Construction of Nonlinear Boolean Functions with Important Cryptographic Properties

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. This paper addresses the problem of obtaining new construction methods for cryptographically significant Boolean functions. We show that for each positive integer m, there are infinitely many integers n (both odd and even), such that it is possible to construct n-variable, m-resilient functions having nonlinearity greater than $2^{n-1} - 2^{\lfloor \frac{n}{2} \rfloor}$. Also we obtain better results than all published works on the construction of n-variable, m-resilient functions, including cases where the constructed functions have the maximum possible algebraic degree $n - m - 1$. Next we modify the Patterson-Wiedemann functions to construct balanced Boolean functions on n-variables having nonlinearity strictly greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ for all odd $n \geq 15$. In addition, we consider the properties strict avalanche criteria and propagation characteristics which are important for design of S-boxes in block ciphers and construct such functions with very high nonlinearity and algebraic degree.

1 Introduction

The following four factors are important in designing Boolean functions for stream cipher applications.

Balancedness. An n-variable Boolean function f is said to be balanced if $wt(f) = 2^{n-1}$, where $wt(.)$ gives the Hamming weight and f is considered to be represented by a binary string of length 2^n.

Nonlinearity. The nonlinearity of an n-variable Boolean function f, denoted by $nl(f)$, is the (Hamming) distance of f from the set of all n-variable affine functions. We denote by $nlmax(n)$ the maximum possible nonlinearity of n-variable functions.

Algebraic Degree. An n-variable Boolean function f can be represented as a multivariate polynomial over $GF(2)$. This polynomial is called the Algebraic Normal Form (ANF) of f. The degree of this polynomial is called the algebraic degree or simply the degree of f and is denoted by $deg(f)$. It is easy to see that the maximum algebraic degree of an n-variable balanced function is $n - 1$.

B. Preneel (Ed.): EUROCRYPT 2000, LNCS 1807, pp. 485–506, 2000.

Correlation Immunity. An n-variable Boolean function $f(X_n, \ldots, X_1)$ is said to be correlation immune (CI) of order m if $Prob(f = 1 \mid X_{i_1} = c_1, \ldots, X_{i_m} = c_m) = Prob(f = 1)$, for any choice of distinct $i_1, \ldots, i_m$ from $1, \ldots, n$ and $c_1, \ldots, c_m$ belong to $\{0, 1\}$. A balanced m-th order correlation immune function is called m-resilient. Siegenthaler [16] proved a fundamental relation between the number of variables n, degree d and order of correlation immunity m of a Boolean function : $m + d \leq n$. Moreover, if the function is balanced then $m + d \leq n - 1$.

The set of all n-variable Boolean functions is denoted by Ω_n. We denote by $A_n(m)$ the set of all balanced n-variable functions which are CI of order m. By an (n, m, d, x) function we mean an n-variable, m-resilient function having degree d and nonlinearity x. By an $(n, 0, d, x)$ function we mean an n-variable, degree d, balanced function with nonlinearity x.

A good Boolean function must possess a "good combination" of the above properties to be used in stream ciphers. Previous works to construct such good functions have proceeded in two ways.

1. In the first approach the degree is ignored and the number of variables and correlation immunity are fixed. One then tries to get a function having as high nonlinearity as possible. This approach has been considered in [15,2] and we call this the $Type-A$ approach.
2. The second approach considers the degree. However, by Siegenthaler's inequality, the maximum possible degree of an n-variable, m-resilient function is $n - m - 1$. Functions achieving this degree have been called *optimized* [7]. As in the first approach one then tries to get as high nonlinearity as possible for optimized functions. Design methods for this class of functions have been considered in [4,7,8,18] and we call this the $Type-B$ approach.

Previous efforts at obtaining resilient functions have sometimes employed *heuristic search techniques* [4,8]. In certain cases these have provided better results than *constructive techniques* [15,7]. The list of all such known cases are as follows : (a) $(7, 0, 6, 56)$, $(9, 0, 7, 240)$ and $(9, 2, 6, 224)$ functions from [4] and (b) $(9, 1, 7, 236)$, $(10, 1, 8, 480)$ and $(11, 1, 9, 976)$ functions from [8]. These examples are indicative of the inadequacies of the current constructive techniques. However, heuristic searches cannot be conducted for moderate to large number of variables.

Here we provide a systematic theory for the design of resilient functions. Our techniques are sharp enough to obtain general results which are better than all the examples mentioned above. Corresponding to the list given above we have $(7, 0, 6, 56)$, $(9, 0, 8, 240)$, $(9, 2, 6, 232)$, $(9, 1, 7, 240)$, $(10, 1, 8, 484)$ and $(11, 1, 9, 992)$ functions. Also we are able to prove some difficult results on the nonlinearity of resilient functions. Here for the first time we show that for each order of resiliency m, there are infinitely many n (both odd and even), such that it is possible to construct n-variable, m-resilient functions having nonlinearity greater than $2^{n-1} - 2^{\lfloor \frac{n}{2} \rfloor}$. One consequence of this result is that it completely disproves the conjecture on nonlinearity made in [8]. We use our techniques to present design algorithms for optimized resilient functions and obtain superior results to all known work in this area (see Section 6 for details). The functions constructed by our methods have a nice representation and though they have quite complicated algebraic normal forms they can be implemented efficiently in hardware. See [12] for details of the hardware implementation.

Next we describe the other contributions of this paper. In Section 7, we use a randomized heuristic to construct for the first time balanced functions with nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ for $n = 15, 17, 19, 21, 23, 25, 27$. We use the functions provided in [9] as the basic input to our algorithm. Earlier these functions [9] were used to obtain balanced functions with nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ only for odd $n \geq 29$ [14]. Also the functions we construct posses maximum algebraic degree $(n-1)$.

S-boxes can be viewed as a set of Boolean functions [10,6]. Propagation Characteristic(PC) and Strict Avalanche Criteria(SAC) are important properties of Boolean functions to be used in S-boxes. Preneel et al [10] provided basic construction techniques for Boolean functions with these properties.

Propagation Characteristic and Strict Avalance Criteria. Let $\overline{X}$ be an n tuple $X_1, \ldots X_n$ and $\overline{\alpha} \in \{0,1\}^n$. A function $f \in \Omega_n$ is said to satisfy
(1) SAC if $f(\overline{X}) \oplus f(\overline{X} \oplus \overline{\alpha})$ is balanced for any $\overline{\alpha}$ such that $wt(\overline{\alpha}) = 1$.
(2) SAC(k) if any function obtained from f by keeping any k input bits constant satisfies SAC.
(3) PC(l) if $f(\overline{X}) \oplus f(\overline{X} \oplus \overline{\alpha})$ is balanced for any $\overline{\alpha}$ such that $1 \leq wt(\overline{\alpha}) \leq l$.
(4) PC(l) of order k if any function obtained from f by keeping any k input bits constant satisfies PC(l).

In [10], it has been shown that for balanced SAC(k) functions on n variables, $deg(f) \leq n - k - 1$. Recently in [6], balanced SAC(k) functions on n variables with $deg(f) = n - k - 1$ has been identified for $n - k - 1 =$ odd. However, construction of such functions for $n - k - 1 =$ even has been left as an open problem. In [6], balanced SAC(k) functions with high algebraic degree have been proposed. However, balanced SAC(k) functions with both high algebraic degree and high nonlinearity have not been studied. PC(l) of order k functions with good nonlinearity and algebraic degree have been reported in [6].

In Section 8, first we improve the algebraic degree and nonlinearity results of the PC(l) of order k functions reported in [6]. Then motivated by the construction methods of SAC(k) functions in [6], we introduce a new cryptographic criterion called the *restricted balancedness* of Boolean functions and show that certain types of bent functions satisfy this property. Also we modify the functions provided by Patterson and Wiedemann [9] to obtain restricted balancedness while keeping the nonlinearity unchanged. For the first time we consider the properties of balancedness, SAC(k), algebraic degree and nonlinearity together. We construct balanced (using the functions with restricted balancedness) SAC(k) functions in Ω_n with maximum possible algebraic degree $n-k-1$ and very high nonlinearity for $k \leq \frac{n}{2} - 1$. This also shows that there exists balanced SAC(k) functions on n variables with $deg(f) = n - k - 1 =$ even, which was posed as an open question in [6]. Also, we present an interesting result on resilient functions satisfying PC(k). In a previous work [15], it was shown that resilient functions satisfy propagation characteristics with respect to a set of input vectors, but not PC(k) for some k.

2 Preliminaries

The Hamming weight (or simply the weight) of a binary string s is denoted by $wt(s)$ and is the number of ones in the string s. The length of a string s is denoted by $\mid s \mid$ and the concatenation of two strings s_1 and s_2 is written as $s_1 s_2$. Given a string s, we define s^c to be the string which is the bitwise complement of s. The operation $x \oplus y$ on two strings x, y performs the bitwise exclusive OR of the strings x and y.

Let s_1, s_2 be two bit strings of length n each. Then $\#(s_1 = s_2)$ (resp. $\#(s_1 \neq s_2)$) denotes the number of positions where s_1 and s_2 are equal (resp. unequal). The Hamming distance between two strings s_1 and s_2, is denoted by $d(s_1, s_2)$ and is given by $d(s_1, s_2) = \#(s_1 \neq s_2) = wt(s_1 \oplus s_2)$. The Walsh distance between the strings s_1 and s_2 is denoted by $wd(s_1, s_2)$ and is given by $wd(s_1, s_2) = \#(s_1 = s_2) - \#(s_1 \neq s_2)$. The relation between these two measures is as follows. Let s_1, s_2 be two binary strings of length x each. Then $wd(s_1, s_2) = x - 2d(s_1, s_2)$.

Given a bit b and a string $s = s_0 \ldots s_{n-1}$, the string b AND $s = s'_0 \ldots s'_{n-1}$, where $s'_i = b$ AND s_i. The Kronecker product of two strings $x = x_0 \ldots x_{n-1}$ and $y = y_0 \ldots y_{m-1}$ is a string of length nm, denoted by
$x \otimes y = (x_0$ AND $y) \ldots (x_{n-1}$ AND $y)$. The direct sum of two strings x and y, denoted by $x\$y$ is given by $x\$y = (x \otimes y^c) \oplus (x^c \otimes y)$. As an example, if $f = 01$, and $g = 0110$, then $f\$g = 01101001$. Note that both the Kronecker product and the direct sum are not commutative operations. The following result will prove to be important later.

Lemma 1. *Let f_1, f_2 be strings of equal length and g a string of length n. Then $d(f_1\$g, f_2\$g) = n \times d(f_1, f_2)$.*

Four basic properties of direct sum of Boolean functions are given below without proof (see also [9,15]).

Proposition 1. *Let $f(X_n, \ldots, X_1) \in \Omega_n$ and $g(Y_m, \ldots, Y_1) \in \Omega_m$, with $\{X_n, \ldots, X_1\} \cap \{Y_m, \ldots, Y_1\} = \emptyset$. Then $f\$g$ is in Ω_{n+m} and*
(a) The ANF of $f\$g$ is given by $f(X_n, \ldots, X_1) \oplus g(Y_m, \ldots, Y_1)$.
(b) $f\$g$ is balanced iff at least one of f and g is balanced.
(c) Let f be k_1-resilient and g be k_2-resilient. Then $f\$g$ is $\max(k_1, k_2)$-resilient. Also $f\$g$ is m-resilient if at least one of f or g is m-resilient.
(d) $nl(f\$g) = 2^n nl(g) + 2^m nl(f) - 2nl(f)nl(g)$.

An n-variable Boolean function $f(X_n, \ldots X_1)$ is said to be affine if the ANF of f is of the form $f(X_n, \ldots, X_1) = \bigoplus_{i=1}^{n} a_i X_i \oplus b$ for $a_i, b \in \{0, 1\}$. If b is 0, then the function is said to be linear. Also f is said to be nondegenerate on t variables if t out of n a_i's are 1 and rest are 0. Next we define the following subsets of linear/affine functions.
1. The set $L_n(k)$ (resp. $F_n(k)$) is the set of all n-variable linear functions (resp.

affine functions) which are non-degenerate on exactly k variables.
2. $UL_n(k) = L_n(k) \cup \ldots \cup L_n(n)$ and $DL_n(k) = L_n(1) \cup \ldots \cup L_n(k)$.
3. $UF_n(k) = F_n(k) \cup \ldots \cup F_n(n)$ and $DF_n(k) = F_n(1) \cup \ldots \cup F_n(k)$.
4. $L_n = L_n(0) \cup L_n(1) \cup \ldots \cup L_n(n)$ and $F_n = F_n(0) \cup F_n(1) \cup \ldots \cup F_n(n)$.
The sets L_n and F_n are respectively the sets of all linear and affine functions of n variables. The following result states three useful properties of affine functions.

Lemma 2. *(a) Let $l \in F_n(m)$ and k $(1 \leq k \leq n)$ be an integer. Then $l = l_1 \$ l_2$ for some $l_1 \in L_{n-k}(r)$ and $l_2 \in F_k(m-r)$ for some $r \geq 0$.*
(b) Let $l_1, l_2 \in F_n$. Then $d(l_1, l_2) = 0, 2^n, 2^{n-1}$ (resp. $wd(l_1, l_2) = 2^n, -2^n, 0$) according as $l_1 = l_2$, $l_1 = l_2^c$ or $l_1 \neq l_2$ or l_2^c.
(c) If l is in $UF_n(m+1)$, then l is m-resilient.

Siegenthaler [16] was the first to define CI functions and point out its importance in stream ciphers [17]. A useful characterization of correlation immunity based on Walsh Transform was obtained in [5]. The following result translates the Walsh transform characterization of correlation immunity to Walsh distances.

Theorem 1. *A n-variable Boolean function f is correlation immune of order m, iff $wd(f, l) = 0$, for all $l \in DF_n(m)$.*

3 Construction Ideas for Resilient Functions

3.1 Basic Results

We first define two subsets of Ω_n. Later we will provide construction methods for certain subsets of these sets which have good cryptographic properties.

Definition 1.
1. $\Gamma(n, k, m) = \{f \in \Omega_n : f = f_0 \ldots f_{2^{n-k}-1}, f_i \in A_k(m),\ wt(f_i) = 2^{k-1}\}$.
2. $\Gamma_1(n, k, m) = \{f \in \Omega_n : f = f_0 \ldots f_{2^{n-k}-1}, f_i \in UF_k(m+1)\}$.

Theorem 2. *$\Gamma(n, k, m) \subseteq A_n(m)$.*

Proof : Observe that if f and g are resilient of order m then so is fg. The result then follows from repeated application of this fact. □

Since any function in $UF_k(m+1)$ is m-resilient, we have the following result.

Lemma 3. *$\Gamma_1(n, k, m) \subset \Gamma(n, k, m)$.*

The set $\Gamma_1 = \bigcup_{n \geq 3} \bigcup_{1 \leq m \leq n-1} \bigcup_{m+1 \leq k \leq n} \Gamma_1(n, k, m)$ was first obtained by Camion et al in [1], though in an entirely different form. We will show that the extension obtained in Theorem 2 is important and provides optimized functions with significantly better nonlinearities.

Theorem 3. *Let $f \in \Gamma(n, k, m)$ be of the form $f_0 \ldots f_{2^{n-k}-1}$. Let the logical AND of r variables, $X_{i_1} \ldots X_{i_r}$ $(i_1, \ldots, i_r \in \{1, \ldots, k\})$ be a term which occurs in the ANF of an odd number of the f_i's. Then the term $X_n \ldots X_{k+1} X_{i_1} \ldots X_{i_r}$ occurs in the algebraic normal form of f.*

Corollary 1. *Let $f \in \Gamma_1(n,k,m)$ be of the form $f_0 \ldots f_{2^{n-k}-1}$ and let X_i ($i \in \{1,\ldots,k\}$) be a variable which occurs in an odd number of the f_i's. Then the term $X_n \ldots X_{n-k+1} X_i$ occurs in the algebraic normal form of f and hence f is of degree $n-k+1$. Moreover, the maximum degree $n-m-1$ is attained when $k = m+2$.*

Corollary 1 was obtained in [15] and it places a restriction on the value of k for optimized functions in $\Gamma_1(n,k,m)$. However, this restriction can be lifted by using Theorem 3.

Lemma 4. *A degree optimized $(n,m,n-m-1,x)$ function is always nondegenerate.*

The ANF of the functions in Γ and Γ_1 are not simple. This is important from a cryptographic point of view. Given n,m,k, in most cases it is possible to choose two functions f_1 and f_2, such that the ANF's of both f_1 and f_2 are complicated and $f_1 \oplus f_2$ is nondegenerate and has a complicated ANF. In particular, one can choose f_1 and f_2, such that all three functions f_1, f_2 and $f_1 \oplus f_2$ do not depend linearly on any input variable. It is also possible to design functions such that each variable occurs in a maximum degree term. This is possible by ensuring each variable occurs an odd number of times as mentioned in Corollary 1.

In the next four subsections we present the ideas behind the basic construction techniques to be used in this paper. In the later sections we combine several of these ideas to construct resilient functions with very high nonlinearities.

3.2 Method Using Direct Sum with Nonlinear Functions

We first consider the set $\Gamma_1(n,k,m)$. A function f in $\Gamma_1(n,k,m)$ is a concatenation of affine functions in $UF_k(m+1)$. Since there are 2^{n-k} slots to be filled and a maximum of $p = \binom{k}{m+1} + \ldots + \binom{k}{k}$ linear functions in $UL_k(m+1)$, it follows that at least one linear function and its complement must together be repeated at least $t = \lceil \frac{2^{n-k}}{p} \rceil$ times. *We call a linear function and its complement a linear couple. When we say that a linear couple is repeated t times, we mean that the corresponding linear function and its complement are repeated t times in total.* Using Lemma 2, any affine function l in F_n can be considered to be a concatenation of some linear couple in F_k. Thus if one is not careful in constructing f, it may happen that f and l agree at all places for some linear couple repeated t times in f. This means that the nonlinearity drops by $t2^{k-1}$ and gives a lower bound of $2^{n-1} - t2^{k-1}$ on the nonlinearity of f. This is the bound obtained in [15]. However, one can construct $f \in \Gamma_1(n,k,m)$ with significantly better nonlinearities. The following result is the key to the construction idea.

Theorem 4. *Let $f \in \Gamma_1(n,k,m)$ be of the form $f_1 \ldots f_p$ where, $p = 2^{n-k-r}$ for some r and for each i, f_i is in Ω_{k+r} and is of the form $f_i = g_i \$ \lambda_i$, where g_i is a maximum nonlinear function on r variables and λ_i is in $UL_k(m+1)$. Also the λ_i's are distinct. Then $nl(f) = 2^{n-1} - (2^r - 2 \times nlmax(r))2^{k-1}$.*

Proof : By construction f is a concatenation of linear couples λ_i, λ_i^c from $UF_k(m+1)$. Let l be in F_n and is a concatenation of linear couple μ, μ^c for some μ in L_k. If $\lambda_i \neq \mu$ for any i, then $d(f,l) = 2^{n-1}$. On the other hand if $\lambda_i = \mu$, for some i, then $d(f,l) = (2^{n-k} - 2^r)2^{k-1} + d(g_i\$\lambda_i, \eta_i\$\mu)$, for some η_i in F_r. From Lemma 1, $d(g_i\$\lambda_i, \eta_i\$\mu) = 2^k d(g_i, \eta_i)$ and so $d(f,l) = 2^{n-1} - (2^r - 2d(g_i, \eta_i))2^{k-1}$. Since g_i is a maximum nonlinear function on r variables, $nl(g_i) = nlmax(r)$ and so $nlmax(r) \leq d(g_i, \eta_i) \leq 2^r - nlmax(r)$. Hence we get, $2^{n-1} - (2^r - 2nlmax(r))2^{k-1} \leq d(f,l) \leq 2^{n-1} + (2^r - 2nlmax(r))2^{k-1}$. This gives $nl(f) = 2^{n-1} - (2^r - 2 \times nlmax(r))2^{k-1}$. □

3.3 Fractional Nonlinearity and Its Effect

In the previous section we considered the case when each linear couple is repeated t times, where t is a power of 2. In general it might be advantageous to repeat a linear couple t times even when t is not a power of 2. To see the advantage we need to introduce the notion of nonlinearity of "fractional functions". Let $2^{r-1} < t \leq 2^r$. Given a string l of length 2^r, let $First(l,t)$ be a string consisting of the first t bits of l. The (fractional) nonlinearity of a string g of length t is denoted by $fracnl(g)$ and defined as $fracnl(g) = \min_{l \in F_r} d(First(l,t), g)$. Given a positive integer t, the maximum possible fractional nonlinearity attainable by any string of length t is denoted by $Fracnlmax(t)$ and defined as $Fracnlmax(t) = \max_{g \in \{0,1\}^t} fracnl(g)$. When $t = 2^r$, $Fracnlmax(t) = nlmax(r)$. Also $Fracnlmax(2^r + 1) = nlmax(r)$ and $Fracnlmax(2^r - 1) = nlmax(r) - 1$. It is clear that $Fracnlmax(t)$ is a nondecreasing function. If a linear couple is repeated 2^r times, then by Theorem 4, the fall in nonlinearity is by a factor of $(2^r - 2 \times nlmax(r))$. Motivated by this we define $Effect(t) = t - 2Fracnlmax(t)$ as the factor by which nonlinearity falls when a linear couple is repeated t times. In the construction of a function f in $\Gamma_1(n,k,m)$ if the distinct linear couples are repeated $t_1, \ldots, t_p$ times then $nl(f) = \min_{1 \leq i \leq p}(2^{n-1} - 2^{k-1}Effect(t_i))$. The interesting point about $Effect(t)$ is that it is not a monotone increasing function. An important consequence of this is that the nonlinearity may fall by a lesser amount when a linear couple is repeated more times.

1. $Effect(2^r - 1) = 2^r - 1 - 2(nlmax(r) - 1) = 2^r + 1 - 2nlmax(r) = Effect(2^r + 1) > Effect(2^r)$.
2. $Effect(2^r) \geq Effect(2^{r-1})$ and $Effect(2^r) > Effect(2^{r-2} + 1)$.
3. If r is odd, $Effect(2^r) > Effect(2^{r-1} + 1)$.
4. If r is even, $Effect(2^r) < Effect(2^{r-1} + 1)$, assuming $nlmax(r-1) = 2^{r-2} - 2^{\frac{r-2}{2}}$. If $r - 1 \geq 15$, the calculations are more complicated because of the existence of functions in [9].

One can also define fractional nonlinearity and $Effect()$ for balanced strings (provided t is even). We believe that the idea of fractional nonlinearity is important and to the best of our knowledge it has not appeared in the literature before.

3.4 Use of All Linear Functions

Here we show how to extend the set Γ_1. To construct a function $f \in \Gamma_1(n, k, m)$ we have to concatenate affine functions in $UF_k(m+1)$. However, it is possible to use all the affine functions in F_k to construct n-variable, m-resilient functions. Let l be a function in L_k which is nondegenerate on r $(1 \leq r \leq m)$ variables. Then ll^c is 1-resilient and repeating this procedure $m - r + 1$ times one can construct a function g in $UL_{k+m-r+1}(m+1)$. The linear couple g, g^c can then be used in the construction of m-resilient functions. The importance of this technique lies in the fact that it helps in reducing the repetition factor of linear couples in $UF_k(m+1)$. However, one should be careful in ascertaining that the loss in nonlinearity due to the use of affine functions from $DF_k(m)$ does not exceed the loss in repeating linear couples from $UF_k(m+1)$. In Theorem 9 and Theorem 10, we show examples of how this technique can be used to construct optimized functions.

3.5 Use of Nonlinear Resilient Function

Here also we extend Γ_1, though in a different way. Corollary 1 places a restriction on the value of k in $\Gamma_1(n, k, m)$ for optimized functions : $k = m + 2$. This in turn restricts the number of linear couples to be used in the construction to $m + 3$, thus increasing the repetition factor. However, if we allow $k > m + 2$, the problem is that the degree will fall. To compensate this we use one nonlinear m-resilient function on k variables and having degree $k - m - 1$ with the maximum possible nonlinearity. By Theorem 3, the overall function will have degree $n - m - 1$ but the number of available linear couples increases to $\mid UF_k(m+1) \mid > \mid UF_{m+2}(m+1) \mid$. This reduces the repetition factor. In Subsection 5.2, we outline a design procedure for optimized functions based on this idea. Also in Section 4, we show how all the above ideas can be combined to disprove the conjecture of Pasalic and Johansson [8] for optimized functions.

4 Nonlinearity of Resilient Functions

A proper subset S of Γ_1 was considered in [2], where only concatenation of linear (not affine) functions were used to construct functions in Γ_1. In particular, it was shown in [2] that the maximum possible nonlinearity for n-variable resilient functions in S is $2^{n-1} - 2^{\lfloor \frac{n}{2} \rfloor}$. In a more recent paper, Pasalic and Johansson [8] have shown that the maximum possible nonlinearity of 6-variable, 1-resilient functions is 24. The same paper conjectured that the maximum possible nonlinearity of n-variable, 1-resilient functions is $2^{n-1} - 2^{\lfloor \frac{n}{2} \rfloor}$. *We provide infinite counterexamples to this conjecture.* In fact, we show that given a fixed order of resiliency m, one can construct n-variable functions which are m-resilient and have nonlinearity greater that $2^{n-1} - 2^{\lfloor \frac{n}{2} \rfloor}$. Moreover, the conjecture is disproved for optimized functions as well as for functions in Γ_1.

Theorem 5. *Let m be a fixed positive integer. Then there are infinitely many odd positive integers n_o (resp. even positive integers n_e), such that one can construct functions f of n_o (resp. n_e) variables which are m-resilient and $nl(f) > 2^{n_o-1} - 2^{\frac{n_o-1}{2}}$ (resp $nl(f) > 2^{n_e-1} - 2^{\frac{n_e}{2}}$).*

Proof : First note that if we can prove the result for odd number of variables and for all $m \geq 1$, then the result is proved for even number of variables and all $m > 1$. We also need a proof for even number of variables and $m = 1$. These we proceed to do via the following sequence of results. □

Theorem 6. *Let m be a fixed positive integer. Choose ϵ, n_1, n_2 such that (a) $n_1 + n_2$ is even, (b) $n_2 - n_1 = \epsilon n_1 = 2k$, for some $k \geq 4$, (c) $\frac{1}{2} \leq \epsilon \leq 1$, (d) $\binom{n_1}{m} + \ldots + \binom{n_1}{0} \leq 2^{(1-\epsilon)n_1} - 1$. Then it is possible to construct an m-resilient function on $n = n_1 + n_2 + 15$ variables having nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}$. Moreover, it is possible to construct such functions having maximum degree $n - m - 1$.*

Proof : First we construct an m-resilient function g on $q = n_1 + n_2$ variables having nonlinearity $nl(g) = 2^{q-1} - 2^{\frac{q}{2}-1} - 2^{n_1-1}$. Then we let $f = h\$g$, where h is a function on 15 variables having nonlinearity $nl(h) = 16276 = 2^{14} - 108$. This h can be constructed using the method of [9]. The function f is m-resilient (from Proposition 1) and the overall nonlinearity of f is obtained as $nl(f) = nl(h)2^q + nl(g)2^{15} - 2nl(h)nl(g)$. Simplifying, we get $nl(f) = 2^{q+14} - 108(2^{\frac{n_2-n_1}{2}} + 1)2^{n_1}$. Using $n_2 - n_1 = 2k$, this simplifies to $nl(f) = 2^{q+14} - 108(2^k + 1)2^{n_1}$. On the other hand, $\frac{n-1}{2} = 7 + n_1 + k$. Since $108(2^k + 1) < 2^{7+k}$ for $k \geq 4$, we get $nl(f) > 2^{n-1} - 2^{\frac{n-1}{2}}$. Thus if we show how to construct g then the proof will be complete.

The function g is in $\Gamma_1(q, n_1, m)$ and is constructed in a way similar to that in Theorem 4. Since g is to be m-resilient we are restricted to using linear couples from $UF_{n_1}(m+1)$ and there are $2^{n_1} - p$ linear couples in $UF_{n_1}(m+1)$, where, $p = \binom{n_1}{m} + \ldots + \binom{n_1}{0} \leq 2^{(1-\epsilon)n_1} - 1$ These have to be used to fill up 2^{n_2} slots and so the maximum repetition factor for each linear couple is $\lceil \frac{2^{n_2}}{p} \rceil = 2^{n_2 - n_1} + 1$ by choice of the parameters ϵ, n_1, n_2. Thus each linear couple is repeated either $2^{n_2-n_1} + 1$ times or $2^{n_2-n_1}$ times. Suppose a linear couples are repeated $2^{n_2-n_1} + 1$ times and b linear couples are repeated $2^{n_2-n_1}$ times. Let $\lambda_1, \ldots, \lambda_a$ be distinct linear functions from $UL_{n_1}(m+1)$ and $\mu_1, \ldots, \mu_b$ be distinct linear functions from $UL_{n_1}(m+1)$ which are also distinct from $\lambda_1, \ldots, \lambda_a$. Let $\alpha_1, \ldots, \alpha_a$ and $\beta_1, \ldots, \beta_b$ be bent functions of $n_2 - n_1$ variables. The function g is a concatenation of the following sequence of functions: $\alpha_1\$\lambda_1, \ldots, \alpha_a\$\lambda_a, \beta_1\$\mu_1, \ldots, \beta_b\$\mu_b, \lambda_1, \ldots, \lambda_a$.
Using the same idea as in the proof of Theorem 4 one can show that $nl(g) = 2^{q-1} - (2^{\frac{q}{2}-1} + 2^{n_1-1})$. This completes the proof of the first part of the Theorem.

To obtain maximum possible degree $n - m - 1$ in the above construction we do the following. In the constructed function f, replace the last 2^{n_1} bits by an n_1-variable, m-resilient optimized function. Using Theorem 3 it follows that f becomes optimized. Also nonlinearity remains greater than $2^{n-1} - 2^{\frac{n-1}{2}}$. □

Example: For $m = 1$*, choose* $n_1 = 10, n_2 = 16$ *and* $\epsilon = \frac{3}{5}$*. This provides* 1*-resilient,* 41*-variable functions* f *with nonlinearity* $2^{40} - 2^{20} + 52 \times 2^{10} > 2^{40} - 2^{20}$*. To obtain maximum degree* 39*, replace the last* $2^{n_1} = 1024$ *bits of such a function* f *by a nonlinear* 10*-variable,* 1*-resilient, degree* 8 *function (see Theorem 9 later). This provides* $(41, 1, 39, x)$ *function with* $x > 2^{40} - 2^{20} + 51 \times 2^{10}$*. For* $m = 2$*, choose* $n_1 = 16, n_2 = 24$ *and* $\epsilon = \frac{1}{2}$*. This provides* 2*-resilient,* 55*-variable functions with nonlinearity* $2^{54} - 2^{27} + 212 \times 2^{16}$*. As before we can obtain* $(55, 2, 52, y)$ *functions with* $y > 2^{54} - 2^{27} + 211 \times 2^{16}$*.*

Corollary 2. *The functions* f *and* g *constructed in the proof of Theorem 6 belong to* Γ_1*.*

Corollary 3. *For odd* n*, let* f *be an* n*-variable,* m*-resilient function having* $nl(f) > 2^{n-1} - 2^{\frac{n-1}{2}}$ *and let* g *be a* $2k$*-variable bent function. Then* $f\$g$ *is an* $n + 2k$*-variable,* m*-resilient function with* $nl(f\$g) > 2^{n+2k-1} - 2^{\frac{n+2k-1}{2}}$*. Consequently, if Theorem 6 holds for some odd* n_0*, then it also holds for all odd* $n > n_0$*.*

To prove Theorem 5, the only case that remains to be settled is $m = 1$ for even number of variables.

Theorem 7. *For each even positive integer* $n \geq 12$*, one can construct* 1*-resilient functions* f *of* n*-variables having* $nl(f) > 2^{n-1} - 2^{\frac{n}{2}}$*. Moreover,* f *is in* Γ_1*.*

Proof : Let $n = 2p$ and consider the set $\Gamma_1(2p, p-1, 1)$. We show how to construct a function in $\Gamma_1(2p, p-1, 1)$ having nonlinearity $2^{2p-1} - 3 \times 2^{p-2}$ which is greater than $2^{2p-1} - 2^p$. Since we are constructing functions in $\Gamma_1(2p, p-1, 1)$ we have to use linear couples from the set $UF_{p-1}(2)$. The number of available linear couples is $2^{p-1} - p$. Since there are 2^{p+1} slots to be filled the maximum repetition factor is $\lceil \frac{2^{p+1}}{2^{p-1}-p} \rceil = 5$. Thus the linear couples are to be repeated either 5 times or 4 times. Then as in the construction of g in the proof of Theorem 6, one can construct a function f having nonlinearity $2^{2p-1} - 3 \times 2^{p-2}$. Since f is a concatenation of linear couples from $UF_{p-1}(2)$ it follows that f is 1-resilient. □

The above constructions can be modified to get optimized functions also. We illustrate this by providing construction methods for $(2p, 1, 2p-2, x)$ functions with $x > 2^{2p-1} - 2^p$ for $p \geq 6$. The constructed functions are not in Γ_1.

Theorem 8. *For* $p \geq 6$*, it is possible to construct* $(2p, 1, 2p-2, x)$ *functions with* x *greater than* $2^{2p-1} - 2^p$*.*

Proof : As in the proof of Theorem 7, we write $2p = (p+1) + (p-1)$ and try to fill up 2^{p+1} slots using 1-resilient $(p-1)$-variable functions to construct a function $f \in \Omega_{2p}$. As before we use linear couples from $UF_{p-1}(2)$, but here we use these linear couples to fill up only $2^{p+1} - 1$ slots. The extra slot is filled up by a balanced $(p-1, 1, p-3, y)$ function g. The repetition factor for each linear couple is again at most 5 and the construction is again similar to Theorem 6. The nonlinearity is calculated as follows. Let l be in F_{2p}. The function g contributes at least y to $d(f,l)$. Ignoring the slot filled by g, the contribution to $d(f,l)$ from the linear couples is found as in Theorem 4. This gives the following inequality $2^{2p-1}-2^p+y \leq d(f,l) \leq 2^{2p-1}-y < 2^{2p-1}+2^p-y$. Hence $d(f,l) = 2^{2p-1}-2^p+y$. An estimate of y is obtained as follows. If $p-1$ is odd we use Theorem 10. If $p-1$ is even, then we recursively use the above construction. □

It is also possible to construct 1-resilient, 10-variable functions having nonlinearity $484 > 2^9 - 2^5$. This construction for optimized function combines all the construction ideas given in Section 3. The result disproves the conjecture of Pasalic and Johansson [8] for 10-variable functions.

Theorem 9. *It is possible to construct* $(10, 1, 8, 484)$ *functions.*

Proof : We write $10 = 6 + 4$ and concatenate affine functions of 4 variables to construct the desired function f. However, if we use only affine functions then the degree of f is less than 8. To improve the degree we use exactly one nonlinear $(4, 1, 2, 4)$ function h. By Theorem 3, this ensures that the degree of the resulting function is 8. This leaves $2^6 - 1$ slots to be filled by affine functions of 4 variables. If we use only functions from $UF_4(2)$, then the maximum repetition factor is 6 and the resulting nonlinearity is low. Instead we repeat the 11 linear couples in $UF_4(2)$ only 5 times each. This leaves $2^6 - 1 - 55 = 8$ slots to be filled up. We now use functions from $F_4(1)$. However, these are not resilient. But for $l \in F_4(1)$, ll^c is resilient. Since there are exactly 4 functions in $F_4(1)$ and each is repeated exactly 2 times, this uses up the remaining 8 slots. Let $g_1, \ldots, g_{11}$ be bent functions on 2 variables and let $\lambda_1, \ldots, \lambda_{11}$ be the 11 linear functions in $UL_4(2)$. Also let $\mu_1, \ldots, \mu_4$ be the 4 linear functions in $L_4(1)$. Then the function f is concatenation of the following sequence of functions: $g_1\$\lambda_1, \ldots, g_{11}\$\lambda_{11}, \mu_1\mu_1^c, \ldots, \mu_4\mu_4^c, \lambda_1, \ldots, \lambda_{11}h$. The nonlinearity calculation of f is similar to the previous proofs. Let l be in F_{10}. The worst case occurs when l is concatenation of λ_i and λ_i^c for some $1 \leq i \leq 11$. In this case $d(f,l) = (2^6 - 1 - 5)2^3 + 2^4 + 4 = 484$. □

The functions constructed by the methods of Theorem 9 and Theorem 8 are not in Γ_1 and do not require the use of a 15-variable nonlinear function from [9]. *It is important to note that the nonlinearity of functions constructed using Theorem 9 cannot be achieved using concatenation of only affine functions. Moreover, in this construction it is not possible to increase the nonlinearity by relaxing the optimality condition on degree, i.e., allowing the degree to be less than* 8.

The maximum possible nonlinearity of Boolean functions is equal to the covering radius of first order Reed-Muller codes. Patterson and Weidemann showed that for odd $n \geq 15$ the covering radius and hence the maximum possible nonlinearity of an n-variable function exceeds $2^{n-1} - 2^{\frac{n-1}{2}}$. Seberry et al [14] showed that for odd $n \geq 29$, it is possible to construct balanced functions with nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}$. Theorem 6 establishes a similar result for optimized resilient functions of odd number of variables n for $n \geq 41$.

5 Construction of Optimized Resilient Functions

Here we consider construction of optimized functions. We start with the following important result.

Theorem 10. *It is possible to construct (a)* $(2p+1, 0, 2p, 2^{2p}-2^p)$ *functions for* $p \geq 1$*, (b)* $(2p+1, 1, 2p-1, 2^{2p}-2^p)$ *functions for* $p \geq 2$*, (c)* $(2p, 1, 2p-2, 2^{2p-1}-2^p)$ *functions for* $p \geq 2$ *and (d)* $(2p, 2, 2p-3, 2^{2p-1}-2^p)$ *functions for* $p \geq 3$*.*

Proof : We present only the constructions (proofs are similar to Section 4).
(a) If $p = 1$, let $f = X_3 \oplus X_1X_2$. For $p \geq 2$ consider the following construction. Let $\lambda_1, \lambda_2, \lambda_3$ be the functions in $UL_2(1)$ and λ_4 the (all zero) function in $L_2(0)$. Let h_1 be a bent function on $2p-2$ variables, h_2 be a maximum nonlinear balanced function on $2p-3$ variables. If $p = 2$ let h_3, h_4 be strings of length 1 each and for $p \geq 3$ let h_3, h_4 be maximum nonlinear strings of length $2^{2p-4}+1$ and $2^{2p-4}-1$ respectively. Let f be a concatenation of the following sequence of functions: $h_1\$\lambda_1, h_2\$\lambda_4, h_3\$\lambda_2, h_4\$\lambda_3$. It can be shown that f is a $(2p+1, 0, 2p, 2^{2p}-2^p)$ function.
(b) Let $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ be the functions in $UL_3(2)$ and μ_1, μ_2, μ_3 the functions in $L_3(1)$. For $p = 2$, let $f = \lambda_1\lambda_2\lambda_3\lambda_4$. For $p = 3$, let f be the concatenation of the following sequence of functions.
$h_1\$\lambda_1, h_2\$\lambda_2, \mu_1\mu_1^c, \mu_2\mu_2^c, \mu_3\mu_3^c, \lambda_3, \lambda_4$, where h_1 and h_2 are 2-variable bent functions. For $p \geq 4$, we have the following construction. Let $g_i = \mu_i\mu_i^c$, for $1 \leq i \leq 3$,. Let h_1, h_2 be bent functions of $2p-4$ variables, h_3, h_4, h_5 be bent functions of $2p-6$ variables and h_6, h_7 be two strings of lengths $2^{2p-6}+1$ and $2^{2p-6}-1$ and (fractional) nonlinearity $nlmax(2p-6)$ and $nlmax(2p-6)-1$ respectively. Let f be a concatenation of the following sequence of functions.
$h_1\$\lambda_1, h_2\$\lambda_2, h_3\$g_1, h_4\$g_2, h_5\$g_3, h_6\$\lambda_3, h_7\$\lambda_4$. It can be shown that f is a $(2p+1, 1, 2p-1, 2^{2p}-2^p)$ function.
(c) and (d) follow from (a) and (b) on noting that if f is a $(2p+1, m, 2p-m, x)$ function then ff^c is a $(2p+2, m+1, 2p-m, 2x)$ function. □

Note that item (a), (b) of Theorem 10 can also be proved using different techniques by modifying a special class of bent functions. See [13] for the detailed construction methods.

5.1 Method Using Direct Sum with a Nonlinear Function

Here we consider the set $\Gamma_1(n, k, m)$ and show how to construct optimized functions with very high nonlinearities in this set. We build upon the idea described in Subsection 3.2. Since we consider optimized functions, Corollary 1 determines $k = m+2$ and at least one variable in $\{X_k, \ldots, X_1\}$ must occur in odd number of the f_i's. We recall from Subsection 3.3, that $Fracnlmax(2^r-1) = nlmax(r)-1$, $Fracnlmax(2^r+1) = nlmax(r)$, $Fracnlmax(2^r) = nlmax(r)$ and $Effect(t) = t - 2Fracnlmax(t)$.

Given n and m, we construct an optimized function f in $\Gamma_1(n, m+2, m)$. We define a variable *template* to be a list of the form $(s, (s_1, t_1), \ldots, (s_k, t_k))$, where $\sum_{j=1}^{k} s_j = s$ and $\sum_{j=1}^{k} s_j t_j = 2^{n-m-2}$. The value s is the number of distinct linear couples to be used from the set $UF_{m+2}(m+1)$ and for each j, $(1 \le j \le k)$, s_j linear couples are to be used t_j times each. While constructing *template* one has to be careful in ascertaining that at least one variable occurs in an odd number of functions overall. This gives rise to the various cases in Algorithm A. Since an n-variable, $(n-2)$-resilient function must have degree 1 and hence be linear, we consider only the cases $1 \le m < n-2$.

ALGORITHM A

input: (n, m) with $1 \le m < n-2$.

output: A $(n, m, n-m-1, x)$ function f. We determine x in Theorem 11.

BEGIN

1. Let $p = m+3$ and $2^{r-1} < \lceil \frac{2^{n-m-2}}{m+3} \rceil \le 2^r$. Let $i = p - 2^{n-m-2-r}$, i.e., $(p-i)2^r = 2^{n-m-2}$. Now several cases arise.
2. $r = 0, i > 0$: Here f is the concatenation of $(p-i-1)$ functions containing X_1 and the one function not containing X_1 from the set $UL_{m+2}(m+1)$. Output f and STOP.
3. $r = 0, i = 0$, $m+2$ is odd: *template* $= (p, (p, 1))$.
4. $r > 0, i = 0$, r is even: *template* $= (p, (p-2, 2^r), (1, 2^r+1), (1, 2^r-1))$.
5. $r > 0, i = 0$, r is odd: *template* $= (\frac{p}{2}+2, (\frac{p}{2}-1, 2^{r+1}), (1, 2^r), (1, 2^{r-1}+1), (1, 2^{r-1}-1))$.
6. $r = 1, i > 0$: *template* $= (p-i+1, (p-i-1, 2), (2, 1))$.
7. $r = 2, i > 1$: *template* $= (p-i+2, (p-i-1, 4), (1, 2), (2, 1))$.
8. $r \ge 2, i = 1$, r is even: *template* $= (p, (p-2, 2^r), (1, 2^{r-1}+1), (1, 2^{r-1}-1))$.
9. $r \ge 2, i = 1$, r is odd:
template $= (\frac{p+3}{2}, (\frac{p-3}{2}, 2^{r+1}), (1, 2^r), (1, 2^{r-1}+1), (1, 2^{r-1}-1))$.
10. $r > 2, i > 1$: *template* $= (p-i+2, (p-i-1, 2^r), (1, 2^{r-1}), (1, 2^{r-2}+1), (1, 2^{r-2}-1))$.
11. Let *template* $= (s, (s_1, t_1), \ldots, (s_k, t_k))$. For each j, choose $l_j^1, \ldots, l_j^{s_j}$ to be distinct linear functions from $UL_{m+2}(m+1)$ and $g_j^1, \ldots, g_j^{s_j}$ to be strings of length t_j and having maximum possible nonlinearity. (Note that the g's may be fractional strings.) Then f is the concatenation of the following sequence of functions
$g_1^1\$l_1^1, \ldots, g_1^{s_1}\$l_1^{s_1}, g_2^1\$l_2^1, \ldots, g_2^{s_2}\$l_2^{s_2}, \ldots, g_k^1\$l_k^1, \ldots, g_k^{s_k}\$l_k^{s_k}$.

END.

Theorem 11. *Algorithm A constructs a* $(n, n-m-1, m, x)$*-function* f *in* $\Gamma_1(n, m+2, m)$*, where the values of* x *in different cases (corresponding to the line numbers of Algorithm A) are as follows. (2)* $2^{n-1} - 2^{m+1}$ *(3)* $2^{n-1} - 2^{m+1}$ *(4)* $2^{n-1} - 2^{m+1} \mathit{Effect}(2^r+1)$ *(5)* $2^{n-1} - 2^{m+1} \mathit{Effect}(2^{r+1})$ *(6)* $2^{n-1} - 2^{m+2}$ *(7)* $2^{n-1} - 2^{m+2}$ *(8)* $2^{n-1} - 2^{m+1} \mathit{Effect}(2^{r-1}+1)$ *(9)* $2^{n-1} - 2^{m+1} \mathit{Effect}(2^{r+1})$ *(10)* $2^{n-1} - 2^{m+1} \mathit{Effect}(2^r)$.

Example: Using Algorithm A it is possible to construct $(9, 3, 5, 224)$ *functions having template* $= (6, (3, 4), (1, 2), (2, 1))$.

5.2 Use of Nonlinear Resilient Function

Here we use the idea of Subsection 3.5 to provide a construction method for optimized resilient functions. The constructed functions are not in Γ_1.

Let $nla(n,m)$ be the nonlinearity of a function obtained by Algorithm A with (n,m) as input. Similarly, let $nlb(n,m)$ be the highest nonlinearity of a function obtained using Algorithm B (described below) on input (n,m) and ranging c from 1 to $n-m-2$. We obtain an expression for $nlb(n,m)$ in Theorem 12. Let $nlx(n,m)$ be the maximum of $nla(n,m)$ and $nlb(n,m)$.

ALGORITHM B

input : (n,m,c), with $1 \le m < n-2$ and $1 \le c \le n-m-2$.
output : A balanced $(n,m,n-m-1,x_c)$ function f_c. The value of x_c is given in Lemma 5.

BEGIN

1. If $n <= 5$, use Algorithm A with input (n,m) to construct a function f. Output f and stop.
2. Let $p = \binom{m+c+2}{m+1} + \ldots + \binom{m+c+2}{m+c+2}$ and $2^{r-1} < \lceil \frac{2^{n-(m+c+2)}}{p} \rceil \le 2^r$. Let $i = p - 2^{n-(m+c+2)-r}$, i.e., $(p-i)2^r = 2^{n-(m+c+2)}$.
3. $i=0, r=0$: *template* $= (p-1,(p-1,1))$.
4. $i>0, r=0$: *template* $= (p-i-1,(p-i-1,1))$.
5. $i>0, r=1$: *template* $= (p-i,(p-i-1,2),(1,1))$.
6. $i=0, r>0$, r is even: *template* $= (p,(p-1,2^r),(1,2^r-1))$.
7. $i=0, r>0$, r is odd:
template $= (\frac{p}{2}+2,(\frac{p}{2}-1,2^{r+1}),(1,2^r),(1,2^{r-1}),(1,2^{r-1}-1))$.
8. $i>0, r=2$: *template* $= (p+1,(p-1,4),(1,2),(1,1))$.
9. $i=1, r>2$, r is even: *template* $= (p,(p-2,2^r),(1,2^{r-1}),(1,2^{r-1}-1))$.
10. $i=1, r\ge 2$, r is odd:
template $= (\frac{p+3}{2},(\frac{p-3}{2},2^{r+1}),(1,2^r),(1,2^{r-1}),(1,2^{r-1}-1))$.
11. $i>1, r>2$:
template $= (p-i+2,(p-i-1,2^r),(1,2^{r-1}),(1,2^{r-2}),(1,2^{r-2}-1))$.
12. Using *template* and linear couples from $UF_{m+c+2}(m+1)$, we first build a string f_1 as in Algorithm A. Then the function f_c is $f_1 g$, where g is a $(m+c+2,m,1+c,y)$ function, where $y = nlx(m+c+2,m)$.

END.

Note that the use of the function $nlx(n,m)$ makes Algorithm B a recursive function. Let the nonlinearity of a function f_c constructed by Algorithm B on input (n,m,c) be $nlbs(n,m,c)$.

Lemma 5. *Let f_c be constructed by Algorithm B. Then f_c is a balanced $(n,m,n-m-1,x_c)$ function, where $x_c = nlbs(n,m,c)$ and the values of x_c in the different cases (corresponding to the line numbers of Algorithm B) are as follows : (3) $2^{n-1}-2^k+y$ (4) $2^{n-1}-2^k+y$ (5) $2^{n-1}-3\times 2^{k-1}+y$ (6) $2^{n-1}-(1+\mathit{Effect}(2^r-1))2^{k-1}+y$ (7) $2^{n-1}-(1+\mathit{Effect}(2^{r+1}))2^{k-1}+y$ (8) $2^{n-1}-3\times 2^{k-1}+y$ (9) $2^{n-1}-(1+\mathit{Effect}(2^{r-1}-1))2^{k-1}+y$ (10) $2^{n-1}-(1+\mathit{Effect}(2^{r+1}))2^{k-1}+y$ (11) $2^{n-1}-(1+\mathit{Effect}(2^r))2^{k-1}+y$ where $k=m+c+2$, $y=nlx(m+c+2,m)$.*

Algorithm B is used iteratively over the possible values of c from 1 to $n-m-2$ and the function with the best nonlinearity is chosen. The maximum possible nonlinearity $nlb(n, m)$ obtained by using Algorithm B in this fashion is given by the following theorem.

Theorem 12. $nlb(n, m) \geq max_{1 \leq c \leq n-m-2} nlbs(n, m, c)$.

Example: Using Algorithm B one can construct $(9, 2, 6, 232)$ *functions in* $\Gamma(9, 5, 2)$ *having template* $(15, (15, 1))$ *and a* $(5, 2, 2, 8)$ *function g is used to fill the* $16th$ *slot.*

6 Comparison to Existing Research

Here we show the power of our techniques by establishing the superiority of our results over all known results in this area.

The best known results for $Type - A$ approach follows from the work of [2]. However, they considered only a proper subset S of Γ_1 and obtained a bound of $2^{n-1} - 2^{\lfloor \frac{n}{2} \rfloor}$ on the nonlinearity of resilient functions. Also in [8], it was conjectured that this is the maximum possible nonlinearity of resilient functions. All the results in Section 4 provide higher nonlinearities than this bound. In particular, this bound is broken and hence the conjecture is disproved for the set Γ_1 as well as for optimized functions.

n	$m = 1$			$m = 2$			$m = 3$			$m = 4$		
	[7]	[8]	Our	[7]	[4]	Our	[7]	nla	nlb	[7]	nla	nlb
8	108	112	112^a	88	-	112^b	80	96	80	32	96	32
9	220	236	240^b	216	224	232^e	176	224	208	160	192	160
10	476	480	484^c	440	-	480^b	432	448	464	352	448	416
11	956	976	992^b	952	-	984^e	880	960	944	864	896	928
12	1980	-	1996^d	1912	-	1984^b	1904	1920	1968	1760	1920	1888

a:Algorithm A; b: Theorem 10; c: Theorem 9; d: Theorem 8; e: Algorithm B.

For the $Type - B$ approach the best known results follow from the work of [15,4], [7,8,18]. In [4], exhaustive search techniques are used to obtain $(5, 0, 4, 12)$ and $(7, 0, 6, 56)$ functions. For 9 variables, they could only obtain $(9, 0, 7, 240)$ functions and not $(9, 0, 8, 240)$ functions. Also such techniques cannot be used for large number of variables. In contrast, Theorem 10 can be used to construct $(2p + 1, 0, 2p, 2^{2p} - 2^p)$ functions for all $p \geq 1$ and hence is clearly superior to the results of [4].

In the Table, we compare the nonlinearities of optimized $(n, m, n - m - 1, x)$ functions. The columns nla and nlb are the nonlinearities obtained by Algorithm A and Algorithm B respectively. We do not compare results with [15], since it is clear that Algorithm A significantly improves on the lower bound on nonlinearity obtained in [15].

The table clearly shows the superiority of our method compared to the previous methods. Also it can be checked that the nonlinearities obtained in Theorem 11 are better than those obtained in [7] for all orders of resiliency. We can construct $(9, 3, 5, 224)$ functions and $(9, 2, 6, 232)$ functions using Algorithm A and Algorithm B respectively. These improve over the $(9, 2, 6, 224)$ functions of [4] both in terms of order of resiliency and nonlinearity.

7 Nonlinearity of Balanced Functions

In this section we discuss the nonlinearity and algebraic degree for balanced functions. Patterson and Wiedemann [9] constructed 15-variable functions with nonlinearity 16276 and weight 16492. Seberry, Zhang and Zheng [14] used such functions to construct balanced functions with nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ for odd $n \geq 29$. In [14], there was an unsuccessful attempt to construct balanced 15-variable functions having nonlinearity greater than $16256 = 2^{14} - 2^7$. First let us provide the following two technical results.

Proposition 2. *Let $f \in \Omega_n$ and $f = f_1 f_2$, where $f_1, f_2 \in \Omega_{n-1}$. If $wt(f)$ is odd then algebraic degree of f is n. Moreover, if both $wt(f_1)$ and $wt(f_2)$ are odd then the algebraic degree of f is $n - 1$.*

Proposition 3. *Given a balanced function $f \in \Omega_n$ with $nl(f) = x$, one can construct balanced $f' \in \Omega_n$ with $nl(f') \geq x - 2$ and $deg(f') = n - 1$.*

Now, we identify an important result which is the first step towards constructing a balanced 15-variable function with nonlinearity greater than 16256.

Proposition 4. *It is possible to construct $f \in \Omega_{15}$ with nonlinearity 16276 and weight 16364.*

Proof : Consider a function $f_1 \in \Omega_{15}$ with $nl(f_1) = 16276$ and $wt(f_1) = 16492$. From [9], we know that there are 3255 linear functions in L_{15} at a distance 16364 from f_1. Let l be one of these 3255 linear functions. Define $f = f_1 \oplus l$. Then $f \in \Omega_{15}$, $nl(f) = nl(f_1) = 16276$ and $wt(f) = wt(f_1 \oplus l) = d(f_1, l) = 16364$. □

Next we have the following randomized heuristic for constructing highly nonlinear balanced functions for odd $n \geq 15$.

Algorithm 1 : RandBal(n)

1. Let f be a function constructed using Proposition 4. Let $n = 2k + 15$, $k \geq 0$ and let $F \in \Omega_n$ be defined as follows. For $k = 0$, take $F = f$, and for $k > 0$, take $F = f(X_1, \ldots, X_{15}) \oplus g(X_{16}, \ldots, X_n)$, where $g \in \Omega_{2k}$ is a bent function. Note that $nl(F) = 2^{n-1} - 2^{\frac{n-1}{2}} + 20 \times 2^k$ and $wt(F) = 2^{n-1} - 20 \times 2^k$.
2. Divide the string F in Ω_n into 20×2^k equal contiguous substrings, with the last substring longer than the rest.
3. In each substring choose a position with 0 value uniformly at random and change that to 1. This generates a balanced function $F_b \in \Omega_n$.
4. If $nl(F_b) > 2^{n-1} - 2^{\frac{n-1}{2}}$, then report. Go to step 1 and continue.

We have run this experiment number of times and succeeded in obtaining plenty of balanced functions with nonlinearities $2^{14} - 2^7 + 6$, $2^{16} - 2^8 + 18$,

$2^{18}-2^9+46$ and $2^{20}-2^{10}+104$ respectively for 15, 17, 19 and 21 variables. It is possible to distribute the 0's and 1's in the function in a manner (changing step 2, 3 in Algorithm 1) such that weight of the upper and lower half of the function are odd. This provides balanced functions with maximum algebraic degree $(n-1)$ and the same nonlinearity as before. Note that, running Algorithm 1 for large n is time consuming. However, we can extend the experimental results in a way similar to that in [9]. Consider a bent function $g(Y_1, \ldots, Y_{2k}) \in \Omega_{2k}$ and $f(X_1, \ldots, X_{21})$ with nonlinearity $2^{20} - 2^{10} + 104$ as obtained from Algorithm RandBal(). Let $h \in \Omega_{21+2k}$ such that $h = g \oplus f$. Then it can be checked that $nl(h) = 2^{20+2k} - 2^{10+k} + 104 \times 2^k$. These functions can be modified to get algebraic degree $(n-1)$ as in Proposition 3. Thus we get the following result.

Theorem 13. *One can construct balanced Boolean functions on $n = 15 + 2k$ $(k \geq 0)$ variables with nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}$. Moreover, such functions can have algebraic degree $(n-1)$.*

Dobbertin [3] provided a recursive procedure for modifying a general class of bent functions to obtain highly nonlinear balanced Boolean functions on even number of variables. A special case of this procedure which modifies Maiorana-McFarland class of bent functions was provided in [14]. For even n, it is conjectured in [3] that the maximum value of nonlinearity of balanced functions, which we denote by $nlbmax()$, satisfies the recurrence: $nlbmax(n) = 2^{n-1} - 2^{\frac{n}{2}} + nlbmax(\frac{n}{2})$.

We next provide a combined interlinked recursive algorithm to construct highly nonlinear balanced functions for both odd and even n. Note that for even number of variables, Algorithm 2 uses a special case of the recursive construction in [3]. Further we show how to obtain maximum algebraic degree. The input to this algorithm is n and the output is balanced $f \in \Omega_n$ with currently best known nonlinearity.

Algorithm 2 : BalConstruct(n)

1. If n is odd

   a) if $3 \leq n \leq 13$ construct f using Theorem 10(a).

   b) if $15 \leq n \leq 21$ return f to be the best function constructed by RandBal(n).

   c) if $n \geq 23$

      (i) Let $h_1 \in \Omega_{n-21}$ be bent and $g_1 \in \Omega_{21}$ be the best nonlinear function constructed by RandBal(n).

      Let $f_1 \in \Omega_n$ be such that $f_1 = h_1 \oplus g_1$.

      (ii) Let $h_2 =$ BalConstruct($n-15$) and $g_2 \in \Omega_{15}$ as in Proposition 4.

      Let $f_2 \in \Omega_n$ be such that $f_2 = h_2 \oplus g_2$.

      (iii) If $nl(f_1) \geq nl(f_2)$ return f_1 else return f_2.

2. If n is even

   Let $h =$ BalConstruct($\frac{n}{2}$). Let f be the concatenation of h followed by $2^{\frac{n}{2}} - 1$ distinct nonconstant linear functions on $\frac{n}{2}$ variables. Return f.

End Algorithm.

The following points need to be noted for providing the maximum algebraic degree $n-1$.

1. For odd $n \leq 13$, Theorem 10(a) guarantees degree $(n-1)$.
2. For odd n, $15 \leq n \leq 21$, modification of algorithm RandBal() guarantees

algebraic degree $(n-1)$ without dropping nonlinearity.
3. For odd $n \geq 23$, using Proposition 3, degree $(n-1)$ can be achieved sacrificing nonlinearity by at most 2.
4. For even n, recursively ensure that algebraic degree of h (in Step 2 of BalConstruct()) is $\frac{n}{2}-1$.

In this section we have shown how to heuristically modify the Patterson-Wiedemann functions to obtain balancedness while retaining nonlinearity higher than the bent concatenation bound. However, the question of mathematically constructing such functions remains open. Also settling the conjecture in [3] is an important unsolved question.

8 Propagation Characteristics, Strict Avalanche Criteria

In this section we provide important results on propagation characteristics and strict avalanche criteria. The following is a general construction of Boolean functions introduced in [6].

$$f(X_1,\ldots,X_s,Y_1,\ldots,Y_t) = [X_1,\ldots,X_s]Q[Y_1,\ldots,Y_t]^T \oplus g(X_1,\ldots,X_s), \qquad \textbf{(*)}$$

where Q is an $s \times t$ binary matrix and $g(X_1,\ldots,X_s)$ is any function.
Under certain conditions on Q, the function f satisfies PC(l) of order k (see [6]). Moreover, according to the proof of [6, Theorem 16], $nl(f) = 2^t nl(g)$ and $deg(f) = deg(g)$. It is possible to significantly improve the results of [6] by using functions constructed by the methods of Section 7.

Theorem 14. *For odd s, it is possible to construct PC(l) of order k function f such that (a) $deg(f) = s-1$ and $nl(f) \geq 2^{t+s-1} - 2^{t+\frac{s-1}{2}}$ for $3 \leq s \leq 13$, (b) $deg(f) = s$ and $nl(f) > 2^{t+s-1} - 2^{t+\frac{s-1}{2}}$ for $s \geq 15$.*

Proof : For $3 \leq s \leq 13$, s odd, we can consider $g \in \Omega_s$ as the function available from Theorem 10(a) with algebraic degree $s-1$ and nonlinearity $2^{s-1}-2^{\frac{s-1}{2}}$. For $s \geq 15$, one can consider $g \in \Omega_s$ with nonlinearity $2^{s-1}-2^{\frac{s-1}{2}}+20\times 2^{\frac{s-15}{2}}-1$ and algebraic degree s. This can be obtained by considering a function on s variables with maximum known nonlinearity and then making $wt(g)$ odd by toggling one bit. This will provide the full algebraic degree and decrease the nonlinearity by at most 1 only. □

For odd s, the corresponding result in [6] is $deg(f) = \frac{s-1}{2}$ and $nl(f) \geq 2^{t+s-1} - 2^{t+\frac{s-1}{2}}$ which is clearly improved in Theorem 14.

Now we show how to obtain maximum algebraic degree in this construction at the cost of small fall in nonlinearity. For odd s between 3 and 13, $deg(g)$ can be made s by changing one bit of g. This decreases $nl(g)$ by one. The corresponding parameters of f are $deg(f) = s$ and $nl(f) \geq 2^{t+s-1} - 2^{t+\frac{s-1}{2}} - 2^t$. For even s, the result in [6] is $deg(f) = \frac{s}{2}$ and $nl(f) \geq 2^{t+s-1} - 2^{t+\frac{s}{2}-1}$. As before by changing one bit of g we can ensure $deg(f) = s$ and $nl(f) \geq 2^{t+s-1} - 2^{t+\frac{s}{2}-1} - 2^t$. Also in [13], we show that it is possible to construct PC(1) functions with nonlinearity strictly greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ for all odd $n \geq 15$.

Next we turn to the study of SAC(k) combined with the properties of balancedness, degree and nonlinearity. *This is the first time that all these properties* *are being considered together with $SAC(k)$.* The proofs for the next few results are quite involved. Hence we present the constructions clearly and only sketch the proofs.

In [6], **(*)** has been used for the construction of SAC(k) function by setting $s = n-k-1$, $t = k+1$ and Q to be the $(n-k-1)\times(k+1)$ matrix whose all elements are 1. Under these conditions the function f takes the form $f(X_1, \ldots, X_n) = (X_1 \oplus \ldots \oplus X_{n-k-1})(X_{n-k} \oplus \ldots \oplus X_n) \oplus g(X_1, \ldots, X_{n-k-1})$. Moreover, it was shown that f is balanced if $\mid \{\overline{X} \mid g(\overline{X}) = 0, \overline{X}Q = 0\} \mid=\mid \{\overline{X} \mid g(\overline{X}) = 1, \overline{X}Q = 0\} \mid$ where $\overline{X} = (X_1, \ldots, X_{n-k-1})$. It is important to interpret this idea with respect to the truth table of g. This means that f is balanced if $\#\{\overline{X} \mid g(\overline{X}) = 0, wt(\overline{X}) = \text{ even }\} = \#\{\overline{X} \mid g(\overline{X}) = 1, wt(\overline{X}) = \text{ even }\}$. Thus, in the truth table we have to check for balancedness of g restricted to the rows where the weight of the input string is even. In half of such places g must be 0 and in the other half g must be 1. Motivated by this discussion we make the following definition of *brEven* (restricted balancedness with respect to inputs with even weight) and *brOdd* (restricted balancedness with respect to inputs with odd weight).

Definition 2. *Let $g \in \Omega_p$, $\overline{X} = (X_1, \ldots, X_p)$. Then g is called brEven (resp. brOdd) if $\#\{g(\overline{X}) = 0 \mid wt(\overline{X}) = even\} = \#\{g(\overline{X}) = 1 \mid wt(\overline{X}) = even\} = 2^{p-2}$ (resp. $\#\{g(\overline{X}) = 0 \mid wt(\overline{X}) = odd\} = \#\{g(\overline{X}) = 1 \mid wt(\overline{X}) = odd\} = 2^{p-2}$).*

The next result is important as it shows that certain types of bent functions can be brEven. This allows us to obtain balanced SAC(k) functions with very high nonlinearity which could not be obtained in [6].

Proposition 5. *For p even, it is possible to construct bent functions $g \in \Omega_p$ which are brEven.*

Proof : First note that g is brEven iff g^c is brEven. Let $q = 2^{\frac{p}{2}}$. For $0 \le i \le q-1$ let $l_i \in L_{\frac{p}{2}}$ be the linear function $a_{\frac{p}{2}} X_{\frac{p}{2}} \oplus \ldots \oplus a_1 X_1$, where $a_{\frac{p}{2}} \ldots a_1$ is the $\frac{p}{2}$-bit binary expansion of i. We provide construction of bent functions $g(X_1, \ldots, X_p)$ which are brEven. Let $\overline{X} = (X_1, \ldots, X_p)$.
Case 1: $\frac{p}{2} \equiv 1 \bmod 2$. Let $g = l_0 f_1 \ldots f_{q-2} l_{q-1}$, where $f_1, \ldots, f_{q-2} \in \{l_1, \ldots, l_{q-2}, l_1^c, \ldots, l_{q-2}^c\}$ and for $i \neq j$, $f_i \neq f_j$ and $f_i \neq f_j^c$. It is well known that such a g is bent [11]. We show that g is brEven. First we have the following three results which we state without proofs.
(a) $\#\{l_0(X_1, \ldots, X_{\frac{p}{2}}) = 0 \mid wt(X_1, \ldots, X_{\frac{p}{2}}) = \text{ even }\} = 2^{\frac{p}{2}-1}$ and $\#\{l_0(X_1, \ldots, X_{\frac{p}{2}}) = 1 \mid wt(X_1, \ldots, X_{\frac{p}{2}}) = \text{ even }\} = 0$.
(b) Since the f_i's are degenerate affine functions in $L_{\frac{p}{2}}$, it is possible to show that individually they are both brEven and brOdd.
(c) Using the fact that $q = \frac{p}{2}$ is odd and $l_{q-1} = X_1 \oplus \ldots \oplus X_{\frac{p}{2}}$, it is possible to show, $\#\{l_{q-1}(X_1, \ldots, X_{\frac{p}{2}}) = 0 \mid wt(X_1, \ldots, X_{\frac{p}{2}}) = \text{ even }\} = 0$ and $\#\{l_{q-1}(X_1, \ldots, X_{\frac{p}{2}}) = 1 \mid wt(X_1, \ldots, X_{\frac{p}{2}}) = \text{ even }\} = 2^{\frac{p}{2}-1}$. Then using $wt(X_1, \ldots, X_p) = wt(X_1, \ldots, X_{\frac{p}{2}}) + wt(X_{\frac{p}{2}+1}, \ldots, X_p)$ and the fact that g is concatenation of $l_0, f_1, \ldots, f_{q-2}, l_{q-1}$ it is possible to show that g is brEven.
Case 2: For $\frac{p}{2} \equiv 0 \bmod 2$, the result is true for bent functions of the form $g = l_0^c f_1 \ldots f_{q-2} l_{q-1}$. □

In [6, Theorem 32] it has been stated that for $n-k-1 =$ even, there exists balanced SAC(k) functions such that $deg(f) = n-k-2$. The question whether such functions with algebraic degree $n-k-1$ exists has been left as an open question. The next result shows the existence of such functions which proves that the bound on algebraic degree provided in [10] is indeed tight for $k \leq \frac{n}{2} - 1$.

Theorem 15. *Let $(n-k-1) \geq (k+1)$, i.e. $k \leq \frac{n}{2} - 1$ and $n-k-1 =$ even. Then it is possible to construct balanced SAC(k) function $f \in \Omega_n$ such that $deg(f) = n-k-1$. Moreover $nl(f) = 2^{n-1} - 2^{\frac{n+k-1}{2}} - 2^{k+1}$.*

Proof : Use a bent function $g \in \Omega_{n-k-1}$ which is brEven. Out of the 2^{n-k-1} bit positions in g (in the output column of the truth table), there are 2^{n-k-2} positions where $wt(X_1, \ldots, X_{n-k-1}) =$ odd and the value of g at these positions can be toggled without disturbing the brEven property. Since g is bent, $wt(g) =$ even. Thus we choose a row j in the truth table where $wt(X_1, \ldots, X_{n-k-1}) =$ odd and construct g' by toggling the output bit. Thus $wt(g') = wt(g) \pm 1 =$ odd. Hence by Proposition 2, $deg(g') = n-k-1$. Thus, $f(X_1, \ldots, X_n) = (X_1 \oplus \ldots \oplus X_{n-k-1})(X_{n-k} \oplus \ldots \oplus X_n) \oplus g'(X_1, \ldots, X_{n-k-1})$ is balanced SAC(k) with algebraic degree $n-k-1$. Also $nl(g') = nl(g) - 1 = 2^{n-k-2} - 2^{\frac{n-k-1}{2}-1} - 1$. Now, it can be checked that $nl(f) = 2^{k+1} \times nl(g') = 2^{n-1} - 2^{\frac{n+k-1}{2}} - 2^{k+1}$. $\square$

Next we provide similar results for odd $n-k-1$. The result is extremely important in the sense that the functions constructed in [9] can be modified to get restricted balancedness and hence can be used in the construction of highly nonlinear, balanced SAC(k) functions. *We know of no other place where the functions provided by Patterson and Wiedemann [9] have been used in the construction of SAC(k) functions.*

Proposition 6. *For p odd, it is possible to construct brEven $g \in \Omega_p$ with nonlinearity (i) $2^{p-1} - 2^{\frac{p-1}{2}}$ for $p \leq 13$ and (ii) $2^{p-1} - 2^{\frac{p-1}{2}} + 20 \times 2^{\frac{p-15}{2}}$ for $p \geq 15$.*

Proof : For $p \leq 13$, the idea of bent concatenation and similar techniques as in the proof of Proposition 5 can be used. For $p \geq 15$ the construction is different. We just give an outline of the proof. Let $f_1 \in \Omega_{15}$ be one of the functions constructed in [9]. Note that $nl(f_1) = 2^{14} - 2^7 + 20$. Now consider the 32768 functions of the form $f_1 \oplus l$, where $l \in L_{15}$. We have found functions among these which are brOdd (but none which are brEven). Let $f_2(X_1, \ldots, X_{15})$ be such a brOdd function. It is then possible to show that $f_3(X_1, \ldots, X_{15}) = f_2(X_1 \oplus \alpha_1, \ldots, X_{15} \oplus \alpha_{15})$ is brEven when $wt(\alpha_1, \ldots, \alpha_{15})$ is odd. Note that $nl(f_2) = nl(f_3) = nl(f_1)$. Let $g(Y_1, \ldots, Y_{2k})$ be a bent function on $2k$ variables. Define $F \in \Omega_{15+2k}$ as follows. $F = (Y_1 \oplus \ldots \oplus Y_{2k})(g \oplus f_2) \oplus (1 \oplus Y_1 \oplus \ldots \oplus Y_{2k})(g \oplus f_3)$. It can be proved that F is brEven and $nl(F) = 2^{14+2k} - 2^{7+k} + 20 \times 2^k$. $\square$

Theorem 16. *Let $(n-k-1) \geq (k+1)$, i.e. $k \leq \frac{n}{2} - 1$ and $n-k-1 =$ odd. Then it is possible to construct balanced SAC(k) function $f \in \Omega_n$ such that $deg(f) = n-k-1$. Moreover, for $3 \leq n-k-1 \leq 13$, $nl(f) = 2^{n-1} - 2^{\frac{n+k}{2}} - 2^{k+1}$ and for $n-k-1 \geq 15$, $nl(f) = 2^{n-1} - 2^{\frac{n+k}{2}} + 20 \times 2^{\frac{n+k-14}{2}} - 2^{k+1}$.*

This shows that it is possible to construct highly nonlinear balanced functions satisfying SAC(k) with maximum possible algebraic degree $n-k-1$. Functions with all these criteria at the same time has not been considered earlier.

Now we present an interesting result combining resiliency and propagation characteristics. In [15, Theorem 15], propagation criterion of m-resilient functions has been studied. Those functions satisfy propagation criteria with a specific set of vectors. However, they do not satisfy even PC(1) as propagation criteria is not satisfied for some vectors of weight 1. For n even, we present a construction to provide resilient functions in Ω_n which satisfy PC($\frac{n}{2}-1$).

Theorem 17. *It is possible to construct* 1*-resilient functions in* Ω_n*,* n *even, with nonlinearity* $2^{n-1}-2^{\frac{n}{2}}$ *and algebraic degree* $\frac{n}{2}-1$ *which satisfy* $PC(\frac{n}{2}-1)$*.*

Proof : Let $f \in \Omega_{n-2}$ be a bent function, n even. Then it can be checked that $F(X_1,\ldots,X_{n-1}) = (1 \oplus X_{n-1})f(X_1,\ldots,X_{n-2}) \oplus X_{n-1}(1 \oplus f(X_1 \oplus \alpha_1,\ldots,X_{n-2} \oplus \alpha_{n-2}))$ is balanced and satisfies propagation criterion with respect to all nonzero vectors except $(\alpha_1,\ldots,\alpha_{n-2},1)$. Also $nl(F) = 2^{n-2}-2^{\frac{n-2}{2}}$.

Let $G(X_1,\ldots,X_n) = (1 \oplus X_n)F(X_1,\ldots,X_{n-1}) \oplus X_n(F(X_1 \oplus \beta_1,\ldots,X_{n-1} \oplus \beta_{n-1}))$. Then it can be checked that G is balanced and satisfies propagation criterion with respect to all nonzero vectors except $\overline{\alpha} = (\alpha_1,\ldots,\alpha_{n-2},\alpha_{n-1} = 1,\alpha_n = 0)$, $\overline{\beta} = (\beta_1,\ldots,\beta_{n-1},\beta_n = 1)$ and $\overline{\alpha} \oplus \overline{\beta}$. Also G is balanced and $nl(G) = 2^{n-1}-2^{\frac{n}{2}}$.

Take $(\alpha_1,\alpha_2,\ldots,\alpha_{n-2})$ in the construction of F in Ω_{n-1} from $f \in \Omega_{n-2}$ so that $wt(\alpha_1,\alpha_2,\ldots,\alpha_{n-2}) = \frac{n}{2}-1$.
Also $G(X_1,\ldots,X_n) = (1 \oplus X_n)F(X_1,\ldots,X_{n-1}) \oplus X_n(F(X_1 \oplus 1,\ldots,X_{n-1} \oplus 1)$ is correlation immune [1]. Since F is balanced, G is also balanced which proves that G is 1-resilient. Now consider $\overline{\alpha} = (\alpha_1,\ldots,\alpha_{n-2},\alpha_{n-1} = 1,\alpha_n = 0)$, $\overline{\beta} = (\beta_1 = 1,\ldots,\beta_{n+1} = 1,\beta_{n+2} = 1)$. Since $wt(\overline{\alpha}) = \frac{n}{2}-1+1$ and $wt(\overline{\beta}) = n$ we get, $wt(\overline{\alpha} \oplus \overline{\beta}) = \frac{n}{2}$. Note that G satisfies propagation criterion with respect to all the nonzero vectors except $\overline{\alpha},\overline{\beta},\overline{\alpha} \oplus \overline{\beta}$ and hence G satisfies PC($\frac{n}{2}-1$).

Since $f \in \Omega_{n-2}$ is bent, it is possible to construct f with algebraic degree $\frac{n}{2}-1$. It can be checked that $deg(G) = deg(f)$. □

9 Conclusion

In this paper we have considered cryptographically important properties of Boolean functions such as balancedness, nonlinearity, algebraic degree, correlation immunity, propagation characteristics and strict avalanche criteria. The construction methods we propose here are new and they provide functions which were not known earlier.

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. 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.
3. H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. In *Fast Software Encryption*, number 1008 in Lecture Notes in Computer Science, pages 61–74. Springer-Verlag, 1994.
4. E. Filiol and C. Fontaine. Highly nonlinear balanced Boolean functions with a good correlation-immunity. In *Advances in Cryptology - EUROCRYPT'98*. Springer-Verlag, 1998.
5. 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.
6. K. Kurosawa and T. Satoh. Design of SAC/PC(l) of order k Boolean functions and three other cryptographic criteria. In *Advances in Cryptology - EUROCRYPT'97*, Lecture Notes in Computer Science, pages 434–449. Springer-Verlag, 1997.
7. 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.
8. 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.
9. N. J. Patterson and D. H. Wiedemann. Correction to - the covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, IT-36(2):443, 1990.
10. B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of Boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, Lecture Notes in Computer Science, pages 161–173. Springer-Verlag, 1991.
11. O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, 20:300–305, 1976.
12. P. Sarkar and S. Maitra. Construction of nonlinear resilient Boolean functions. *Indian Statistical Institute, Technical Report No. ASD/99/30*, November 1999.
13. P. Sarkar and S. Maitra. Highly nonlinear balanced Boolean functions with important cryptographic properties. *Indian Statistical Institute, Technical Report No. ASD/99/31*, November 1999.
14. 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.
15. 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.
16. T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776–780, September 1984.
17. T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Transactions on Computers*, C-34(1):81–85, January 1985.
18. Y. V. Tarannikov. On a method for the constructing of cryptographically strong Boolean functions. *Moscow State University, French-Russian Institute of Applied Mathematics and Informatics, Preprint No. 6*, October 1999.