New Directions in Design of Resilient Boolean Functions

Palash Sarkar
Applied Statistics Unit
Indian Statistical Institute
203, B.T. Road
Calcutta 700 035
INDIA
e-mail: palash@isical.ac.in

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

8 February, 2000

Indian Statistical Institute
Technical Report No. ASD/2000/04.

Abstract

There has been a recent upsurge of research in the design of resilient Boolean functions for use in stream cipher systems. The existing research concentrates on maximum degree resilient functions and tries to obtain as high nonlinearity as possible. In sharp contrast to this approach, we identify the class of functions with *provably best* possible trade-off among the parameters: number of variables, resiliency, nonlinearity and algebraic degree. 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 naturally leads to the notion of provably best resilient functions. We further show that such best functions can be constructed by the Maiorana-McFarland like technique. In cases where this method fails, we provide new ideas to construct best functions. We also briefly discuss efficient implementation of these functions in hardware.

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

1 Introduction

Stream cipher cryptosystems are extensively used for defence comunications 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 keystrem. This keystream is bitwise XORed with the message bitstream to produce the cipher. The decryption machinery is identical to the encryption machinary.

Siegenthaler [24] was the first to point 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 [23]. Later works on theory of stream ciphers with memoryless Boolean functions have proceeded on two lines. In one direction, Siegenthaler's attack has been successively refined and sharpened in a series of papers [13, 10, 9, 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. We convincingly argue that certain important questions regarding the design problem have to date not been taken up by the researchers in this area. Our results provide satisfactory answers to these questions.

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. It is known that there are certain trade-off involved among these parameters. For example, Siegenthaler showed [23] 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, 22, 3, 5, 12, 16, 20] have approached the construction problem in the following fashion. Fix the number of variables and the order of correlation immunity (and possibly the 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, correlation immunity, nonlinearity and algebraic degree.* Of course just identifying the best functions is not enough. We need methods to construct and *implement these functions efficiently in hardware.*

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 $\overline{\omega} \in \{0,1\}^n$. (Here $W_f()$ 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 [11, 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. *Further we introduce the notion of a (sequence of) Boolean function with the best possible trade-off among the parameters mentioned above (see Section 4). We believe this notion is important and serves as a benchmark for assessing the efficacy of past and future construction methods.*

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 best functions. We discuss the implementation of best functions and show that functions of large number of variables (around 50) can be implemented in hardware (see Subsubsection 4.1.1). However, the Maiorana-McFarland like construction technique does not work in all cases. In such cases, we introduce new sharper construction methods to obtain best 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 3.2 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 in Page 6). Based on these upper bounds, we introduce concepts of Type-I and Type-II optimal resilient functions (see Section 4). Type-II optimal resilient functions achieving the maximum possible algebraic degree are naturally the *best* functions for use in stream ciphers. We have used existing and new techniques to construct such best functions. Also it seems that the construction of certain best functions are difficult. Either obtaining new construction methods for these best 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 immediate practical usefulness in designing secure stream cipher systems.

2 Preliminaries

In this section we introduce a few basic concepts. *By Ω_n we denote the set of all n-variable Boolean functions.* If we consider a Boolean function as the output column of a truth table, then Ω_n is the set of 2^{2^n} distinct binary strings of length 2^n. We denote the addition operator over $GF(2)$ by $\oplus$.

Definition 2.1 *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 1s in S. This is denoted by $wt(S)$. A function $f \in \Omega_n$ 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 2.2 *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 [18] of the resulting key stream. High algebraic degree provides high linear complexity [19, 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 2.3 *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 (resp. linear) functions is denoted by $A(n)$ (resp. $L(n)$). 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. Given an affine function $l \in A(n)$, by $ndg(l)$ we denote the number of variables on which l is nondegenerate.*

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

Definition 2.4 *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 spectra of a Boolean function.*

Xiao and Massey [6] has provided a spectral characterization of correlation immune functions using Walsh transform. We use that as a definition of correlation immunity here.

Definition 2.5 *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 $1 \leq wt(\overline{\omega}) \leq m$. Note that balanced m-th order correlation immune functions are called m-resilient functions and if f is balanced then $W_f(\overline{0}) = 0$. 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 distance and Walsh transform is [12] $W_f(\overline{\omega}) = wd(f, \bigoplus_{i=1}^{i=n} \omega_i X_i)$.

A Boolean function should have balancedness, high nonlinearity, high order of resiliency and high algebraic degree to be used in stream ciphers. By an (n, m, d, x) function we mean an n-variable, m-resilient (balanced m-th order CI) 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.

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, 22, 3, 2]. Here we briefly describe this 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 $F(k)$, 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.

Next we need the following basic result, which is known but we give a proof for the sake of completeness. The notation $f \times g$ denotes 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 2.1 *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 differnce) and the support of $f \times g$ is $A \cap B$. The result follows from the fact that $d(f,g) = wt(f \oplus g) = \mid A \Delta B \mid = \mid A \mid + \mid B \mid - 2 \mid A \cap B \mid$. ∎

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 [11] 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 $n-m-1$. Hence 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 3.1 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 3.1 establishes that $d(f,l)$ is divisible by 2^4.

Theorem 3.1 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 $1 \leq ndg(l) \leq m$, i.e., l is nondegenerate on 1 to m variables. However, this characterization does not state anything about $wd(f,l)$ with $ndg(l) > m$. We show in Theorem 3.3 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 3.1 shows that 2^{m+2} divides $wd(f,l)$ for all l in $L(n)$ with $ndg(l) > m$.

Using Theorem 3.1 and Theorem 3.3 we prove nontrivial upper bounds on the nonlinearity of resilient and correlation immune functions. We believe our results are the first major results on the maximum nonlinearity of resilient functions. These nonlinearity results have deep 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 3.2 is not tight.
2. Based on Theorem 3.2 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, resiliency, nonlinearity and algebraic degree.

Maiorana-McFarland like constructions and its modifications in certain cases can be used to construct functions with the best possible trade-off between nonlinearity and resiliency (see Section 4). However, the existing constructions cannot always be used to achieve the upper bound of Theorem 3.2. This shows the inadequacy of the construction techniques proposed so far. We provide new constructions of resilient functions which achieve the upper bound of Theorem 3.2.

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 [20], 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 3.1 provides a simple proof of the same result.

Lemma 3.1 *Let f be an n-variable function of even weight and $l \in L(n)$. Then $d(f,l)$ (resp. $wd(f,l)$) is congruent to* $0 \bmod 2$ *(resp.* $0 \bmod 4$*).*

Proof : From Lemma 2.1 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. ∎

Lemma 3.2 *Let f be an n-variable, 1-resilient function and $l \in L(n)$. Then $d(f,l)$ (resp. $wd(f,l)$) is congruent to* $0 \bmod 4$ *(resp.* $0 \bmod 8$*).*

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

Proof : Using Lemma 3.2, 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. ∎

The above result was obtained in [16] using an essentially exhaustive computer search. Next we present the major result on the spectral weights of resilient functions.

Theorem 3.1 *Let f be an n-variable, m-resilient (with $n \geq 3$ and $m \leq n-3$) function and $l \in L(n)$. Then $d(f,l)$ (resp. $wd(f,l)$) is congruent to* $0 \bmod 2^{m+1}$ *(resp.* $0 \bmod 2^{m+2}$*).*

Proof : There are three inductions invloved - 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 3.1 provides the base case. If $m = 1$, then Lemma 3.2 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 3.1 and Lemma 3.2 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 3.1, it is possible to obtain an upper bound on the nonlinearity of an n-variable, m-resilient function. Let $nl(n,m)$ be the maximum possible for an n-variable, m-resilient function.

Theorem 3.2 *1. If n is even and $m+1 > \frac{n}{2} - 1$, then $nl(n,m) \leq 2^{n-1} - 2^{m+1}$.*
2. If n is even and $m+1 \leq \frac{n}{2} - 1$, then $nl(n,m) \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{m+1}$.
3. If n is odd and $2^{m+1} > 2^{n-1} - nlmax(n)$, then $nl(n,m) \leq 2^{n-1} - 2^{m+1}$.
4. If n is odd and $2^{m+1} \leq 2^{n-1} - nlmax(n)$, then $nl(n,m)$ 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 spectra 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 3.1 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 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. ∎

We state the boundary case of Theorem 3.2 in the following corollary (see also [3, 16]).

Corollary 3.2 *For $n \geq 4$, $nl(n,n-3) = 2^{n-2}$.*

Proof : From Theorem 3.2 it is clear that $nl(n,n-3) \leq 2^{n-1} - 2^{n-2} = 2^{n-2}$. 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 best function* in Section 4.

Corollary 3.3 *Let $m > \lfloor \frac{n}{2} \rfloor - 2$. Then, $nl(n,m) \leq 2^{n-1} - 2^{m+1} \leq 2^{n-1} - 2^{\lfloor \frac{n-1}{2} \rfloor}$. Further, the spectra of any $(n, m, -, 2^{n-1} - 2^{m+1})$ function is necessarily three valued.*

The upper bound for $nl(n, m)$ given by Theorem 3.2 is listed in Table 1 for the first few interesting cases. The columns represent the resiliency and the rows represent the number of variables. The entries with $*$ represent bounds which has not yet been achieved. Functions can be constructed with parameters satisfying the other entries. In particular, the entries with # represent functions which have been constructed here for the first time.

	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 3.1, Theorem 3.2.

Theorem 3.3 *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 $d(f,l)$ (resp. $wd(f,l)$) is congruent to* $0 \bmod 2^m$ *(resp.* $0 \bmod 2^{m+1}$*).*

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 3.2, we get $d(f,l)$ (resp. $wd(f,l)$) is congruent to 0 mod 4 (resp. 0 mod 8). Using these as the base cases, the proof is similar to the proof of Theorem 3.1. ■

Theorem 3.4 *Let $nlc(n,m)$ denote the highest possible nonlinearity for an n-variable function which is CI of order m. Then we have the following.*
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 spectra of any function achieving the stated bound must be three valued, i.e. the values of the Walsh distances must be $0, \pm 2^{m+1}$.

4 Construction of Resilient Functions

Motivated by Theorem 3.2, we introduce a new notion of optimality for resilient functions. An (n, m, d, x) function is said to be Type-I optimal if x is the upper bound on $nl(n, m)$ provided in Theorem 3.2. However, there is a stronger notion of optimality. Given an n-variable function, there may be more than one possible values of order of resiliency m, such that the upper bound on $nl(n, m)$ is same using Theorem 3.2. We call an n-variable, m-resilient function having nonlinearity x to be Type-II optimal if the function is Type-I optimal and further for any $p > m$ the upper bound on $nl(n,p)$ in Theorem 3.2 is strictly less than x. These notions of optimality can be further strengthened by requiring the degree to be the maximum possible. This can be done by considering Siegenthaler's inequality for balanced functions: $m + d \leq n - 1$, for any n-variable, m-resilient, degree d function. *Thus $(n, m, n-m-1, x)$ Type-II optimal functions achieve the best possible trade-off among the parameters - number of variables, order of resiliency, degree and nonlinearity.* We will refer to such functions as *best* functions.

Example 4.1 *An $(8, 2, 5, 112)$ function is Type-I optimal. Moreover, $(8, 2, -, 112)$ functions are not Type-II optimal since $nl(8, 3) \leq 112$. However, an $(8, 3, -, 112)$ function is Type-II optimal since $nl(8, 4) \leq 96$. Also* *an* $(8,3,4,112)$ *function optimizes the degree and hence it is a best function. From Theorem 3.2, the spectra of any* $(8,3,-,112)$ *function is necessarily three valued. However, this may not necessarily be true for any best function. For example, an* $(8,1,6,116)$ *function (if one exists) will be a best function, but its spectra will not be three valued.*

The way we have defined the notion of optimality it is not guaranteed whether it is possible to construct functions satisfying the notions of Type-I and Type-II optimality introduced above. The tightness of the upper bounds in Theorem 3.2 is contingent on the existence of such functions. However, we will show for certain sequences of best functions, it is possible to construct all but finitely many functions of any such sequence.

We call a best function to be *saturated* if its spectra is three valued according to Corollary 3.3. Thus an $(n, m, n-m-1, x)$-function is called *saturated best* (SB for short) if it is Type-II optimal and its spectra is three valued. For such a function we must necessarily have $m > \frac{n}{2} - 2$. Therefore, the $(8,3,4,112)$ Type-II optimal functions are saturated best. However, the $(8,1,6,116)$ Type-II optimal functions (if at all exist) can not have a three valued Walsh spectra. From Parseval's theorem, if it has a three valued Walsh spectra, then $24^2 \times z = 2^{16}$, which is not possible for integer z. Thus, the $(8,1,6,116)$ Type-II optimal functions are best but not saturated best.

Lemma 4.1 *If an* $(n, m, n-m-1, x)$ *function* f *is an SB function, then so is an* $(n+1, m+1, n-m-1, 2x)$ *function* g.

Proof : Since f is SB, $x = 2^{n-1} - 2^{m+1}$ and so $2x = 2^n - 2^{m+2}$. From Corollary 3.3, $nl(n+1, m+1) \leq 2^n - 2^{m+2}$ and hence the spectra of g is three valued. ∎

This naturally leads to a notion of a sequence of Boolean functions, each of which is an SB function. More precisely, a *saturated best function sequence* (an SBS 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 SB and the upper bound on $nl(n_0 - 1, m_0 - 1)$ in Theorem 3.2 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 SB from Lemma 4.1). Note that $n_j - m_j - 1 = n_0 - m_0 - 1$ and so the degree of all the functions in an SBS are same. Thus an SBS is completely defined by specifying the parameters of a function f_0. Note that the functions which form an SBS 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 SBS is characterized by several parameters and any sequence of functions satisfying these parameters is said to form the particular SBS.

Example 4.2 *The following seqences are SBS's.*
1. $f_0, f_1, \ldots$, *where* f_0 *is an* $(3,0,2,2)$ *function.*
2. $f_0, f_1, \ldots$, *where* f_0 *is an* $(5,1,3,12)$ *function.*
3. $f_0, f_1, \ldots$, *where* f_0 *is an* $(7,2,4,56)$ *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 SBS.*

For $i \geq 0$ we define SBS(i) as follows. An SBS(0) is a sequence $f_{0,0}, f_{0,1}, \ldots$, where $f_{0,0}$ is a $(3,0,2,2)$ function. For $i > 0$, an SBS(i) is a sequence $f_{i,0}, f_{i,1}, \ldots$, where $f_{i,0}$ is a $(3+2i, i, 2+i, 2^{2+2i} - 2^{1+i})$ SB function. Note that all functions in an SBS(i) have the same degree $2+i$. Construction of SBS(0) and SBS(1) are already known. Unfortunately, it is not known whether the initial functions for an SBS(i) exist for $i > 1$. In the next subsection we show how to construct all but finitely many initial functions of any SBS(i).

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

Lemma 4.2 *Any SB function must occur in some SBS(i).*

Proof : First note that any function of SBS(i) has algebraic degree $2+i$. Any SB 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 SBS($d-2$), i.e., in SBS($n-m-3$). ■

4.1 Construction of SBS(i)

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

Lemma 4.3 *Let $f_{i,j}$ be a j-th function of SBS(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 SBS(i). Consequently, if one can construct $f_{i,j}$, then one can construct $f_{i,k}$ for all $k > j$.*

Proof : The proof follows from Lemma 4.1 and the fact that $nl(f_{i,j+1}) = 2nl(f_{i,j})$. ■

This shows that if one can construct any one of the functions in SBS(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 SBS(0) and SBS(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 SBS(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 SBS(i). More precisely, if SBS(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 SBS(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 4.1 *For any SBS(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 $n-k+1 = 2+i$. 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 $t_0 = j$. Using Lemma 4.3 it is possible to construct $f_{i,t}$ for all $t > t_0 = j$. ■

In the proof of the above theorem we use Lemma 4.3 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.

<u>**(I)**</u> The above proof of Theorem 4.1 can be modified so that Lemma 4.3 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 3.2. 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 4.3 we can use a more powerful construction provided in [12]. The method of [12] 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 $Y_{t-j}, \ldots, Y_1$.

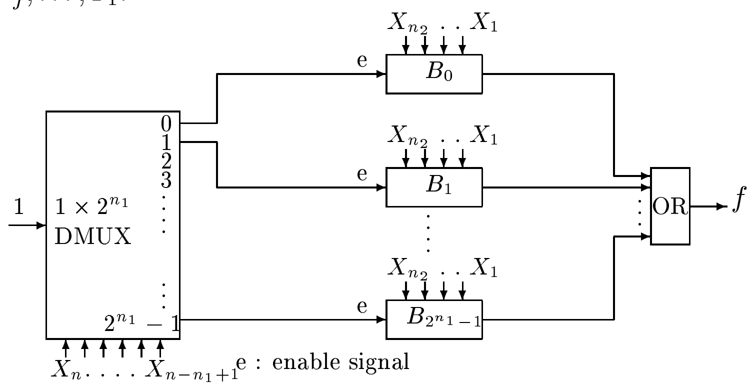

Figure 1: Hardware for Implementing SB functions

4.1.1 Implementation issues

From an implementation point of view, both the above methods can be mapped efficiently in hardware. We briefly discuss these possiblities.

If f is implemented using the sequence of constructors as described in [12] (discussed in item **(II)** above), then it is possible to implement f using a pipelined store and forward architecture. In this case the basic function [12] is $f_{i,j}$ which is constructed in Theorem 4.1 by the Maiorana-McFarland like technique.

Now we describe a simple hardware implementation strategy for the functions constructed in Theorem 4.1 and item **(I)** above. Suppose f is an n-variable function constructed by the Maiorana-McFarland like construction technique. Then we can write $n = n_1 + n_2$, where f is the concatenation of 2^{n_1} suitable linear functions from $L(n_2)$. Each linear function in $L(n_2)$ can be easily implemented using two input XOR gates. Suppose we have blocks $B_0, \ldots, B_{2^{n_1}-1}$ where each block implements one linear function in $L(n_2)$. Further, each block is required to have an enable signal, which determines whether the block should produce an output or not. To implement the function f all that is required is a 1×2^{n_1} demultimlexer, where the variables $X_n, \ldots, X_{n-n_1+1}$ act as the select variables of the demultiplexer. The input line of the demultiplexer is always set to 1 and output line i serves as enable input for block B_i. Clearly such a setup will compute f. The size of the demultiplexer is 2^{n_1} and there are 2^{n_1} blocks. The size of each block is bounded above by n_2. So the total size of the hardware is $O(n_2 2^{n_1})$. If n_1 is not large, then implementation of such functions is feasible. For example, using current technology it is possible to implement functions where $n_1 \leq 25$ and $n_2 \leq 32$.

4.2 A Sharper Construction

For SBS(2) $= f_{2,0}, f_{2,1}, f_{2,2}, \ldots$, Theorem 4.1 can be used to construct $f_{2,t}$ for all $t \geq 3$. Here we show how to construct $f_{2,1}$ ($(8, 3, 4, 112)$ Type-II optimal function). This requires a nontrivial spectral analysis leading to a new construction methodology. However, the construction of $f_{2,0}$ ($(7, 2, 4, 56)$ Type-II optimal function) is not yet known. Thus, we want to construct a 3-resilient function $f \in \Omega_8$ with maximum possible algebraic degree 4 and nonlinearity 112. 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.

Lemma 4.4 *Let f_1, f_2 be two $(7, 3, -, 48)$ functions such that $NZ(f_1) \cap NZ(f_2) = \emptyset$. Let $f \in \Omega_8$ be $f = (1 \oplus X_8)f_1 \oplus X_8 f_2$. Then, f is an $(8, 3, -, 112)$ function.*

First let us construct the function f_2 using linear concatenation. We take four 5-variable linear functions 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 spectra 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 3.2, this is a three valued Walsh spectra.

Next we need to use the following basic idea. *When $d(f_2, l)$ is minimum, then $d(f_1, l)$ must be 2^{n-2}, 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 spectra 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 spectra of the function need to be such that $wd(g, l_{5i}) = 0$ for $1 \leq i \leq 4$. We choose g to be 000001110111111001110010110100010 by running 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 spectra 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 (resp. f_2) which are not in f_2 (resp. f_1). Hence, $f = (1 \oplus X_8)f_1 \oplus X_8 f_2$ is an $(8, 3, 4, 112)$ function. The function is the 256-bit string described below.

0000011101111110011100101101000101111110001000000110001101001011101
1111100010000001100011010010111010000001110111111001110010110100010
0110100110010110011010011001011001101001011010011001011010010110
0110011010011001100110010110011001011010101001011010010101011010

Theorem 4.2 *It is possible to construct $(8, 3, 4, 112)$ and $(9, 4, 4, 224)$ functions.*

Proof : Above we discussed how to construct a $(8, 3, 4, 112)$ function f. Now $X_9 \oplus f$ is a $(9, 4, 4, 224)$ function. Note that we can also construct a $(9, 4, 4, 224)$ function as $(1 \oplus X_9)f(X_8, \ldots, X_1) \oplus X_9(1 \oplus f(1 \oplus X_8, \ldots, 1 \oplus X_1))$ where the function does not depend linearly on X_9. ■

5 On Construction of Small Functions

The maximum nonlinearity question for all Boolean functions on even number of variables has been solved quite some time back [17]. The same question for odd number of variables has been solved for odd $n \leq 7$ [14, 7]. Further, the maximum nonlinearity question is completely solved for balanced and resilient functions on n variables for $n \leq 5$. Now we consider the cases $n = 6$ to $n = 10$ separately.

<u>*Case $n = 6$*</u>: A bent function on 6 variables has nonlinearity 28. It is possible to construct balanced functions on 6 variables having maximum nonlinearity 26 (see [21]). In [16], a computer search was carried out on 6-variable resilient functions and the maximum nonlinearities for 1, 2 and 3 resilient functions were shown to be 24, 24, 16 respectively. These results follow very easily from Corollary 3.1 and Theorem 3.2. Also it is possible to construct $(6, 1, 4, 24)$, $(6, 2, 3, 24)$ and $(6, 3, 2, 16)$ functions.

<u>*Case $n = 7$*</u>: The maximum possible nonlinearity for balanced functions is 56. Here we have shown that the maximum possible nonlinearity for 1, 2, 3, 4 resilient functions are respectively 56, 56, 48, 32. The construction of $(7, 1, 5, 56)$, $(7, 3, 3, 48)$ and $(7, 4, 2, 32)$ functions are known [20]. However, the construction of $(7, 2, -, 56)$ function seems to be a difficult one.

Case $n = 8$: A bent function on 8 variables has nonlinearity 120. The maximum possible nonlinearity of balanced functions is 118. It is possible to construct balanced functions on 8 variables having nonlinearity 116 [21]. The problem of constructing an 8-variable balanced function with nonlinearity 118 has been open for quite some time. Here we present a result which could be an important step in solving this problem.

Theorem 5.1 *Let if possible f be a $(8, 0, -, 118)$ function. Then one can write $f = (1 \oplus X_8)f_1 \oplus X_8 f_2$, where f_1 and f_2 are 7-variable functions having nonlinearity 55 each.*

Proof : First we prove that the degree of f must be 7. If the degree of f is less than 7, then using [7, Lemma 2.1], we can perform an affine transformation on the varibles of f to obtain an 8-variable function g, such that $g = (1 \oplus X_8)g_1 \oplus X_8 g_2$ and the degrees of g_1 and g_2 ($g_1, g_2 \in \Omega_7$) 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 [11]) 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 $2 \bmod 4 \equiv 118 = d(g, \lambda\lambda) = d(g_1, \lambda) + d(g_2, \lambda)$ 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 5.1 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 the question of maximum nonlinearity for resilient 8-variable function. Using Theorem 3.2, the maximum possible nonlinearities for 1, 2, 3, 4, 5-resilient functions are 116, 112, 112, 96, 64 respectively. Construction of $(8, 2, 5, 112), (8, 4, 3, 96), (8, 5, 2, 64)$ functions is known [20]. In Theorem 4.2 we showed how to construct $(8, 3, 4, 112)$ functions. The existence of $(8, 1, -, 116)$ is an open question.
Case $n = 9$: The maximum nonlinearity question for 9-variable functions is an outstanding open problem of coding theory. The known upper bound [8] is 244. It is easy to construct balanced functions with nonlinearity 240. Using Theorem 3.2, the maximum possible nonlinearities for 1, 2, 3, 4, 5, 6-resilient functions are 244, 240, 240, 224, 192, 128 respectively. Construction of $(9, 1, 7, 240), (9, 2, 5, 240), (9, 3, 5, 224), (9, 5, 3, 192), (9, 6, 2, 128)$ functions is known [20]. In Theorem 4.2 we showed how to construct $(9, 4, 4, 224)$ functions. Construction of $(9, 1, -, 244), (9, 2, 6, 240)$ and $(9, 3, -, 240)$ functions are open.
Case $n = 10$: A bent function on 10 variables has nonlinearity 496. The maximum possible nonlinearity of balanced functions is 494. The construction of [21] can provide balanced functions with nonlinearity 492. Using Theorem 3.2, the maximum possible nonlinearities for 1, 2, 3, 4, 5, 6, 7-resilient functions are 492, 488, 480, 480, 448, 384, 256 respectively. Construction of $(10, 1, 8, 484), (10, 2, 7, 480), (10, 3, 5, 480)$, $(10, 3, 6, 464), (10, 4, 5, 448), (10, 5, 4, 448), (10, 6, 3, 384), (10, 7, 2, 256)$ functions is known [20]. Construction of $(10, 1, -, 492), (10, 1, -, 488), (10, 2, -, 488), (10, 3, 6, 480), (10, 4, -, 480)$ functions is currently not known. Next we show how to construct $(10, 3, 6, 480)$ functions. Note that the function we construct is not an SB function and its Walsh spectra is five-valued $(0, \pm 32, \pm 64)$.

Theorem 5.2 *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. ∎

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

[9] 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.

[10] 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.

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

[12] 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.

[13] 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.

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

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

[18] R. A. Rueppel. *Analysis and Design of Stream Ciphers*. Springer Verlag, 1986.

[19] 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.

[20] P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. In *Advances in Cryptology - EUROCRYPT'2000 (to be published)*, Lecture Notes in Computer Science. Springer Verlag, MAY 2000.

[21] 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.

[22] 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.

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

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