A Maiorana–McFarland type construction for resilient Boolean functions on n variables (n even) with nonlinearity $> 2^{n-1} - 2^{n/2} + 2^{n/2-2}$☆

Subhamoy Maitra[a], Enes Pasalic[b,1]

[a]*Applied Statistics Unit, Indian Statistical Institute, 203 B.T. Road, Kolkata 700 108, India*
[b]*INRIA, projet CODES, Domaine de Voluceau, Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France*

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 $2^{n-1} - 2^{n/2} + 2^{n/2-2}$. Here, we show that given any m, one can construct n-variable, m-resilient functions with nonlinearity $2^{n-1} - 11 \cdot 2^{n/2-4}$ for all $n \geqslant 8m+6$ which is strictly greater than $2^{n-1} - 2^{n/2} + 2^{n/2-2}$. We also demonstrate that in some specific cases one may get such nonlinearity even for some values of n, where $n < 8m+6$. Further, we show that for sufficiently large n, it is possible to get such functions with nonlinearity reaching almost $2^{n-1} - 2^{n/2} + \frac{4}{3}2^{n/2-2}$. This is the upper bound on nonlinearity when one uses our basic construction recursively. Lastly, we discuss the autocorrelation property of the functions and show that the maximum absolute value in the autocorrelation spectra is $\leqslant 2^{n-3}$.

Keywords: Boolean function; Resiliency; Nonlinearity; Autocorrelation

1. Introduction

Resilient Boolean functions have important applications in nonlinear combiner model of a stream cipher [23,24,9,1,7,22]. 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 $m \geqslant 1$). Recently (since 2000), a lot of new results have been published in a very short time which include nontrivial nonlinearity (upper) bounds [20,25,29,2,4] 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.

☆ This paper is a revised and extended version of the paper presented in WCC 2003, March 24–28, 2003 at INRIA, Versailles, France.

[1] The initial version of this paper has been written when the author was doing his PhD at Department of Information Technology, Lund University, Sweden.

Consider a Boolean function on n variables with order of resiliency m. Generalized construction methods of resilient functions with higher order of resiliency ($m > n/2 - 2$) and attaining maximum possible nonlinearity have been studied in depth [25,26,8]. Also there are some interesting results available in [19,16]. Construction of highly nonlinear functions with lower order of resiliency has been discussed in [19,12].

In this paper, we consider that n is even. In [15], it has been conjectured that the maximum possible nonlinearity of a resilient function on n variables can be $2^{n-1} - 2^{n/2}$. This conjecture has been turned out to be false [19]. Note that the maximum possible nonlinearity of an n-variable function is $2^{n-1} - 2^{n/2-1}$ and these functions are called bent [18]. It is known that the bent functions cannot be resilient and also it has been shown [20] that for low order of resiliency m ($m \leqslant n/2 - 2$), the maximum possible nonlinearity is upper bounded by $2^{n-1} - 2^{n/2-1} - 2^{m+1}$. Note that the mid point of $2^{n-1} - 2^{n/2}$ (the value conjectured in [15]) and $2^{n-1} - 2^{n/2-1}$ (the nonlinearity for bent function) is $2^{n-1} - 2^{n/2} + 2^{n/2-2}$. Construction of resilient functions having this nonlinearity is known [19,12].

However, till date there has been no evidence of a resilient function having nonlinearity strictly greater than $2^{n-1} - 2^{n/2} + 2^{n/2-2}$. In this paper, we show that it is possible to construct resilient functions having nonlinearity $> 2^{n-1} - 2^{n/2} + 2^{n/2-2}$ for $n \geqslant 14$. 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,

$$f = [f(0,0,\ldots,0), f(1,0,\ldots,0), f(0,1,\ldots,0), \ldots, f(1,1,\ldots,1)].$$

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 kth order products ($0 \leqslant k \leqslant n$) of the variables. More precisely, $f(x_1, \ldots, x_n)$ can be written as

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

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 $0 \leqslant b \leqslant n$. An n-variable function is called nondegenerate 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

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

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 [9], 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

$$W_f(\omega) = 0 \quad \text{for } 0 \leqslant wt(\omega) \leqslant m.$$

As the notation used in [19,20], by an (n, m, d, σ) function we denote an n-variable, m-resilient function with degree d and nonlinearity σ.

Propagation characteristics (PC) and strict avalanche criteria (SAC) [17] are important properties of Boolean functions to be used in S-boxes. Further, Zhang and Zheng [28] identified related cryptographic measures called global avalanche characteristics (GAC).

Let $\alpha \in \{0,1\}^n$ and f be an n-variable Boolean function. Define the autocorrelation value of f with respect to the vector α as

$$\Delta_f(\alpha) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus f(x \oplus \alpha)}$$

and the absolute indicator

$$\Delta_f = \max_{\alpha \in \{0,1\}^n, \alpha \neq \bar{0}} |\Delta_f(\alpha)|.$$

A function is said to satisfy PC(k), if

$$\Delta_f(\alpha) = 0 \quad \text{for } 1 \leqslant wt(\alpha) \leqslant k.$$

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 [22] where the authors considered the algebraic degree and nonlinearity of the functions. Further analysis on this basic method is also available in [13].

Moreover, in [6], 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 [19], where each affine function has been used more than once in form of composition with nonlinear functions. In [19], concatenation of both affine and nonlinear functions has been considered too. The constructions in [19] presented very high nonlinearity. The generalized algorithms, i.e., Algorithms A and B in [19] outline a framework in this direction which has later been analysed in [3].

Our construction idea falls under the general construction paradigm presented in [19]. However, we like to highlight that this specific construction has not been identified in [19,3]. To construct an n-variable resilient function (n even) we use a set of $n/2$ variable linear functions (each exactly once) and a nonlinear resilient function on $n/2 + k$ variables. Under certain conditions, we show that this construction provides higher nonlinearity than the existing results.

Analysis of autocorrelation properties of correlation immune and resilient Boolean functions has gained substantial interest recently as evident from [27,30,31,11,5]. A Boolean function f on n-variables is said to have a linear structure if there exists a nonzero vector $\alpha \in \{0,1\}^n$ such that $|\Delta_f(\alpha)| = 2^n$. In cryptographic terms, this property is undesirable for a Boolean function. In [11,5], it has been identified that some well-known construction of resilient Boolean functions are not good in terms of autocorrelation properties. We show that there is no linear structure in our construction. Further, we analyse the autocorrelation spectra of the functions and provide an upper bound on the absolute indicator Δ_f.

2. The construction method

We first present an existing construction idea [18,19,12].

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*

$$2^{r-1} - 2^{r/2} + 2^{r/2-2} + \varepsilon_r$$

is available, where ε_r is an integer $\geqslant 0$. 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

$$2^{(r+s)-1} - 2^{(r+s)/2} + 2^{(r+s/2)-2} + \varepsilon_r \cdot 2^{s/2}.$$

Putting $n = r + s$, one gets a function f_n with nonlinearity

$$2^{n-1} - 2^{n/2} + 2^{n/2-2} + \varepsilon_r \cdot 2^{(n-r)/2}.$$

The nonlinearity result follows from

$$nl(f_n) = 2^s nl(f_r) + 2^r nl(g_s) - 2nl(f_r)nl(g_s).$$

Note that if $\varepsilon_r = 0$, then $\varepsilon_r \cdot 2^{(n-r)/2}$ is also zero. Hence, using Construction 1, it is not possible to cross the nonlinearity bound of $2^{n-1} - 2^{n/2} + 2^{n/2-2}$ for an n-variable function using a nonlinearity $2^{r-1} - 2^{r/2} + 2^{r/2-2}$ function on r variables, where $r < n$. However, we present a construction in this section, where using a nonlinearity $2^{r-1} - 2^{r/2} + 2^{r/2-2}$ function on r variables, it is possible to get an n-variable function with nonlinearity strictly greater than $2^{n-1} - 2^{n/2} + 2^{n/2-2}$. We show that it is possible to get such better nonlinearity under certain conditions.

Theorem 1. *Let $1 \leqslant m \leqslant n/2 - 2$, and $1 \leqslant k \leqslant n/2 - 1$. Assume that there exists a $(q = n/2 + k, m, d, \tau)$ function h with degree $d > k + 1$. Also, for a fixed $\delta \in \{0,1\}^{n/2-k}$ assume there exists an injective function*

$$\phi : \{0,1\}^k \times (\{0,1\}^{n/2-k} \backslash \{\delta\}) \to \{0,1\}^{n/2}$$

with property that $wt(\phi(y)) > m$ for any $y \in \{0,1\}^{n/2}$.

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

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

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

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

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

Then for (α, β) such that $wt((\alpha, \beta)) \leqslant m$ the both sums in Eq. (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 $\pm 2^{n/2}$. This is because ϕ is injective function and the inner sum is nonzero (actually equal to $2^{n/2}$) only if $\phi(y) = \alpha$ for some $y \in \{0,1\}^{n/2}$. 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 $wt(\alpha) \leqslant m$).

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

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

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

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

Let us emphasize that given a fixed n, there are two main assumptions in Theorem 1.

(1) There are some restrictions on the parameters of the function h.
(2) The injectivity of ϕ puts some restriction on k.

Note that if the function h possesses the maximum possible algebraic degree (known as degree optimized [23,20]) $d = n/2 + k - m - 1$ then $deg(f) = n - m - 1$, i.e., f is also degree optimized. Furthermore, according to nonlinearity result $nl(f) \geqslant 2^{n-1} - 2^{n/2-1} - 2^{q-1} + nl(h)$, 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 present a construction based on Theorem 1.

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

- $d > k + 1$,
- $\tau = 2^{q-1} - 2^{q/2} + 2^{q/2-2} + \varepsilon_q$, *for q even*,
- $\tau = 2^{q-1} - 2^{(q-1)/2} + \varepsilon_q$, *for q odd*,

where $\varepsilon_q \geqslant 0$.

Also, for a fixed $\delta \in \{0,1\}^{n/2-k}$ select an injective function

$$\phi : \{0,1\}^k \times (\{0,1\}^{n/2-k} \backslash \{\delta\}) \to \{0,1\}^{n/2}$$

with property that $wt(\phi(y)) > m$ for any $y \in \{0,1\}^{n/2}$.

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

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

where g is any function on $\{0,1\}^{n/2}$.

Note that for given m and n the injective property of function ϕ in Theorem 1 is guaranteed here due to the condition $\sum_{i=0}^{m} \binom{n/2}{i} \leqslant 2^k$.

Let us now interpret the construction for a specific case. Let δ be an all zero vector and $g(y) = 0$ for all y. Consider all the distinct linear functions on $n/2$ variables which are nondegenerate on at least $m + 1$ variables. There are $u = \sum_{i=m+1}^{n/2} \binom{n/2}{i}$ number of such linear functions. Among them choose any $v = u - \left(2^k - \sum_{i=0}^{m} \binom{n/2}{i}\right) = 2^{n/2} - 2^k$ 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 $(x_1, \ldots, x_{n/2})$.

Then, in language of [19,12], Construction 2 can be interpreted as follows. Concatenate the $(n/2+k, m, d, \tau)$ function h and $v = 2^{n/2} - 2^k$ distinct linear functions on $n/2$ variables which are nondegenerate 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.

The ANF of the function will be

$$f(x, y) = ((1 \oplus y_{n/2}) \cdots (1 \oplus y_{k+1}) h(x_1, \ldots, x_{n/2}, y_1, \ldots, y_k)) \oplus \left(\bigoplus_{i=1}^{v} (1 \oplus a_{n,i} \oplus y_{n/2}) \cdots (1 \oplus a_{n/2+1,i} \oplus y_1) l_i(x_1, \ldots, x_{n/2}) \right), \quad (2)$$

where $(a_{n,i}, \ldots, a_{n/2+1,i})$ is $n/2$-bit binary representation of the integer $2^k - 1 + i$. The bit $a_{n,i}$ is the most significant bit and $a_{n/2+1,i}$ 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 [12,19]. We will discuss this in more detail later. Next, we concentrate on the following theorem which imposes certain restrictions on k for given n, so that we indeed get a nonlinearity $> 2^{n-1} - 2^{n/2} + 2^{n/2-2}$ using Construction 2.

Theorem 2. *The n-variable function f proposed by Construction 2 is an $(n, m, n/2-k+d, v)$ function where*

$$v \geqslant 2^{n-1} - 2^{n/2-1} - 2^{n/4+k/2+\mu-2} + \varepsilon_q.$$

Here, $\mu = \log_2 3$ (respectively $\frac{3}{2}$), if $q = n/2 + k$ is even (respectively odd), and $\varepsilon_q \geqslant 0$.

In particular, for $\varepsilon_q = 0$ the nonlinearity

$$nl(f) > 2^{n-1} - 2^{n/2} + 2^{n/2-2},$$

if $n \geqslant 2k + 8$.

Proof. Results on resiliency and algebraic degree follow from Theorem 1. Also from Theorem 1, we get

$$nl(f) \geqslant 2^{n-1} - 2^{n/2-1} - 2^{q-1} + nl(h),$$

which can be rewritten as

$$nl(f) \geqslant (2^{n-1} - 2^{n/2} + 2^{n/2-2}) + 2^{n/2-2} - 2^{q-1} + nl(h).$$

Set

$$nl(h) = 2^{q-1} - 2^{q/2} + 2^{q/2-2} + \varepsilon_q$$

for q even and

$$nl(h) = 2^{q-1} - 2^{(q-1)/2} + \varepsilon_q$$

for q odd. Note that $a2^b = 2^{b+\log_2 a}$ for positive reals a, b. Thus,

$$v \geqslant (2^{n-1} - 2^{n/2} + 2^{n/2-2}) + 2^{n/4-2}(2^{n/4} - 2^{k/2+\mu}) + \varepsilon_q$$

which gives the result after simplification.

For $\varepsilon_q = 0$ we will show that $n \geqslant 2k + 8$. Here, $nl(f) > 2^{n-1} - 2^{n/2} + 2^{n/2-2}$ gives that

$$2^{n/4-2}(2^{n/4} - 2^{k/2+\mu}) > 0.$$

This happens when

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

Note that n is always even and hence $n/2$ must be an integer, which gives $n/2 \geqslant k + 4$. □

Next, we present a technical result.

Proposition 1. $\sum_{i=0}^{m}\binom{4m+3}{i} \leqslant 2^{4m-1}$ *for all* $m \geqslant 1$.

Proof. It can be checked that the statement is true for $m = 1, 2, 3, 4$. From [10, p. 165],

$$\sum_{i=0}^{\lambda u}\binom{u}{i} \leqslant 2^{uH(\lambda)},$$

where the binary entropy function

$$H(\lambda) = -\lambda \log_2 \lambda - (1-\lambda)\log_2(1-\lambda).$$

Now, $H(\frac{1}{4}) \leqslant 0.82$ and $H(m/(4m+3)) \leqslant H(\frac{1}{4})$, since $H(\lambda)$ is increasing in $0 < \lambda \leqslant 0.5$. Thus,

$$\sum_{i=0}^{m}\binom{4m+3}{i} \leqslant 2^{0.82*(4m+3)} = 2^{3.28m+2.46} = 2^{-0.72m+3.46}2^{4m-1} \leqslant 2^{4m-1}$$

for all $m \geqslant 5$. Hence, the statement is true for all $m \geqslant 1$. □

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

Theorem 3. *Given any* m, *it is possible to construct* $(n, m, 4m+6, 2^{n-1} - 11 \cdot 2^{n/2-4})$ *functions for all* $n \geqslant 8m+6$.

Proof. Following Theorem 3, we have to start with $n_0 = 2k+8$, where n_0 is the smallest n satisfying the assumption $n \geqslant 2k+8$. Further, $q = n_0/2 + k = 2k+4$. The most important point in this proof is that, given m, we choose $k = 4m-1$. Later in the proof we will show that it is always possible to construct a

$$(q = 2k+4, m, d > k+1, 2^{q-1} - 2^{q/2} + 2^{q/2-2})$$

function h.

From Proposition 1,

$$\sum_{i=0}^{m}\binom{4m+3}{i} \leqslant 2^{4m-1}$$

for all $m \geqslant 1$. Hence, we get

$$\sum_{i=0}^{m}\binom{k+4}{i} \leqslant 2^{k}.$$

Given $n_0 = 2k+8 = 2(4m-1)+8 = 8m+6$, it is clear that $\sum_{i=0}^{m}\binom{n_0/2}{i} \leqslant 2^k$ which satisfies the constraint given in Construction 2.

According to the proof of Theorem 2, the nonlinearity of the n_0-variable function f is

$$\begin{aligned} nl(f) &\geqslant (2^{n_0-1} - 2^{n_0/2} + 2^{n_0/2-2}) + 2^{n_0/2-2} - 2^{q-1} + nl(h) \\ &= (2^{n_0-1} - 2^{n_0/2} + 2^{n_0/2-2}) + 2^{n_0/2-2} - 2^{q/2} + 2^{q/2-2} \\ &= (2^{n_0-1} - 2^{n_0/2} + 2^{n_0/2-2}) + 2^{n_0/2-4} \quad (\text{putting } q = n_0 - 4). \end{aligned}$$

Now, we discuss the construction of h. As given in [12], it is possible to get a $(q, m, d, 2^{q-1} - 2^{q/2} + 2^{q/2-2})$ function for $m = 1$ and $q = 8m + 2$. For this function $d = 8 > 4 = k + 1$. Next, we present the case for $m \geqslant 2$.

As given in [21, Proposition 4.2], it is possible to get a $(q, m, d, 2^{q-1} - 2^{q/2} + 2^{q/2-2})$ function under the condition

$$4 \leqslant \frac{2^{p+1}}{2^{p-1} - \sum_{i=0}^{m} \binom{p-1}{i}} \leqslant 5,$$

where $q = 2p$. We prove that this condition is always satisfied when $q = 8m + 2$.

For integer $p \geqslant 1$, it is clear that

$$4 = \frac{2^{p+1}}{2^{p-1}} \leqslant \frac{2^{p+1}}{2^{p-1} - \sum_{i=0}^{m} \binom{p-1}{i}}.$$

Now, we present the proof of

$$\frac{2^{p+1}}{2^{p-1} - \sum_{i=0}^{m} \binom{p-1}{i}} \leqslant 5,$$

when $q = 8m + 2$, i.e., $p = 4m + 1$. Note that

$$\frac{2^{4m+2}}{2^{4m} - \sum_{i=0}^{m} \binom{4m}{i}} = \frac{4}{1 - \sum_{i=0}^{m} \binom{4m}{i} \Big/ 2^{4m}}.$$

As the base case, $\frac{4}{1-\sum_{i=0}^{m}\binom{4m}{i}/2^{4m}} \leqslant 5$ for $m = 2$. Further

$$\frac{4}{1 - \sum_{i=0}^{(m+1)} \binom{4(m+1)}{i} \Big/ 2^{4(m+1)}} < \frac{4}{1 - \sum_{i=0}^{m} \binom{4m}{i} \Big/ 2^{4m}}.$$

Hence, by induction, the proof is true for all $m \geqslant 2$.

Note that for the functions in [21, Proposition 4.2], $d \geqslant p + 1 = 4m + 2 > 4m = k + 1$, 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 $(2^{n-1} - 2^{n/2} + 2^{n/2-2}) + 2^{n/2-4}$ for all $n \geqslant n_0$. It follows from Theorem 1 that the degree of these functions will be $n_0/2 - k + d$. Note that $n_0 = 8m + 6$, and d is at least $4m + 2$. Hence, $n_0/2 - k + d$ is at least $4m + 6$.

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

At this point let us highlight two important issues which can improve the result of Theorem 3.

(1) 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 as will be seen in Section 2.1.
(2) In the proof of Theorem 3, we have fixed $k = 4m - 1$, which gives $n_0 = 8m + 6$. This in turn provides functions with our targeted nonlinearity for $n \geqslant 8m + 6$. We will identify some situations when such nonlinearity may also be found even when $n < 8m + 6$. This we will discuss in Section 2.2.

Now, we present some concrete examples.

Example 1.

(1) *Case* $m=1$: Note that $(10, 1, 8, 488)$ function is available [12]. Here, $q=8m+2=10$, $n=8m+6=14$, $k=4m-1=3$. Verify that $\sum_{i=0}^{1} \binom{14/2}{i} = 8 = 2^k$. Thus, using Construction 2 and the result of Theorem 3 we get a $(14, 1, 12, 8104)$ function. Note that $8104 > 2^{14-1} - 2^{14/2} + 2^{14/2-2}$.

(2) *Case* $m = 2$: Note that $(18, 2, d, 2^{17} - 3 \cdot 2^7)$ function is available using the technique of [21, Proposition 4.2]. Here, $q = 8m + 2 = 18$, $n = 8m + 6 = 22$, $k = 4m - 1 = 7$. Verify that $\sum_{i=0}^{m} \binom{n/2}{i} \leqslant 2^k$ is satisfied. Thus, using Construction 2 and the result of Theorem 3 we get a $(22, 2, 4 + d, 2^{21} - 11 \cdot 2^7)$ 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. 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 [19], it is possible to get a $(19, 1, 17, 2^{18} - 2^9)$ function. This, using Construction 2, provides a $(30, 1, 28, 2^{29} - 2^{14} - 2^9)$ function, as given in Theorem 2.

2.1. Recursive construction

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 Constructions 1 and 2.

Example 3. We know that $(10, 1, 8, 488)$ function is available. Using Construction 2 (first time), we get a $(n, 1, n - 2, 2^{n-1} - 2^{n/2} + 2^{n/2-2} + 2^{n/2-4})$ function for $n = 14$. The algebraic degree of this 14-variable function will be 12. Call this function g_1.

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

One more recursion using Construction 2 (third time) provides $(n, 1, n-2, 2^{n-1} - 2^{n/2} + 2^{n/2-2} + 2^{n/2-4} + 2^{n/2-6} + 2^{n/2-8})$ function for $n = 22$. Call this function h_2. Note that since we have started from a degree optimized 10-variable function, we will go on getting degree optimized functions in this case. Thus, the algebraic degree of h_2 will be 20.

One can use the 14-variable function g_1 and then use Construction 1 to construct an $n = 22$ variable function h_1 (similar to what mentioned in Theorem 3). The function h_1 will be an $(n, 1, 12, 2^{n-1} - 2^{n/2} + 2^{n/2-2} + 2^{n/2-4})$ function.

Note that both the nonlinearity and algebraic degree of h_2 are better than h_1.

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. Note that the functions provided by means of Theorem 3 are not degree optimized.

Proposition 2. *It is possible to construct* $(n, 1, n - 2, 2^{n-1} - 2^{n/2} + \frac{4}{3}(1 - (\frac{1}{4})^{z+1})2^{n/2-2})$ *functions for* $n = 10 + 4z$, $z > 0$.

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

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

Proof. The proof follows from Proposition 2, 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* $(n, m, n-4m, 2^{n-1} - 2^{n/2} + \frac{4}{3}(1 - (\frac{1}{4})^{z+1})2^{n/2-2})$ *functions for* $n = 8m + 2 + 4z$, $z > 0$. *For a sufficiently large* n, *it is possible to get a* $(n, m, n - 4m, v)$ *function, where* $v \approx 2^{n-1} - 2^{n/2} + \frac{4}{3}2^{n/2-2}$.

Table 1
Finding minimum n given m for Construction 2

m	k, n_0 Theorem 3	min k_1 such that $\sum_{i=0}^{m}\binom{k_1+4}{i} \leqslant 2^{k_1}$	min k_2 such that $5\sum_{i=0}^{m}\binom{k_2+1}{i} \leqslant 2^{k_2+1}$	$k=$ $\max(k_1, k_2)$	min $n=$ $2k+8$
2	7, 22	6	7	7	22
3	11, 30	9	9	9	26
4	15, 38	11	11	11	30
5	19, 46	14	14	14	36
6	23, 54	16	16	16	40
7	27, 62	19	18	19	46
8	31, 70	21	20	21	50
9	35, 78	23	23	23	54
10	39, 86	26	25	26	60

Proof. The nonlinearity result follows similar to Proposition 2 and Corollary 1. The result for 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 $(n - m - 1) - (3m - 1)$. □

Remark 1. Consider that the starting function h on $8m+2$ variables is degree optimized. Then it is possible to construct $(n, m, (n - m - 1), 2^{n-1} - 2^{n/2} + \frac{4}{3}(1 - (\frac{1}{4})^{z+1})2^{n/2-2})$ functions for $n = 8m + 2 + 4z$. Further, for a sufficiently large n, it is possible to get a $(n, m, (n-m-1), v)$ function, where $v \approx 2^{n-1} - 2^{n/2} + \frac{4}{3}2^{n/2-2}$. Note that, for the case $m = 1$, the 10-variable function is degree optimized. Thus, we get the degree optimized result as given in Proposition 2 and Corollary 1.

2.2. *High nonlinearity for $n < 8m + 6$*

Form Theorem 3, we get that given any m, it is possible to construct $(n, m, 4m + 6, 2^{n-1} - 2^{n/2} + 2^{n/2-2} + 2^{n/2-4})$ functions for all $n \geqslant 8m + 6$. Thus, following Theorem 3, the first time such a function is found when $n = 8m + 6$. Basically, we need to control two constraint in optimized manner. As given in Construction 2, we need $\sum_{i=0}^{m}\binom{n/2}{i} \leqslant 2^k$. Further, from Theorem 2, $n \geqslant 2k + 8$. Hence, one needs to satisfy $\sum_{i=0}^{m}\binom{k+4}{i} \leqslant 2^k$. From the proof of Theorem 3, we need $2^{p+1}/2^{p-1} - \sum_{i=0}^{m}\binom{p-1}{i} \leqslant 5$, where $q = 2p$. Since, $q = n/2 + k = 2k + 4$, we have $p = k + 2$. Thus, one needs to satisfy $2^{k+3}/2^{k+1} - \sum_{i=0}^{m}\binom{k+1}{i} \leqslant 5$ which gives, $5\sum_{i=0}^{m}\binom{k+1}{i} \leqslant 2^{k+1}$. Hence, given m, one needs to find out the minimum k such that

$$\sum_{i=0}^{m}\binom{k+4}{i} \leqslant 2^k \quad \text{and} \quad 5\sum_{i=0}^{m}\binom{k+1}{i} \leqslant 2^{k+1}$$

and then $n = 2k + 8$ will provide the minimum value of n when one gets a nonlinearity $> 2^{n-1} - 2^{n/2} + 2^{n/2-2}$ using our construction. The value $k = 4m - 1$ in Theorem 3 indeed satisfies these conditions, but we want to find if it is possible in some cases when $k < 4m - 1$. In this direction, we present some results in Table 1. Note that, given an $m \geqslant 3$, the minimum value of n is strictly less than the value that has been chosen as n_0 in Theorem 3. In the table, we list the observation upto $m = 10$ and the value of n in the last column gives the minimum value for which one can construct an m-resilient function with nonlinearity $(2^{n-1} - 2^{n/2} + 2^{n/2-2} + 2^{n/2-4})$ using our technique as described in Construction 2.

Further it may be observed that for $m \geqslant 3$, the value of k is determined by the value of k_1 as given in Table 1. We like to present the following two interesting observations.

(1) Given $3 \leqslant m \leqslant 10$, if one calculates the minimum k such that $\sum_{i=0}^{m} \binom{k+4}{i} \leqslant 2^k$ is satisfied, then that value of k automatically satisfies $5\sum_{i=0}^{m} \binom{k+1}{i} \leqslant 2^{k+1}$.
(2) Note that $\lceil 7m/3 \rceil + 2$ is almost a tight bound for k in the range $2 \leqslant m \leqslant 10$. It is not equal only in the case $m = 4$, when $\lceil 7m/3 \rceil + 2 = 12$. In all the other cases it is same as given in Table 1.

3. Autocorrelation property

In this section, we analyse the autocorrelation spectra of our construction. We follow Construction 2, with the additional constraint that comes from Theorem 2 which gives that the minimum value of n must be $2k + 8$. In fact, at any stage of the recursive construction as mentioned in Section 2.1, we use the function h to be on $n/2 + k$ variables and the function f to be on n variables, with $n = 2k + 8$. This gives that h is basically a function on $n - 4$ variables.

Theorem 5. *Consider the Construction 2 with the constraint $n = 2k + 8$. Then $\Delta_f \leqslant 2^{n-3}$.*

Proof. Here, $n/2 - k = 4$. Thus, we fix a $\delta \in \{0, 1\}^4$. We have an injective function

$$\phi : \{0, 1\}^{n/2-4} \times (\{0, 1\}^4 \backslash \{\delta\}) \to \{0, 1\}^{n/2}$$

with property that $wt(\phi(y)) > m$ for any $y \in \{0, 1\}^{n/2}$. Then for $x, y \in \{0, 1\}^{n/2}$, and $y = (y', y'') \in \{0, 1\}^{n/2-4} \times \{0, 1\}^4$ we 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 $\{0, 1\}^{n/2}$. Now, we will consider different cases for ζ', ζ''. We consider $\alpha = (\zeta, \zeta', \zeta'')$ and relate x with ζ, y' with ζ' and y'' with ζ'', i.e., $\zeta \in \{0, 1\}^{n/2}$, $\zeta' \in \{0, 1\}^{n/2-4}$ and $\zeta'' \in \{0, 1\}^4$.

(1) *ζ'' nonzero vector*: Let α be such that ζ'' is not an all zero vector. Note that one can write $f(x, y) = h_{[y'']}(x, y')$ for a specific y''. In this case, $h_{[\delta]}(x, y') = h(x, y')$. When $y'' \neq \delta$, then $h_{[y'']}(x, y')$ is basically concatenation of $2^{n/2-4}$ many distinct $n/2$-variable affine functions. Thus, $\Delta_f(\alpha) = 2\sum_{x \in \{0,1\}^{n/2}, y' \in \{0,1\}^{n/2-4}} (-1)^{h_{[\delta]}(x,y') \oplus h_{[\delta \oplus \zeta'']}((x,y') \oplus (\zeta, \zeta'))}$. The other terms will have no contribution since $\sum_{x \in \{0,1\}^{n/2}} (-1)^{l_i(x) \oplus l_j(x \oplus \zeta)} = 0$ when l_i, l_j are distinct linear functions, thus $\sum_{x \in \{0,1\}^{n/2}, y' \in \{0,1\}^{n/2-4}} (-1)^{h_{[\mu]}(x,y') \oplus h_{[\mu \oplus \zeta'']}((x,y') \oplus (\zeta, \zeta'))} = 0$ when $\mu \neq \delta$. Hence, $|\Delta_f(\alpha)| \leqslant 2 \cdot 2^{n-4} = 2^{n-3}$.
(2a) *ζ'' all zero vector, ζ' nonzero vector*: Let α be such that ζ'' is an all zero vector but ζ' is not an all zero vector. Using the similar argument as above, $\Delta_f(\alpha) = \sum_{x \in \{0,1\}^{n/2}, y' \in \{0,1\}^{n/2-4}} (-1)^{h_{[\delta]}(x,y') \oplus h_{[\delta]}((x,y') \oplus (\zeta, \zeta'))} = \Delta_h(\zeta, \zeta')$.
(2b) *ζ'', ζ' both all zero vectors*: Now, we consider that both ζ'', ζ' are all zero vectors, but ζ is not. Consider a Maiorana–McFarland type bent function $b(x, y) = \pi(y)x \oplus g(y)$, where π is a permutation function. In particular, consider $\pi(y) = \phi(y)$ for $y'' \neq \delta$. Since b is bent, we know that $\Delta_b(\alpha) = 0$ for any nonzero α. Thus, $\sum_{x \in \{0,1\}^{n/2}, y \in \{0,1\}^{n/2}} (-1)^{b(x,y) \oplus b((x,y) \oplus (\zeta, (\zeta', \zeta'')))} = 0$.
This gives, $\sum_{x \in \{0,1\}^{n/2}, y' \in \{0,1\}^{n/2-4}, y'' \in \{0,1\}^4, y'' \neq \delta} (-1)^{b(x,y',y'') \oplus b((x,y',y'') \oplus (\zeta, \zeta', \zeta''))} = -\sum_{x \in \{0,1\}^{n/2}, y' \in \{0,1\}^{n/2-4}, y'' = \delta} (-1)^{b(x,y',y'') \oplus b((x,y',y'') \oplus (\zeta, \zeta', \zeta''))}$,
i.e., $|\sum_{x \in \{0,1\}^{n/2}, y' \in \{0,1\}^{n/2-4}, y'' \in \{0,1\}^4, y'' \neq \delta} (-1)^{b(x,y',y'') \oplus b((x,y',y'') \oplus (\zeta, \zeta', \zeta''))}| \leqslant 2^{n-4}$,
i.e., $|\sum_{x \in \{0,1\}^{n/2}, y' \in \{0,1\}^{n/2-4}, y'' \in \{0,1\}^4, y'' \neq \delta} (-1)^{f(x,y',y'') \oplus f((x,y',y'') \oplus (\zeta, \zeta', \zeta''))}| \leqslant 2^{n-4}$.
Hence, $|\Delta_f(\alpha)| \leqslant 2^{n-4} + |\Delta_h(\zeta, \zeta')|$.

From the above discussion, it is clear that $\Delta_f \leqslant 2^{n-3}$. □

Now, we present a concrete example of 14-variable function f and show that in this case the Δ_f value is much better than the upper bound provided in Theorem 5. We start with the (10, 1, 8, 488) function h as mentioned in [12]. The truth table of the function is described below in hexadecimal format.

```
6F4FC675EE280B7135159C4BB472512B6F4FC635EE280B7135159C4BB472512B
6F4FC635EE280B7135159C4BB472512B90B0398A11D7F48ECAEA63B44B8DAED4
CA8A932DD2E4A84D90D0C977C8BEF217CA8A932DD2E4A84D90D0C977CABEF217
CA8A932DD2E4A84D90D0C977CABEF21735756CD22D1B57B26F2F368837410DE8
```

We calculate that $\Delta_h = 320$. Now, according to Construction 2 (see also Example 1) we get a (14, 1, 12, 8104) function f. Theorem 5 gives $\Delta_f \leqslant 2^{14-3} = 2048$. We checked that the exact value of Δ_f is only 864.

As another example, we start with the (10, 1, 8, 488) function h as mentioned in [14]. The truth table of the function is described below in hexadecimal format.

```
EA80C080D5555555B3333333E66666668F0F0F0F5A5A5A5ABC3C3C3C69696969
80FF00FF55AA55AA33CC33CC669966998FF00FF05AA55AA53CC33CC369966996
8000FFFFD555AAAA3333CCCC666699990F0FF0F05A5AA5A53C3CC3C369699696
80FFFF0055AAAA5533CCCC33669999660FF0F00F5AA5A55A3CC3C33C69968660
```

It has been reported in [14] that $\Delta_h = 48$. We checked that the exact value of Δ_f is 800 in this case. Though the value of Δ_f is improved from 864 (in the previous case) to 800, we really do not get as high an improvement, where Δ_h is improved a lot from 320 (in the previous example) to 48. It is of importance to analyse the autocorrelation spectra of Δ_f in more detail to get the exact behaviour.

4. Conclusion

In this paper, for the first time we present resilient functions with nonlinearity $> 2^{n-1} - 2^{n/2} + 2^{n/2-2}$ for $n \geqslant 14$. It is known that up to eight variables the maximum possible nonlinearity of a resilient function is $2^{n-1} - 2^{n/2} + 2^{n/2-2}$. 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 $2^{n-1} - 2^{n/2} + 2^{n/2-2} + 2^{n/2-4}$ for all $n \geqslant 8m + 6$. Applying Construction 2, we have shown that for sufficiently large n, it is possible to get such functions with nonlinearity $\approx 2^{n-1} - 2^{n/2} + \frac{4}{3}2^{n/2-2}$. This is the upper bound on maximum possible nonlinearity when Construction 2 is applied recursively. Later, we made some improvements in certain cases and found that for $m \geqslant 3$, it is also possible to find $n < 8m + 6$ and we specifically identified the cases for $m \leqslant 10$ in Table 1. The autocorrelation property of the functions has also been studied and it has been shown that the maximum absolute value in the autocorrelation spectra is $\leqslant 2^{n-3}$. It seems that more subtle analysis may show that the functions possess much better autocorrelation property than the upper bound described here.

Acknowledgements

The authors like to thank the anonymous reviewers whose comments helped in improving both the editorial and technical quality of the paper. We also like to acknowledge the technical discussion with Prof. Claude Carlet during WCC 2003 which helped in presenting and analysing the main construction of the paper in a more generalized framework.

References

[1] P. Camion, C. Carlet, P. Charpin, N. Sendrier, On correlation immune functions, in: Advances in Cryptology—CRYPTO'91, Lecture Notes in Computer Science, vol. 576, Springer, Berlin, 1992, pp. 86–100.
[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, Springer, Berlin, 2001, pp. 131–144.
[3] C. Carlet, A larger class of cryptographic Boolean functions via a study of the Maiorana–McFarland constructions, in: Advances in Cryptology—CRYPTO 2002, Lecture Notes in Computer Science, vol. 2442, Springer, Berlin, 2002, pp. 549–564.
[4] C. Carlet, P. Sarkar, Spectral domain analysis of correlation immune and resilient Boolean functions, Finite Fields Appl. 8 (1) (2002) 120–130.
[5] P. Charpin, E. Pasalic, On propagation characteristics of resilient functions, in: SAC 2002, Lecture Notes in Computer Science, vol. 2595, Springer, Berlin, 2003, pp. 175–195.

[6] S. Chee, S. Lee, D. Lee, S.H. Sung, On the correlation immune functions and their nonlinearity, in: Advances in Cryptology—ASIACRYPT '96, Lecture Notes in Computer Science, vol. 1163, Springer, Berlin, 1996, pp. 232–243.
[7] C. Ding, G. Xiao, W. Shan, The Stability Theory of Stream Ciphers, Lecture Notes in Computer Science, vol. 561, Springer, Berlin, 1991.
[8] M. Fedorova, Y.V. Tarannikov, On the constructing of highly nonlinear resilient Boolean functions by means of special matrices, in: Progress in Cryptology—INDOCRYPT 2001, Lecture Notes in Computer Science, vol. 2247, Springer, Berlin, 2001, pp. 254–266.
[9] X. Guo-Zhen, J. Massey, A spectral characterization of correlation immune combining functions, IEEE Trans. Inform. Theory 34 (3) (1988) 569–571.
[10] R.W. Hamming, Coding and Information Theory, Prentice-Hall, Englewood Cliffs, NJ, 07632, 1980.
[11] S. Maitra, Autocorrelation properties of correlation immune Boolean functions, INDOCRYPT 2001, Lecture Notes in Computer Science, vol. 2247, Springer, Berlin, December 2001, pp. 242–253.
[12] S. Maitra, E. Pasalic, Further constructions of resilient Boolean functions with very high nonlinearity, IEEE Trans. Inform. Theory 48 (7) (2002) 1825–1834.
[13] S. Maitra, P. Sarkar, Highly nonlinear resilient functions optimizing Siegenthaler's inequality, in: Advances in Cryptology—CRYPTO'99, Lecture Notes in Computer Science, vol. 1666, Springer, Berlin, August 1999, pp. 198–215.
[14] S. Maity, S. Maitra, Minimum distance between bent and 1-resilient Boolean functions, in: Workshop on Fast Software Encryption, FSE 2004, New Delhi, India, February 5–7, 2004, Lecture Notes in Computer Science, vol. 3017, Springer, Berlin, 2004, pp. 143–160.
[15] E. Pasalic, T. Johansson, Further results on the relation between nonlinearity and resiliency of Boolean functions, in: IMA Conference on Cryptography and Coding, Lecture Notes in Computer Science, vol. 1746, Springer, Berlin, 1999, pp. 35–45.
[16] E. Pasalic, S. Maitra, T. Johansson, 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, vol. 6, Elsevier Science, Amsterdam, 2001.
[17] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, J. Vandewalle, Propagation characteristics of Boolean functions, in: Advances in Cryptology—EUROCRYPT'90, Lecture Notes in Computer Science, Springer, Berlin, 1991, pp. 161–173.
[18] O.S. Rothaus, On bent functions, J. Combin. Theory, Ser. A 20 (1976) 300–305.
[19] P. Sarkar, S. Maitra, Construction of nonlinear Boolean functions with important cryptographic properties, in: Advances in Cryptology—EUROCRYPT 2000, Lecture Notes in Computer Science, vol. 1807, Springer, Berlin, 2000, pp. 485–506.
[20] P. Sarkar, S. Maitra, Nonlinearity bounds and constructions of resilient Boolean functions, in: Advances in Cryptology—CRYPTO 2000, Lecture Notes in Computer Science, vol. 1880, Springer, Berlin, 2000, pp. 515–532.
[21] P. Sarkar, S. Maitra, Construction of nonlinear resilient Boolean functions using "small" affine functions, IEEE Trans. Inform. Theory 50 (9) (2004) 2185–2193, this paper is a revised version of some portion of [19].
[22] J. Seberry, X.M. Zhang, Y. Zheng, On constructions and nonlinearity of correlation immune Boolean functions, in: Advances in Cryptology—EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, Springer, Berlin, 1994, pp. 181–199.
[23] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, IEEE Trans. Inform. Theory IT-30 (5) (1984) 776–780.
[24] T. Siegenthaler, Decrypting a class of stream ciphers using ciphertext only, IEEE Trans. Comput. C-34 (1) (1985) 81–85.
[25] Y.V. Tarannikov, On resilient Boolean functions with maximum possible nonlinearity, in: Progress in Cryptology—INDOCRYPT 2000, Lecture Notes in Computer Science, vol. 1977, Springer, Berlin, 2000, pp. 19–30.
[26] Y.V. Tarannikov, New constructions of resilient Boolean functions with maximal nonlinearity, in: Fast Software Encryption—FSE 2001, Lecture Notes in Computer Science, vol. 2355, Springer, Berlin, 2002, pp. 66–77.
[27] Y.V. Tarannikov, P. Korolev, A. Botev, Autocorrelation coefficients and correlation immunity of Boolean functions, in: ASIACRYPT 2001, Lecture Notes in Computer Science, vol. 2248, Springer, Berlin, 2001, pp. 460–479.
[28] X.M. Zhang, Y. Zheng, GAC—the criterion for global avalanche characteristics of cryptographic functions, J. Universal Comput. Sci. 1 (5) (1995) 316–333.
[29] Y. Zheng, X.M. Zhang, Improved upper bound on the nonlinearity of high order correlation immune functions, in: Selected Areas in Cryptography—SAC 2000, Lecture Notes in Computer Science, vol. 2012, Springer, Berlin, 2000, pp. 264–274.
[30] Y. Zheng, X.M. Zhang, On relationships among propagation degree, nonlinearity and correlation immunity, in: Advances in Cryptology—ASIACRYPT 2000, Lecture Notes in Computer Science, vol. 1976, Springer, Berlin, 2000, pp. 470–482.
[31] Y. Zheng, X.M. Zhang, New results on correlation immunity, in: ICISC 2000, Lecture Notes in Computer Science, vol. 2015, Springer, Berlin, 2001, pp. 49–63.