Boolean Functions with Five Controllable Cryptographic Properties

Pantelimon Stănică*[a], Soo Hak Sung[b]

[a] Auburn University Montgomery, Department of Mathematics
Montgomery, AL 36124-4023, USA, e-mail: stanica@strudel.aum.edu
[b] Department of Applied Mathematics, Pai Chai University
Taejon 302-735, South Korea, e-mail: sungsh@mail.pcu.ac.kr

Corresponding author:

Soo Hak Sung
Department of Applied Mathematics
Pai Chai University
Doma-2-Dong, Seo-Gu
Taejon 302-735
South Korea

E-mail: sungsh@mail.pcu.ac.kr
Tel: 82-42-520-5369
Fax: 82-42-520-5365

[*] Also Associated to the *Institute of Mathematics of Romanian Academy*, Bucharest-Romania

Boolean Functions with Five Controllable Cryptographic Properties

Abstract

The Strict Avalanche Criterion (SAC) was introduced by Webster and Tavares in a study of cryptographic design criteria. This is an indicator for local property. In order to improve the global analysis of cryptographically strong functions, Zhang and Zheng introduced the global avalanche characteristics (GAC). The sum-of-squares indicator related to the GAC is defined as $\sigma_f = \sum_v \Delta_f^2(v)$, where $\Delta_f(v) = \sum_x (-1)^{f(x)\oplus f(x\oplus v)}$. In this paper, we give a few methods to construct Boolean functions controlling five good cryptographic properties, namely balancedness, good local and global avalanche characteristics, high nonlinearity and high algebraic degree. We improve upon the results of Stănică, and Zhang and Zheng.

Keywords: Cryptography, Nonlinearity, Boolean functions, Strict Avalanche Criterion, Global Avalanche Characteristics

1 Introduction

Boolean functions, components of S-boxes which are employed in block ciphers, must satisfy one or more properties to resist cryptanalytic attacks. In this paper, we construct functions with will satisfy five of these properties: balancedness, local and global avalanche characteristics, high nonlinearity and high algebraic degree. The *Strict Avalanche Criterion* (*SAC*) was introduced by Webster and Tavares [10] in a study of design criteria for certain cryptographic functions. A Boolean function is said to satisfy the SAC if complementing a single bit results in changing the output bit with probability exactly one half. In [2], Preneel et al. introduced the propagation criterion of degree k (PC of degree k or PC(k)), which generalizes the SAC. A function satisfies the PC(k) if by complementing at most k bits the output changes with probability exactly one half. Obviously PC(1) is equivalent to the SAC property. For a function f on $V_n = Z_2^n$, we see that f satisfies the PC(k) if and only if $\sum\limits_{x \in V_n} f(x) \oplus f(x \oplus v) = 2^{n-1}$ for all vectors v with Hamming weight $1 \leq wt(v) \leq k$, or equivalently, $\Delta_f(v) = 0$, where $\Delta_f(v) = \sum\limits_{x \in V_n} (-1)^{f(x) \oplus f(x \oplus v)}$ is the *autocorrelation function*.

Although, the PC is a very important concept in designing the encryption algorithms and one-way hash functions, it is a measure for local avalanche and hence has various limitations in capturing properties of vital importance to cryptographic algorithms. Zhang and Zheng [11] introduced the global avalanche characteristics (GAC) to forecast the overall avalanche characteristics of a cryptographic function. They proposed two indicators related to GAC: the *sum-of-squares indicator*

$$\sigma_f = \sum_{\alpha} \Delta_f^2(\alpha),$$

and the *absolute indicator*

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

The smaller σ_f and Δ_f, the better the GAC of a function. Obviously, $2^{2n} \leq \sigma_f \leq 2^{3n}$ and $0 \leq \Delta_f \leq 2^n$. The upper bound for σ_f holds if and only if f is affine and the lower bound holds if and only if f is bent function. Son et al. [7] proved $\sigma_f \geq 2^{2n} + 2^{n+3}$, when f is a balanced Boolean function, and Sung et al. [9] improved the lower bound by considering the number of vectors satisfying the PC. Recently, Stănică [8] proposed constructions of balanced Boolean functions satisfying the SAC with good local and global avalanche characteristics. In this paper, we improve his results. In particular, the sum-of-squares indicator is improved significantly, being very close to that of bent functions. In addition to improving the global indicator, our functions have also high algebraic degree, while maintaining high nonlinearity and good avalanche characteristics.

2 Definitions

Let $a = (a_1, \cdots, a_n)$ and $b = (b_1, \cdots, b_n)$ be two elements in V_n. The scalar product of a and b, is defined as $a \cdot b = a_1 b_1 \oplus \cdots \oplus a_n b_n$. We will use the following definitions and results throughout the paper.

1. An *affine* Boolean function is of the form $f(x) = \oplus_{i=1}^{n} a_i x_i \oplus b$. f is *linear* if $b = 0$.

2. The *Hamming weight*, $wt(v)$, is defined as the number of ones in $v \in V_n$. f is *balanced* if $wt(f) = 2^{n-1}$. The *Hamming distance* between $f, g : V_n \rightarrow V_1$ is $d(f, g) = wt(f \oplus g)$.

3. The *Walsh-Hadamard* transform of a real-valued function f on V_n is the function $\mathcal{F}_f : V_n \rightarrow R$ defined as $\mathcal{F}_f(w) = \sum_{x \in V_n} f(x)(-1)^{w \cdot x}$.

4. The *nonlinearity* of a function f is defined as $N_f = \min_{l \in A_n} d(f, l)$, where A_n is the class of all affine functions on V_n. Equivalently, $N_f = 2^{n-1} - \frac{1}{2} \max_{w \in V_n} |\mathcal{F}_{\hat{f}}(w)|$ (see Meier and Staffelbach [1]), where $\hat{f}$ means $(-1)^f$.

5. A function f satisfies the *propagation criterion (PC)* with respect to $v \in V_n$ if $f(x) \oplus f(x \oplus v)$ is balanced, or equivalently $\Delta_f(v) = 0$.

6. A Boolean function is called *perfect nonlinear* if it satisfies the PC with respect to all non-zero vectors. A Boolean function f is called *bent* if $\mathcal{F}_{\hat{f}}(v) = \pm 2^{n/2}$ for all vectors v. Hence, bent function exists only for n even, and it is not balanced. Note that these two definitions are equivalent. For further results on bent function, see Rothaus [3].

7. The *sum-of-squares indicator* σ_f is equal to $\dfrac{1}{2^n} \displaystyle\sum_{w \in V_n} \mathcal{F}^4_{\hat{f}}(w)$ (see Zhang and Zheng [11]).

3 Constructions of Good Cryptographic Boolean Functions

We give three methods (by using bent functions), for constructing balanced Boolean functions, which satisfy the SAC, have good GAC, high nonlinearity and high algebraic degree.

3.1 Boolean Functions On V_{2k}

To construct a good cryptographic Boolean function on V_{2k}, we need the following lemmas. The proof of Lemma 1 is easy and is omitted.

Lemma 1. *Let g be a Boolean function on V_n defined as $g(x) = g(x_1, \cdots, x_n) = x_1 \oplus x_2 \oplus x_1x_2 \oplus 1$. Then $\mathcal{F}_{\hat{g}}(0) = 2^{n-1}$, $\mathcal{F}_{\hat{g}}(a) = -2^{n-1}$, if $a = \epsilon_1, \epsilon_2, \epsilon_1 + \epsilon_2$, and $\mathcal{F}_{\hat{g}}(a) = 0$, otherwise, where $\epsilon_i = (\overbrace{0, \cdots, 0, 1}^{i}, 0, \cdots, 0)$.*

A function constructed as in the following well-known lemma (see Rothaus [3]) is called a Maiorana-McFarland bent function.

Lemma 2. *Let $n = 2k$. Define a Boolean function $f : V_n \to V_1$ as $f(y,x) = \phi(y) \cdot x$, where $y, x \in V_k$, and ϕ is a permutation of V_k. Then $\mathcal{F}_{\hat{f}}(b,a) = 2^k(-1)^{b\cdot\phi^{-1}(a)}$. In particular, f is a bent function.*

We now construct a balanced function on V_{2k} with many good cryptographic properties, by using a bent function and the function g (on V_k) of Lemma 1.

Construction 1. *Let $n = 2k$. Let h be a Boolean function on V_n defined as $h(y,x) = \phi(y) \cdot x$, where ϕ is a permutation of V_k fixing $0, \epsilon_1, \epsilon_2$, and $\epsilon_1 + \epsilon_2$. Define a Boolean function f on V_n as*

$$f(y,x) = \begin{cases} g(x), & \text{if } y = 0, \\ 1 \oplus g(x), & \text{if } y = \epsilon_1 + \epsilon_2, \\ h(y,x), & \text{otherwise.} \end{cases}$$

Theorem 1. *Let f be given by the Construction 1. Then the following statements hold:*

(i) f is balanced.

(ii) f satisfies the SAC.

(iii) the nonlinearity is $N_f = 2^{n-1} - 2^{\frac{n}{2}}$.

(iv) the sum-of-squares indicator is $\sigma_f = 2^{2n} + 3 \cdot 2^{\frac{3}{2}n+1}$.

(v) the algebraic degree is $\deg(f) = k + 1$.

Proof. (i). Since $\phi(0) = 0$ and $\phi(\epsilon_1 + \epsilon_2) = \epsilon_1 + \epsilon_2$, the Walsh-Hadamard transform of f is

$$\begin{aligned} \mathcal{F}_{\hat{f}}(b,a) &= \sum_{y,x} (-1)^{f(y,x)} (-1)^{(b,a)\cdot(y,x)} \\ &= \sum_{x} (-1)^{g(x)} (-1)^{a\cdot x} + \sum_{x} (-1)^{1 \oplus g(x)} (-1)^{b_1 \oplus b_2 \oplus a\cdot x} \\ &\quad + \sum_{\substack{y,x \\ y \neq 0, \epsilon_1+\epsilon_2}} (-1)^{\phi(y)\cdot x} (-1)^{(b,a)\cdot(y,x)} \end{aligned}$$

$$
\begin{aligned}
&= \sum_x (-1)^{g(x)}(-1)^{a\cdot x} - (-1)^{b_1\oplus b_2}\sum_x (-1)^{g(x)}(-1)^{a\cdot x} \\
&\quad + \sum_{y,x}(-1)^{\phi(y)\cdot x}(-1)^{(b,a)\cdot(y,x)} - \sum_x (-1)^{a\cdot x} - \sum_x (-1)^{x_1\oplus x_2}(-1)^{b_1\oplus b_2\oplus a\cdot x} \\
&= \mathcal{F}_{\hat{g}}(a) - (-1)^{b_1\oplus b_2}\mathcal{F}_{\hat{g}}(a) + \mathcal{F}_{\hat{h}}(b,a) \\
&\qquad\qquad - \sum_x (-1)^{a\cdot x} - (-1)^{b_1\oplus b_2}\sum_x (-1)^{(a\oplus(\epsilon_1+\epsilon_2))\cdot x}.
\end{aligned}
$$

By Lemma 2, $\mathcal{F}_{\hat{h}}(b,a) = 2^k(-1)^{b\cdot\phi^{-1}(a)}$. Thus, it follows that

$$
\mathcal{F}_{\hat{f}}(b,a) = \begin{cases} (1-(-1)^{b_1\oplus b_2})\mathcal{F}_{\hat{g}}(a), & \text{if } a = 0, \epsilon_1+\epsilon_2, \\ (1-(-1)^{b_1\oplus b_2})\mathcal{F}_{\hat{g}}(a) + 2^k(-1)^{b\cdot\phi^{-1}(a)}, & \text{otherwise.} \end{cases}
$$

Note that f is balanced if and only if $\mathcal{F}_{\hat{f}}(0) = 0$. Since $\mathcal{F}_{\hat{f}}(0,0) = 0$, f is balanced.

(ii). Let $e = (\beta, \alpha)$ denote any vector in V_n with Hamming weight 1. For the convenience of notation, we let $S_e = \sum_{y,x} f(y,x) \oplus f((y,x)\oplus e)$. It suffices to prove that $S_e = 2^{n-1}$. We first note that $\sum_{y,x} h(y,x)\oplus h((y,x)\oplus e) = 2^{n-1}$, since h is a bent function by Lemma 2. We proceed with several cases.

Case 1. $\beta = \epsilon_1$ and $\alpha = 0$. In this case, we obtain that

$$
\begin{aligned}
S_e &= \sum_{y,x}[f(y,x)\oplus f(y\oplus\beta,x)] = \sum_{y,x}[h(y,x)\oplus h(y\oplus\beta,x)] \\
&\quad - 2\sum_x[(\phi(0)\cdot x)\oplus(\phi(\epsilon_1)\cdot x)] - 2\sum_x[(\phi(\epsilon_2)\cdot x)\oplus(\phi(\epsilon_1+\epsilon_2)\cdot x)] \\
&\quad + 2\sum_x[g(x)\oplus(\phi(\epsilon_1)\cdot x)] + 2\sum_x[(\phi(\epsilon_2)\cdot x)\oplus 1\oplus g(x)] \\
&= \sum_{y,x}[h(y,x)\oplus h(y\oplus\beta,x)] - 2\sum_x x_1 - 2\sum_x x_1 + 2\sum_x(x_2\oplus x_1x_2\oplus 1) \\
&\quad + 2\sum_x(x_1\oplus x_1x_2) = 2^{n-1} - 2^k - 2^k + 3\cdot 2^{k-1} + 2^{k-1} = 2^{n-1}.
\end{aligned}
$$

Case 2. $\beta = \epsilon_2$ and $\alpha = 0$. Similarly, as before we obtain $S_e = 2^{n-1}$.

Case 3. $\beta = \epsilon_i$ $(3 \leq i \leq k)$ and $\alpha = 0$.

$$\begin{aligned} S_e &= \sum_{y,x}[f(y,x) \oplus f(y \oplus \beta, x)] = \sum_{y,x}[h(y,x) \oplus h(y \oplus \beta, x)] \\ &- 2\sum_x[(\phi(0) \cdot x) \oplus (\phi(\epsilon_i) \cdot x)] - 2\sum_x[(\phi(\epsilon_1 + \epsilon_2) \cdot x) \oplus (\phi(\epsilon_1 + \epsilon_2 + \epsilon_i) \cdot x)] \\ &+ 2\sum_x[g(x) \oplus (\phi(\epsilon_i) \cdot x)] + 2\sum_x[(1 \oplus g(x)) \oplus (\phi(\epsilon_1 + \epsilon_2 + \epsilon_i) \cdot x)] \\ &=: I_1 - 2I_2 - 2I_3 + 2I_4 + 2I_5. \end{aligned}$$

As noted before, $I_1 = 2^{n-1}$. Since $\phi(y)$ are distinct vectors in V_k, we have $I_i = 2^{k-1}$ $(i = 2, 3)$. By Lemma 1, $g(x) \oplus a \cdot x$ is balanced for any a except for $0, \epsilon_1, \epsilon_2, \epsilon_1 + \epsilon_2$, and so $I_i = 2^{k-1}$ $(i = 4, 5)$. Thus, $S_e = 2^{n-1}$.

Case 4. $\beta = 0$. In this case, we have that

$$\begin{aligned} S_e &= \sum_{y,x} f(y,x) \oplus f(y, x \oplus \alpha) \\ &= \sum_{y,x} h(y,x) \oplus h(y, x \oplus \alpha) - \sum_x(\phi(0) \cdot x) \oplus (\phi(0) \cdot (x \oplus \alpha)) \\ &\quad - \sum_x(\phi(\epsilon_1 + \epsilon_2) \cdot x) \oplus (\phi(\epsilon_1 + \epsilon_2) \cdot (x \oplus \alpha)) \\ &\quad + \sum_x g(x) \oplus g(x \oplus \alpha) + \sum_x(1 \oplus g(x)) \oplus (1 \oplus g(x \oplus \alpha)) \\ &=: I_1 - I_2 - I_3 + I_4 + I_5 \end{aligned}$$

We first note that $I_4 = I_5$. As in the previous case, $I_1 = 2^{n-1}$. Since $\phi(0) = 0, I_2 = 0$. For I_3, I_4, we proceed with three subcases.

Case 4-1. $\beta = 0$ and $\alpha = \epsilon_1$. In this case, $I_3 = \sum_x x_1 \oplus x_2 \oplus ((x_1 \oplus 1) \oplus x_2) = 2^k$, and $I_4 = \sum_x(x_1 \oplus x_2 \oplus x_1x_2 \oplus 1) \oplus ((x_1 \oplus 1) \oplus x_2 \oplus (x_1 \oplus 1)x_2 \oplus 1) = 2^{k-1}$. Thus, $S_e = 2^{n-1}$.

Case 4-2. $\beta = 0$ and $\alpha = \epsilon_2$. Same method as in Case 4-1 implies $S_e = 2^{n-1}$.

Case 4-3. $\beta = 0$ and $\alpha = \epsilon_i$ $(3 \leq i \leq k)$. It follows easily that $I_3 = I_4 = 0$ and so $S_e = 2^{n-1}$.

Therefore, we obtain that $S_e = 2^{n-1}$ for any vector $e \in V_n$ with weight 1, that is, f satisfies the SAC.

(iii). By the proof of (i), it follows that $\max_{b,a}|\mathcal{F}_{\hat{f}}(b,a)| = \max\{2|\mathcal{F}_{\hat{g}}(0)|, 2|\mathcal{F}_{\hat{g}}(\epsilon_1+\epsilon_2)|, \max_{a\neq 0,\epsilon_1+\epsilon_2} 2|\mathcal{F}_{\hat{g}}(a)|+2^k\}$. From Lemma 1, we have that $\max_{b,a}|\mathcal{F}_{\hat{f}}(b,a)| = 2^{k+1}$, which implies that $N_f = 2^{n-1} - 2^{\frac{n}{2}}$.

(iv). By the proof of (i), we have that

$$\begin{aligned}\sum_{b,a}\mathcal{F}^4_{\hat{f}}(b,a) &= \sum_b \mathcal{F}^4_{\hat{f}}(b,0) + \sum_b \mathcal{F}^4_{\hat{f}}(b,\epsilon_1+\epsilon_2) + \sum_{\substack{b,a\\ a\neq 0,\epsilon_1+\epsilon_2}} \mathcal{F}^4_{\hat{f}}(b,a)\\ &= \sum_b (1-(-1)^{b_1\oplus b_2})^4\mathcal{F}^4_{\hat{g}}(0) + \sum_b (1-(-1)^{b_1\oplus b_2})^4\mathcal{F}^4_{\hat{g}}(\epsilon_1+\epsilon_2)\\ &\quad + \sum_{\substack{b,a\\ a\neq 0,\epsilon_1+\epsilon_2}} \{(1-(-1)^{b_1\oplus b_2})\mathcal{F}_{\hat{g}}(a) + 2^k(-1)^{b\cdot\phi^{-1}(a)}\}^4.\end{aligned}$$

The first term equals $2^{k+3}\mathcal{F}^4_{\hat{g}}(0)$ and the second term equals $2^{k+3}\mathcal{F}^4_{\hat{g}}(\epsilon_1+\epsilon_2)$. The last term can be written as

$$\begin{aligned}&\sum_{\substack{b,a\\ a\neq 0,\epsilon_1+\epsilon_2}} (1-(-1)^{b_1\oplus b_2})^4\mathcal{F}^4_{\hat{g}}(a) + \sum_{\substack{b,a\\ a\neq 0,\epsilon_1+\epsilon_2}} 2^{4k}\\ &+6\sum_{\substack{b,a\\ a\neq 0,\epsilon_1+\epsilon_2}} (1-(-1)^{b_1\oplus b_2})^2\mathcal{F}^2_{\hat{g}}(a)2^{2k}\\ &+4\sum_{\substack{b,a\\ a\neq 0,\epsilon_1+\epsilon_2}} (1-(-1)^{b_1\oplus b_2})\mathcal{F}_{\hat{g}}(a)2^{3k}(-1)^{b\cdot\phi^{-1}(a)}\\ &+4\sum_{\substack{b,a\\ a\neq 0,\epsilon_1+\epsilon_2}} (1-(-1)^{b_1\oplus b_2})^3\mathcal{F}^3_{\hat{g}}(a)2^{k}(-1)^{b\cdot\phi^{-1}(a)}\\ &=: I_1 + I_2 + 6I_3 + 4I_4 + 4I_5.\end{aligned}$$

We can easily obtain that $I_1 = 2^{k+3}\sum_{a\neq 0,\epsilon_1+\epsilon_2}\mathcal{F}^4_{\hat{g}}(a)$, $I_2 = 2^{5k}(2^k-2)$, and $I_3 = 2^{3k+1}\sum_{a\neq 0,\epsilon_1+\epsilon_2}\mathcal{F}^2_{\hat{g}}(a)$. We calculate the term I_4. For $a \neq 0, \epsilon_1+\epsilon_2$, we have that

$$\sum_b (1-(-1)^{b_1\oplus b_2})(-1)^{b\cdot\phi^{-1}(a)} = \sum_b (-1)^{b\cdot\phi^{-1}(a)} - \sum_b (-1)^{b\cdot(\phi^{-1}(\epsilon_1+\epsilon_2)\oplus\phi^{-1}(a))} = 0.$$

It follows that $I_4 = 0$. Finally, we calculate the term I_5. For $a \neq 0, \epsilon_1+\epsilon_2$, we have that

$$\sum_b (1-(-1)^{b_1\oplus b_2})^3(-1)^{b\cdot\phi^{-1}(a)} = \sum_b (4-4(-1)^{b_1\oplus b_2})(-1)^{b\cdot\phi^{-1}(a)} = 0,$$

which implies that $I_5 = 0$. Hence, we have that

$$\sum_{b,a} \mathcal{F}^4_{\hat{f}}(b,a) = 2^{k+3}\mathcal{F}^4_{\hat{g}}(0) + 2^{k+3}\mathcal{F}^4_{\hat{g}}(\epsilon_1+\epsilon_2) + 2^{5k}(2^k-2)$$
$$+ 2^{k+3} \sum_{a\neq 0,\epsilon_1+\epsilon_2} \mathcal{F}^4_{\hat{g}}(a) + 6\cdot 2^{3k+1} \sum_{a\neq 0,\epsilon_1+\epsilon_2} \mathcal{F}^2_{\hat{g}}(a).$$

By Lemma 1, the sum-of-squares indicator is $\sigma_f = 2^{4k} + 6\cdot 2^{3k}$.

(v). We note that

$$\begin{aligned} f(y,x) =&(y_1\oplus 1)(y_2\oplus 1)\cdots(y_k\oplus 1)\phi(0)\cdot x\\ &\oplus (y_1\oplus 1)(y_2\oplus 1)\cdots y_k\phi(1)\cdot x\oplus\\ &\vdots\\ &\oplus y_1y_2\cdots y_k\phi(\epsilon_1)\cdot x \oplus (y_1\oplus 1)(y_2\oplus 1)\cdots(y_k\oplus 1)(\phi(0)\cdot x\oplus g(x))\\ &\oplus y_1y_2\cdots(y_k\oplus 1)(\phi(\epsilon_1+\epsilon_2)\cdot x\oplus 1\oplus g(x))\\ =&(y_1\oplus 1)(y_2\oplus 1)\cdots(y_k\oplus 1)\phi(0)\cdot x\oplus(y_1\oplus 1)(y_2\oplus 1)\cdots y_k\phi(1)\cdot x\oplus\\ &\vdots\\ &\oplus y_1y_2y_3\cdots y_k\phi(\epsilon_1)\cdot x\\ &\oplus (y_1\oplus 1)(y_2\oplus 1)\cdots(y_k\oplus 1)(x_1\oplus x_2\oplus x_1x_2\oplus 1)\\ &\oplus y_1y_2(y_3\oplus 1)\cdots(y_k\oplus 1)x_1x_2, \end{aligned}$$

since $\phi(0)=0, \phi(\epsilon_1+\epsilon_2)=\epsilon_1+\epsilon_2$, and $g(x)=x_1\oplus x_2\oplus x_1x_2\oplus 1$. The term $y_1y_2y_3\cdots y_kx_1x_2$ is cancelled because this term appears two times in the above expression. The terms $y_1y_2y_3\cdots y_kx_1$ and $y_1y_2y_3\cdots y_kx_2$ are not cancelled, since these terms appear $2^{k-1}+1$ times. Hence $\deg(f) = k+1$. $\diamondsuit$

Stănică [8] constructed a class of highly nonlinear balanced functions with good local and global avalanche characteristics. More precisely, he constructed a Boolean function f on V_{2k} satisfying the following properties:

(a) f is balanced.

(b) f satisfies the SAC.

(c) the nonlinearity is $N_f = 2^{2k-1} - 2^k$.

(d) the sum-of-squares indicator is $\sigma_f = 2^{4k+2}$.

Observe that the sum-of-squares indicator of Theorem 1 is an improvement of that of Stănică [8]. On the other hand, Zhang and Zheng [11] constructed a balanced function on V_{2k} with the nonlinearity $N_f \geq 2^{2k-1} - 2^k$. We believe that the nonlinearity is in fact $2^{2k-1} - 2^k$. The sum-of-squares indicator of the function is the same as ours. However, their construction does not ensure the SAC property. Therefore, Theorem 1 can also be regarded as an improvement of the result of Zhang and Zheng [11]. We would like to point out that in either case, our functions have also high algebraic degree, which is an improvement in itself.

3.2 Boolean Functions On V_{2k+1}

We present two methods for constructing balanced Boolean functions on V_{2k+1} with good cryptographic properties. For the first construction, we need the following lemma. The proof is easy and it is omitted.

Lemma 3. *Let h be a Boolean function on V_n. Define a Boolean function f on V_{n+1} as $f(y_1, y_2, x) = h(y_2, x) \oplus y_1(y_2 \oplus 1)$, where $y_i \in V_1$ $(1 \leq i \leq 2)$ and $x \in V_{n-1}$. Then $\mathcal{F}_{\hat{f}}(b_1, b_2, a) = \mathcal{F}_{\hat{h}}(b_2, a) + (-1)^{1 \oplus b_1} \mathcal{F}_{\hat{h}}(1 \oplus b_2, a)$.*

Theorem 2. *Let $h = (h_1, h_2)$ be a bent function on V_{2k} with h_2 balanced, where (h_1, h_2) is the concatenation of h_1 and h_2. Define f on V_{2k+1} as $f = (h_1, h_2, 1 \oplus h_1, h_2)$. Then the following statements hold:*

(i) f is balanced.

(ii) f satisfies the SAC.

(iii) the nonlinearity is $N_f = 2^{2k} - 2^k$.

(iv) the sum-of-squares indicator is $\sigma_f = 2^{4k+3}$.

Proof. The proofs of (i) and (ii) are straightforward. The proofs of (iii) and (iv) follow from Lemma 3. ◇

We now construct a balanced function on V_{2k+1} with smaller sum-of-squares indicator than that of Theorem 2. To do this, we need the following lemma. The proof is straightforward and is omitted.

Lemma 4. *Let h be a Boolean function on V_s, and g be a Boolean function on V_t. Define a Boolean function f on V_{s+t} by $f(y,x) = h(y) \oplus g(x)$. Then the following statements hold:*

(i) $\mathcal{F}_{\hat{f}}(b,a) = \mathcal{F}_{\hat{h}}(b)\mathcal{F}_{\hat{g}}(a)$.

(ii) $\Delta_f(b,a) = \Delta_h(b)\Delta_g(a)$.

(iii) the nonlinearity is $N_f = 2^t N_h + 2^s N_g - 2N_h N_g$.

(iv) the sum-of-squares indicator is $\sigma_f = \sigma_h \sigma_g$.

We remark that a lower bound of the nonlinearity, for a Boolean function as in Lemma 4, was obtained by Seberry et al. ([4], [5]). However, we get the exact nonlinearity of f.

The following corollary is well known (see Seberry et al. [6]).

Corollary 1. *Let f, g, h be as in Lemma 4. If h or g is balanced, then f is balanced.*

Proof. It follows from Lemma 4 (i).

By using a computer program, we easily obtained a Boolean function g on V_5 with the following properties:

(a) g is balanced.

(b) g satisfies the SAC.

(c) the nonlinearity is $N_g = 12$ (the highest nonlinearity for any Boolean function on V_5).

(d) the sum-of-squares indicator is $\sigma_g = 1,664$.

Theorem 3. *Let g be a Boolean function on V_5 as above. Let h be a bent function on V_{2k-4}. Define a function f on V_{2k+1} as $f(y,x) = h(y) \oplus g(x)$. Then the following are true:*

(i) f is balanced.

(ii) f satisfies the SAC.

(iii) the nonlinearity is $N_f = 2^{2k} - 2^k$.

(iv) the sum-of-squares indicator is $\sigma_f = 1.625 \times 2^{4k+2}$.

Proof. The proof of (i) follows from Corollary 1. The remaining statements follow from Lemma 4. ◇

Stănică [8] constructed a balanced function on V_{2k+1} satisfying the SAC. He also proved that the nonlinearity is $N_f \geq 2^{2k} - 2^k$, and the sum-of-squares-indicator is $2^{4k+4} \leq \sigma_f \leq 2^{4k+5}$. On the other hand, Zhang and Zheng [11] constructed a balanced function on V_{2k+1} with the nonlinearity $N_f \geq 2^{2k} - 2^k$ and the sum-of-squares indicator $\sigma_f = 2^{4k+3}$. But the construction does not ensure the SAC property. The sum-of-squares indicator of Theorem 3 is less than those of [8] and [11]. Therefore, Theorem 3 can be regarded as an improvement of the results of [8] and [11].

Acknowledgments

The authors would like to thank the anonymous referee for his/her helpful comments, which improved significantly the presentation of the paper. The first author was partially supported by a Junior Faculty Award from The School of Sciences at his present institution. The second author was supported in part by the Ministry of Information & Communication of Korea.

References

[1] W. Meier and O. Staffelbach, Nonlinearity criteria for cryptographic functions, Adv. in Cryptology-Eurocrypt'89, LNCS, Springer-Verlag, Berlin, Heidelberg, New York, 434 (1990) pp. 549-562.

[2] B. Preneel, W.V. Leekwijck, L.V. Linden, R. Govaerts, and J. Vandewalle, Propagation characteristics of Boolean functions, Adv. in Cryptology-Eurocrypt'90, LNCS, Springer-Verlag, Berlin, Heidelberg, New York, 473 (1991) pp. 161-173.

[3] O.S. Rothaus, On bent functions, *J. Combin. Th.*, Ser. A, Vol. 20 (1976) pp. 300-305.

[4] J. Seberry, X.-M. Zhang, and Y. Zheng, On constructions and nonlinearity of correlation immune function functions, Adv. in Cryptology-Eurocrypt'93, LNCS, Springer-Verlag, Berlin, Heidelberg, New York, 765 (1994) pp. 181-199.

[5] J. Seberry, X.-M. Zhang, and Y. Zheng, Relationships among the nonlinearity criteria, Adv. in Cryptology-Eurocrypt'94, LNCS, Springer-Verlag, Berlin, Heidelberg, New York,

950 (1995) pp. 376-388.

[6] J. Seberry, X.-M. Zhang, and Y. Zheng, Nonlinearity and propagation characteristics of balanced Boolean functions, *Inform. and Comput.*, Vol. 119, No. 1 (1995) pp. 1-13.

[7] J.J. Son, J.I. Lim, S. Chee, and S.H. Sung, Global avalanche characteristics and nonlinearity of balanced Boolean functions, *Inform. Process. Lett.*, Vol. 65, No. 3 (1998) pp. 139-144.

[8] P. Stănică, Nonlinearity, local and global avalanche characteristics of Boolean balanced functions, *Discrete Mathematics* **248** (2002), pp. 181-193.

[9] S.H. Sung, S. Chee, and C. Park, Global avalanche characteristics and propagation criterion of balanced Boolean functions, *Inform. Process. Lett.*, Vol 69, No. 1 (1999) pp. 21-24.

[10] A.F. Webster and S.E. Tavares, On the design of S-boxes, Adv. in Cryptology-Crypto'85, LNCS, Springer-Verlag, Berlin, Heidelberg, New York, 218 (1986) pp. 523-534.

[11] X.-M. Zhang and Y. Zheng, GAC-the criterion for global avalanche characteristics of cryptographic functions, *J. Universal Comput. Sci.*, Vol. 1, No. 5 (1995) pp. 320-337.