\alpha_j)$ is odd.

Once again we use Lemma 6. There exist two cases to be considered.

Case 2.1: we have an integer $t > 1$ such that $\langle \xi, \ell_j \rangle = 0$ for all j where $HW(\alpha_j) \leq q + 2(t-1)$ and $HW(\alpha_j)$ is odd, and there also exists j_0 with $HW(\alpha_{j_0}) = q + 2t$ satisfying $\langle \xi, \ell_{j_0} \rangle \neq 0$. By using Lemma 6, we can conclude that $|\langle \xi, \ell_{j_0} \rangle| \geq 2^{q+2t}$. Thus the lemma holds in Case 2.1.

Case 2.2: $\langle \xi, \ell_j \rangle = 0$ for all j where $HW(\alpha_j)$ is odd. Clearly the lemma holds. □

Applying Lemma 7, we can extend Theorem 5 in the following way.

Theorem 7. *Let f be an odd mth-order correlation immune function on V_n. Then either $N_f \leq 2^{n-1} - 2^{m+1}$ holds for $\frac{1}{2}n - 1 \leq m < 0.6n - 0.4$ or f has a non-zero linear structure.*

Proof. If f is balanced, $N_f \leq 2^{n-1} - 2^{m+1}$ holds due to Theorem [9]. Thus we only need to consider the unbalanced case. From Lemma 7, there there two cases to be considered. Case 1: there exists some j_0 such that $|\langle \xi, \ell_{j_0} \rangle| \geq 2^{m+2}$. In this case, we have proved the theorem by using Lemma 1. Case 2: $\langle \xi, \ell_j \rangle = 0$ for all j where $HW(\alpha_j)$ is odd. Set $W = \{\alpha | \alpha \in V_n, \ HW(\alpha) \text{ is even}\}$. Thus W is an $(n-1)$-dimensional subspace of V_n. From the property of f, obviously, $\Im^* \subseteq W$. From Theorem 4, f has a non-zero liear structure. □

Note that the nonlinearity of any Boolean function on V_n is upper-bounded by $2^{n-1} - 2^{\frac{1}{2}n-1}$. For $m \leq \frac{1}{2}n - 2$, we have $2^{n-1} - 2^{\frac{1}{2}n-1} \leq 2^{n-1} - 2^{m+1}$. Hence the inequality $N_f \leq 2^{n-1} - 2^{m+1}$ is trivial when $m \leq \frac{1}{2}n - 2$, although it still holds. For this reason, we require that $m \geq \frac{1}{2}n - 1$ in Theorem 7.

Theorem 7 represents an extension of Theorem 5. The latter is stated for the case of $0.6n - 0.4 \leq m \leq n - 2$.

7 Conclusion Remarks

This paper includes three main results. (1) We have presented a tight lower bound on the absolute indicator for GAC of an mth-order correlation immune function on V_n, and proved that a correlation immune function achieves the low bound for the absolute indicator if and only if it is affine. (2) We have established a relationship between correlation immunity and non-zero linear structures. (3) We have shown that given an odd mth-order correlation immune function f on V_n, the nonlinearity N_f of f satisfies $N_f \leq 2^{n-1} - 2^{m+1}$ for $\frac{1}{2}n - 1 \leq m < 0.6n - 0.4$ otherwise f has a non-zero linear structure. This is an extension of a known result that holds for $0.6n - 0.4 \leq m \leq n - 2$. It would be interesting to known whether or not Theorem 7 can be extended to the case of an even m.

Some observations on upper bounds on nonlinearity for a "small" m were made by Sarkar and Maitra in [9]. For instance, they showed that $N_f \leq 2^{n-1} -$

$2^{\frac{1}{2}n-1} - 2^m$ when n is even and $m \leq \frac{1}{2}n - 1$, and $N_f \leq 2^{n-1} - 2^{\frac{1}{2}n-1} - 2^{m+1}$ when f is balanced, n is even and $m \leq \frac{1}{2}n - 1$. It is not clear whether these bounds are tight.

Acknowledgment

The second author was supported by a Queen Elizabeth II Fellowship (227 23 1002). Both authors would like to thank Yuriy Tarannikov and Subhamoy Maitra for pointing out an error in an earlier version.

References

1. P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation-immune functions. In *Advances in Cryptology - CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 87–100. Springer-Verlag, Berlin, Heidelberg, New York, 1991.
2. Claude Carlet. Partially-bent functions. *Designs, Codes and Cryptography*, 3:135–145, 1993.
3. C. Ding, G. Xiao, and W. Shan. *The Stability Theory of Stream Ciphers*, volume 561 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Heidelberg, New York, 1991.
4. Xiao Guo-Zhen and J. L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Transactions on Information Theory*, 34(3):569–571, 1988.
5. M. Hermelin and K. Nyberg. Correlation properties of the bluetooth combiner generator. In *The 2nd International Conference on Information Security and Cryptology (ICISC'99), Seoul, Korea*, volume 1787 of *Lecture Notes in Computer Science*, pages 17–29. Springer-Verlag, Berlin, Heidelberg, New York, 1999.
6. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, New York, Oxford, 1978.
7. W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology - EUROCRYPT'89*, volume 434 of *Lecture Notes in Computer Science*, pages 549–562. Springer-Verlag, Berlin, Heidelberg, New York, 1990.
8. O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.
9. P. Sarkar and S. Maitra. Nonlinearity bounds and constructions of resilient boolean functions. In *Advances in Cryptology - CRYPTO2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 515–532. Springer-Verlag, Berlin, Heidelberg, New York, 2000.
10. T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30 No. 5:776–779, 1984.
11. 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. (`http://www.jucs.org/`).
12. X. M. Zhang and Y. Zheng. Cryptographically resilient functions. *IEEE Transactions on Information Theory*, 43(5):1740–1747, 1997.

13. Y. Zheng and X. M. Zhang. Plateaued functions. In *Advances in Cryptology - ICICS'99*, volume 1726 of *Lecture Notes in Computer Science*, pages 284–300. Springer-Verlag, Berlin, Heidelberg, New York, 1999.
14. Y. Zheng and X. M. Zhang. Improved upper bound on the nonlinearity of high order correlation immune functions. In *Selected Areas in Cryptography, 7th Annual International Workshop, SAC2000*, volume xxxx of *Lecture Notes in Computer Science*, pages xxx–xxx. Springer-Verlag, Berlin, Heidelberg, New York, 2000. (in Pre-Proceedings pages 258-269).
15. Y. Zheng and X. M. Zhang. On relationships among avalanche, nonlinearity and correlation immunity. In *Advances in Cryptology - ASIACRYPT2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 470–482. Springer-Verlag, Berlin, Heidelberg, New York, 2000.