# Highly nonlinear balanced Boolean functions with good local and global avalanche characteristics

Subhamoy Maitra

*Computer & Statistical Service Centre, Indian Statistical Institute, 203, B.T. Road, Calcutta 700 035, India*

Received 28 May 2001; received in revised form 20 November 2001

Communicated by L.A. Hemaspaandra

**Abstract**

Here we deal with an interesting subset of $n$-variable balanced Boolean functions which satisfy strict avalanche criteria. These functions achieve the sum-of-square indicator value (a measure for global avalanche criteria) strictly less than $2^{2n+1}$ and nonlinearity strictly greater than $2^{n-1} - 2^{\lfloor n/2 \rfloor}$. These parameters are currently best known. Moreover, these functions do not possess any nonzero linear structure. The technique involves a well-known simple construction coupled with very good initial functions obtained by computer search, which were not known earlier. 

*Keywords:* Combinatorial problems; Cryptography; Boolean function; Nonlinearity; Balancedness; Strict avalanche criteria; Global avalanche criteria

## 1. Introduction

Strict avalanche criteria (SAC) is an important property of Boolean functions for application in S-boxes [16]. However, some limitations of strict avalanche criteria have been identified in [17] and the concept of global avalanche criteria (GAC) has been introduced. Recently the works on GAC have received a lot of attention [12,15,4,13,14,3].

Here we provide balanced $n$-variable SAC functions with very good GAC property in terms of sum-of-square indicator (see Section 2 for definition). We achieve the sum-of-square indicator value strictly less than $2^{2n+1}$. Also these functions possess currently best known nonlinearity. For even $n$, the nonlinearity is strictly greater than $2^{n-1} - 2^{n/2}$ and for odd $n$, the nonlinearity is strictly greater than $2^{n-1} - 2^{(n-1)/2}$. These functions do not possess any nonzero linear structure. To date, functions with this kind of parameters are not known in the literature. In fact our results supersede the results of [13,14,3] in this direction.

Our method needs good initial functions. For $n$ even, we start with a 6-variable balanced SAC function with sum-of-square indicator value $7552 < 2^{2\cdot 6+1}$ and nonlinearity $26 = 2^{6-1} - 2^{6/2} + 2^{6/2-2}$. Using this we get balanced SAC functions on $n$-variables ($n \geqslant 6$ even) with sum-of-square indicator strictly less than $2^{2n+1}$ and nonlinearity $2^{n-1} - 2^{n/2} + 2^{n/2-2}$. The situation is even more interesting for the case of $n$ odd. Here we use a modification [11] of Patterson–Wiedemann functions [7,8]. The initial function is a 15-variable balanced SAC function with sum-of-square indicator value $1,270,799,360 < 2^{2\cdot 15+1}$ and nonlinearity $2^{15-1} - 2^{(15-1)/2} + 6$. Using this, we

find balanced SAC functions on $n$ variables ($n \geqslant 15$ odd) with sum-of-square indicator strictly less than $2^{2n+1}$ and nonlinearity $2^{n-1} - 2^{(n-1)/2} + 6 \cdot 2^{(n-15)/2}$. Note that the 15-variable function we use here is not the same one that has been described in [11,5,4]. We once again run the experiment of [11] and found functions with better parameters than what is obtained in [11,5,4].

The functions we propose here are suitable for applications in S-boxes. To resist differential cryptanalysis [2], the SAC and GAC properties are important. Moreover, high nonlinearity is required for resisting linear cryptanalysis [6].

## 2. Preliminaries

In this section we introduce a few basic concepts. By $\Omega_n$ we mean the set of $n$-variable Boolean functions. We denote the addition operator over GF(2) by $\oplus$.

Let $s, s_1, s_2$ be binary strings of same length $\lambda$. The bitwise complement of $s$ is denoted by $s^c$. We denote by $\#(s_1 = s_2)$ (respectively $\#(s_1 \neq s_2)$), the number of places where $s_1$ and $s_2$ are equal (respectively unequal). The Hamming distance between $s_1, s_2$ is denoted by $d(s_1, s_2)$, i.e.,

$$d(s_1, s_2) = \#(s_1 \neq s_2).$$

The Walsh distance $wd(s_1, s_2)$, between $s_1$ and $s_2$, is defined as

$$wd(s_1, s_2) = \#(s_1 = s_2) - \#(s_1 \neq s_2).$$

Note that $wd(s_1, s_2) = \lambda - 2d(s_1, s_2)$. The Hamming weight or simply the weight of $s$ is the number of ones in $s$ and is denoted by $wt(s)$. An $n$-variable Boolean function can be viewed as a binary string of length $2^n$, which is the output column of the truth table. 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., $wt(f) = 2^{n-1}$).

An $n$-variable Boolean function $f$ can be uniquely represented by a multivariate polynomial over GF(2). Let $f(X_n, \ldots, X_1)$ be an $n$-variable function. We can write

$$f = a_0 \oplus \left( \bigoplus_{i=1}^{n} a_i X_i \right) \oplus \left( \bigoplus_{1 \leqslant i \neq j \leqslant n} a_{ij} X_i X_j \right) \oplus \cdots \oplus a_{12\ldots n} X_1 X_2 \ldots X_n,$$

where the coefficients $a_0, a_i, a_{ij}, \ldots, a_{12\ldots n} \in \{0, 1\}$. This representation of $f$ is called the algebraic normal form (ANF) of $f$. The number of variables in the highest order product term with nonzero coefficient is called the algebraic degree, or simply degree of $f$.

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 $nl(f)$ of an $n$-variable function $f$ is defined as

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

i.e., $nl(f)$ is the distance of $f$ from the set of all $n$-variable affine functions.

Propagation Characteristic (PC) [9] and Strict Avalanche Criteria (SAC) [16] are important properties of Boolean functions to be used in S-boxes. Let $\overline{X}$ be an $n$-tuple $X_n, \ldots, X_1$ and $\overline{\alpha} \in \{0, 1\}^n$. A function $f \in \Omega_n$ is said to satisfy SAC if

$$f(\overline{X}) \oplus f(\overline{X} \oplus \overline{\alpha})$$

is balanced for any $\overline{\alpha}$ such that $wt(\overline{\alpha}) = 1$.

However, Zhang and Zheng [17] justified that SAC and PC have some limitations in identifying certain desirable cryptographic properties of a Boolean function. In this direction they have proposed the idea of Global Avalanche Characteristics (GAC). Next we state two important indicators of GAC.

Let $\overline{X} \in \{0, 1\}^n$ be an $n$-tuple $X_n, \ldots, X_1$ and $\overline{\alpha} \in \{0, 1\}^n$ be an $n$-tuple $\alpha_n, \ldots, \alpha_1$. Let $f \in \Omega_n$ and

$$\Delta_f(\overline{\alpha}) = wd\big(f(\overline{X}), f(\overline{X} \oplus \overline{\alpha})\big),$$

the autocorrelation value of $f$ with respect to the vector $\overline{\alpha}$. The sum-of-square indicator

$$\sigma_f = \sum_{\overline{\alpha} \in \{0,1\}^n} \Delta_f^2(\overline{\alpha}).$$

The absolute indicator

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

Let us also define

$\boldsymbol{T}_f = \{\bar{\alpha} \mid \Delta_f(\bar{\alpha}) \neq 0\}$ and
$\boldsymbol{Q}_f = \{\bar{\alpha} \mid \Delta_f(\bar{\alpha}) = 0\}$.

Note that $\boldsymbol{T}_f \cup \boldsymbol{Q}_f = \{0,1\}^n$.

It is clear that $\Delta_f(\bar{\alpha}) = 0$ iff $f(\bar{X}) \oplus f(\bar{X} \oplus \bar{\alpha})$ is balanced. Also $|\Delta_f(\bar{\alpha})| = 2^n$ iff $f(\bar{X}) \oplus f(\bar{X} \oplus \bar{\alpha})$ is constant and $\bar{\alpha}$ is called a linear structure of $f$. It should be noted that $\bar{0}$ is always a linear structure for a Boolean function. However, existence of any nonzero linear structure is cryptographically undesirable.

## 3. Basic construction and its properties

First we consider the following well known construction [10].

**Construction 1.** *Let $h \in \Omega_n$ and $m \geqslant 2$ be an even integer. Then consider the function*

$$g(X_{n+m}, \ldots, X_1) = b(X_{n+m}, \ldots, X_{n+1}) \oplus h(X_n, \ldots, X_1),$$

*where $b(X_{n+m}, \ldots, X_{n+1})$ is a bent function.*

Next we present the main result which is to be used to estimate the parameters of the constructed Boolean functions.

**Theorem 1.** *Let $h \in \Omega_n$ be a balanced Boolean function which satisfies SAC, has the nonlinearity value $x$, sum-of-square indicator value $\sigma_h = 2^{2n+\varepsilon}$ and absolute indicator value $\Delta_h = 2^{n-k}$. Consider $g \in \Omega_{n+m}$ as in Construction 1, where $m \geqslant 2$ is even. Then $g$ is a balanced Boolean function which satisfies SAC, has the nonlinearity value $2^n nl(b) + 2^m x - 2x\, nl(b)$, sum-of-square indicator value $\sigma_g = 2^{2(n+m)+\varepsilon}$ and absolute indicator value $\Delta_g = 2^{(n+m)-k}$. Also note that $|\boldsymbol{T}_g| = |\boldsymbol{T}_h|$.*

**Proof.** The nonlinearity and balancedness result of $g$ is known [11]. For the other parts we need the following analysis. We denote

$$\bar{\alpha} = (\alpha_{n+m}, \ldots, \alpha_{n+1}, \alpha_n, \ldots, \alpha_1),$$
$$\bar{\alpha}' = (\alpha_n, \ldots, \alpha_1),$$
$$\bar{\alpha}'' = (\alpha_{n+m}, \ldots, \alpha_{n+1}),$$

and

$$\bar{X} = (X_{n+m}, \ldots, X_{n+1}, X_n, \ldots, X_1),$$
$$\bar{X}' = (X_n, \ldots, X_1),$$
$$\bar{X}'' = (X_{n+m}, \ldots, X_{n+1}).$$

Note that,

$$g(\bar{X}) \oplus g(\bar{X} \oplus \bar{\alpha}) = b(\bar{X}'') \oplus b(\bar{X}'' \oplus \bar{\alpha}'') \oplus h(\bar{X}') \oplus h(\bar{X}' \oplus \bar{\alpha}').$$

Now consider two different cases.

*Case* 1. When $\bar{\alpha}''$ is a zero vector, then $g(\bar{X}) \oplus g(\bar{X} \oplus \bar{\alpha}) = c(\bar{X}'') \oplus h(\bar{X}') \oplus h(\bar{X}' \oplus \bar{\alpha}')$, where $c(\bar{X}'') = b(\bar{X}'') \oplus b(\bar{X}'')$ is the constant zero function on $m$ variables. Thus,

$$wd\big(g(\bar{X}), g(\bar{X} \oplus \bar{\alpha})\big) = 2^m \cdot wd\big(h(\bar{X}'), h(\bar{X}' \oplus \bar{\alpha}')\big).$$

*Case* 2. When $\bar{\alpha}''$ is a nonzero vector, then $b(\bar{X}'') \oplus b(\bar{X}'' \oplus \bar{\alpha}'')$ is always a balanced function since $b$ is bent [10,3]. Thus, $g(\bar{X}) \oplus g(\bar{X} \oplus \bar{\alpha})$ is always balanced, which gives

$$wd\big(g(\bar{X}), g(\bar{X} \oplus \bar{\alpha})\big) = 0.$$

Now,

$$|\boldsymbol{T}_g| = \big|\{\bar{\alpha} \mid \Delta_g(\bar{\alpha} \neq 0)\}\big| = \big|\{\bar{\alpha}' \mid \Delta_h(\bar{\alpha}' \neq 0)\}\big| = |\boldsymbol{T}_h|.$$

This is because if $\bar{\alpha}''$ is nonzero then $\Delta_g(\bar{\alpha}) = 0$.

Since $h$ satisfies SAC, we have

$$wd\big(h(\bar{X}'), h(\bar{X}' \oplus \bar{\alpha}')\big) = 0 \quad \text{for } wt(\bar{\alpha}') = 1.$$

Thus, $wd(g(\bar{X}), g(\bar{X} \oplus \bar{\alpha})) = 2^m \cdot 0 = 0$, when $wt(\bar{\alpha}) = 1$, and $\bar{\alpha}''$ is zero. This is from Case 1. From Case 2, we get that whenever $\bar{\alpha}''$ is nonzero, then $wd(g(\bar{X}), g(\bar{X} \oplus \bar{\alpha})) = 0$. Hence, $g$ also satisfies SAC.

From Case 1, we have $\Delta_g = 2^m \cdot \Delta_h = 2^m \cdot 2^{n-k} = 2^{(n+m)-k}$. Since each element of $\boldsymbol{T}_g$ corresponds to each element of $\boldsymbol{T}_h$, and each nonzero value of $\Delta_h(\bar{\alpha}')$ is multiplied by $2^m$ to get $\Delta_g(\bar{\alpha})$, we have, $\sigma_g = (2^m)^2 \sigma_h = 2^{2(n+m)+\varepsilon}$. □

Theorem 1 underlines the requirement of good initial functions. One standard way of obtaining SAC functions is the following [5]. Recapitulate that, given a function $f \in \Omega_n$, we define

$$\boldsymbol{Q}_f = \{\bar{\alpha} \in \{0,1\}^n \mid \Delta_f(\bar{\alpha}) = 0\}.$$

If there exists $n$ linearly independent vectors in $Q_f$, then we can construct a nonsingular $n \times n$ matrix $B_f$ whose rows are linearly independent vectors from $Q_f$. Now we construct a function $f'(\overline{X}) = f(\overline{X}B_f)$. Here we interpret $\overline{X} \in \{0,1\}^n$, the $n$-tuple $X_n, \ldots, X_1$ as a row vector for matrix multiplication purpose. Note that both $f', f$ have the same nonlinearity and algebraic degree. Also the balancedness condition is preserved. Moreover, $\Delta_{f'}(\overline{\alpha}) = 0$ for $wt(\overline{\alpha}) = 1$. This ensures that $f'$ satisfies SAC. Thus this is basically a linear transformation method. We refer this method as LT-method in the following discussion.

## 4. Choice of proper initial functions

In this section we show how to use basic computer search techniques to find good initial functions.

### 4.1. The 6-variable functions

We select the five-variable functions $f_5$ with the property $nl(f_5) = 12$, $\Delta_{f_5} = 16, \sigma_{f_5} = 1664 < 2^{10.71}$. These functions are available in [1]. Then we try the functions of the form $(1 \oplus X_6)f_5(\overline{X}) \oplus X_6 f_5(A\overline{X})$, for all possible $5 \times 5$ nonsingular binary matrix $A$. We concentrate on the functions of nonlinearity 26 and $\sigma_{f_6} < 8192$. Once we obtain such functions, we use LT-method (if possible) to transform them to SAC functions. Using this method, we find 6-variable functions with desired parameters. One example is the following function $f_6$ satisfying SAC, represented as its truth table,

00111110000011010011000110101001010111000001101001100011010100101011000011101010010001111111010110.

The parameters of this function are $nl(f_6) = 26$, $\Delta_{f_6} = 32, \sigma_{f_6} = 7552 < 2^{12.89}$. The algebraic degree of this function is 5.

### 4.2. The 15-variable functions

Here we consider 15-variable balanced SAC functions. In [11] construction of a balanced 15-variable function with nonlinearity 16,262 has been provided. In [5], it was shown how a 15-variable balanced SAC function $f'_{15}$ with nonlinearity 16,262 can be obtained using LT-method. Also the function has been analyzed in detail [5,4] where $\Delta_{f'_{15}} = 216$ has been reported. We have also checked that $\sigma_{f'_{15}} = 1{,}270{,}938{,}368$ for the function.

Note that the heuristic technique proposed in [11, Algorithm 1, p. 500] was motivated towards finding out 15-variable balanced Boolean functions with very good nonlinearity. We run the same algorithm to find a function $f_{15}$ keeping in mind the $\Delta_{f15}, \sigma_{f15}$ values also. In this way we find functions $f_{15}$ with the parameters $nl(f_{15}) = 16{,}262$, $\Delta_{f_{15}} = 208, \sigma_{f_{15}} = 1{,}270{,}799{,}360$. It is clear that the values $\Delta_{f_{15}}, \sigma_{f_{15}}$ are better (less) than $\Delta_{f'_{15}}, \sigma_{f'_{15}}$ provided in [11,5,4]. It is not possible to provide the truth table of the function as it is a bit string of length $2^{15}$. Also the algebraic normal form is too complicated to write here. Note that, $\Delta_{f_{15}} = 208 < 2^{7.71}$, $\sigma_{f_{15}} = 1{,}270{,}799{,}360 < 2^{30.25}$. The algebraic degree of this function is 14.

### 4.3. The main result

Given the discussion above we now present the main result to provide the subset of Boolean functions satisfying SAC with very good autocorrelation properties.

**Theorem 2.** *It is possible to construct balanced SAC function $f$ with the following parameters.*

(1) *For even $n \geqslant 6$, it is possible to construct $f \in \Omega_n$ such that*

$$nl(f) = 2^{n-1} - 2^{n/2} + 2^{n/2-2},$$
$$\Delta_f = 2^{n-1} \quad \text{and} \quad \sigma_f < 2^{2n+0.89}.$$

(2) *For odd $n \geqslant 15$, it is possible to construct $f \in \Omega_n$ such that*

$$nl(f) = 2^{n-1} - 2^{(n-1)/2} + 6 \cdot 2^{(n-15)/2},$$
$$\Delta_f = 208 \cdot 2^{n-15} < 2^{n-7.29} \quad \text{and}$$
$$\sigma_f < 2^{2n+0.25}.$$

**Proof.** The proof follows from Theorem 1 using the initial functions mentioned in Sections 4.1 and 4.2. □

## 5. Results and comparison to existing works

Here we provide balanced SAC functions on $n$ variables with nonlinearity strictly greater than $2^{n-1} - 2^{\lfloor n/2 \rfloor}$ and sum-of-square indicator value strictly less than $2^{2n+1}$. These functions do not possess any linear structure and the absolute indicator value is less than or equal to $2^{n-1}$, which is moderate. These functions are suitable for applications in S-boxes. The SAC and GAC properties will be useful in resisting differential cryptanalysis [2] and the high nonlinearity will resist the linear cryptanalysis [6].

Note that in [13], construction of balanced SAC functions $f$ with $nl(f) = 2^{n-1} - 2^{\lfloor n/2 \rfloor}$ and $\sigma_f = 2^{2n+1+\varepsilon}$ was proposed, where $\varepsilon = 0$ for $n$ odd and $\varepsilon = 1$ for $n$ even. Since the results in [13] are better than in [14] in this direction, here we compare our results with [13]. Our results in Theorem 2 clearly supersede the results of [13] for odd $n \geqslant 15$ and even $n \geqslant 6$. Our proof techniques are also much simpler than [13]. The functions of [13] possess nonzero linear structures. Note that $\Delta_f = 2^n$ if the function $f$ possesses any nonzero linear structure. Our results on $\Delta_f$ in Theorem 2 show that our functions do not possess any linear structure.

Now we compare our results with those of [3]. In [3], sum-of-square indicator for a function $f$ is denoted as $V(f)$. In [3, Example 4, p. 519], functions $f$ on $n$ variables ($n$ odd and $n \geqslant 5$) have been proposed with the following parameters. The values are

$$nl(f) = 2^{n-1} - 2^{(n-1)/2},$$
$$\Delta_f = 2^{n-1}, \quad \sigma_f = 2^{2n+1} - 3 \cdot 2^{2n-3}$$

(the statement $V(f) = 2^{2n-3}$ in [3, Example 4, p. 519] is a typographical error). For even $n \geqslant 8$, the results in [3, Example 2, p. 515] give the following parameters. The values are

$$nl(f) = 2^{n-1} - 2^{n/2}, \quad \Delta_f = 2^n$$

(there is nonzero linear structure) and $\sigma_f$ value either $2^{2n+2} - 3 \cdot 2^{2n-3}$ or $2^{2n+2}$ (the statement $V(f_2) = 2^{2n-2}$ is a typographical error). Thus it is clear that our results in Theorem 2 supersede the results of [3] for functions on both odd and even number of variables.

Thus, our results of Theorem 2 provide the currently best known parameters in this aspect. For a more summarized description we now provide tabular representations (see Tables 1 and 2).

Table 1
Comparison for even number of variables $n \geqslant 6$

| Ref. | $nl(f)$ | $\sigma_f$ | $\Delta_f$ |
|---|---|---|---|
| [13] | $2^{n-1} - 2^{n/2}$ | $2^{2n+2}$ | $2^n$ |
| [3] | $2^{n-1} - 2^{n/2}$ | $2^{2n+2} - 3 \cdot 2^{2n-3}$ or $2^{2n+2}$ | $2^n$ |
| Our | $2^{n-1} - 2^{n/2} + 2^{n/2-2}$ | $2^{2n+0.89}$ | $2^{n-1}$ |

Table 2
Comparison for odd number of variables $n \geqslant 15$

| Ref. | $nl(f)$ | $\sigma_f$ | $\Delta_f$ |
|---|---|---|---|
| [13] | $2^{n-1} - 2^{(n-1)/2}$ | $2^{2n+1}$ | $2^n$ |
| [3] | $2^{n-1} - 2^{(n-1)/2}$ | $2^{2n+1} - 3 \cdot 2^{2n-3}$ | $2^{n-1}$ |
| Our | $2^{n-1} - 2^{(n-1)/2} + 6 \cdot 2^{(n-15)/2}$ | $2^{2n+0.25}$ | $2^{n-7.29}$ |

Table 3
Comparison for 8-variable balanced SAC functions

| Results | $nl(f)$ | $\sigma_f$ | $\Delta_f$ |
|---|---|---|---|
| Of [13] | 112 | 262,144 | 256 |
| Example 2 [3], function $f_1$ | 112 | 237,568 | 256 |
| Example 2 [3], function $f_2$ | 112 | 262,144 | 256 |
| Our | 116 | 120,832 | 128 |

Table 4
Comparison for 15-variable balanced SAC functions

| Results | $nl(f)$ | $\sigma_f$ | $\Delta_f$ |
|---|---|---|---|
| Of [13] | 16,256 | 2,147,483,648 | 32,768 |
| Example 4 [3], function $f$ | 16,256 | 1,744,830,464 | 16,384 |
| Our | 16,262 | 1,270,799,360 | 208 |

To demonstrate the scenario for small number of variables we provide a tabular comparison with the examples in [13,3] for 8-variable and 15-variable functions (see Tables 3 and 4). All the parameters are for balanced SAC functions. The functions described from [3] do not satisfy SAC, but using LT-method it is possible to get SAC functions from them.

Now we consider the algebraic degree of our construction. Note that for the case when $n$ is even, we start with an initial function of 6 variables (Section 4.1). This function has the algebraic degree 5. We also use a bent function in the Construction 1. If the overall construction generates a function on $n$-variables, then the bent function is of $n-6$ variables. Note that, the maximum possible algebraic degree of a bent function of $n-6$ variables is $\frac{1}{2}(n-6)$ [10,3]. Thus for $n$ even, the algebraic degree of the con-

structed function is $\max(5, \frac{1}{2}(n-6))$, i.e., for large $n$, the algebraic degree of our constructed function is $\frac{1}{2}(n-6)$. Similarly, for odd $n$, the algebraic degree of our constructed function is $\max(14, \frac{1}{2}(n-15))$, as the initial 15-variable function we consider is of degree 14 (Section 4.2). Thus, for large $n$, the algebraic degree of our constructed function is $\frac{1}{2}(n-15)$. Similar technique has been used in [3, Example 4, p. 519] to get functions (on $n$ variables, $n$ odd) with algebraic degree $\frac{1}{2}(n-5)$, as the initial function used was of 5 variables. The algebraic degree in our construction is only 5 less than that of [3], but the other parameters like nonlinearity, $\Delta_f$, $\sigma_f$ are much better in our case. Note that to get improvement for odd $n$, $5 \leqslant n \leqslant 13$, we need $n$-variable functions with better properties than what is provided in [3]. Construction of such functions is an interesting open question in this direction. It will also be of interest to get SAC functions with nonlinearity, $\Delta_f$, $\sigma_f$ values as in our case with algebraic degree as high as $(n-1)$.

## Acknowledgements

The author likes to acknowledge the anonymous reviewers for their comments which have substantially improved the presentation and technical quality of this paper.

## References

[1] E.R. Berlekamp, L.R. Welch, Weight distributions of the cosets of the (32, 6) Reed–Muller code, IEEE Trans. Inform. Theory IT-18 (1) (1972) 203–207.

[2] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, in: Advances in Cryptology—CRYPTO'90, Lecture Notes in Comput. Sci., Vol. 537, Springer, Berlin, 1991, pp. 2–21.

[3] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, Propagation characteristics and correlation immunity of highly nonlinear Boolean functions, in: Advances in Cryptology—EUROCRYPT'00, Lecture Notes in Comput. Sci., Vol. 1807, Springer, Berlin, 2000, pp. 507–522.

[4] S. Maitra, Highly nonlinear balanced Boolean functions with very good autocorrelation property, in: Workshop on Coding and Cryptography, Electronic Notes in Discrete Math., Elsevier, Amsterdam, 2001.

[5] S. Maitra, P. Sarkar, Modifications of Patterson–Wiedemann functions for cryptographic applications, IEEE Trans. Inform. Theory (2002), To appear.

[6] M. Matsui, Linear cryptanalysis method for DES cipher, in: Advances in Cryptology—EUROCRYPT'93, Lecture Notes in Comput. Sci., Vol. 765, Springer, Berlin, 1994, pp. 386–397.

[7] N.J. Patterson, D.H. Wiedemann, The covering radius of the $(2^{15}, 16)$ Reed–Muller code is at least 16,276, IEEE Trans. Inform. Theory IT-29 (3) (1983) 354–356.

[8] N.J. Patterson, D.H. Wiedemann, Correction to the covering radius of the $(2^{15}, 16)$ Reed–Muller code is at least 16,276, IEEE Trans. Inform. Theory IT-36 (2) (1990) 443.

[9] 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 Comput. Sci., Vol. 473, Springer, Berlin, 1991, pp. 161–173.

[10] O.S. Rothaus, On bent functions, J. Combin. Theory, Ser. A 20 (1976) 300–305.

[11] P. Sarkar, S. Maitra, Construction of nonlinear Boolean functions with important cryptographic properties, in: Advances in Cryptology—EUROCRYPT'00, Lecture Notes in Comput. Sci., Vol. 1807, Springer, Berlin, 2000, pp. 485–506.

[12] J.J. Son, J.I. Lim, S. Chee, S.H. Sung, Global avalanche characteristics and nonlinearity of balanced Boolean functions, Inform. Process. Lett. 65 (1998) 139–144.

[13] P. Stanica, S.H. Sung, Improving the nonlinearity of certain balanced Boolean functions with good local and global avalanche characteristics, Inform. Process. Lett. 79 (4) (2001) 167–172.

[14] P. Stanica, Nonlinearity, local and global avalanche characteristics of balanced Boolean functions, Discrete Mathematics 248 (2002) 181–193.

[15] S.H. Sung, S. Chee, C. Park, Global avalanche characteristics and propagation criterion of balanced Boolean functions, Inform. Process. Lett. 69 (1999) 21–24.

[16] A.F. Webster, S.E. Tavares, On the design of S-boxes, in: Advances in Cryptology—CRYPTO'85, Lecture Notes in Comput. Sci., Vol. 218, Springer, Berlin, 1986, pp. 523–534.

[17] X.M. Zhang, Y. Zheng, GAC—the criterion for global avalanche characteristics of cryptographic functions, J. Universal Comput. Sci. 1 (5) (1995) 316–333.