Construction of Balanced Boolean Functions with High Nonlinearity and Good Autocorrelation Properties

Deng Tang[1], Weiguo Zhang[2], and Xiaohu Tang[1]

Abstract

Boolean functions with high nonlinearity and good autocorrelation properties play an important role in the design of block ciphers and stream ciphers. In this paper, we give a method to construct balanced Boolean functions with n variables, where $n \geq 10$ is an even integer, satisfying strict avalanche criterion (SAC). Compared with the known balanced Boolean functions with SAC property, the constructed functions possess the highest nonlinearity and the best global avalanche characteristics (GAC) property.

Keywords: Boolean functions, nonlinearity, balancedness, strict avalanche criterion, global avalanche characteristics

1 Introduction

Boolean functions are the building blocks of symmetric cryptographic systems. They are used for S-box designing in block ciphers and utilized as nonlinear filters and combiners in stream ciphers. Generally speaking, cryptographic Boolean functions should satisfy various criteria simultaneously, mainly balancedness, high nonlinearity and good autocorrelation properties, to resist linear cryptanalysis and differential cryptanalysis particularly.

In 1985, Webster and Tavares introduced the concept of the strict avalanche criterion (SAC) when searching for principles for designing DES-like data encryption algorithms [2]. Since characterizing an important property that whenever a single input bit is complemented, each of the output bits changes with a probability of one half, immediately SAC turned out to be a widely accepted cryptographic criterion for Boolean functions. However in 1995, Zhang and Zheng pointed out that SAC is a measure for local avalanche and hence has some limitations [12]. So, they introduced the global avalanche characteristics (GAC), which including two indicators: the absolute indicator and the sum-of-squares indicator, to forecast the overall avalanche characteristics of a Boolean function [12].

[1] D. Tang and X.H. Tang are with the Provincial Key Lab of Information Coding and Transmission, Institute of Mobile Communications, Southwest Jiaotong University, Chengdu, 610031, China. Email: dengtanghome@qq.com, xhutang@ieee.org

[2] Weiguo Zhang is with the ISN Laboratory, Xidian University, Xi'an, 710071, China. Email: w.g.zhang@qq.com

Table 1. Comparison among balanced SAC Boolean functions

Constructions	n even	N_f	Δ_f	σ_f
Canteaut *et al.* [1]	$n \geq 8$	$2^{n-1} - 2^{n/2}$	2^n	2^{2n+2}
Stănică [9]	$n \geq 4$	2^{n-2}	2^n	2^{3n-2}
Stănică [9]	$n \geq 8$	$2^{n-1} - 2^{n/2}$	2^n	2^{2n+2}
Stănică and Sung [7]	$n \geq 8$	$2^{n-1} - 2^{n/2}$	$-$	2^{2n+2}
Maitra [11]	$n \geq 6$	$2^{n-1} - 2^{n/2-1} - 2^{n/2-2}$	2^{n-1}	$2^{2n+0.89}$
Stănică and Sung [8]	$n \geq 4$	$2^{n-1} - 2^{n/2}$	$-$	$2^{2n} + 6 \cdot 2^{3n/2}$
Ours (Theorem 2)	$n \geq 10$	$2^{n-1} - 2^{n/2-1} - 2^{\lceil n/4 \rceil}$	$2^{n/2} + 2^{\lceil n/4 \rceil + 1}$	$2^{2n} + 5 \cdot 2^{3n/2} + 2^{n+3}$

For even number of variables, the well-known bent functions possess possible highest nonlinearity and the best autocorrelation properties. Unfortunately, bent functions are not balanced and then are improper for direct use. Therefore, constructing the balanced Boolean function f with SAC property, which is called balanced SAC Boolean function in this paper for short, high nonlinearity N_f and very good GAC property (low absolute indicator Δ_f and low sum-of-squares indicator σ_f) is very desirable. Addressing this problem, many works have been done, for instance [1, 7, 9, 11, 8], which are summarized in Table 1.

In this paper we propose a method to construct balanced SAC Boolean functions on even number of variables with very good GAC property and high nonlinearity. Our construction is based on a modification of the Maiorana-McFarland (M-M) class bent functions [6]. As a result, we can obtain a large class of balanced SAC Boolean function f with $N_f = 2^{n-1} - 2^{n/2-1} - 2^{\lceil n/4 \rceil}$, $\Delta_f \leq 2^{n/2} + 2^{\lceil n/4 \rceil + 1}$, and $\sigma_f \leq 2^{2n} + 5 \cdot 2^{3n/2} + 2^{n+2}$ ($n = 0 \mod 4$) or $\sigma_f \leq 2^{2n} + 5 \cdot 2^{3n/2} + 2^{n+3}$ ($n = 2 \mod 4$), where $n \geq 10$ is an even integer. It is seen from Table 1 that our Boolean function is the better than all the known results with respect to all the three parameters.

The organization of this paper is as follows. In Section 2, the notations and the necessary preliminaries required for the subsequent sections are reviewed. In Section 3, our construction and main results are presented. The proof of the main results are given in Section 4. Finally, Section 5 concludes the paper.

2 Preliminaries

Let $\mathbb{F}_2 = \{0, 1\}$ and $\mathbb{F}_2^n$ be the vector space of n-tuples over $\mathbb{F}_2$. In this paper, some additions of bits will be considered in $\mathbb{Z}$ and denoted by $+$, and some will be computed over $\mathbb{F}_2$ (i.e., modulo 2) and denoted by $\oplus$. For simplicity, if there is no ambiguity, we shall use $+$ to denote the addition of vectors of $\mathbb{F}_2^n$.

Denote $\mathcal{B}_n$ the set of Boolean functions of n variables. A Boolean function with n variables is a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. The basic representation of a Boolean function $f(x_1, \cdots, x_n)$ is by its truth table, i.e.,

$$(f(0, \cdots, 0, 0), f(0, \cdots, 0, 1), f(0, \cdots, 1, 0), f(0, \cdots, 1, 1), \cdots, f(1, \cdots, 1, 1)).$$

Furthermore, any Boolean function $f \in \mathcal{B}_n$ can be uniquely represented by a multivariate polynomial over $\mathbb{F}_2$, called the algebraic normal form (ANF), of the form:

$$f(x_1, \cdots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} a_u \Big(\prod_{j=1}^{n} x_j^{u_j} \Big),$$

where $a_u \in \mathbb{F}_2$ and $u = (u_1, \cdots, u_n)$. The algebraic degree, denoted by $deg(f)$, is the maximal value of $w_H(u)$ such that $a_u \neq 0$, where the Hamming weight $w_H(u)$ of a binary vector $u \in \mathbb{F}_2^n$ is the number of its nonzero coordinates (i.e. the size of $\{1 \leq i \leq n \,|\, u_i \neq 0\}$). A Boolean function is said to be an affine function if its degree is at most 1. The set of all affine functions is denoted by A_n. To resist the Berlekamp-Massey attack [5], any Boolean function used in a cryptosystem should have high algebraic degree.

Another important cryptographic property for a Boolean function is nonlinearity. The nonlinearity N_f of a Boolean function $f \in \mathcal{B}_n$ is defined as

$$N_f = \min_{g \in A_n} (d_H(f, g)),$$

where $d_H(f, g)$ is the Hamming distance between f and g, i.e., $d_H(f, g) = |\{x \in \mathbb{F}_2^n \,|\, f(x) \neq g(x)\}|$. In other words, the nonlinearity N_f is the minimum Hamming distance between f and all the affine functions.

The nonlinearity can also be expressed by the Walsh transform of f. Let $x = (x_1, x_2, \cdots, x_n)$ and $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ both belong to $\mathbb{F}_2^n$ and $x \cdot \alpha = x_1\alpha_1 \oplus x_2\alpha_2 \oplus \cdots \oplus x_n\alpha_n$, then the Walsh transform of $f \in \mathcal{B}_n$ at α is defined by

$$W_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \alpha \cdot x}.$$

We say that $f \in \mathcal{B}_n$ is balanced if its Hamming weight equals 2^{n-1}, where the Hamming weight of a Boolean function $f \in \mathcal{B}_n$ (denoted by $w_H(f)$) is the size of its support $\{x \in \mathbb{F}_2^n \,|\, f(x) \neq 0\}$. Obviously, f is balanced if and only if $W_f(\mathbf{0}) = 0$. Then, by the Walsh transform the nonlinearity of a Boolean function $f \in \mathcal{B}_n$ can be computed as

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_2^n} |W_f(\alpha)|.$$

Any cryptographic Boolean function should have high nonlinearity for resisting the Best Affine Approximation (BAA) [4]. So, the value of $\max_{\alpha\in\mathbb{F}_2^n}|W_f(\alpha)|$ should be low. However, it is limited by the Parseval's equality, which states that the Walsh transform of a Boolean function $f\in\mathcal{B}_n$ satisfies

$$\sum_{\alpha\in\mathbb{F}_2^n} W_f^2(\alpha)=2^{2n}.$$

Consequently, $N_f\leq 2^{n-1}-2^{n/2-1}$ for any Boolean function $f\in\mathcal{B}_n$. The functions achieving this bound are called bent functions [6], which only exist for even n.

For reducing the likelihood between the outputs and the inputs of a Boolean functions, it is desirable for function to have low additive autocorrelation. The autocorrelation function of a Boolean function f at the shift α is defined by

$$C_f(\alpha)=\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+f(x+\alpha)}.$$

f is said to satisfy strict avalanche criterion (SAC) if

$$C_f(\alpha)=0,\ w_H(\alpha)=1.$$

Global avalanche characteristics (GAC) describes the overall avalanche characteristics of f, which are related to two indicators: the absolute indicator

$$\Delta_f=\max_{\alpha\neq\mathbf{0}}|C_f(\alpha)|$$

and the sum-of-squares indicator

$$\sigma_f=\sum_{\alpha\in\mathbb{F}_2^n}C_f^2(\alpha).$$

An important relation between σ_f and the Walsh transform as follows [3]

$$W_f^2(b)=\sum_{\alpha\in\mathbb{F}_2^n}C_f(\alpha)(-1)^{b\cdot\alpha}. \tag{1}$$

which results in

$$\sum_{\alpha\in\mathbb{F}_2^n}W_f^4(\alpha)=2^n\sigma_f. \tag{2}$$

3 Construction and Main results

This section presents a method for constructing balanced SAC Boolean functions with very good GAC and high nonlinearity properties.

For simplicity, denote $x' = (x_1, \cdots, x_{n/2-1})$ for a given vector $x = (x_1, \cdots, x_{n/2}) \in \mathbb{F}_2^{n/2}$ from now on.

Construction: Let $n \geq 4$ be an even number. Let $x = (x_1, \cdots, x_{n/2})$, and $y = (y_1, \cdots, y_{n/2})$. Let $S = \mathbb{F}_2^{n/2} \setminus \{\mathbf{0}, \mathbf{1}\}$ and $T = \mathbb{F}_2^{n/2} \setminus \{\mathbf{0}, \mathbf{1}\}$, where $\mathbf{0} = (0, \cdots, 0) \in \mathbb{F}_2^{n/2}$ and $\mathbf{1} = (1, \cdots, 1) \in \mathbb{F}_2^{n/2}$. Let ϕ be a bijective mapping from S to T satisfying $\phi(x) = \phi(x + \mathbf{1}) + \mathbf{1}$ when $w_H(x) = 1$.

Then we construct a cryptographic Boolean function $f \in \mathcal{B}_n$ as follows:

$$f(x, y) = \begin{cases} \phi(x) \cdot y, & \text{if } x \neq \mathbf{0} \text{ and } x \neq \mathbf{1} \\ g_0(y), & \text{if } x = \mathbf{0} \\ g_1(y), & \text{if } x = \mathbf{1} \end{cases} \tag{3}$$

where

$$g_0(y) = (\mathbf{1} \cdot y) \cdot h(y')$$

and

$$g_1(y) = g_0(y) + \mathbf{1} \cdot y + 1$$

in which $h(y')$ is an $(n/2-1)$-variable balanced Boolean function with nonlinearity as large as possible, i.e., $\max_{\alpha \in \mathbb{F}_2^{n/2-1}} |W_h(\alpha)| \leq 2^{\lceil \frac{n/2-1-1}{2} \rceil + 1} = 2^{\lceil n/4 \rceil}$ and $N_h \geq 2^{n/2-2} - 2^{\lceil n/4 \rceil - 1}$.

We have the following main results.

Theorem 1. *Let $n \geq 4$ be an even number. Let f be an n-variable Boolean function given by* (3). *Then the following statements hold:*

1) f is balanced;

2) $N_f \geq 2^{n-1} - 2^{n/2-1} - 2^{\lceil n/4 \rceil}$;

3) f satisfy SAC;

4) $\Delta_f \leq 2^{n/2+1}$;

5) $\sigma_f \leq \begin{cases} 2^{2n} + 5 \cdot 2^{3n/2} + 2^{n+3}, & \textit{if } n = 2 \pmod 4 \\ 2^{2n} + 5 \cdot 2^{3n/2} + 2^{n+2}, & \textit{if } n = 0 \pmod 4. \end{cases}$

Example 1. *Let $n = 12$. Let ϕ be a bijective mapping from $\mathbb{F}_2^6 \setminus \{\mathbf{0}, \mathbf{1}\}$ to $\mathbb{F}_2^6 \setminus \{\mathbf{0}, \mathbf{1}\}$ such that $\phi(x) = x$, where $x \in \mathbb{F}_2^6 \setminus \{\mathbf{0}, \mathbf{1}\}$. Choose $h = (1,1,1,1,0,1,0,1,1,1,0,0,1,0,0,1,0,0,0,0,1,$ $0,1,0,0,0,1,1,0,1,1,0)$, which has $\max_{\beta \in \mathbb{F}_2^5} |W_h(\beta)| = 2^{\lceil n/4 \rceil} = 8$ and $\Delta_h = 2^{n/2-1} = 32$. Then it is checked by program that the f given by* (3) *is a balanced Boolean function satisfy SAC, and f has the following parameters*

1) $N_f = 2008$*;*

2) $\Delta_f = 128$*;*

3) $\sigma_f = 18104320$*,*

which coincides with Theorem 1.

From the proof of Theorem 1 which will be given in next section, it is easy to see that the nonlinearity and GAC property of $f \in \mathcal{B}_n$ heavily rely on the nonlinearity and absolute indicator of the balanced function $h(y') \in \mathcal{B}_{n/2-1}$.

Therefore, firstly we can lower the the absolute indicator Δ_f by choosing some specific functions $h(y') \in \mathcal{B}_{n/2-1}$ with small absolute indicator Δ_h, for example the Boolean functions by Zhang and Zheng in [12].

Theorem 2. *Let* $n \geq 10$ *be an even number. Let* h *be an* $(n/2-1)$*-variable Boolean function given in [12] satisfying*

- $\max_{\alpha \in \mathbb{F}_2^{n/2-1}} |W_h(\alpha)| \leq 2^{n/4}$ *and* $\Delta_h \leq 2^{n/4}$ *for* $n = 0 \pmod 4$*, or*
- $\max_{\alpha \in \mathbb{F}_2^{n/2-1}} |W_h(\alpha)| \leq 2^{(n+2)/4}$ *and* $\Delta_h \leq 2^{(n+2)/4}$ *for* $n = 2 \pmod 4$

Then,

$$\Delta_f \leq 2^{n/2} + 2^{\lceil n/4 \rceil + 1}.$$

Example 2. *Let* $n = 12$*. Let* ϕ *be a bijective mapping from* $\mathbb{F}_2^6 \backslash \{\boldsymbol{0}, \boldsymbol{1}\}$ *to* $\mathbb{F}_2^6 \backslash \{\boldsymbol{0}, \boldsymbol{1}\}$ *such that* $\phi(x) = x$*, where* $x \in \mathbb{F}_2^6 \setminus \{\boldsymbol{0}, \boldsymbol{1}\}$*. Choose* h *as a* 5*-variable Boolean function given by (13) in [12], i.e.,* $h = (1,1,1,1,1,0,1,0,1,1,0,0,0,1,1,0,0,0,0,0,0,0,1,1,0,1,1,0,\ 0,1,0,1)$*, which has* $\max_{\beta \in \mathbb{F}_2^5} |W_h(\beta)| = \Delta_h = 2^{\lceil n/4 \rceil} = 8$*. Then verified by program,* f *constructed by* (3) *satisfies that*

1) $\Delta_f = 80$*;*

2) $\sigma_f = 18104320$*,*

which is consistent with Theorem 2. In contrast to the previous one in Example 1, this function f *has all the same properties but smaller absolute indicator* Δ_f*.*

Secondly for some specific cases, it is possible to improve the nonlinearity and lower GAC indicators of f simultaneously by taking the appropriate functions in [10]. For example, in [10] Maitra has constructed a balanced function $h \in \mathcal{B}_{15}$ with $N_h = 2^{14} - 2^7 + 6$ and $\Delta_h \leq 2^{(15+1)/2} - 16$. Based on it, we can construct a balanced SAC Boolean function $f \in \mathcal{B}_{32}$ with $N_f \geq 2^{31} - 2^{15} - 2^8 + 12$, $\Delta_f \leq 2^{16} + 2^9 - 32$ and $\sigma_f < 2^{64} + 5 \cdot 2^{48} + 2^{34}$, whereas by Theorem 2 $N_f \geq 2^{31} - 2^{15} - 2^8$, $\Delta_f \leq 2^{16} + 2^9$ and $\sigma_f \leq 2^{64} + 5 \cdot 2^{48} + 2^{34}$.

4 The Proof of Main results

In order to prove our main results, we need the following three useful lemmas.

Lemma 1. *Given $\beta \in \mathbb{F}_2^n$, then*

- *$\beta = \mathbf{0}$ or $\beta = \mathbf{1}$, then $W_{g_0}(\beta) = 2^{n/2-1}$.*
- *$\beta \neq \mathbf{0}$ and $\beta \neq \mathbf{1}$, then $|W_{g_0}(\beta)| \leq 2^{\lceil \frac{n}{4} \rceil}$.*

Proof: Let $\beta = (\beta_1, \cdots, \beta_{2^{n/2}})$. By definition, we have

$$\begin{aligned} W_{g_0(y)}(\beta) &= \sum_{y \in \mathbb{F}_2^{n/2}} (-1)^{g_0(y)+\beta\cdot y} \\ &= \sum_{\mathbf{1}\cdot y=1} (-1)^{h(y')+\beta'\cdot y'+\beta_{n/2}\cdot y_{n/2}} + \sum_{\mathbf{1}\cdot y=0} (-1)^{\beta'\cdot y'+\beta_{n/2}\cdot y_{n/2}} \\ &= \sum_{\mathbf{1}'\cdot y'=1, y_{n/2}=0} (-1)^{h(y')+\beta'\cdot y'} + \sum_{\mathbf{1}'\cdot y'=0, y_{n/2}=1} (-1)^{h(y')+\beta'\cdot y'+\beta_{n/2}} \\ &\quad + \sum_{\mathbf{1}'\cdot y'=0, y_{n/2}=0} (-1)^{\beta'\cdot y'} + \sum_{\mathbf{1}'\cdot y'=1, y_{n/2}=1} (-1)^{\beta'\cdot y'+\beta_{n/2}} \end{aligned}$$

When $\beta_{n/2} = 0$, it becomes

$$\begin{aligned} W_{g_0(y)}(\beta) &= \sum_{y' \in \mathbb{F}_2^{n/2-1}} (-1)^{h(y')+\beta'\cdot y'} + \sum_{y' \in \mathbb{F}_2^{n/2-1}} (-1)^{\beta'\cdot y'} \\ &= \begin{cases} W_h(\beta'), & \text{if } \beta \neq \mathbf{0} \\ 2^{n/2-1} + W_h(\mathbf{0}), & \text{if } \beta = \mathbf{0}. \end{cases} \end{aligned}$$

When $\beta_{n/2} = 1$, set $\gamma' = \beta' + \mathbf{1}'$. It gives

$$\begin{aligned} W_{g_0(y)}(\beta) &= -\sum_{y' \in \mathbb{F}_2^{n/2-1}} (-1)^{h(y')+\gamma'\cdot y'} + \sum_{y' \in \mathbb{F}_2^{n/2-1}} (-1)^{\gamma'\cdot y'} \\ &= \begin{cases} -W_h(\beta' + \mathbf{1}'), & \text{if } \beta \neq \mathbf{1} \\ 2^{n/2-1} - W_h(\mathbf{0}), & \text{if } \beta = \mathbf{1}. \end{cases} \end{aligned}$$

Recall that h is balanced, i.e., $W_h(0) = 0$, and $\max_{\beta \in \mathbb{F}_2^{n/2-1}} |W_h(\beta)| \leq 2^{\lceil n/4 \rceil}$, we finish the proof.

□

Lemma 2. *Let $s(x')$ be an $(n/2-1)$-variable Boolean function. Then,*

$$\sum_{\mathbf{1}\cdot x=c} (-1)^{s(x')} = \sum_{y' \in \mathbb{F}_2^{n/2-1}} (-1)^{s(x')}$$

where $c = 0$ or $c = 1$ is a constant.

***Proof*:** Without loss of generality, assume that $c = 0$. Then, the equation can be rewritten as

$$\sum_{\mathbf{1}\cdot x=c}(-1)^{s(x')} \quad = \sum_{\mathbf{1}'\cdot x'=0,x_{n/2=0}}(-1)^{s(x')} + \sum_{\mathbf{1}'\cdot x'=1,x_{n/2=1}}(-1)^{s(x')},$$

which leads to the conclusion.

□

Lemma 3. *Define*

$$\Gamma = \sum_{\boldsymbol{1}\cdot b=0}\Big(\big(\sum_{\boldsymbol{1}\cdot y=0}(-1)^{g_0(y)+g_0(y+b)}\big)^2 + \big(\sum_{\boldsymbol{1}\cdot y=1}(-1)^{g_0(y)+g_0(y+b)}\big)^2\Big),$$

then

$$\Gamma \leq \begin{cases} 2^{3n/2-3}+2^n, & \text{if } n = 2 \pmod 4\\ 2^{3n/2-3}+2^{n-1}, & \text{if } n = 0 \pmod 4). \end{cases}$$

***Proof*:** From the construction of the function g_0 over $\mathbb{F}_2^{n/2}$, we get

$$\begin{aligned}
\Gamma &= \sum_{\mathbf{1}\cdot b=\mathbf{0}}\Big(\big(\sum_{\mathbf{1}\cdot y=0}(-1)^{(\mathbf{1}\cdot y)\cdot h(y')+(\mathbf{1}\cdot(y+b))\cdot h(y'+b')}\big)^2 + \big(\sum_{\mathbf{1}\cdot y=1}(-1)^{(\mathbf{1}\cdot y)\cdot h(y')+(\mathbf{1}\cdot(y+b))\cdot h(y'+b')}\big)^2\Big)\\
&= 2^{3n/2-3} + \sum_{\mathbf{1}\cdot b=0}\big(\sum_{\mathbf{1}\cdot y=1}(-1)^{h(y')+h(y'+b')}\big)^2\\
&= 2^{3n/2-3} + \sum_{b'\in\mathbb{F}_2^{n/2-1}}\big(\sum_{y'\in\mathbb{F}_2^{n/2-1}}(-1)^{h(y')+h(y'+b')}\big)^2\\
&= 2^{3n/2-3} + \sum_{b'\in\mathbb{F}_2^{n/2-1}} C_h^2(b')
\end{aligned}$$

where we use Lemma 2 twice in the third identity.

According to the equations $\sum_{\alpha\in\mathbb{F}_2^{n/2-1}} W_h^4(\alpha) = 2^{n/2-1}\cdot\sum_{\beta\in\mathbb{F}_2^{n/2-1}} C_h^2(\beta)$ by (2) and $\sum_{\alpha\in\mathbb{F}_2^{n/2-1}} W_h^2(\alpha) = 2^{n-2}$ by Parseval's equality, we can easily deduce that

$$\begin{aligned}
\sum_{\beta\in\mathbb{F}_2^{n/2-1}} C_h^2(\beta) &\leq 2^{n/2-1}\cdot\max_{\alpha\in\mathbb{F}_2^{n/2-1}} W_h^2(\alpha)\\
&\leq \begin{cases} 2^n, & \text{if } n = 2 \pmod 4\\ 2^{n-1}, & \text{if } n = 0 \pmod 4). \end{cases}
\end{aligned}$$

This completes the proof.

□

Now, we are able to to prove Theorem 1.

***Proof of Theorem 1*:** 1) and 2). For $\alpha \in \mathbb{F}_2^{n/2}$ and $\beta \in \mathbb{F}_2^{n/2}$, we have

$$\begin{aligned} W_f(\alpha,\beta) &= \sum_{x\in S, y\in\mathbb{F}_2^n} (-1)^{\phi(x)\cdot y+\alpha\cdot x+\beta\cdot y} + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+\beta\cdot y} + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_1(y)+\mathbf{1}\cdot\alpha+\beta\cdot y} \\ &= \sum_{x\in S}(-1)^{\alpha\cdot x} \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{(\phi(x)+\beta)\cdot y} + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+\beta\cdot y} + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+\beta\cdot y+\mathbf{1}\cdot y+\mathbf{1}\cdot\alpha+1} \\ &= \begin{cases} (-1)^{\phi^{-1}(\beta)\cdot\alpha}\cdot 2^{n/2} + W_{g_0}(\beta) - (-1)^{\mathbf{1}\cdot\alpha} W_{g_0}(\beta+\mathbf{1}), & \text{if } \beta \neq \mathbf{0} \text{ and } \beta\neq\mathbf{1} \\ W_{g_0}(\mathbf{0}) - (-1)^{\mathbf{1}\cdot\alpha} W_{g_0}(\mathbf{1}), & \text{if } \beta = \mathbf{0} \\ W_{g_0}(\mathbf{1}) - (-1)^{\mathbf{1}\cdot\alpha} W_{g_0}(\mathbf{0}), & \text{if } \beta = \mathbf{1}. \end{cases} \end{aligned}$$

Hence, $W_f(0,0) = 0$ and $|W_f(\alpha,\beta)| \leq 2^{n/2} + 2^{\lceil\frac{n}{4}\rceil+1}$. The assertions of 1) and 2) then follow.

3). Notice that

$$C_f(a,b) \;=\; \sum_{x,y\in\mathbb{F}_2^{n/2}} (-1)^{f(x,y)+f(x+a,y+b)}$$

which can be classified into four cases:

- $a = \mathbf{0}$ and $b = \mathbf{0}$. Obviously $C_f(a,b) = 2^n$.

- $a = \mathbf{0}$ and $b \neq \mathbf{0}$.

$$\begin{aligned} & C_f(a,b) \\ =\; & \sum_{x\in S, y\in\mathbb{F}_2^{n/2}} (-1)^{\phi(x)\cdot b} + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+g_0(y+b)} + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_1(y)+g_1(y+b)} \\ =\; & 2^{n/2}\sum_{x\in S}(-1)^{\phi(x)\cdot b} + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+g_0(y+b)} + (-1)^{\mathbf{1}\cdot b} \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+g_0(y+b)} \\ =\; & 2^{n/2}(\sum_{z\in\mathbb{F}_2^{n/2}} (-1)^{z\cdot b} - (-1)^{\mathbf{0}\cdot b} - (-1)^{\mathbf{1}\cdot b}) + (1+(-1)^{\mathbf{1}\cdot b})C_{g_0}(b) \\ =\; & -2^{n/2}(1+(-1)^{\mathbf{1}\cdot b}) + C_{g_0}(b)(1+(-1)^{\mathbf{1}\cdot b}) \\ =\; & \begin{cases} 0, & \text{if } \mathbf{1}\cdot b = 1 \\ -2^{n/2+1} + 2C_{g_0}(b), & \text{if } \mathbf{1}\cdot b = 0 \text{ and } b \neq \mathbf{0}, \end{cases} \end{aligned} \tag{4}$$

where the substitution $z = \phi(x)$ is used in the third identity.

- $a = \mathbf{1}$.

$$\begin{aligned}
& C_f(a,b) \\
= \ & \sum_{x\in S}(-1)^{\phi(x+\mathbf{1})\cdot b} \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{(\phi(x)+\phi(x+\mathbf{1}))\cdot y} + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+g_1(y+b)} + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_1(y)+g_0(y+b)} \\
= \ & \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+g_0(y+b)+\mathbf{1}\cdot(y+b)+1} + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+g_0(y+b)+\mathbf{1}\cdot y+1} \\
= \ & \begin{cases} 0, & \text{if } b = \mathbf{0} \\ 0, & \text{if } \mathbf{1}\cdot b = 1 \\ -2 \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+g_0(y+b)+\mathbf{1}\cdot y}, & \text{if } \mathbf{1}\cdot b = 0 \text{ and } b \neq \mathbf{0}. \end{cases}
\end{aligned}$$

- $a \neq \mathbf{0}$ and $a \neq \mathbf{1}$.

$$\begin{aligned}
& C_f(a,b) \\
= \ & \sum_{x\in S\setminus\{a,a+\mathbf{1}\},y\in\mathbb{F}_2^{n/2}} (-1)^{f(x,y)+f(x+a,y+b)} \\
& + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{f(a,y)+f(\mathbf{0},y+b)} + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{f(a+\mathbf{1},y)+f(\mathbf{1},y+b)} \\
& + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{f(\mathbf{0},y)+f(a,y+b)} + \sum_{,y\in\mathbb{F}_2^{n/2}} (-1)^{f(\mathbf{1},y)+f(a+\mathbf{1},y+b)} \\
= \ & \sum_{x\in S\setminus\{a,1+a\}} (-1)^{\phi(x+a)\cdot b} \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{(\phi(x)+\phi(x+a))\cdot y} \\
& + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{\phi(a)\cdot y+g_0(y+b)} + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{\phi(a+\mathbf{1})\cdot y+g_1(y+b)} \\
& + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+\phi(a)\cdot(y+b)} + \sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_1(y)+\phi(a+\mathbf{1})\cdot(y+b)} \\
= \ & 2\cdot(-1)^{\phi(a)\cdot b}\cdot W_{g_0}(\phi(a)) + 2\cdot(-1)^{\phi(a+\mathbf{1})\cdot b}\cdot W_{g_1}(\phi(a+\mathbf{1})) \\
= \ & 2\cdot(-1)^{\phi(a)\cdot b}\cdot W_{g_0}(\phi(a)) - 2\cdot(-1)^{\phi(a+\mathbf{1})\cdot b}\cdot W_{g_0}(\phi(a+\mathbf{1})+\mathbf{1}) \qquad (5)
\end{aligned}$$

where we make use of the fact that

$$W_{g_1}(\phi(a+\mathbf{1})) = -W_{g_0}(\phi(a+\mathbf{1})+\mathbf{1})$$

since $g_1(y) = g_0(y) + \mathbf{1}\cdot y + 1$.

If $w_H(a,b) = 1$, there are two subcases ($a = \mathbf{0}$ and $w_H(b) = 1$) or ($w_H(a) = 1$ and $b = \mathbf{0}$). For the former, it follows from (4) that $C_f(a,b) = 0$. Regarding the later, we see $C_f(a,b) = 0$ from (5) where $\phi(a) = \phi(a+1)+1$ for $w_H(a) = 1$. Therefore, f satisfies SAC.

4) We prove that $\Delta_f = \max_{a\neq\mathbf{0} \text{ or } b\neq\mathbf{0}} |C_f(a,b)| \leq 2^{n/2+1}$ by further investigating the following three subcases in above cases.

- $a=\mathbf{0}$, $\mathbf{1}\cdot b=0$, and $b\neq\mathbf{0}$. we have

$$\begin{aligned} C_f(a,b) &= -2^{n/2+1}+2\sum_{y\in\mathbb{F}_2^{n/2}}(-1)^{g_0(y)+g_0(y+b)} \\ &= -2^{n/2+1}+2\Big(\sum_{\mathbf{1}\cdot y=0}(-1)^{(\mathbf{1}\cdot y)\cdot h(y')+(\mathbf{1}\cdot(y+b))\cdot h(y'+b')} \\ &\quad +\sum_{\mathbf{1}\cdot y=1}(-1)^{(\mathbf{1}\cdot y)\cdot h(y')+(\mathbf{1}\cdot(y+b))\cdot h(y'+b')}\Big) \\ &= -2^{n/2+1}+2\cdot 2^{n/2-1}+2\sum_{y'\in\mathbb{F}_2^{n/2-1}}(-1)^{h(y')+h(y'+b')} \\ &= -2^{n/2}+2\sum_{y'\in\mathbb{F}_2^{n/2-1}}(-1)^{h(y')+h(y'+b')} \qquad (6) \end{aligned}$$

  where the last identity follow from Lemma 2.

  Substituting the trivial bound that $\Delta_h \leq 2^{n/2-1}$ into (6), we get

$$|C_f(a,b)| \leq 2^{n/2+1}.$$

- $a=\mathbf{1}$, $\mathbf{1}\cdot b=0$, and $b\neq\mathbf{0}$. Similarly, we have

$$|C_f(a,b)| \leq 2^{n/2+1}.$$

- $a\neq\mathbf{0}$ and $a\neq\mathbf{1}$. Hence by Lemma 1,

$$|C_f(a,b)| \leq 4\max_{a\neq\mathbf{0} \text{ and } a\neq\mathbf{1}}(|W_{g_0}(\phi(a))|, |W_{g_0}(\phi(a+\mathbf{1})+\mathbf{1})|)$$

  which is $\leq 4\cdot 2^{\lceil n/4\rceil} = 2^{\lceil n/4\rceil+2}$.

5) Summing all the nonzero value $C_f^2(a,b)$, we have

$$\begin{aligned} \sigma_f &= 2^{2n}+4\sum_{a\in\mathbb{F}_2^{n/2}\backslash\{\mathbf{0},\mathbf{1}\},b\in\mathbb{F}_2^{n/2}}\big((-1)^{\phi(a)\cdot b}W_{g_0}(\phi(a))-(-1)^{\phi(a+\mathbf{1})\cdot b}W_{g_0}(\phi(a+\mathbf{1})+\mathbf{1})\big)^2 \\ &\quad +4\sum_{a=\mathbf{0},b\neq\mathbf{0},\mathbf{1}\cdot b=\mathbf{0}}(-2^{n/2}+C_{g_0}(b))^2+4\sum_{a=\mathbf{1},b\neq\mathbf{0},\mathbf{1}\cdot b=\mathbf{0}}(\sum_{y\in\mathbb{F}_2^{n/2}}(-1)^{g_0(y)+g_0(y+b)+\mathbf{1}\cdot y+1})^2 \\ &= 2^{2n}+4S+4U \qquad (7) \end{aligned}$$

where

$$S=\sum_{a\in\mathbb{F}_2^{n/2}\backslash\{\mathbf{0},\mathbf{1}\},b\in\mathbb{F}_2^{n/2}}\big((-1)^{\phi(a)\cdot b}W_{g_0}(\phi(a))-(-1)^{\phi(a+\mathbf{1})\cdot b}W_{g_0}(\phi(a+\mathbf{1})+1)\big)^2$$

and

$$U \quad = \quad \sum_{\mathbf{1}\cdot b=\mathbf{0}, b\neq\mathbf{0}} (-2^{n/2} + C_{g_0}(b))^2 + \sum_{\mathbf{1}\cdot b=\mathbf{0}, b\neq\mathbf{0}} (\sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+g_0(y+b)+\mathbf{1}\cdot y+1})^2.$$

In what follows, we calculate S and U respectively.

Firstly,

$$\begin{aligned}
S \quad = \quad & \sum_{a\in\mathbb{F}_2^{n/2}\setminus\{\mathbf{0},\mathbf{1}\}} \sum_{b\in\mathbb{F}_2^{n/2}} \big(W_{g_0}^2(\phi(a)) + W_{g_0}^2(\phi(a+\mathbf{1})+1) \\
& -2 \sum_{a\in\mathbb{F}_2^{n/2}\setminus\{\mathbf{0},\mathbf{1}\}} \sum_{b\in\mathbb{F}_2^{n/2}} (-1)^{(\phi(a)+\phi(a+\mathbf{1}))\cdot b} W_{g_0}(\phi(a)) \cdot W_{g_0}(\phi(a+\mathbf{1})+\mathbf{1})\big) \\
= \quad & 2^{n/2} \cdot \sum_{a\in\mathbb{F}_2^{n/2}\setminus\{\mathbf{0},\mathbf{1}\}} \big(W_{g_0}^2(\phi(a)) + W_{g_0}^2(\phi(a+\mathbf{1})+\mathbf{1})\big) \\
& -2 \sum_{a\in\mathbb{F}_2^{n/2}\setminus\{\mathbf{0},\mathbf{1}\}} W_{g_0}(\phi(a)) \cdot W_{g_0}(\phi(a+\mathbf{1})+\mathbf{1}) \sum_{b\in\mathbb{F}_2^{n/2}} (-1)^{(\phi(a)+\phi(a+\mathbf{1}))\cdot b} \\
= \quad & 2^{n/2} \cdot \Big(\sum_{c\in\mathbb{F}_2^{n/2}} W_{g_0}^2(c) + \sum_{d\in\mathbb{F}_2^{n/2}} W_{g_0}^2(d) - 2W_{g_0}^2(\mathbf{0}) - 2W_{g_0}^2(\mathbf{1})\Big) + 0 \\
= \quad & 2^{n/2} \cdot \big(2^n + 2^n - 2W_{g_0}^2(\mathbf{0}) - 2W_{g_0}^2(\mathbf{1}))\big) \\
= \quad & 2^{n/2} \cdot \big(2^n + 2^n - 4 \cdot (2^{n/2-1})^2\big) \\
= \quad & 2^{3n/2} \qquad (8)
\end{aligned}$$

where we set two permutations $c = \phi(a)$ and $d = \phi(a+\mathbf{1})+\mathbf{1}$ in the third identity and use the Parseval's equality $\sum_{c\in\mathbb{F}_2^{n/2}} W_{g_0}^2(c) = \sum_{d\in\mathbb{F}_2^{n/2}} W_{g_0}^2(d) = 2^n$ in the fourth identity.

Next,

$$\begin{aligned}
U \quad = \quad & 2^n \cdot (2^{n/2-1} - 1) + \sum_{\mathbf{1}\cdot b=\mathbf{0}, b\neq\mathbf{0}} C_{g_0}^2(b) - 2^{n/2+1} \sum_{\mathbf{1}\cdot b=\mathbf{0}, b\neq\mathbf{0}} C_{g_0}(b) \\
& + \sum_{\mathbf{1}\cdot b=\mathbf{0}, b\neq\mathbf{0}} (\sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+g_0(y+b)+\mathbf{1}\cdot y+1})^2 \qquad (9) \\
= \quad & 2^{3n/2-1} - 2^n + U_1 - 2^{n/2+1} U_2
\end{aligned}$$

where

$$\begin{aligned}
U_1 &= \sum_{\mathbf{1}\cdot b=\mathbf{0},b\neq\mathbf{0}} C_{g_0}^2(b) + \sum_{\mathbf{1}\cdot b=\mathbf{0},b\neq\mathbf{0}} (\sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+g_0(y+b)+\mathbf{1}\cdot y+1})^2 \\
&= \sum_{\mathbf{1}\cdot b=\mathbf{0}} \Big((\sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+g_0(y+b)})^2 + (\sum_{y\in\mathbb{F}_2^{n/2}} (-1)^{g_0(y)+g_0(y+b)+\mathbf{1}\cdot y+1})^2 \Big) - 2^n \\
&= \sum_{\mathbf{1}\cdot b=\mathbf{0}} \Big(\big(\sum_{\mathbf{1}\cdot y=0} (-1)^{g_0(y)+g_0(y+b)} + \sum_{\mathbf{1}\cdot y=\mathbf{1}} (-1)^{g_0(y)+g_0(y+b)} \big)^2 \\
&\quad + \big(\sum_{\mathbf{1}\cdot y=\mathbf{1}} (-1)^{g_0(y)+g_0(y+b)} - \sum_{\mathbf{1}\cdot y=\mathbf{0}} (-1)^{g_0(y)+g_0(y+b)} \big)^2 \Big) - 2^n \\
&= \sum_{\mathbf{1}\cdot b=\mathbf{0}} \Big(2\big(\sum_{\mathbf{1}\cdot y=\mathbf{0}} (-1)^{g_0(y)+g_0(y+b)} \big)^2 + 2\big(\sum_{\mathbf{1}\cdot y=\mathbf{1}} (-1)^{g_0(y)+g_0(y+b)} \big)^2 \Big) - 2^n \qquad (10)
\end{aligned}$$

which is $\leq 2^{3n/2-2} + 2^n$ for $n = 2 \pmod 4$ and $\leq 2^{3n/2-2}$ for $n = 0 \pmod 4$ by Lemma 3, and

$$U_2 = \sum_{\mathbf{1}\cdot b=\mathbf{0},b\neq\mathbf{0}} C_{g_0}(b) = \sum_{\mathbf{1}\cdot b=\mathbf{0}} C_{g_0}(b) - 2^{n/2}.$$

Note that from (1) we have

$$\sum_{\mathbf{1}\cdot b=\mathbf{0}} C_{g_0}(b) - \sum_{\mathbf{1}\cdot b=\mathbf{1}} C_{g_0}(b) = \sum_{b\in\mathbb{F}_2^{n/2}} C_{g_0}(b)(-1)^{\mathbf{1}\cdot b} = W_{g_0}^2(\mathbf{1}) = 2^{n-2}$$

and

$$\sum_{\mathbf{1}\cdot b=\mathbf{0}} C_{g_0}(b) + \sum_{\mathbf{1}\cdot b=\mathbf{1}} C_{g_0}(b) = \sum_{b\in\mathbb{F}_2^{n/2}} C_{g_0}(b)(-1)^{\mathbf{0}\cdot b} = W_{g_0}^2(\mathbf{0}) = 2^{n-2}.$$

Then, we have

$$\sum_{\mathbf{1}\cdot b=\mathbf{0}} C_{g_0}(b) = 2^{n-2}$$

which leads to

$$U_2 = 2^{n-2} - 2^{n/2}. \qquad (11)$$

Combining (9)-(11), we have

$$\begin{aligned}
U &= 2^{3n/2-1} - 2^n + U_1 - 2^{n/2+1} U_2 \\
&\leq \begin{cases} 2^{3n/2-2} + 2^{n+1}, & \text{if } n = 2 \pmod 4 \\ 2^{3n/2-2} + 2^n, & \text{if } n = 0 \pmod 4). \end{cases}
\end{aligned}$$

Associated with (7) and (8), it results in the assertion 5).

□

5 Conclusion

In this paper, we describe a method for constructing balanced SAC Boolean functions on even number of variables with very good GAC property and high nonlinearity. As a consequence, we obtain a large class of balanced SAC Boolean functions which provide currently best known GAC property.

References

[1] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "Propagation characteristics and correlation immunity of highly nonlineaar Boolean functions," in *Advances in Cryptology - EUROCRYPTO'00 (Lecture Notes in Computer Sceince).* Berlin, Germany: Springer-Verlag, 2000, vol. 1807, pp. 507-522.

[2] A. F. Webster and S. E. Tavares, "On the design of S-box," in A*dvances in Cryptology - CRYPTO'85 (Lecture Notes in Computer Sceince).* Berlin, Germany: Springer-Verlag, 1986, vol. 218, pp. 523-524.

[3] C. Carlet, "Partially-bent functions," *Des., Codes Cryptogr.*, no. 3, pp. 135-145, 1993.

[4] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers (Lecture Notes in Computer Science).* Berlin, Germany: Springer-Verlag, 1991, vol. 561.

[5] Massey, J. L. "Shift-register analysis and BCH decoding," *IEEE Trans. Inf. Theory*, vol. 15, pp. 122-127, 1969.

[6] O. S. Rothaus, "On bent functions," *J. Comb. Theory*, Ser. A, vol. 20, pp. 300-305, 1976.

[7] P. Stănică, S. H. Sung, "Improving the nonlinearity of certain balanced Boolean functions with good local and global avalanche characteristics," *Inf. Process. Lett.*, vol. 79, pp. 167-172, 2001.

[8] P. Stănică, S. H. Sung, "Boolean functions with five controllable cryptographic properties," *Des., Codes Cryptogr.*, vol. 31, no. 2, pp. 147-157, 2004.

[9] P. Stănică, "Nonlinearity, local and global avalanche characteristics of balanced Boolean functions," *Discr. Math.*, vol. 248, pp. 181-193, 2002.

[10] S. Maitra, "Highly nonlinear balanced Boolean functions with very good autocorrelation property," in *Proc. Workshop on Coding and Cryptography - WCC 2001.* Amsterdam, The Netherlands: Elsevier, 2001, vol. 6, Electronic Notes in Discrete Mathematics.

[11] S. Maitra, "Highly nonlinear balanced Boolean funcitons with good local and global avalanche characteristics," *Inf. Process. Lett.*, vol. 83, pp. 281-286, 2002.

[12] X.M. Zhang and Y. Zheng, "GAC-the criterion for global avalanche characteristics of cryptographic fnctions," *J. Universal Comput. Sci.*, vol. 1, no. 5, pp. 320-337, 1995.