A Maiorana-McFarland type Construction for Resilient Boolean Functions on n Variables (n Even) with Nonlinearity $> 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$

Enes Pasalic
Department of Information Technology,
Lund University,
P. O. Box 118,
221 00 Lund, SWEDEN
E-mail: enes@it.lth.se

Subhamoy Maitra
Applied Statistics Unit,
Indian Statistical Institute,
203 B. T. Road, Calcutta,
Pin 700 108, INDIA
E-mail: subho@isical.ac.in

Abstract

In this paper we present a construction method of m-resilient Boolean functions with very high nonlinearity for low values of m. The construction only considers functions in even number of variables n. So far the maximum nonlinearity attainable by resilient functions was $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$. Here we show that given any m, one can construct n-variable, m-resilient functions with nonlinearity $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} + 2^{\frac{n}{2}-4}$ for all $n \geq 8m+6$. Further we show that for sufficiently large n, it is possible to get such functions with nonlinearity reaching almost $2^{n-1} - 2^{\frac{n}{2}} + \frac{4}{3}2^{\frac{n}{2}-2}$. This is the upper bound on nonlinearity when one uses our basic construction recursively.

Keyword : Boolean Function, Resiliency, Nonlinearity.

1 Introduction

Resilient Boolean functions have important applications in nonlinear combiner model of a stream cipher [18, 19, 7, 1, 6, 17]. Construction of resilient Boolean functions, with as high nonlinearity as possible, has been an important research question from mid eighties (by abuse of notation, when we call a Boolean function resilient, we mean an m-resilient function for some $m \geq 1$). Recently (since 2000), a lot of new results have been published in a very short time which include nontrivial nonlinearity (upper) bounds [16, 20, 23, 2, 4] and construction of resilient functions attaining either those bounds or reaching very close. In such a scenario, getting resilient functions with a nonlinearity, that has not been demonstrated earlier, is becoming harder.

Consider a Boolean function on n variables with order of resiliency m. Generalized construction methods of resilient functions with higher order of resiliency ($m > \frac{n}{2} - 2$) and attaining maximum possible nonlinearity have been studied in depth [20, 21, 22]. Also there are some interesting results available in [14, 12]. Construction of highly nonlinear functions with lower order of resiliency has been discussed in [14, 10].

In this paper we consider that n is even. In [11], it has been conjectured that the maximum possible nonlinearity of a resilient function on n variables can be $2^{n-1} - 2^{\frac{n}{2}}$. This conjecture has been turned out to be false [14]. Note that, the maximum possible nonlinearity of an

n-variable function is $2^{n-1} - 2^{\frac{n}{2}-1}$ and these functions are called bent [13]. It is known that the bent functions can not be resilient and also it has been shown [16] that for low order of resiliency m ($m \leq \frac{n}{2} - 2$), the maximum possible nonlinearity is upper bounded by $2^{n-1} - 2^{\frac{n}{2}-1} - 2^{m+1}$. Note that the mid point of $2^{n-1} - 2^{\frac{n}{2}}$ (the value conjectured in [11]) and $2^{n-1} - 2^{\frac{n}{2}-1}$ (the nonlinearity for bent function) is $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$. Construction of resilient functions having this nonlinearity is known [14, 10].

However, till date there has been no evidence of a resilient function having nonlinearity strictly greater than $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$. In this paper, we show that it is possible to construct resilient functions having nonlinearity $> 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$ for $n \geq 14$. Our construction is based on combination of linear functions with a suitable nonlinear resilient function.

1.1 Preliminaries

A Boolean function on n variables may be viewed as a mapping from $\{0,1\}^n$ into $\{0,1\}$. A Boolean function $f(x_1, \ldots, x_n)$ is also interpreted as the output column of its *truth table* f, i.e., a binary string of length 2^n, $f = [f(0,0,\cdots,0), f(1,0,\cdots,0), f(0,1,\cdots,0), \ldots, f(1,1,\cdots,1)]$.

The *Hamming distance* between S_1, S_2 is denoted by $d(S_1, S_2)$, i.e., $d(S_1, S_2) = \#(S_1 \neq S_2)$. Also the *Hamming weight* or simply the weight of a binary string S is the number of ones in S. This is denoted by $wt(S)$. An n-variable function f is said to be *balanced* if its output column in the truth table contains equal number of 0's and 1's (i.e., $wt(f) = 2^{n-1}$).

Denote addition operator over $GF(2)$ by $\oplus$. An n-variable Boolean function $f(x_1, \ldots, x_n)$ 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, $f(x_1, \ldots, x_n)$ can be written as

$$a_0 \oplus \bigoplus_{1 \leq i \leq n} a_i x_i \oplus \bigoplus_{1 \leq i < j \leq n} a_{ij} x_i x_j \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \ldots x_n,$$

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 the degree of f and denoted by $deg(f)$.

Take $0 \leq b \leq n$. An n-variable function is called non degenerate on b variables if its ANF contains exactly b distinct input variables.

Functions of degree at most one are called *affine* functions. An affine function with constant term equal to zero is called a *linear* function. The set of all n-variable affine (respectively linear) functions is denoted by $A(n)$ (respectively $L(n)$). The nonlinearity of an n-variable function f is

$$nl(f) = min_{g \in A(n)}(d(f, g)),$$

i.e., the distance from the set of all n-variable affine functions.

Let $x = (x_1, \ldots, x_n)$ and $\omega = (\omega_1, \ldots, \omega_n)$ both belong to $\{0,1\}^n$ and

$$x \cdot \omega = x_1\omega_1 \oplus \ldots \oplus x_n\omega_n.$$

Let $f(x)$ be a Boolean function on n variables. Then the *Walsh transform* of $f(x)$ is a real valued function over $\{0,1\}^n$ which is defined as

$$W_f(\omega) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus x \cdot \omega}.$$

In terms of Walsh spectra, the nonlinearity of f is given by

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in \{0,1\}^n} |W_f(\omega)|.$$

In [7], an important characterization of resilient functions has been presented, which we use as the definition here. A function $f(x_1, \ldots, x_n)$ is m-resilient iff its Walsh transform satisfies

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

As the notation used in [14, 16], by an (n, m, d, σ) function we denote an n-variable, m-resilient function with degree d and nonlinearity σ.

Now we present a brief outline of the construction methods which are related to our construction. Construction of resilient functions by concatenating the truth tables of small affine functions was first described in [1]. However, the analysis has been made in terms of orthogonal arrays. This construction has been revisited in more details in [17] where the authors considered the algebraic degree and nonlinearity of the functions. Further analysis on this basic method is also available in [9].

Moreover, in [5], construction of functions with concatenation of small affine functions under certain conditions has been discussed. All these constructions used each small affine functions exactly once. A major advancement in this area has been done in [14], where each affine function has been used more than once in form of composition with nonlinear functions. In [14], concatenation of both affine and nonlinear functions has been considered too. The constructions in [14] presented very high nonlinearity. The generalized algorithms, i.e., Algorithm A and Algorithm B in [14] outline a framework in this direction which has later been analysed in [3].

Our construction idea falls under the general construction paradigm presented in [14]. However we like to highlight that this specific construction has not been identified in [14, 3]. To construct an n-variable resilient function (n even) we use a set of $\frac{n}{2}$ variable linear functions (each exactly once) and a nonlinear resilient function on $\frac{n}{2} + k$ variables. Under certain conditions, we show that this construction provides higher nonlinearity than the existing results.

2 The Construction Method

We start with an existing construction idea. See [13, 14, 10] for more details about this construction.

Construction 1 *Let r, s be even. Consider that an r-variable, m-resilient, degree d function $f_r(x_1, \ldots, x_r)$ having nonlinearity $2^{r-1} - 2^{\frac{r}{2}} + 2^{\frac{r}{2}-2} + \epsilon_r$ is available, where ϵ_r is an integer ≥ 0. Let us select a bent function on s variables $g_s(y_1, \ldots, y_s)$. Then the function $f_r(x_1, \ldots, x_r) \oplus g_s(y_1, \ldots, y_s)$ is an $(r+s)$-variable, m-resilient, (at least) degree d (the degree is exactly d if $s < 2d$) function with nonlinearity $2^{(r+s)-1} - 2^{\frac{r+s}{2}} + 2^{\frac{r+s}{2}-2} + \epsilon_r \cdot 2^{\frac{s}{2}}$. Putting $n = r + s$, one gets a function f_n with nonlinearity $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} + \epsilon_r \cdot 2^{\frac{n-r}{2}}$.*

The nonlinearity result follows from $nl(f_n) = 2^s\, nl(f_r) + 2^r\, nl(g_s) - 2\, nl(f_r)\, nl(g_s)$. Note that, if $\epsilon_r = 0$, then $\epsilon_r \cdot 2^{\frac{n-r}{2}}$ is also zero. Hence, using Construction 1, it is not possible to cross the nonlinearity bound of $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$ for an n-variable function using a nonlinearity

$2^{r-1}-2^{\frac{r}{2}}+2^{\frac{r}{2}-2}$ function on r variables, where $r<n$. However, we present a construction in this section, where using a nonlinearity $2^{r-1}-2^{\frac{r}{2}}+2^{\frac{r}{2}-2}$ function on r variables, it is possible to get an n-variable function with nonlinearity strictly greater than $2^{n-1}-2^{\frac{n}{2}}+2^{\frac{n}{2}-2}$. We show that it is possible to get such better nonlinearity under certain conditions.

Theorem 1 *Let $1 \leq m \leq n/2-2$, and $1 \leq k \leq n/2-1$. Assume that there exists a $(q=n/2+k, m, d, \tau)$ function h with degree $d>k+1$. Also, for a fixed $\delta \in \{0,1\}^{\frac{n}{2}-k}$ assume there exists an injective function $\phi : \{0,1\}^k \times \{0,1\}^{\frac{n}{2}-k} \setminus \{\delta\} \rightarrow \{0,1\}^{\frac{n}{2}}$ with property that $wt(\phi(y)) > m$ for any $y \in \{0,1\}^{\frac{n}{2}}$.*

Then for $x, y \in \{0,1\}^{\frac{n}{2}}$, and $y=(y', y'') \in \{0,1\}^k \times \{0,1\}^{\frac{n}{2}-k}$ construct the function

$$f(x,y) = \begin{cases} \phi(y)\cdot x \oplus g(y), & y'' \neq \delta; \\ h(x,y'), & y''=\delta, \end{cases}$$

where g is any function on $\{0,1\}^{\frac{n}{2}}$. Then the function f is an m-resilient function of degree $n/2-k+d$ and nonlinearity $nl(f) \geq 2^{n-1}-2^{\frac{n}{2}-1}-2^{q-1}+nl(h)$.

Proof : Let $(\alpha,\beta) \in \{0,1\}^{\frac{n}{2}} \times \{0,1\}^{\frac{n}{2}}$ and denote by $\beta=(\beta', \beta'')$ for $\beta' \in \{0,1\}$ and $\beta'' \in \{0,1\}^{\frac{n}{2}-k}$. Then,

$$\begin{aligned} W_f(\alpha,\beta) &= \sum_x \sum_y (-1)^{f(x,y)\oplus(x,y)\cdot(\alpha,\beta)} = \sum_{y''}(-1)^{y''\cdot\beta''} \sum_{y'}\sum_x (-1)^{f(x,y)\oplus x\cdot\alpha\oplus y'\cdot\beta'} = \\ &= \underbrace{\sum_{x,y'|y''=\delta} (-1)^{h(x,y')\oplus x\cdot\alpha\oplus y'\cdot\beta'}}_{W_h(\alpha,\beta')} + \sum_{y|y''\neq\delta} (-1)^{g(y)\oplus beta\cdot y} \sum_x (-1)^{(\phi(y)\oplus\alpha)\cdot x}. \qquad (1) \end{aligned}$$

Then for (α,β) such that $wt((\alpha,\beta)) \leq m$ the both sums in Equation (1) are equal to zero. This is obvious for the left-hand sum since h is an m-resilient function. The right-hand sum is zero due to the injection property and the weight restriction on ϕ. Hence, f is m-resilient.

In case $wt(\alpha,\beta) > m$ the left-hand sum in (1) is a Walsh transform of h in point (α,β'). The second sum is either 0 or $\pm 2^{\frac{n}{2}}$. This is because ϕ is injective function and the inner sum is nonzero (actually equal to $2^{\frac{n}{2}}$) only if $\phi(y)=\alpha$ for some $y \in \{0,1\}^{\frac{n}{2}}$. Thus, for any given α there will be exactly either one (ϕ is injective) or no one y such that $\phi(y)=\alpha$ (the 'no one' case corresponds to those α with $wt(\alpha) \leq m$).

Noting that $\max_{\alpha,\beta'} |W_h(\alpha,\beta')| = 2^q - 2nl(h)$, we obtain

$$\max_{\alpha,\beta} |W_f(\alpha,\beta)| \leq \max_{\alpha,\beta'} |W_h(\alpha,\beta')| + 2^{\frac{n}{2}} = 2^q - 2nl(h) + 2^{\frac{n}{2}}.$$

By using, $\max_{\alpha,\beta} |W_f(\alpha,\beta)| = 2^n - 2nl(f)$, we prove that $nl(f) \geq 2^{n-1}-2^{\frac{n}{2}-1}-2^{q-1}+nl(h)$.

The maximum degree term in the ANF of f related to function h is $\frac{n}{2}-k+d$. On the other hand, for any given y the function $\phi(y)\cdot x + g(y)$ is affine on x. Hence, the maximum degree term related to this constituent part is $\frac{n}{2}+1$. The condition $d-k>1$ guarantees that the degree $\frac{n}{2}-k+d$ term(s) can not be canceled by the degree $\frac{n}{2}+1$ term(s). ∎

Note that, if the function h possesses the maximum possible algebraic degree (known as degree optimized [18, 16]) $d=\frac{n}{2}+k-m-1$ then $deg(f)=n-m-1$, i.e., f is also degree optimized. Furthermore, according to nonlinearity result $nl(f) \geq 2^{n-1}-2^{\frac{n}{2}-1}-2^{q-1}+nl(h)$, which means that the nonlinearity of f is increased by choosing a function h with maximum possible nonlinearity for suitably chosen $q=n/2+k$.

Next we concentrate on practical issues regarding the construction given in Theorem 1.

Construction 2 *Let $1 \leq m \leq n/2-2$, and k be a positive integer satisfying $\sum_{i=0}^{m} \binom{n/2}{i} \leq 2^k$. Assume that there exists a $(q = n/2 + k, m, d, \tau)$ function h satisfying,*

- $d > k + 1$,
- $\tau = 2^{q-1} - 2^{\frac{q}{2}} + 2^{\frac{q}{2}-2} + \epsilon_q$, *for q even,*
- $\tau = 2^{q-1} - 2^{\frac{q-1}{2}} + \epsilon_q$, *for q odd,*

where $\epsilon_q \geq 0$.

Consider all the distinct linear functions on $\frac{n}{2}$ variables which are non degenerate on at least $m+1$ variables. There are $u = \sum_{i=m+1}^{\frac{n}{2}} \binom{\frac{n}{2}}{i}$ number of such linear functions. Among them choose any $v = u - (2^k - \sum_{i=0}^{m} \binom{n/2}{i}) = 2^{\frac{n}{2}} - 2^k$ linear functions and list these distinct linear functions by $l_1, \ldots, l_v$ in any arbitrary order. These linear functions are on the variables $(x_1, \ldots, x_{\frac{n}{2}})$. Then for $x, y \in \{0,1\}^{\frac{n}{2}}$ construct the function

$$
\begin{aligned}
f(x,y) \;=\; & \Big((1 \oplus y_{\frac{n}{2}}) \ldots (1 \oplus y_{k+1})\, h(x_1, \ldots, x_{\frac{n}{2}}, y_1, \ldots, y_k)\Big) \\
& \oplus \left(\bigoplus_{i=1}^{v} (1 \oplus a_{n,i} \oplus y_{\frac{n}{2}}) \ldots (1 \oplus a_{\frac{n}{2}+1,i} \oplus y_1)\, l_i(x_1, \ldots, x_{\frac{n}{2}}) \right),
\end{aligned} \tag{2}
$$

where $(a_{n,i}, \ldots, a_{\frac{n}{2}+1,i})$ is $\frac{n}{2}$-bit binary representation of the integer $2^k - 1 + i$. The bit $a_{n,i}$ is the most significant bit and $a_{\frac{n}{2}+1,i}$ is the least significant bit.

The function h, satisfying the above conditions, can be obtained for certain values of m using the construction techniques proposed in [10, 14]. We will discuss this in more detail later. Also notice that for given m and n the injective property of function ϕ in Theorem 1 corresponds to the condition $\sum_{i=0}^{m} \binom{n/2}{i} \leq 2^k$ in Construction 2.

In language of [14, 10], Construction 2 can be interpreted as follows. Concatenate the $(\frac{n}{2} + k, m, d, \tau)$ function h and $v = 2^{\frac{n}{2}} - 2^k$ distinct linear functions on $\frac{n}{2}$ variables which are non degenerate on at least $m+1$ variables. This will provide an n-variable function. Here concatenation means the concatenation of the truth tables of the functions. Next we concentrate on the following theorem which imposes certain restrictions on k for given n, so that we indeed get a nonlinearity $> 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$ using Construction 2.

Theorem 2 *The n-variable function f proposed by Construction 2 is an $(n, m, \frac{n}{2} - k + d, \nu)$ function where $\nu \geq \left(2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}\right) + 2^{\frac{n}{4}-2}\left(2^{\frac{n}{4}} - 2^{\frac{k}{2}+\mu}\right) + \epsilon_q$. Here $\mu = \log_2 3$ (respectively $\frac{3}{2}$), if $q = \frac{n}{2} + k$ is even (respectively odd), and $\epsilon_q \geq 0$.*

In particular, for $\epsilon_q = 0$ the nonlinearity $nl(f) > 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$, if

$$
\frac{n}{2} > \begin{cases} k + 3, & \text{for odd } \; q = \frac{n}{2} + k; \\ k + 3.17, & \text{for even } \; q = \frac{n}{2} + k. \end{cases}
$$

Proof: Results on resiliency and algebraic degree follow from Theorem 1. Also by Theorem 1, $nl(f) \geq 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{q-1} + nl(h)$, which can be rewritten as $nl(f) \geq \left(2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}\right) + 2^{\frac{n}{2}-2} - 2^{q-1} + nl(h)$. Set $nl(h) = 2^{q-1} - 2^{\frac{q}{2}} + 2^{\frac{q}{2}-2} + \epsilon_q$ for q even and $nl(h) = 2^{q-1} - 2^{\frac{q-1}{2}} + \epsilon_q$ for q odd. The first part of statement is proved by noting that $a2^b = 2^{b+\log_2 a}$ for positive reals a, b.

To prove the second part we assume $\epsilon_q = 0$. Then, $nl(f) > 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$ gives that $2^{\frac{n}{4}-2}\left(2^{\frac{n}{4}} - 2^{\frac{k}{2}+\mu}\right) > 0$. Hence, $\frac{n}{4} > \frac{k}{2} + \mu$ and the proof is completed by substituting the value of μ depending on evenness of q. ■

We now present the main result which establishes the existence of m-resilient functions ($m \leq n/2 - 2$) with nonlinearity better than previously best known.

Theorem 3 *Given any m, it is possible to construct $(n, m, 4m+6, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} + 2^{\frac{n}{2}-4})$ functions for all $n \geq 8m + 6$.*

Proof : Given m, take $k = 4m - 1$. Later in the proof we will show that it is always possible to construct a $(q = 2k + 4, m, d > k + 1, 2^{q-1} - 2^{\frac{q}{2}} + 2^{\frac{q}{2}-2})$ function h.

Let us first prove that $\sum_{i=0}^{m} \binom{4m+3}{i} \leq 2^{4m-1}$ for all $m \geq 1$. It can be checked that the statement is true for $m = 1, 2, 3, 4$. From [8, Page 165], $\sum_{i=0}^{\lambda u} \binom{u}{i} \leq 2^{uH(\lambda)}$, where the binary entropy function $H(\lambda) = -\lambda \log_2 \lambda - (1-\lambda)\log_2(1-\lambda)$. Now $H(\frac{1}{4}) \leq 0.82$ and $H(\frac{m}{4m+3}) \leq H(\frac{1}{4})$, since $H(\lambda)$ is increasing in $0 < \lambda \leq 0.5$. Thus, $\sum_{i=0}^{m} \binom{4m+3}{i} \leq 2^{0.82*(4m+3)} = 2^{3.28m+2.46} = 2^{-0.72m+3.46} 2^{4m-1} \leq 2^{4m-1}$ for all $m \geq 5$. Hence the statement is true for all $m \geq 1$.

Since $\sum_{i=0}^{m} \binom{4m+3}{i} \leq 2^{4m-1}$ for all $m \geq 1$, we get $\sum_{i=0}^{m} \binom{k+4}{i} \leq 2^k$. If we take $n_0 = 2k + 8 = 8m + 6$ then $\sum_{i=0}^{m} \binom{\frac{n_0}{2}}{i} \leq 2^k$.

According to the proof of the Theorem 2, the nonlinearity of the n_0-variable function f is $nl(f) \geq \left(2^{n_0-1} - 2^{\frac{n_0}{2}} + 2^{\frac{n_0}{2}-2}\right) + 2^{\frac{n_0}{2}-2} - 2^{q-1} + nl(h) = \left(2^{n_0-1} - 2^{\frac{n_0}{2}} + 2^{\frac{n_0}{2}-2}\right) + 2^{\frac{n_0}{2}-2} - 2^{\frac{q}{2}} + 2^{\frac{q}{2}-2} = \left(2^{n_0-1} - 2^{\frac{n_0}{2}} + 2^{\frac{n_0}{2}-2}\right) + 2^{\frac{n_0}{2}-4}$.

Now we discuss the construction of h. As given in [10], it is possible to get a $(q, m, d, 2^{q-1} - 2^{\frac{q}{2}} + 2^{\frac{q}{2}-2})$ function for $m = 1$ and $q = 8m + 2$. For this function $d = 8 > 4 = k + 1$. Next we present the case for $m \geq 2$.

As given in [15, Proposition 4.2], it is possible to get a $(q, m, d, 2^{q-1} - 2^{\frac{q}{2}} + 2^{\frac{q}{2}-2})$ function under the condition $4 \leq \frac{2^{p+1}}{2^{p-1} - \sum_{i=0}^{m} \binom{p-1}{i}} \leq 5$, where $q = 2p$. We prove that this condition is always satisfied when $q = 8m + 2$.

It is clear that $4 \leq \frac{2^{p+1}}{2^{p-1} - \sum_{i=0}^{m} \binom{p-1}{i}}$. Now we present the proof of $\frac{2^{p+1}}{2^{p-1} - \sum_{i=0}^{m} \binom{p-1}{i}} \leq 5$, when $q = 8m + 2$, i.e., $p = 4m + 1$. Note that $\frac{2^{4m+2}}{2^{4m} - \sum_{i=0}^{m} \binom{4m}{i}} = \frac{4}{1 - \frac{\sum_{i=0}^{m} \binom{4m}{i}}{2^{4m}}}$. As the base case, $\frac{4}{1 - \frac{\sum_{i=0}^{m} \binom{4m}{i}}{2^{4m}}} \leq 5$ for $m = 2$. Further $\frac{4}{1 - \frac{\sum_{i=0}^{(m+1)} \binom{4(m+1)}{i}}{2^{4(m+1)}}} < \frac{4}{1 - \frac{\sum_{i=0}^{m} \binom{4m}{i}}{2^{4m}}}$. Hence, by induction, the proof is true for all $m \geq 2$.

Note that for the functions in [15, Proposition 4.2], $d \geq p + 1 = 4m + 2 > 4m = k + 1$, thus the degree condition is also satisfied. Further, since h is m-resilient, from Theorem 1 the n_0-variable function is also m-resilient.

Once such a function on n_0 variables is found, using Construction 1, it is possible to get functions with nonlinearity $\left(2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}\right) + 2^{\frac{n}{2}-4}$ for all $n \geq n_0$. It follows from Theorem 1 that the degree of these functions will be $\frac{n_0}{2} - k + d$. Note that $n_0 = 8m + 6$, and d is at least $4m + 2$. Hence $\frac{n_0}{2} - k + d$ is at least $4m + 6$.

Thus, given any m, we will get $(n, m, 4m+6, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} + 2^{\frac{n}{2}-4})$ functions for all $n \geq 8m+6$. ■

Note that we use the Construction 1 in the proof of Theorem 3 only to make a generalized statement. Recursive use of Construction 2 will always provide better results (see Example 4, Proposition 1 and Theorem 4 in the following subsection).

2.1 Further Discussion

In this section we first present some concrete examples and then prove important results related to the recursive use of Construction 2.

Example 1 *Let us construct an $m = 1$ resilient function using the Construction 2. Then using the result of Theorem 3, we can construct an $n = 8m+6 = 14$ variable function, which in turn requires a $(q = 8m+2 = 10, 1, d, 488 = 2^{10-1} - 2^{\frac{10}{2}} + 2^{\frac{10}{2}-2})$ function h. Note that $(10, 1, 8, 488 = 2^{10-1} - 2^{\frac{10}{2}} + 2^{\frac{10}{2}-2})$ functions are available [10]. Take $k = 4m-1 = 3$. We can also verify the calculation by noting that $\sum_{i=0}^{1} \binom{14/2}{i} = 8 = 2^3$, i.e., $k = 3$. Hence, we get a $(14, 1, 12, 2^{14-1} - 2^{\frac{14}{2}} + 2^{\frac{14}{2}-2} + 2^{\frac{14}{2}-4})$ function.*

In the following example, we do not directly use Theorem 3 where q is always even, but use the idea given in Theorem 2 where there is a scope of using a function where q is odd.

Example 2 *Consider the construction of a 30-variable function. Take a $(14, 1, 12, 2^{14-1} - 2^{\frac{14}{2}} + 2^{\frac{14}{2}-2} + 8)$ function as a starting point. Using Construction 1, one gets $(30, 1, 12, 2^{30-1} - 2^{\frac{30}{2}} + 2^{\frac{30}{2}-2} + 8 \cdot 2^8)$ function. Call this function h_1. Note that $8 \times 2^8 = 2^{11}$.*

Now we explain the strategy using Construction 2. We know that $\binom{30/2}{0} + \binom{30/2}{1} = 2^4$. Using the technique presented in [14], it is possible to get a $(19, 1, 17, 2^{19-1} - 2^{\frac{19-1}{2}})$ function. This, using Construction 2, provides a $(30, 1, 28, 2^{30-1} - 2^{\frac{30}{2}} + 2^{\frac{30}{2}-2} + 2^{13} - 2^9)$ function, as given in Theorem 2. Call this function h_2.

Both h_1, h_2 have nonlinearity $> 2^{30-1} - 2^{\frac{30}{2}} + 2^{\frac{30}{2}-2}$. However, note that $28 = deg(h_2) > deg(h_1) = 12$ and $nl(h_2) - nl(h_1) = 2^{13} - 2^9 - 2^{11} = 2^{12} + 3 \cdot 2^9$.

We further demonstrate our construction by considering the case $m = 2$.

Example 3 *The first case when the conditions of Theorem 2 are satisfied for $m = 2$ is the case $n = 8m+6 = 22$. Here $k = 4m-1 = 7$. It can be verified that $\sum_{i=0}^{m} \binom{n/2}{i} \leq 2^k$ is satisfied for $k = 7$. Also $q = n/2 + k = 18$ and we need a $(18, 2, d, 2^{17} - 2^9 + 2^7)$ function h. Such a function can be obtained using the technique of [15, Proposition 4.2].*

Then the function f, as described in Construction 2, is an $(n = 22, 2, \frac{n}{2} - k + d = 4 + d, \nu)$ function, where $\nu = 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} + 2^{\frac{n}{2}-4}$.

In the proof of Theorem 3, we use the Construction 1 just to make a generalized statement. However, we like to point out the advantage of recursively applying only Construction 2 instead of using the combination of Construction 1 and Construction 2.

Example 4 *We know that $(10, 1, 8, 488)$ function is available. Using Construction 2 (first time), we get a $(n, 1, n-2, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} + 2^{\frac{n}{2}-4})$ function for $n = 14$.*

Now use this function as the initial function h (of Construction 2, second time) which is a $(q, 1, q-2, 2^{q-1} - 2^{\frac{q}{2}} + 2^{\frac{q}{2}-2} + 2^{\frac{q}{2}-4})$ *function for* $q = 14$ *and take* $n = q + 4 = 18$. *In this case we will get a* $(n, 1, n-2, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} + 2^{\frac{n}{2}-4} + 2^{\frac{n}{2}-6})$ *function for* $n = 18$.

One more recursion using Construction 2 (third time) provides $(n, 1, n-2, 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} + 2^{\frac{n}{2}-4} + 2^{\frac{n}{2}-6} + 2^{\frac{n}{2}-8})$ *function for* $n = 22$.

Note that since we have started from a degree optimized 10-variable function, we will go on getting degree optimized functions in this case.

The examples above clearly indicate that the Construction 2 is to be preferred to Construction 1 when iteratively applied, and it is actually advantageous both in terms of nonlinearity and algebraic degree. We demonstrate the implications of the above reasoning by the following generalized construction method of degree optimized 1-resilient functions. Notice that the functions provided by means of Theorem 3 are not degree optimized.

Proposition 1 *It is possible to construct* $(n, 1, n-2, 2^{n-1} - 2^{\frac{n}{2}} + \frac{4}{3}(1 - (\frac{1}{4})^{z+1})2^{\frac{n}{2}-2})$ *functions for* $n = 10 + 4z$.

Proof : We start with the $(10, 1, 8, 488)$ function and then use the Construction 2 recursively z times. Then we get $(n, 1, n-2, 2^{n-1} - 2^{\frac{n}{2}} + \sum_{i=0}^{z} 2^{\frac{n}{2}-2-2i})$ functions for $n = 10 + 4z$. The proof follows from $\sum_{i=0}^{z} 2^{\frac{n}{2}-2-2i} = \frac{4}{3}(1 - (\frac{1}{4})^{z+1})2^{\frac{n}{2}-2}$. ■

Corollary 1 *It is possible to construct* $(n, 1, n-2, \nu)$ *function with* $\nu \approx 2^{n-1} - 2^{\frac{n}{2}} + \frac{4}{3}2^{\frac{n}{2}-2}$ *for sufficiently large* n.

Proof : The proof follows from Proposition 1, noting $(\frac{1}{4})^{z+1}$ tends to 0 as z takes an increasingly large value. ■

Thus we can make the following general statement.

Theorem 4 *It is possible to construct* $(n, m, (n-m-1)-(3m-1), 2^{n-1} - 2^{\frac{n}{2}} + \frac{4}{3}(1 - (\frac{1}{4})^{z+1})2^{\frac{n}{2}-2})$ *functions for* $n = 8m + 2 + 4z$. *For a sufficiently large* n, *it is possible to get a* $(n, m, (n-m-1)-(3m-1), \nu)$ *function, where* $\nu \approx 2^{n-1} - 2^{\frac{n}{2}} + \frac{4}{3}2^{\frac{n}{2}-2}$.

Proof : The nonlinearity result follows similar to Proposition 1 and Corollary 1. The result from algebraic degree is as follows. The algebraic degree of the q-variable function, in the proof of Theorem 3, is at least $4m + 2$. Since $q = 8m + 2$, the maximum possible algebraic degree is $q - m - 1 = (8m + 2) - (m - 1) = 7m + 1$ for that function. Thus the deficiency in algebraic degree is at most $(7m + 1) - (4m + 2) = 3m - 1$ with respect to a degree optimized function. Once we start using Construction 2, no more deficiency of algebraic degree will be incorporated. Hence in the final construction we will get the algebraic degree $(n - m - 1) - (3m - 1)$. ■

3 Conclusion

In this paper for the first time we present resilient functions with nonlinearity $> 2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$ for $n \geq 14$. It is known that up to 8-variables the maximum possible nonlinearity of a resilient function is $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2}$. Thus important open questions include the cases for $n = 10, 12$. Moreover, we have provided a generalized construction method for m-resilient functions with nonlinearity $2^{n-1} - 2^{\frac{n}{2}} + 2^{\frac{n}{2}-2} + 2^{\frac{n}{2}-4}$ for all $n \geq 8m + 6$. It is expected to get

functions with such nonlinearity (may be more) in many special cases where $n < 8m+6$ using the techniques mentioned in this paper. Finally we have shown that for sufficiently large n, it is possible to get such functions with nonlinearity $\approx 2^{n-1} - 2^{\frac{n}{2}} + \frac{4}{3}2^{\frac{n}{2}-2}$. This is the upper bound on maximum possible nonlinearity when Construction 2 is applied recursively.

Acknowledgment: The authors like to thank the anonymous reviewers whose comments improved both the editorial and technical quality of the paper.

References

[1] P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation immune functions. In *Advances in Cryptology - CRYPTO'91*, number 576 in Lecture Notes in Computer Science, pages 86–100. Springer-Verlag, 1992.

[2] C. Carlet. On the coset weight divisibility and nonlinearity of resilient and correlation immune functions. In *Sequences and Their Applications - SETA 2001*, Discrete Mathematics and Theoretical Computer Science, pages 131–144. Springer Verlag, 2001.

[3] C. Carlet. A larger Class of Cryptographic Boolean Functions via a Study of the Maiorana-McFarland Constructions. In *Advances in Cryptology - CRYPTO 2002*, number 2442 in Lecture Notes in Computer Science, pages 549–564. Springer Verlag, 2002.

[4] C. Carlet and P. Sarkar. Spectral domain analysis of correlation immune and resilient Boolean functions. *Finite Fields and Its Applications*, 8(1):120–130, January 2002.

[5] 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.

[6] C. Ding, G. Xiao, and W. Shan. *The Stability Theory of Stream Ciphers.* Number 561 in Lecture Notes in Computer Science. Springer-Verlag, 1991.

[7] 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.

[8] R. W. Hamming. *Coding and Information Theory.* Prentice-Hall, Inc., Englewood Cliffs, N. J. 07632, 1980.

[9] 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.

[10] S. Maitra and E. Pasalic. Further constructions of resilient Boolean functions with very high nonlinearity. *IEEE Transactions on Information Theory*, 48(7):1825–1834, 2002.

[11] 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.

[12] E. Pasalic, S. Maitra, T. Johansson and P. Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity. In *Workshop on Coding and Cryptography - WCC 2001*, Paris, January 8–12, 2001. Electronic Notes in Discrete Mathematics, Volume 6, Elsevier Science, 2001.

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

[14] P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. In *Advances in Cryptology - EUROCRYPT 2000*, number 1807 in Lecture Notes in Computer Science, pages 485–506. Springer Verlag, 2000.

[15] P. Sarkar and S. Maitra. Construction of Nonlinear Resilient Boolean Functions Using "Small" Affine Functions. Submitted to Journal of Cryptology in January 2001. This paper is a revised version of some portion of [14], available at www.isical.ac.in/šubho.

[16] P. Sarkar and S. Maitra. Nonlinearity bounds and constructions of resilient Boolean functions. In *Advances in Cryptology - CRYPTO 2000*, number 1880 in Lecture Notes in Computer Science, pages 515–532. Springer Verlag, 2000.

[17] J. Seberry, X. M. Zhang, and Y. Zheng. On constructions and nonlinearity of correlation immune Boolean functions. In *Advances in Cryptology - EUROCRYPT'93*, number 765 in Lecture Notes in Computer Science, pages 181–199. Springer-Verlag, 1994.

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

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

[20] Y. V. Tarannikov. On resilient Boolean functions with maximum possible nonlinearity. In *Progress in Cryptology - INDOCRYPT 2000*, number 1977 in Lecture Notes in Computer Science, pages 19–30. Springer Verlag, 2000.

[21] Y. V. Tarannikov. New constructions of resilient Boolean functions with maximal nonlinearity. In *Fast Software Encryption - FSE 2001*, pages 70–81 (in preproceedings).

[22] M. Fedorova and Y. V. Tarannikov. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices. In *Progress in Cryptology - INDOCRYPT 2001*, number 2247 in LNCS, pages 254–266. Springer Verlag, 2001.

[23] Y. Zheng and X. M. Zhang. Improved upper bound on the nonlinearity of high order correlation immune functions. In *Selected Areas in Cryptography - SAC 2000*, number 2012 in Lecture Notes in Computer Science, pages 264–274. Springer Verlag, 2000.