Nonlinearity Bounds and Constructions of Resilient Boolean Functions

Palash Sarkar[1] and Subhamoy Maitra[2]

[1] Applied Statistics Unit, Indian Statistical Institute,
203, B T Road, Calcutta 700 035, INDIA
palash@isical.ac.in
[2] Computer and Statistical Service Center, Indian Statistical Institute,
203, B T Road, Calcutta 700 035, INDIA
subho@isical.ac.in

Abstract. In this paper we investigate the relationship between the nonlinearity and the order of resiliency of a Boolean function. We first prove a sharper version of McEliece theorem for Reed-Muller codes as applied to resilient functions, which also generalizes the well known Xiao-Massey characterization. As a consequence, a nontrivial upper bound on the nonlinearity of resilient functions is obtained. This result coupled with Siegenthaler's inequality leads to the notion of best possible trade-off among the parameters: number of variables, order of resiliency, nonlinearity and algebraic degree. We further show that functions achieving the best possible trade-off can be constructed by the Maiorana-McFarland like technique. Also we provide constructions of some previously unknown functions.

Keywords: Boolean functions, Balancedness, Algebraic Degree, Nonlinearity, Correlation Immunity, Resiliency, Stream Ciphers, Combinatorial Cryptography.

1 Introduction

Stream cipher cryptosystems are extensively used for defence communications worldwide and provide a reliable and efficient method of secure communication. In the standard model of stream cipher the outputs of several independent Linear Feedback Shift Register (LFSR) sequences are combined using a nonlinear Boolean function to produce the keystream. This keystream is bitwise XORed with the message bitstream to produce the cipher. The decryption machinery is identical to the encryption machinery.

Siegenthaler [23] pointed out that if the combining function is not chosen properly then the whole system is susceptible to a divide-and-conquer attack. He also defined the class of functions which can resist such attacks [22]. Moreover, such functions must also provide resistance against other well known attacks [4]. Later work on stream ciphers with memoryless Boolean functions have proceeded along two lines. In one direction, Siegenthaler's attack has been successively

M. Bellare (Ed.): CRYPTO 2000, LNCS 1880, pp. 515–532, 2000.

refined and sharpened in a series of papers [14,11,10,15]. On the other hand, in another direction, researchers have tried to design better and better Boolean functions for use in stream cipher systems. Here we concentrate on this second direction of research.

It is now generally accepted that for a Boolean function to be used in stream cipher systems it must satisfy several properties - balancedness, high nonlinearity, high algebraic degree and high order of correlation immunity (see Section 2 for definitions). Also a balanced correlation immune function is called a resilient function. However, we would like to point out that though the necessity of these properties is undisputed, it is by no means clear that these are also sufficient to resist all kinds of attacks. In fact, for practical stream cipher systems, security is judged by the ability of the system to guard against the currently known attacks. In such a situation, it is important to understand the exact degree of protection that a particular system provides. The present effort should be viewed as a contribution to the development of this understanding.

Each of the above mentioned parameters provide protection against a class of attacks. Also it is known that there are certain trade-offs involved among the above parameters. For example, Siegenthaler showed [22] that for an n-variable function, of degree d and order of correlation immunity m, the following holds: $m + d \leq n$. Further, if the function is balanced then $m + d \leq n - 1$. However, the exact nature of trade-off between order of correlation immunity and nonlinearity has not been previously investigated. A series of papers [1,21,3,5,13,16,19] have approached the construction problem in the following fashion. Fix the number of variables and the order of correlation immunity (and possibly the algebraic degree) and try to design balanced functions with as high nonlinearity as possible. Many interesting ideas have been used and successively better results have been proved.

Thus, the natural question that arises is, what is the maximum nonlinearity achievable with a fixed number of variables and a fixed order of correlation immunity? More generally, the crucial question is when can we say that a balanced Boolean function achieves *the best possible trade-off* among the following parameters: number of variables, order of correlation immunity, nonlinearity and algebraic degree? From a practical point of view, a designer of a stream cipher system will typically try to achieve a balance between the size of the hardware and the security of the system. The size of the hardware is directly proportional to the number of input variables of the combining Boolean function. On the other hand, the parameters nonlinearity, algebraic degree and order of resiliency have to be chosen to be large enough so that the current attacks do not succeed in reasonable time. Thus it is important to have *good* functions on *small* number of variables. A natural choice for good functions are those which achieve the best possible trade-off among the above mentioned parameters. Thus the ability to identify, construct and implement such functions is very important from the designer's point of view.

In a more theoretical direction, one of the main results we prove is that if f is an n-variable, m-resilient function, then $W_f(\overline{\omega}) \equiv 0 \bmod 2^{m+2}$, for all

$\overline{\omega} \in \{0,1\}^n$, where $W_f()$ is the Walsh transform of f. This is a generalization of the famous Xiao-Massey characterization of correlation immune functions. More importantly, the result has a root in coding theory. From Siegenthaler's inequality it is known that any n-variable, m-resilient function has degree at most $n-m-1$ and hence is in Reed-Muller code $\mathcal{R}(n-m-1,n)$. The famous McEliece theorem [12, Page 447] when applied to Reed-Muller code $\mathcal{R}(n-m-1,n)$ guarantees that $W_f(\overline{\omega}) \equiv 0 \bmod 2^{1+\lfloor \frac{n-1}{n-m-1} \rfloor}$. The above mentioned result that we prove is much sharper. From this result we obtain a nontrivial upper bound on the nonlinearity of n-variable, m-resilient functions. In a series of papers Hou [8,7,9], has investigated the covering radius problem for Reed-Muller codes. The covering radius of first order Reed-Muller code is equal to the maximum possible nonlinearity of n-variable functions. As observed before, an m-resilient function is in $\mathcal{R}(n-m-1,n)$, but it does not seem that the current results on the covering radius of higher order Reed-Muller codes can be applied to obtain an upper bound on the maximum possible nonlinearity of m-resilient functions.

We show that one of the existing construction methods (the Maiorana-McFarland like construction technique) can provide all but finitely many functions of certain infinite sequences of functions which provide best possible trade-off among the parameters: number of variables, order of resiliency, nonlinearity and algebraic degree. However, the Maiorana-McFarland like construction technique does not work in all cases. In such cases, we introduce a new sharper construction method to obtain such functions. Functions with these parameters were not known earlier. We also discuss important issues on functions with small number of variables in Section 5.

Future work on resilient Boolean functions should proceed along the following lines. It is not clear whether the upper bounds on nonlinearity of resilient functions obtained in Theorem 2 are tight. It will be a major task to show that in certain cases the upper bounds are not tight and to obtain sharper upper bounds. However, in significantly many cases these upper bounds can be shown to be tight (for example see Table 1 in Section 3). Based on these upper bounds, we introduce concepts of Type-I and Type-II resilient functions (see Section 4). Type-II resilient functions with maximum possible algebraic degree are well suited for use in stream ciphers. We have used existing and new techniques to construct such functions. Also it seems that the construction of these functions are difficult in some cases. Either obtaining new construction methods for these functions or showing their non-existence should be the main theme of any further work. On one hand these are combinatorially challenging problems and on the other hand their answers have direct relevance to the task of designing secure stream cipher systems.

2 Preliminaries

In this section we introduce a few basic concepts. Note that we denote the addition operator over $GF(2)$ by $\oplus$.

Definition 1. *For binary strings S_1, S_2 of same length λ, we denote by $\#(S_1 = S_2)$ (respectively $\#(S_1 \neq S_2)$), the number of places where S_1 and S_2 are equal (respectively unequal). The Hamming distance between S_1, S_2 is denoted by $d(S_1, S_2)$, i.e. $d(S_1, S_2) = \#(S_1 \neq S_2)$. The Walsh Distance $wd(S_1, S_2)$, between S_1 and S_2, is defined as, $wd(S_1, S_2) = \#(S_1 = S_2) - \#(S_1 \neq S_2)$. Note that, $wd(S_1, S_2) = \lambda - 2\, d(S_1, S_2)$. Also the Hamming weight or simply the weight of a binary string S is the number of ones in S. This is denoted by $wt(S)$. An n-variable function f is said to be balanced if its output column in the truth table contains equal number of 0's and 1's (i.e. $wt(f) = 2^{n-1}$).*

Definition 2. *An n-variable Boolean function $f(X_n, \ldots, X_1)$ can be considered to be a multivariate polynomial over $GF(2)$. This polynomial can be expressed as a sum of products representation of all distinct k-th order products $(0 \leq k \leq n)$ of the variables. More precisely, $f(X_n, \ldots, X_1)$ can be written as $a_0 \oplus (\bigoplus_{i=1}^{i=n} a_i X_i) \oplus (\bigoplus_{1 \leq i \neq j \leq n} a_{ij} X_i X_j) \oplus \ldots \oplus a_{12\ldots n} X_1 X_2 \ldots X_n$ where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \{0, 1\}$. This representation of f is called the algebraic normal form (ANF) of f. The number of variables in the highest order product term with nonzero coefficient is called the algebraic degree, or simply degree of f.*

In the stream cipher model, the combining function f must be so chosen that it increases the linear complexity [17] of the resulting key stream. High algebraic degree provides high linear complexity [18,4] and hence it is desirable for f to have high algebraic degree. Another important cryptographic property for a Boolean function is high nonlinearity. A function with low nonlinearity is prone to *Best Affine Approximation* (BAA) [4, Chapter 3] attack.

Definition 3. *Functions of degree at most one are called affine functions. An affine function with constant term equal to zero is called a linear function. The set of all n-variable affine (respectively linear) functions is denoted by $A(n)$ (respectively $L(n)$). The nonlinearity of an n variable function f is $nl(f) = min_{g \in A(n)}(d(f, g))$, i.e. the distance from the set of all n-variable affine functions.*

An important tool for the analysis of Boolean function is its Walsh transform, which we define next.

Definition 4. *Let $\overline{X} = (X_n, \ldots, X_1)$ and $\overline{\omega} = (\omega_n, \ldots, \omega_1)$ both belong to $\{0, 1\}^n$ and $\overline{X}.\overline{\omega} = X_n \omega_n \oplus \ldots \oplus X_1 \omega_1$. Let $f(\overline{X})$ be a Boolean function on n variables. Then the Walsh transform of $f(\overline{X})$ is a real valued function over $\{0, 1\}^n$ that can be defined as $W_f(\overline{\omega}) = \sum_{\overline{X} \in \{0,1\}^n} (-1)^{f(\overline{X}) \oplus \overline{X}.\overline{\omega}}$. The Walsh transform is sometimes called the spectral distribution or simply the spectrum of a Boolean function.*

Xiao and Massey [6] provided a spectral characterization of correlation immune functions. Here we state this characterization as the definition of correlation immunity.

Definition 5. *A function $f(X_n, \ldots, X_1)$ is m-th order correlation immune (CI) iff its Walsh transform W_f satisfies $W_f(\overline{\omega}) = 0$, for $1 \leq wt(\overline{\omega}) \leq m$. Further, if f is balanced then $W_f(\overline{0}) = 0$. Balanced m-th order correlation immune functions are called m-resilient functions. Thus, a function $f(X_n, \ldots, X_1)$ is m-resilient iff its Walsh transform W_f satisfies $W_f(\overline{\omega}) = 0$, for $0 \leq wt(\overline{\omega}) \leq m$.*

The relationship between Walsh transform and Walsh distance is [13] $W_f(\overline{\omega}) = wd(f, \bigoplus_{i=1}^{i=n} \omega_i X_i)$.

We will require the following basic result, which is known [12, Page 8], but we give a proof for the sake of completeness. Let $f \times g$ denote the Boolean function h whose ANF is the product (over $GF(2)$) of the ANFs (which are polynomials over $GF(2)$) of f and g, i.e., $h(X_n, \ldots, X_1) = f(X_n, \ldots, X_1) \times g(X_n, \ldots, X_1)$.

Lemma 1. *Let $f(X_n, \ldots, X_1)$ and $g(X_n, \ldots, X_1)$ be two n-variable functions. Then $d(f, g) = wt(f) + wt(g) - 2wt(f \times g)$.*

Proof. Let $F_2^n = \{0, 1\}^n$. The function f can be completely described by a subset A of F_2^n, such that $(b_n, \ldots, b_1) \in F_2^n$ is in A iff $f(b_n, \ldots, b_1) = 1$. This set A is usually called the support of f. We can get a similar support B for g. The support of $f \oplus g$ is $A \Delta B$ (symmetric difference) and the support of $f \times g$ is $A \cap B$. The result follows from the fact that $d(f, g) = wt(f \oplus g) = \mid A \Delta B \mid = \mid A \mid + \mid B \mid - 2 \mid A \cap B \mid$. □

2.1 Some Useful Notations

Before proceeding, we would like to introduce a few notations for future convenience. Recall from Definition 3 that $nl(f)$ denotes the nonlinearity of a Boolean function f. We use $nlmax(n)$ to denote the maximum possible nonlinearity of an n-variable function. The maximum possible nonlinearity of an n-variable, m-resilient function is denoted by $nlr(n, m)$ and the maximum possible nonlinearity of an n-variable function which is CI of order m is denoted by $nlc(n, m)$.

By an (n, m, d, x) function we mean an n-variable, m-resilient function with degree d and nonlinearity x. By $(n, 0, d, x)$ function we mean a balanced n-variable function with degree d and nonlinearity x. In the above notation the degree component is replaced by a '$-$', i.e., $(n, m, -, x)$, if we do not want to specify the degree.

Further, given an affine function $l \in A(n)$, by $ndg(l)$ we denote the number of variables on which l is nondegenerate.

2.2 Maiorana-McFarland Like Construction Technique

There are several construction methods for resilient Boolean functions in the literature. Perhaps the most important of all these is the Maiorana-McFarland like construction technique which has been investigated in a number of previous papers [1,21,3,2,19]. Here we briefly describe the basic method. Let π be a map from $\{0, 1\}^r$ to $\{0, 1\}^k$, where for any $\overline{X} \in \{0, 1\}^r$, $wt(\pi(\overline{X})) \geq m + 1$. Let $f : \{0, 1\}^{r+k} \rightarrow \{0, 1\}$ be a Boolean function defined as $f(\overline{X}, \overline{Y}) = \overline{Y}.\pi(\overline{X}) \oplus g(\overline{X})$,

where $\overline{X} \in \{0,1\}^r$, $\overline{Y} \in \{0,1\}^k$ and $\overline{Y}.\pi(\overline{X})$ is the inner product of $\overline{Y}$ and $\pi(\overline{X})$. Then f is m-resilient. It is possible to interpret f as a concatenation of 2^r affine functions $l_0, \ldots, l_{2^r-1}$ from $A(k)$, the set of k-variable affine functions, where $ndg(l_i) \geq m+1$. Later we will use this method to construct certain sequences of resilient functions.

3 Spectral Weights of CI and Resilient Functions

In this section we prove a crucial result on the divisibility properties of the spectral weights of correlation immune and resilient functions. Such a result has an analogue in the McEliece Theorem [12] for Reed-Muller codes: *the weight of any function in $\mathcal{R}(r,n)$ is divisible by $2^{\lfloor \frac{n-1}{r} \rfloor}$, where $\mathcal{R}(r,n)$ is the set of all n-variable Boolean functions of degree at most r.* If f is an n-variable, m-resilient function, using Siegenthaler's inequality we know that the degree of f is at most $n-m-1$. For any linear function $l \in L(n)$, we have $f \oplus l$ is in $\mathcal{R}(n-m-1,n)$ and so $wt(f \oplus l) = d(f,l)$ is divisible by $2^{\lfloor \frac{n-1}{n-m-1} \rfloor}$. However, this result is not sharp enough to prove a nontrivial upper bound on the nonlinearity of resilient functions. In Theorem 1 we prove that for any n-variable, m-resilient function f and $l \in L(n)$, $d(f,l)$ is divisible by 2^{m+1}. This is a much stronger result. For example, if $n = 7$ and $m = 3$, McEliece Theorem guarantees that $d(f,l)$ is divisible by 2^2. On the other hand Theorem 1 establishes that $d(f,l)$ is divisible by 2^4.

Theorem 1 also sharpens the Xiao-Massey characterization [6] of correlation immune functions. A Boolean function f is m-th order CI iff $wd(f,l) = 0$ for all $l \in L(n)$ with $1 \leq ndg(l) \leq m$. However, this characterization does not state anything about $wd(f,l)$ with $ndg(l) > m$. We show in Theorem 3 that 2^{m+1} divides $wd(f,l)$ for all l in $L(n)$ with $ndg(l) > m$. For resilient functions the Xiao-Massey characterization can only be extended to include the condition that Walsh distance between f and the all zero function is 0. However, Theorem 1 shows that 2^{m+2} divides $wd(f,l)$ for all l in $L(n)$ with $ndg(l) > m$.

Using Theorem 1 and Theorem 3 we prove nontrivial upper bounds on the nonlinearity of resilient and correlation immune functions. Previous works related to upper bound on nonlinearity of resilient functions were attempted in [3,16]. In [3] an upper bound was obtained for a very small subset of resilient functions. It was shown in [19], that it is possible to construct resilient functions, outside the subset of [3], with nonlinearity more than the upper bound obtained in [3]. In [16], the maximum nonlinearity issue for 6-variable resilient functions has been completely settled by exhaustive computer search technique. Corollary 1 provides a simple proof of the same result.

Lemma 2. *Let f be an n-variable function of even weight and $l \in L(n)$. Then $d(f,l)$ (respectively $wd(f,l)$) is congruent to* 0 mod 2 *(respectively* 0 mod 4*).*

Proof. From Lemma 1 we know that $d(f,l) = wt(f) + wt(l) - 2wt(f \times l)$. Since all the terms on the right are even it follows that $d(f,l)$ is also even. □

The next result is a simple consequence of the fact that $\mathcal{R}(m,n)$ is orthogonal to $\mathcal{R}(n-m-1,n)$ [12, Page 375].

Lemma 3. *Let f be an n-variable ($n \geq 3$), 1-resilient function and $l \in L(n)$. Then $d(f,l)$ (respectively $wd(f,l)$) is congruent to* 0 mod 4 *(respectively* 0 mod 8*).*

Proof. Since f is 1-resilient, by Siegenthaler's inequality we know that degree of f is at most $n-2$. If l is in $L(n)$, then $f \times l$ is a function of degree at most $n-1$ and hence $wt(f \times l)$ is even. Thus $d(f,l) = wt(f)+wt(l)-2wt(f \times l) \equiv wt(f) \bmod 4$. As f is balanced, $wt(f) \equiv 0 \bmod 4$, and consequently $d(f,l) \equiv 0 \bmod 4$. □

Corollary 1. *The maximum nonlinearity for a six variable* 1*-resilient function is* 24*.*

Proof. Using Lemma 3, we know that for any $l \in L(6)$ and any 1-resilient function f, $d(f,l) \equiv 0 \bmod 4$. Thus the possible values for $d(f,l)$ are $32 \pm 4k$, for some $k \geq 0$. If for every l, $k \leq 1$, then f must be bent and hence cannot be resilient. So there must be some l, such that $d(f,l) = 32 \pm 8$. But then the nonlinearity is at most 24. □

Next we present the major result on the spectral weights of resilient functions.

Theorem 1. *Let f be an n-variable, m-resilient (with $n \geq 3$ and $m \leq n-3$) function and $l \in L(n)$. Then $d(f,l)$ (respectively $wd(f,l)$) is congruent to* 0 mod 2^{m+1} *(respectively* 0 mod 2^{m+2}*).*

Proof. There are three inductions involved : on the number of variables n, on the order of resiliency m and on the number of variables in the linear function l, which we denote by $k = ndg(l)$.
Base for induction on n: It is possible to verify the result for $n = 3$. Assume the result is true for all functions on less than n variables (with $n \geq 4$).
Inductive Step for induction on n: Let f be an n-variable function.

Now we use induction on m. The induction on m is carried out separately for odd and even values.
Base for induction on m: If $m = 0$, then f is a balanced function and Lemma 2 provides the base case.
If $m = 1$, then Lemma 3 provides the base case.

Next we make the induction hypothesis that if f is $(m-2)$-resilient (with $m-2 \geq 0$), and $l \in L(n)$, then $d(f,l) \equiv 0 \bmod 2^{m-1}$.
Inductive Step for induction on m: Let f be m-resilient and let l be any function in $L(n)$. We now use induction on the number of variables k in l (i.e., $l \in L(n)$ is nondegenerate on exactly k variables).
Base for induction on k: $k \leq m$, since f is m-resilient $d(f,l) = 2^{n-1} \equiv 0 \bmod 2^{m+1}$.
Inductive Step for induction on k: Let $k > m$ and using Lemma 2 and Lemma 3 we can assume $k \geq 2$. Without loss of generality assume X_n and X_{n-1} are present

in l. Write $l = X_n \oplus X_{n-1} \oplus \lambda$, where λ is nondegenerate on at most $k-2$ variables. Also define $\lambda_1 = X_n \oplus \lambda$ and $\lambda_2 = X_{n-1} \oplus \lambda$. Using induction hypothesis on k, we know $d(f, \lambda) \equiv d(f, \lambda_1) \equiv d(f, \lambda_2) \equiv 0 \bmod 2^{m+1}$. Let $g_{00}, g_{01}, g_{10}, g_{11}$ be $(n-2)$-variable functions defined by $g_{ij}(X_{n-2}, \ldots, X_1) = f(i, j, X_{n-2}, \ldots, X_1)$. Since λ has at most $n-2$ variables, there is a function $\mu \in L(n-2)$ which has the same set of variables as λ. Denote by a_{ij} the value $d(g_{ij}, \mu)$. Since $\lambda, \lambda_1, \lambda_2$ have less than k variables, using the induction hypothesis on k we have the following equations.

1. $d(f, \lambda) = a_{00} + a_{01} + a_{10} + a_{11} = k_1 2^{m+1}$,
2. $d(f, \lambda_1) = a_{00} + a_{01} - a_{10} - a_{11} = k_2 2^{m+1}$,
3. $d(f, \lambda_2) = a_{00} - a_{01} + a_{10} - a_{11} = k_3 2^{m+1}$, and
4. $d(f, l) = a_{00} - a_{01} - a_{10} + a_{11}$.

From the first three equations, we can express a_{01}, a_{10} and a_{11} in terms of a_{00}. This gives us

$a_{01} = (k_1 + k_3)2^m - a_{00}$, $a_{10} = (k_1 + k_2)2^m - a_{00}$ and $a_{11} = -(k_2 + k_3)2^m + a_{00}$.

Now using equation 4, we get $d(f, l) = 4a_{00} - (k_1 + k_2 + k_3)2^{m+1}$. Since f is m-resilient and g is obtained from f by setting two variables to constant values, g is an $(n-2)$-variable, $(m-2)$-resilient function. First assume m is even, then $m-2$ is also even. Using the induction hypothesis on n and the induction hypothesis on even m we have $a_{00} = d(g, \mu) \equiv 0 \bmod 2^{m-1}$. The argument is similar for odd m. (This is the reason for choosing the base cases separately for $m = 0$ and $m = 1$.) Hence $d(f, l) \equiv 0 \bmod 2^{m+1}$. □

Using Theorem 1, it is possible to obtain an upper bound on the nonlinearity of an n-variable, m-resilient function.

Theorem 2. *1. If n is even and $m+1 > \frac{n}{2} - 1$, then $nlr(n, m) \leq 2^{n-1} - 2^{m+1}$.*
2. If n is even and $m+1 \leq \frac{n}{2} - 1$, then $nlr(n, m) \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{m+1}$.
3. If n is odd and $2^{m+1} > 2^{n-1} - nlmax(n)$, then $nlr(n, m) \leq 2^{n-1} - 2^{m+1}$.
4. If n is odd and $2^{m+1} \leq 2^{n-1} - nlmax(n)$, then $nlr(n, m)$ is the highest multiple of 2^{m+1} which is less than or equal to $2^{n-1} - nlmax(n)$.
Further in cases 1 and 3, the spectrum of any function achieving the stated bound must be three valued, i.e. the values of the Walsh distances must be $0, \pm 2^{m+2}$.

Proof. We prove only cases 1 and 2, the other cases being similar.
1. Using Theorem 1 for any n-variable, m-resilient function f and $l \in L(n)$, we have $d(f, l) \equiv 0 \bmod 2^{m+1}$. Thus $d(f, l) = 2^{n-1} \pm k2^{m+1}$ for some k. Clearly k cannot be 0 for all l and hence the nonlinearity of f is at most $2^{n-1} - 2^{m+1}$.
2. As in 1, we have $d(f, l) = 2^{n-1} \pm k2^{m+1}$ for some k. Let $2^{\frac{n}{2}-1} = p2^{m+1}$ (we can write in this way as $m < \frac{n}{2} - 1$). If for all l we have $k \leq p$, then f must necessarily be bent and hence cannot be resilient. Thus there must be some l such that the corresponding $k > p$. This shows that the nonlinearity of f is at most $2^{n-1} - 2^{\frac{n}{2}-1} - 2^{m+1}$.

The proof of the last statement follows from the fact that if the Walsh distances are not three valued $0, \pm 2^{m+2}$, then $\pm 2^{m+i}$ must be a Walsh distance value for $i \geq 3$. The nonlinearity for such a function is clearly less than the stated bound. □

In Table 1 we provide some examples of the upper bound provided in Theorem 2. The boundary case of Theorem 2 is given in the following corollary (see also [3,16]).

Corollary 2. *For $n \geq 4$, $nlr(n, n-3) = 2^{n-2}$.*

Proof. From Theorem 2 it is clear that $nlr(n, n-3) \leq 2^{n-1} - 2^{n-2} = 2^{n-2}$. Moreover, it is easy to construct an $(n, n-3, 2, 2^{n-2})$ function by concatenating two distinct linear functions from $L(n-1)$, each of which are nondegenerate on $n-2$ variables. □

We also need the following corollary which will be used to define the concept of *saturated function* in Section 4.

Corollary 3. *Let $m > \lfloor \frac{n}{2} \rfloor - 2$. Then, $nlr(n, m) \leq 2^{n-1} - 2^{m+1} \leq 2^{n-1} - 2^{\lfloor \frac{n-1}{2} \rfloor}$. Further, the spectrum of any $(n, m, -, 2^{n-1} - 2^{m+1})$ function is necessarily three valued.*

Table 1. The entries represent the upper bound on $nlr(n, m)$ given by Theorem 2, where n is the number of variables and m is the order of resiliency. Entries with $*$ represent bounds which have not yet been constructed. Entries with # represent bounds which have been constructed here for the first time.

n \ m	1	2	3	4	5	6	7	8
5	12	8	0					
6	24	24	16	0				
7	56	56*	48	32	0			
8	116*	112	112#	96	64	0		
9	244*	240	240*	224#	192	128	0	
10	492*	480	480	480*	448	384	256	0

The set of n-variable m-th order correlation immune functions is a superset of n-variable m-resilient functions. The following two results are for correlation immune functions and are similar to Theorem 1 and 2.

Theorem 3. *Let f be an n-variable, m-th order correlation immune (with $n \geq 3$ and $m \leq n-2$) function and $l \in L(n)$. Then $d(f, l)$ (respectively $wd(f, l)$) is congruent to* 0 mod 2^m *(respectively* 0 mod 2^{m+1}*).*

Proof. We have to note that if a function f is 1st order correlation immune (CI) then $d(f, l)$ is even ($wd(f, l) \equiv 0 \bmod 4$) for any linear function l. Now given a 2nd order CI function, by Siegenthaler's inequality we know that degree of f is at most $n-2$. Thus, similar to the proof of Lemma 3, we get $d(f, l)$ (respectively $wd(f, l)$) is congruent to 0 mod 4 (respectively 0 mod 8). Using these as the base cases, the proof is similar to the proof of Theorem 1. □

Theorem 4. *1. If n is even and $m > \frac{n}{2} - 1$, then $nlc(n, m) \leq 2^{n-1} - 2^m$.*
2. If n is even and $m \leq \frac{n}{2} - 1$, then $nlc(n, m) \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2^m$.
3. If n is odd and $2^m > 2^{n-1} - nlmax(n)$, then $nlc(n, m) \leq 2^{n-1} - 2^m$.
4. If n is odd and $2^m \leq 2^{n-1} - nlmax(n)$, then $nlc(n, m)$ is the highest multiple of 2^m which is less than or equal to $2^{n-1} - nlmax(n)$.
Further in cases 1 and 3, the spectrum of any function achieving the stated bound must be three valued, i.e. the values of the Walsh distances must be $0, \pm 2^{m+1}$.

The nonlinearity bounds proved in this section have the following important consequences.
1. These bounds set up a *benchmark* by which one can measure the efficacy of any new construction method for resilient functions. It will also be a major task to show that in certain cases the upper bound of Theorem 2 is not tight.
2. Based on Theorem 2 and Siegenthaler's inequality, we are able to satisfactorily identify the class of Boolean functions achieving the best possible trade-off among the parameters : number of variables, order of resiliency, nonlinearity and algebraic degree.

4 Construction of Resilient Functions

Motivated by Theorem 2, we introduce two classes of resilient functions. An (n, m, d, x) function is said to be of Type-I if x is the upper bound on $nlr(n, m)$ provided in Theorem 2. Note that, given an n-variable function, there may be more than one possible values of order of resiliency m, such that the upper bound on $nlr(n, m)$ is same using Theorem 2. We call an n-variable, m-resilient function having nonlinearity x to be of Type-II if the function is of Type-I and further for any $p > m$ the upper bound on $nlr(n, p)$ in Theorem 2 is strictly less than x. These notions of trade-offs can be further strengthened by requiring the degree to be the maximum possible. For this we require Siegenthaler's inequality for resilient functions: $m + d \leq n - 1$, for any n-variable, m-resilient, degree d function. *Thus $(n, m, n - m - 1, x)$ Type-II functions achieve the best possible trade-off among the parameters : number of variables, order of resiliency, degree and nonlinearity.*

Example 1. An $(8, 2, 5, 112)$ function is of Type-I. Moreover, $(8, 2, -, 112)$ functions are not of Type-II since $nlr(8, 3) \leq 112$. However, an $(8, 3, -, 112)$ function is of Type-II since $nlr(8, 4) \leq 96$. Also an $(8, 3, 4, 112)$ function maximizes the algebraic degree and hence provides best possible trade-off among the parameters we consider here. From Theorem 2, the spectrum of any $(8, 3, -, 112)$ function is necessarily three valued. However, this may not necessarily be true for any Type-II function. For example, an $(8, 1, 6, 116)$ function (if one exists) will be of Type-II, but its spectrum will not be three valued.

The way we have defined Type I and Type II functions, it is not guaranteed that such functions always exist. The tightness of the upper bounds in Theorem 2 is contingent on the existence of such functions. However, we will show for certain

sequences of Type-II functions, it is possible to construct all but finitely many functions of any such sequence.

We call a Type-II function to be *saturated* if its spectrum is three valued according to Corollary 3. Thus an $(n, m, n-m-1, x)$-function is called a *saturated maximum degree* function if it is of Type-II and its spectrum is three valued. For such a function we must necessarily have $m > \lfloor \frac{n}{2} \rfloor - 2$. Therefore, the $(8, 3, 4, 112)$ functions are of Type II and are also saturated maximum degree functions. However, the $(8, 1, 6, 116)$ Type-II functions (if they exist) can not have a three valued Walsh spectrum. From Parseval's theorem, if it has a three valued Walsh spectrum, then $24^2 \times z = 2^{16}$, which is not possible for integral z. Thus, $(8, 1, 6, 116)$ functions are of Type-II and have maximum degree but are not saturated.

Lemma 4. *If an $(n, m, n-m-1, x)$ function f is a saturated function, then so is an $(n+1, m+1, n-m-1, 2x)$ function g.*

Proof. Since f is saturated, $x = 2^{n-1} - 2^{m+1}$ and so $2x = 2^n - 2^{m+2}$. From Corollary 3, $nlr(n+1, m+1) \leq 2^n - 2^{m+2}$ and hence the spectrum of g is three valued. □

This naturally leads to a notion of a sequence of Boolean functions, each of which is a saturated maximum degree function. More precisely, a *saturated function sequence* (an SS for short), is an infinite sequence of Boolean functions $f_0, f_1, \ldots$, where f_0 is an $(n_0, m_0, n_0 - m_0 - 1, x_0)$ function which is a Type II, saturated maximum degree function and the upper bound on $nlr(n_0 - 1, m_0 - 1)$ in Theorem 2 is strictly less than $\frac{x_0}{2}$. Also for $j \geq 0$, f_{j+1} is an $(n_j + 1, m_j + 1, n_j - m_j - 1, 2x_j)$ function (and hence is also saturated from Lemma 4). Note that $n_j - m_j - 1 = n_0 - m_0 - 1$ and so the degree of all the functions in an SS are same. Thus an SS is completely defined by specifying the parameters of a function f_0. Note that the functions which form an SS is not unique, i.e., there can be more than one distinct $(n_0, m_0, n_0 - m_0 - 1, x_0)$ functions and all of them are possible representatives for f_0. Thus a particular SS is characterized by several parameters and any sequence of functions satisfying these parameters is said to form the particular SS.

Example 2. The following seqences are SS's.
1. $f_0, f_1, \ldots$, where f_0 is a $(3, 0, 2, 2)$ function.
2. $f_0, f_1, \ldots$, where f_0 is a $(5, 1, 3, 12)$ function.
3. $f_0, f_1, \ldots$, where f_0 is a $(7, 2, 4, 56)$ function.

It is not known whether $(7, 2, 4, 56)$ functions exists. However, we show how to construct an $(8, 3, 4, 112)$ function, which is f_1 in this SS.

Definition 6. *For $i \geq 0$ we define SS(i) as follows. An SS(0) is a sequence $f_{0,0}, f_{0,1}, \ldots$, where $f_{0,0}$ is a $(3, 0, 2, 2)$ function and $f_{0,j}$ is a $(3 + j, j, 2, 2^{j+1})$ function for $j > 0$. For $i > 0$, an SS(i) is a sequence $f_{i,0}, f_{i,1}, \ldots$, where $f_{i,0}$ is a $(3 + 2i, i, 2 + i, 2^{2+2i} - 2^{1+i})$ function which is a Type II, saturated maximum degree function. Also for $j > 0$, $f_{i,j}$ is a $(3 + 2i + j, i + j, 2 + i, 2^{2+2i+j} - 2^{1+i+j})$ function.*

Note that all functions in an SS(i) have the same degree $2+i$. Construction of SS(0) and SS(1) are already known. Unfortunately, it is not known whether the initial functions for an SS(i) exist for $i > 1$. In the next subsection we show how to construct all but finitely many initial functions of any SS(i).

Now we will concentrate on the construction problem of saturated sequences. In defining SS we stated that any function in an SS must be a saturated function. However, the converse that given any saturated function, it must occur in some SS(i) is not immediate. The following result proves this and justifies the fact that we can restrict our attention to the construction problem for SS(i) only.

Lemma 5. *Any saturated function must occur in some SS(i).*

Proof. First note that any function of SS(i) has algebraic degree $2+i$. Any saturated function f must be an $(n, m, n-m-1, 2^{n-1}-2^{m+1})$ function having degree $d = n-m-1$. Hence f must occur in SS($d-2$), i.e., in SS($n-m-3$). □

4.1 Construction of SS(i)

Here we show that the Maiorana-McFarland like construction procedure can be used to construct all but finitely many functions of any SS(i). First we state the following result which is easy to prove using Lemma 4.

Lemma 6. *Let $f_{i,j}$ be a j-th function of SS(i). Then the function $g = Y \oplus f_{i,j}$ (where the variable Y does not occur in $f_{i,j}$) is an $f_{i,j+1}$ function of SS(i). Consequently, if one can construct $f_{i,j}$, then one can construct $f_{i,k}$ for all $k > j$.*

This shows that if one can construct any one of the functions in SS(i), then it is possible to construct any function in the succeeding part of the sequence. Thus it is enough if we can construct the first function of each sequence. This is possible for SS(0) and SS(1) since construction of $(3, 0, 2, 2)$ and $(5, 1, 3, 12)$ functions are known. However, the construction problem for the first function of SS(i) for $i > 1$ is an ongoing research problem. Here we show that the Maiorana-McFarland like construction procedure can be used to construct all but finitely many functions of any SS(i). More precisely, if SS(i) $= f_{i,0}, f_{i,1} \ldots$, then we show how to construct $f_{i,t}$ for all $t \geq t_0$, where t_0 is such that $2^{1+i} = 3 + i + t_0$. For SS(2), this gives $t_0 = 3$. Moreover, in Subsection 4.2, we show how to construct $f_{2,1}$ and $f_{2,2}$. This leaves open the problem of constructing $f_{i,t}$, with $t < t_0$ and $i \geq 3$ as a challenging research problem.

Theorem 5. *For any SS(i) $= f_{i,0}, f_{i,1}, \ldots$, it is possible to construct $f_{i,t}$ for all t greater than or equal to some t_0.*

Proof. The first function $f_{i,0}$ is a $(3+2i, i, 2+i, 2^{2+2i}-2^{1+i})$ function. We show that for some j, $f_{i,j}$ is constructible by Maiorana-McFarland like construction techniques. Let j be such that $2^{1+i} = 3 + i + j$. A function $f_{i,j}$ is to be an $(n = 3+2i+j, i+j, 2+i, 2^{2+2i+j} - 2^{1+i+j})$. We show how to construct such a function. Consider the set Λ of all $k = 2+i+j$-variable linear functions which are nondegenerate on at least $1+i+j$ variables. Clearly there are $\binom{2+i+j}{2+i+j}$ +

$\binom{2+i+j}{1+i+j} = 3+i+j$ such linear functions. Consider an n-variable function f (a string of length 2^n) formed by concatenating 2^{n-k} functions from Λ. Since $2^{n-k} = 2^{1+i} = 3+i+j = \mid \Lambda \mid$, we use each of the functions in Λ exactly once in the formation of f. Since each function in Λ is nondegenerate on $1+i+j$ variables each of these functions is $(i+j)$-resilient. Let $V = \{X_{2+i+j}, \ldots, X_1\}$ be the set of variables which are involved in the linear functions in Λ. Each of the variables in V occur in $2^{1+i}-1$ of the linear functions in Λ. Thus each variable occurs an odd number of times and hence the degree of f is $n-k+1 = 2+i$. Moreover, this implies that each of the n input variables of the function occurs in the maximum degree term. Since each linear function is used once, the nonlinearity of f is $2^{n-1}-2^{k-1} = 2^{2+2i+j}-2^{1+i+j}$. Thus f is a $(3+2i+j, i+j, 2+i, 2^{2+2i+j}-2^{1+i+j})$ function and can be taken as $f_{i,j}$. Take $t_0 = j$. Then using Lemma 6 it is possible to construct $f_{i,t}$ for all $t > t_0 = j$. □

In the proof of the above theorem we use Lemma 6 to construct $f_{i,t}$ for all $t > j$, given the function $f_{i,j}$. Thus $f_{i,t}(Y_{t-j}, \ldots, Y_1, \overline{X}) = Y_{t-j} \oplus \ldots \oplus Y_1 \oplus f_{i,j}(\overline{X})$. This results in the function $f_{i,t}$ depending linearly on the variables $Y_{t-j}, \ldots, Y_1$. This is not recommendable from cryptographic point of view. There are two ways to avoid this situation.

(I) The above proof of Theorem 5 can be modified so that Lemma 6 is not required at all. In fact, the linear concatenation technique used to construct $f_{i,j}$ can directly be used to construct $f_{i,t}$. In $f_{i,j}$, a total of 2^{1+i} slots were filled up using the $3+i+j$ different linear functions (each exactly once) and this was made possible by the fact that $2^{1+i} = 3+i+j$. In constructing $f_{i,t}$ directly we will still have to fill 2^{1+i} slots but the number of linear functions that can be used will increase to $3+i+t$. Hence no linear function need to be used more than once and as a result the nonlinearity obtained will achieve the upper bound of Theorem 2. The ANF of the resulting $f_{i,t}$ will depend nonlinearly on all the variables $Y_{t-j}, \ldots, Y_1$.

(II) After obtaining $f_{i,j}$, instead of using Lemma 6 we can use a more powerful construction provided in [13]. The method of [13] shows that if f is an m-resilient function, then g defined as $g(Y, \overline{X}) = (1 \oplus Y)f(\overline{X}) \oplus Y(a \oplus f(\overline{X} \oplus \overline{\alpha}))$, is an $(m+1)$-resilient function, where $\overline{\alpha}$ is an all one vector and $a = m \bmod 2$. This also guarantees that g does not depend linearly on Y. Hence if we use this technique repeatedly to construct $f_{i,t}$ from $f_{i,j}$, then the ANF of the resulting $f_{i,t}$ will depend nonlinearly on all the variables $Y_{t-j}, \ldots, Y_1$.

4.2 A Sharper Construction

For SS(2) $= f_{2,0}, f_{2,1}, f_{2,2}, \ldots$, Theorem 5 can be used to construct $f_{2,t}$ for all $t \geq 3$. Here we show how to construct $f_{2,1}$ (an $(8, 3, 4, 112)$ function). However, the construction of $f_{2,0}$, the $(7, 2, 4, 56)$ Type-II function, is not yet known.

For a Boolean function f, we define $NZ(f) = \{\overline{\omega} \mid W_f(\overline{\omega}) \neq 0\}$, where W_f is the Walsh transform of f. The following result is the first step in the construction of $(8, 3, 4, 112)$ function.

Lemma 7. *Let f_1, f_2 be two $(7, 3, -, 48)$ functions such that $NZ(f_1) \cap NZ(f_2) = \emptyset$. Let $f = (1 \oplus X_8)f_1 \oplus X_8 f_2$. Then, f is an $(8, 3, -, 112)$ function.*

First let us construct the function f_2 using concatenation of linear functions. We take four 5-variable linear functions with each of them nondegenerate on at least 4 variables : $l_{51} = X_1 \oplus X_2 \oplus X_3 \oplus X_4$, $l_{52} = X_1 \oplus X_2 \oplus X_3 \oplus X_5$, $l_{53} = X_1 \oplus X_2 \oplus X_4 \oplus X_5$ and $l_{54} = X_1 \oplus X_3 \oplus X_4 \oplus X_5$. We consider $f_2 = l_{51}l_{52}l_{53}l_{54}$, concatenation of the four linear functions. It is easy to see that since each l_{5i} is 3-resilient, f_2 is also 3-resilient. Note that each of the variables X_2, X_3, X_4, X_5 occurs in exactly three linear functions, so algebraic degree of f_2 is 3. Moreover, nonlinearity of f_2 is $3 \times 16 = 48$.

Now let us analyze the Walsh spectrum of f_2. Note that for the linear functions λ of the form $a_7X_7 \oplus a_6X_6 \oplus l_{5i}$, $a_7, a_6 \in \{0, 1\}, 1 \leq i \leq 4$, $wd(f_2, \lambda)$ is nonzero. There are 16 such functions in $L(7)$. For the rest of the functions λ_1 in $L(7)$, $wd(f_2, \lambda_1)$ is zero. Also, note that according to the Theorem 2, this is a three valued Walsh spectrum.

Next we need to use the following basic idea. *When $d(f_2, l)$ is minimum, then $d(f_1, l)$ must be 64, i.e., when $wd(f_2, l)$ is maximum, then $wd(f_1, l)$ must be 0.* We now construct another $(7, 3, 3, 48)$ function, having a three valued Walsh spectrum such that $wd(f_1, \lambda)$ is zero for all λ of the form $a_7X_7 \oplus a_6X_6 \oplus l_{5i}$, $a_7, a_6 \in \{0, 1\}, 1 \leq i \leq 4$.

We start from a $(5, 1, 3, 12)$ function g. The Walsh spectrum of the function need to be such that $wd(g, l_{5i}) = 0$ for $1 \leq i \leq 4$. We choose g to be 00000111011111001110010110100010 by running a computer program. Then we construct $f_1 = X_7 \oplus X_6 \oplus g$. Note that f_1 is a $(7, 3, 3, 48)$ function and the Walsh spectrum of f_1 is such that $wd(f_1, \lambda)$ is zero for all λ of the form $a_7X_7 \oplus a_6X_6 \oplus l_{5i}$, $a_7, a_6 \in \{0, 1\}, 1 \leq i \leq 4$. Thus, $NZ(f_1) \cap NZ(f_2) = \emptyset$. Also there are degree three terms in f_1 (respectively f_2) which are not in f_2 (respectively f_1). Hence, $f = (1 \oplus X_8)f_1 \oplus X_8 f_2$ is an $(8, 3, 4, 112)$ function. The output column of the function is a 256-bit string and is as follows in hexadecimal format.

```
077C  E5A2  F883  1A5D  F883  1A5D  077C  E5A2
6996  6996  6969  9696  6699  9966  5AA5  A55A
```

Theorem 6. *It is possible to construct $(8, 3, 4, 112)$ and $(9, 4, 4, 224)$ functions.*

Proof. Above we discussed how to construct an $(8, 3, 4, 112)$ function f. Further a $(9, 4, 4, 224)$ function can be constructed as either $(1 \oplus X_9)f(X_8, \ldots, X_1) \oplus X_9(1 \oplus f(1 \oplus X_8, \ldots, 1 \oplus X_1))$ or $X_9 \oplus f$. □

5 On Construction of Small Functions

First we consider balanced functions. The maximum possible nonlinearities for balanced functions on 7, 8, 9 and 10 variables are 56, 118, 244 and 494 respectively. In [20], construction of nonlinear balanced functions on even number of variables was considered. The values obtained for 8 and 10 variables are respectively 116 and 492. In [19], the degree was considered and construction of

$(7,0,6,56), (8,0,7,116), (9,0,8,240)$ and $(10,0,9,492)$ functions were presented. The existence of $(8,0,-,118)$ functions have been open for quite some time. We next present a result which could be an important step in solving this problem.

Theorem 7. *Let if possible f be a $(8,0,-,118)$ function. Then degree of f must be 7 and it is possible to write $f = (1 \oplus X_8)f_1 \oplus X_8 f_2$, where f_1 and f_2 are 7-variable functions each having nonlinearity 55 and degree 7.*

Proof. First we prove that the degree of f must be 7. If the degree of f is less than 7, then using a result of Hou [7, Lemma 2.1], we can perform an affine transformation on the varibles of f to obtain an 8-variable function g, such that $g(X_8, X_7, \ldots, X_1) = (1 \oplus X_8)g_1(X_7, \ldots, X_1) \oplus X_8 g_2(X_7, \ldots, X_1)$ and the degrees of g_1 and g_2 are each less than or equal to 5. The affine transformation preserves the weight and nonlinearity of f and so $wt(f) = wt(g) = wt(g_1) + wt(g_2)$ and $nl(f) = nl(g)$. Since f is balanced, $wt(g_1) + wt(g_2) = wt(g) = wt(f) = 128 \equiv 0 \bmod 4$. Also $wt(g_1)$ and $wt(g_2)$ are both even since their degrees are less than or equal to 5. Hence $wt(g_1) \equiv wt(g_2) \equiv 0 \bmod 4$ or $wt(g_1) \equiv wt(g_2) \equiv 2 \bmod 4$. Since g_1, g_2 are 7-variable functions with degree ≤ 5, it follows that (see [12]) for any linear function $l \in L(7)$, $d(g_1, l) \equiv wt(g_1) \bmod 4$ and $d(g_2, l) \equiv wt(g_2) \bmod 4$. Hence for any $l \in L(7)$,
$d(g_1, l) \equiv d(g_2, l) \bmod 4$ and so $d(g_1, l) + d(g_2, l) \equiv 0 \bmod 4$ (**).
Since the nonlinearity of g is 118, there exists $\lambda \in L(7)$ such that one of the following must hold: (1) $d(g, \lambda\lambda) = 118$, (2) $d(g, \lambda\lambda) = 138$, (3) $d(g, \lambda\lambda^c) = 118$, (4) $d(g, \lambda\lambda^c) = 138$. Here we consider only case (1), other ones being similar. From (1) we have $118 = d(g, \lambda\lambda) = d(g_1, \lambda) + d(g_2, \lambda)$ and so $d(g_1, \lambda) + d(g_2, \lambda) = 118 \equiv 2 \bmod 4$ which is a contradiction to equation (**).

Thus the degree of f is 7. Without loss of generality we consider $X_7 \ldots X_1$ is a degree 7 term in the ANF of f. We put $f_1(X_7, \ldots, X_1) = f(X_8 = 0, X_7, \ldots, X_1)$ and $f_2(X_7, \ldots, X_1) = f(X_8 = 1, X_7, \ldots, X_1)$. Thus both f_1, f_2 are of degree 7 and hence of odd weight and so $nl(f_1), nl(f_2) \leq 55$. It can be proved that if any of $nl(f_1)$ or $nl(f_2)$ is ≤ 53, then $nl(f) < 118$. □

The major implication of Theorem 7 is that if it is not possible to construct $(8,0,7,118)$ function by concatenating two 7-variable, degree 7, nonlinearity 55 functions, then the maximum nonlinearity of balanced 8-variable functions is 116.

Now we turn to resilient functions. We first present a construction of a previously unknown function.

Theorem 8. *It is possible to construct $(10,3,6,480)$ functions.*

Proof. We construct a function f by concatenating linear functions from $L(5)$ as follows. There are 10 functions $\mu_0, \ldots, \mu_9$ in $L(5)$ which are nondegenerate on exactly 3 variables. Also there are 5 functions $\lambda_0, \ldots, \lambda_4$ in $L(5)$ which are nondegenerate on exactly 4 variables. The function f is the concatenation of the following sequence of functions,
$\lambda_0\lambda_0\lambda_0\lambda_0^c\lambda_1\lambda_1\lambda_1\lambda_1^c\lambda_2\lambda_2\lambda_3\lambda_4\mu_0\mu_0^c\mu_1\mu_1^c\mu_2\mu_2^c\mu_3\mu_3^c\mu_4\mu_4^c\mu_5\mu_5^c\mu_6\mu_6^c\mu_7\mu_7^c\mu_8\mu_8^c\mu_9\mu_9^c$.
The functions λ_i and $\mu_j\mu_j^c$ are both 3-resilient and hence f is 3-resilient too.

It can be checked that there are variables between $X_5, \ldots, X_1$ which occur odd number of times overall in the above sequence. Hence the degree of f is 6. Also the nonlinearity of f can be shown to be 480. □

Note that the constructed function is not a saturated function and its Walsh spectrum is five-valued $(0, \pm 32, \pm 64)$.

In Table 2, we list some of the best known functions. Also Table 3 provides some open problems.

Table 2. Some best known functions. The $(8, 3, 4, 112)$ and $(9, 4, 4, 224)$ functions are from Theorem 6 and the $(10, 3, 6, 480)$ function is from Theorem 8. All the other constructions were known previously [21,19].

n	
7	(7,1,5,56), (7,3,3,48), (7,4,2,32)
8	(8,1,6,112), (8,2,5,112), (8,3,4,112), (8,4,3,96), (8,5,2,64)
9	(9,1,7,240), (9,2,5,240), (9,3,5,224), (9,4,4,224), (9,5,3,192), (9,6,2,128)
10	(10,1,8,484), (10,2,7,480), (10,3,6,480), (10,4,5,448), (10,5,4,448), (10,6,3,384), (10,7,2,256)

Table 3. Existence of functions with these parameters is not known.

n	
7	(7,2,−,56)
8	(8,1,−,116)
9	(9,1,−,244), (9,2,6,240)
10	(10,1,−,492), (10,1,−,488), (10,2,−,488), (10,4,−,480)

Notes : In a recent work [24], Tarannikov showed that the maximum possible nonlinearity of an n-variable, m-resilient function is $2^{n-1} - 2^{m+1}$ for $\frac{2n-7}{3} \leq m \leq n-2$ and functions achieving this nonlinearity must have maximum possible algebraic degree $n - m - 1$. Also a construction method for such n-variable functions with the additional restriction that each variable occurs in a maximum degree term is provided for m in the range $\frac{2n-7}{3} \leq m \leq n - \log_2 \frac{n-2}{3} - 2$.

Acknowledgement

The authors are grateful to the anonymous referees for many comments which helped to improve the presentation of the paper.

References

1. P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation immune functions. In *Advances in Cryptology - CRYPTO'91*, pages 86–100. Springer-Verlag, 1992.
2. C. Carlet. More correlation immune and resilient functions over Galois fields and Galois rings. In *Advances in Cryptology - EUROCRYPT'97*, pages 422–433. Springer-Verlag, May 1997.
3. S. Chee, S. Lee, D. Lee, and S. H. Sung. On the correlation immune functions and their nonlinearity. In *Advances in Cryptology, Asiacrypt 96*, number 1163 in Lecture Notes in Computer Science, pages 232–243. Springer-Verlag, 1996.
4. C. Ding, G. Xiao, and W. Shan. *The Stability Theory of Stream Ciphers*. Number 561 in Lecture Notes in Computer Science. Springer-Verlag, 1991.
5. E. Filiol and C. Fontaine. Highly nonlinear balanced Boolean functions with a good correlation-immunity. In *Advances in Cryptology - EUROCRYPT'98*. Springer-Verlag, 1998.
6. X. Guo-Zhen and J. Massey. A spectral characterization of correlation immune combining functions. *IEEE Transactions on Information Theory*, 34(3):569–571, May 1988.
7. X. Hou. Covering radius of the Reed-Muller code $R(1,7)$ - a simpler proof. *Journal of Combinatorial Theory, Series A*, 74(3):337–341, 1996.
8. X. Hou. On the covering radius of $R(1,m)$ in $R(3,m)$. *IEEE Transactions on Information Theory*, 42(3):1035–1037, 1996.
9. X. Hou. On the norm and covering radius of the first order Reed-Muller codes. *IEEE Transactions on Information Theory*, 43(3):1025–1027, 1997.
10. T. Johansson and F. Jonsson. Fast correlation attacks based on turbo code techniques. In *Advances in Cryptology - CRYPTO'99*, number 1666 in Lecture Notes in Computer Science, pages 181–197. Springer-Verlag, August 1999.
11. T. Johansson and F. Jonsson. Improved fast correlation attacks on stream ciphers via convolutional codes. In *Advances in Cryptology - EUROCRYPT'99*, number 1592 in Lecture Notes in Computer Science, pages 347–362. Springer-Verlag, May 1999.
12. F. J. MacWillams and N. J. A. Sloane. *The Theory of Error Correcting Codes*. North Holland, 1977.
13. S. Maitra and P. Sarkar. Highly nonlinear resilient functions optimizing Siegenthaler's inequality. In *Advances in Cryptology - CRYPTO'99*, number 1666 in Lecture Notes in Computer Science, pages 198–215. Springer Verlag, August 1999.
14. W. Meier and O. Staffelbach. Fast correlation attack on stream ciphers. In *Advances in Cryptology - EUROCRYPT'88*, volume 330, pages 301–314. Springer-Verlag, May 1988.
15. S. Palit and B. K. Roy. Cryptanalysis of LFSR-encrypted codes with unknown combining functions. In *Advances in Cryptology - ASIACRYPT'99*, number 1716 in Lecture Notes in Computer Science, pages 306–320. Springer Verlag, November 1999.
16. E. Pasalic and T. Johansson. Further results on the relation between nonlinearity and resiliency of Boolean functions. In *IMA Conference on Cryptography and Coding*, number 1746 in Lecture Notes in Computer Science, pages 35–45. Springer-Verlag, 1999.
17. R. A. Rueppel. *Analysis and Design of Stream Ciphers*. Springer Verlag, 1986.

18. R. A. Rueppel and O. J. Staffelbach. Products of linear recurring sequences with maximum complexity. *IEEE Transactions on Information Theory*, IT-33:124–131, January 1987.
19. P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. In *Advances in Cryptology - EUROCRYPT 2000*, number 1807 in Lecture Notes in Computer Science, pages 491–512. Springer Verlag, 2000.
20. J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearly balanced Boolean functions and their propagation characteristics. In *Advances in Cryptology - CRYPTO'93*, pages 49–60. Springer-Verlag, 1994.
21. J. Seberry, X. M. Zhang, and Y. Zheng. On constructions and nonlinearity of correlation immune Boolean functions. In *Advances in Cryptology - EUROCRYPT'93*, pages 181–199. Springer-Verlag, 1994.
22. T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776–780, September 1984.
23. T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Transactions on Computers*, C-34(1):81–85, January 1985.
24. Y. V. Tarannikov. On resilient Boolean functions with maximum possible nonlinearity. *Cryptology ePrint Archive, eprint.iacr.org, No. 2000/005*, 2000.