Improving the Nonlinearity of Certain Balanced Boolean Functions with Good Local and Global Avalanche Characteristics

Pantelimon Stănică[1*], Soo Hak Sung[2†]

[1]Auburn University Montgomery, Department of Mathematics
Montgomery, AL 36117, USA, e-mail: *stanpan@strudel.aum.edu*,
[2]Department of Applied Mathematics, Pai Chai University
Taejon 302-735, South Korea, e-mail: *sungsh@www.paichai.ac.kr*

Keywords: Cryptography; Boolean functions; Nonlinearity; Avalanche Characteristics

1 Definitions and Preliminaries

The design and evaluation of cryptographic functions requires the definition of design criteria. In [2], Preneel *et al.* introduced the *propagation criterion of degree k* (PC of degree k or $PC(k)$): a function satisfies the $PC(k)$ if by complementing at most k bits the output changes with probability exactly one half. This is a generalization of the *Strict Avalanche Criterion* or SAC (for $k = 1$), introduced by Webster and Tavares in [6].

As many authors observed, the PC is a very important concept in designing cryptographic primitives used in data encryption algorithms and hash functions. However, the PC captures only local properties of the function. In order to improve the global analysis of cryptographically strong functions, Zhang and Zheng [7] introduced another criterion, which measures the *Global Avalanche Characteristics* (GAC) of a Boolean function. They proposed two indicators related to the GAC: the *absolute* indicator $\Delta_f = \max_{\alpha \neq 0} |\Delta_f(\alpha)|$,

*The first author was partially supported by a grant from the Auburn University Montgomery Research Grant-in-Aid Program; he is also associated with the Institute of Mathematics of Romanian Academy
†The second author was supported in part by KOSEF 97-01-00-13-01-5

and the *sum-of-squares* indicator $\sigma_f = \sum_\alpha \Delta_f^2(\alpha)$, where the *autocorrelation* $\Delta_f(\alpha) = \sum_{x \in \mathbf{Z}_2^n} \hat{f}(x)\hat{f}(x \oplus \alpha)$ is the autocorrelation function and $\hat{f}(x) = (-1)^{f(x)}$. The $PC(k)$ can be expressed in terms of the autocorrelation function. If f is defined on $V_n = \mathbf{Z}_2^n$, we see that f satisfies the $PC(k)$ if and only if $\sum_{x \in \mathbf{Z}_2^n} f(x) \oplus f(x \oplus c) = 2^{n-1}$, for any element c with Hamming weight $1 \leq wt(c) \leq k$, or equivalently, $\Delta_f(c) = 0$. If f is $PC(n)$ we say that f is a *bent function*.

There is an interest in computing bounds of the two indicators for various classes of Boolean functions. The smaller σ_f, Δ_f the better the GAC of a function. Zhang and Zheng obtained some bounds on the two indicators: $2^{2n} \leq \sigma_f \leq 2^{3n}, 0 \leq \Delta_f \leq 2^n$. Recently, Son, Lim, Chee and Sung [3] proved $\sigma_f \geq 2^{2n} + 2^{n+3}$, when f is a balanced Boolean function, and Sung, Chee and Park [5] showed that if f also satisfies the PC with respect to $A \subset \mathbf{Z}_2^n$, $t = |A|$, then

$$\sigma_f \geq \begin{cases} 2^{2n} + 2^6(2^n - t - 1), \text{ if } 0 \leq t \leq 2^n - 2^{n-3} - 1, t \text{ odd} \\ 2^{2n} + 2^6(2^n - t + 2), \text{ if } 0 \leq t \leq 2^n - 2^{n-3} - 1, t \text{ even} \\ \left(1 + \frac{1}{2^n - 1 - t}\right) 2^{2n}, \text{ if } 2^n - 2^{n-3} - 1 < t \leq 2^n - 2. \end{cases} \quad (1)$$

The problem of constructing Boolean functions which satisfy two or more design criteria seems to be a difficult task. In [4], the first author proved that for some SAC balanced functions, $2^{2n}(1 + p) \leq \sigma_f \leq 2^{3n-2}, \Delta_f = 2^n$, where p is the number of linear structures (with even Hamming weight) for the first half of f. He also found some SAC balanced functions with good GAC ($3 \cdot 2^{2n} \leq \sigma_f \leq 4 \cdot 2^{2n+\epsilon}$, where $\epsilon = 0, 1$ for n even, respectively, odd), and nonlinearity $N_f \geq 2^{n-1} - 2^{[\frac{n+1}{2}]}$ (where $[x]$ is the largest positive integer less than or equal to x.). The result proved the existence of Boolean functions with good nonlinearity and GAC close to that of bent functions, while being balanced and satisfying SAC.

In this paper we construct functions which are balanced, have nonlinearity $N_f \geq 2^{n-1} -$

$2^{[\frac{n}{2}]}$, are SAC, and the sum-of-squares indicator satisfies $2^{2n+1} \leq \sigma_f \leq 2^{2n+1+\epsilon}$, where $\epsilon = 0, 1$ if n is odd, respectively, even, thus improving on the nonlinearity of certain balanced functions, while keeping good local and global avalanche characteristics (it is known that N_f must be large to avoid the linear attack). Regarding the inequalities for N_f, σ_f, we prove that we have equality for odd dimensions, and that our functions are PC with respect to all but two vectors, the nonzero vector being a linear structure for f. For even dimensions, we conjecture equality for σ_f and that f is PC with respect to all but four vectors. We point out that if the conjecture is true, then we have equality for the nonlinearity in this case, as well. Although the proof we provide produces $N_f \geq 2^{n-1} - 2^{[\frac{n}{2}]}$, all of our examples suggest equality.

Definition 1.

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

2. *The* truth table *of f is the binary sequence* $f = (v_1, v_2, \ldots, v_{2^n})$, *where the bits v_i's are the values of* $f(x)$, *when x runs through the vectors* $b_1 = (0, \ldots, 0)$, $b_2 = (0, \ldots, 0, 1)$, $\ldots$ *of* V_n *in lexicographical order.*

3. *We call e_i the i-th* basis vector *of* V_n.

4. *We call a function* balanced *if the number of ones is equal to the number of zeroes in its truth table.*

5. *The* Hamming weight *of a binary vector v, denoted by* $wt(v)$ *is defined as the number of ones it contains. The* Hamming distance *between two functions* $f, g : V_n \to V_1$, *denoted by* $d(f, g)$ *is defined as* $wt(f \oplus g)$.

6. *The* nonlinearity *of a function f, denoted by N_f is defined as* $\min_{\phi \in A_n} d(f, \phi)$, *where A_n is*

the class of all affine function on V_n.

7. *A vector $\alpha \in V_n$ is a* linear structure *of f if $f(x) \oplus f(x \oplus \alpha)$ is constant for any x.*

8. *If X, Y are two strings of the same length, $(X|Y)$ means that X and Y occupy the same positions in the first and the second half of some function.*

9. *Define the set of 4-bit blocks* $T = \{A = 0,0,1,1;\ \bar{A} = 1,1,0,0;\ B = 0,1,0,1;\ \bar{B} = 1,0,1,0;\ C = 0,1,1,0;\ \bar{C} = 1,0,0,1;\ D = 0,0,0,0;\ \bar{D} = 1,1,1,1\}$.

10. *If some bits of an affine function l agree with the the corresponding bits in a function f, we say that l* cancels *those bits in f.*

11. *If u is a given string in f, and g is any Boolean function, we use* $u^g =$ the string of bits in g which occupy the same positions as the bits in the string u (for instance, if $u = f(b_i)f(b_j)\ldots$, for some $i, j, \ldots$, then $u^g = g(b_i)g(b_j)\ldots$)

12. *If a function is a concatenation of either $A/\bar{A}$ or $B/\bar{B}$ or $C/\bar{C}$ or $D/\bar{D}$ we say that it is* based on *A or B or C or D.*

The following can be proved using the truth table of f.

Lemma 2 (*Folklore Lemma*). *Any affine function $f = I_1 \ldots I_{2^{n-2}}$ satisfies: I_1 is in T, I_2 is I_1 or $\bar{I}_1$, $I_3 I_4$ is $I_1 I_2$ or $\bar{I}_1 \bar{I}_2$, etc., $I_{2^{n-3}+1} \ldots I_{2^{n-2}}$ is $I_1 \ldots I_{2^{n-3}}$ or $\bar{I}_1 \ldots \bar{I}_{2^{n-3}}$.*

2 Balanced Boolean functions with high nonlinearity and good local and global avalanche characteristics

We are now able to construct our first class of balanced Boolean functions of high nonlinearity with good local and global avalanche characteristics. If H, I, J, K are strings (in f) of the same length made up of concatenations of consecutive blocks, then the notation $(HJ|IK)$ means that the pairs H, I and J, K each occupy the same positions in the first

and second halves of the function (with 2^n bits). We shall use the term *segment* for a portion of a function such as the portion defined above. We define now a transformation $\mathcal{O}(g)$ ("opposite") which maps an affine function based on $M \in T$, into an affine function based on the same M. If $g = X_1 X_2 \dots X_{2^{n-2}}$, then $\mathcal{O}(g) = Y_1 Y_2 \dots Y_{2^{n-2}}$ is constructed by the following algorithm, supported by the *Folklore Lemma*:

Step 1. $Y_1 = X_1$.

Step $i+2$. *For any* $0 \le i \le n-3$, *if* $X_{2^i+1} \dots X_{2^{i+1}} = X_1 \dots X_{2^i}$, *then* $Y_{2^i+1} \dots Y_{2^{i+1}} = \bar{Y}_1 \dots \bar{Y}_{2^i}$. *If* $X_{2^i+1} \dots X_{2^{i+1}} = \bar{X}_1 \dots \bar{X}_{2^i}$, *then* $Y_{2^i+1} \dots Y_{2^{i+1}} = Y_1 \dots Y_{2^i}$.

By induction on n, we can easily prove

Lemma 3. $\mathcal{O}(\bar{g}) = \overline{\mathcal{O}(g)}$.

Construction 1. *Let* $n \ge 8$ *and* g_i^j, $1 \le i \le 2^{[\frac{n-1}{2}]-3}, 1 \le j \le 4$ *be affine functions on* $V_{[\frac{n}{2}-1]}$, *with* g_i^j *based on* A, B, C, D, *for* $j = 1, 2, 3, 4$, *respectively. Concatenate the* $2^{[\frac{n-1}{2}]}$ *segments (which are concatenations of affine functions)* $U_{4i+j-4} = (g_i^j \mathcal{O}(g_i^j) | g_i^j \mathcal{O}(\bar{g}_i^j))$, $U_{2^{[\frac{n-1}{2}]-1}+4i+j-4} = (\bar{g}_i^j \mathcal{O}(g_i^j) | \bar{g}_i^j \mathcal{O}(\bar{g}_i^j))$, *to obtain a function* f *on* V_n. *The segments can be placed arbitrarily, but for each* j *and for any pair* s, t *with* $1 \le s < t \le 2^{[\frac{n-1}{2}]-3}$, $g_s^j \ne g_t^j$ *or* $\bar{g}_t^j$ *(i.e., their sum is balanced).*

Remark 4. *The last condition is trivially fulfilled for* $n = 8$, *since* $2^{[\frac{n-1}{2}]-3} = 1$.

In the next theorem we construct our good cryptographic functions.

Theorem 5. *Let* $n \ge 8$. *Let* f *on* V_n *be given by Construction 1. Then* f *is balanced, satisfies the* SAC, *has the nonlinearity* $N_f \ge 2^{n-1} - 2^{[\frac{n}{2}]}$ *and the sum-of-squares indicator satisfies*

$$2^{2n+1} \le \sigma_f \le 2^{2n+1+\epsilon}, \text{ where } \epsilon = 0, 1 \text{ if } n \text{ is odd, respectively, even.} \tag{2}$$

Our proof relies on the following combinatorial lemma, which has some interest of its own: it gives information on the weight of cosets of such functions.

Lemma 6. *Given any two segments $U_r, U_p, r, p \leq 2^{[\frac{n-1}{2}]-1}$ as in Construction 1, based on the same block $M \in T$ and any affine function l based on M, then*

$$C_l(U_r U_p) \leq 2^{[\frac{n}{2}]-1} + 2^{[\frac{n}{2}]-3}, \tag{3}$$

where $C_l(X)$ is the number of blocks in X that are cancelled by the affine function l.

Proof. Without loss of generality we may assume that $n = 2k$ and U_r, U_p and l are made up of A and $\bar{A}$. The affine function l can have the following forms on the positions corresponding to U_r, U_l: $(LLLL|LLLL)$, $(LLLL|\bar{L}\bar{L}\bar{L}\bar{L})$, $(LL\bar{L}\bar{L}|LL\bar{L}\bar{L})$, $(LL\bar{L}\bar{L}|\bar{L}\bar{L}LL)$, $(L\bar{L}L\bar{L}|L\bar{L}L\bar{L})$, $(L\bar{L}L\bar{L}|\bar{L}L\bar{L}L)$, $(L\bar{L}\bar{L}L|L\bar{L}\bar{L}L)$, $(L\bar{L}\bar{L}L|\bar{L}LL\bar{L})$. The computations are similar for each form of l, so we first consider the case where $U_r^l = U_p^l$, precisely, where l, on the positions of U_r, U_p is $(LLLL|LLLL)$. We write $U_r = (H\mathcal{O}(H)|H\mathcal{O}(\bar{H}))$, $U_p = (G\mathcal{O}(G)|G\mathcal{O}(\bar{G}))$. In order to find the number of blocks cancelled by l we find the Hamming distance between $U_r U_p$ and $U_r^l U_p^l$. We get

$$\begin{aligned} wt(U_r U_p \oplus U_r^l U_p^l) &= 2wt(H \oplus L) + wt(\mathcal{O}(H) \oplus L) + wt(\mathcal{O}(\bar{H}) \oplus L) \\ &\quad + 2wt(G \oplus L) + wt(\mathcal{O}(G) \oplus L) + wt(\mathcal{O}(\bar{G}) \oplus L) \\ &= 2wt(H \oplus L) + 2wt(G \oplus L) + 2^k \geq 2wt(G \oplus H) + 2^k = 2^{k-1} + 2^k, \end{aligned}$$

which implies that $C_l(U_r U_p) \leq \frac{1}{4}(2^{k+2} - 2^k - 2^{k-1}) = 2^{k-1} + 2^{k-3}$. The remaining cases are similar. □

Remark 7. *The previous lemma refers to two segments in the first half of the function. The same result holds if the two segments are in the second half of the function.*

Now we are ready to prove the theorem.

Proof of Theorem 5. We consider the case of n even, that is $n = 2k$. The function f can be written as a concatenation of affine functions (by Construction 1),

$$\begin{aligned}&[g_1^1\mathcal{O}(g_1^1)\cdots g_1^4\mathcal{O}(g_1^4)\cdots g_{2^{k-4}}^1\mathcal{O}(g_{2^{k-4}}^1)\cdots \quad \bar{g}_1^1\mathcal{O}(g_1^1)\cdots\bar{g}_1^4\mathcal{O}(g_1^4)\cdots\bar{g}_{2^{k-4}}^1\mathcal{O}(g_{2^{k-4}}^1)\cdots\\ &g_1^1\mathcal{O}(\bar{g}_1^1)\cdots g_1^4\mathcal{O}(\bar{g}_1^4)\cdots g_{2^{k-4}}^1\mathcal{O}(\bar{g}_{2^{k-4}}^1)\cdots \quad \bar{g}_1^1\mathcal{O}(\bar{g}_1^1)\cdots\bar{g}_1^4\mathcal{O}(\bar{g}_1^4)\cdots\bar{g}_{2^{k-4}}^1\mathcal{O}(\bar{g}_{2^{k-4}}^1)\cdots]. \end{aligned} \tag{4}$$

Since any affine function that occurs in f, appears 2 times and its complement appears also 2 times, then f is balanced. In order to show that f satisfies the SAC, we use the Walsh-Hadamard transform in the form deduced in [1]: f satisfies the SAC if and only if

$$\begin{aligned}&(\hat{v}_1\hat{v}_{2^{i-1}+1}+\hat{v}_2\hat{v}_{2^{i-1}+2}+\cdots+\hat{v}_{2^{i-1}}\hat{v}_{2^i})+\\ &(\hat{v}_{2^i+1}\hat{v}_{2^i+2^{i-1}+1}+\cdots+\hat{v}_{2^i+2^{i-1}}\hat{v}_{2^{i+1}})+\cdots+\\ &(\hat{v}_{2^n-2^i+1}\hat{v}_{2^n-2^{i-1}+1}+\cdots+\hat{v}_{2^n-2^{i-1}}\hat{v}_{2^n})=0,\end{aligned} \tag{5}$$

for each $i = 1, 2, \ldots, n$, where $\hat{v}_i = (-1)^{v_i}$, or equivalently (if $i \geq 3$),

$$(X_1 \odot X_{2^{i-3}+1}+\cdots+X_{2^{i-3}}\odot X_{2^{i-2}})+\cdots=0, \tag{6}$$

for each $i = 3, 4, \ldots, n$, where $M \odot N$ is equal to the number of 0's minus the number of 1's in $M \oplus N$ and $f = X_1 \cdots X_{2^{n-2}}$.

By associating the 4-bit blocks $\{A, \bar{A}\} \Longleftrightarrow \{B, \bar{B}\}$ and $\{C, \bar{C}\} \Longleftrightarrow \{D, \bar{D}\}$, we see that the relation (5) holds, if $i \leq 2$. From the definition of the operator $\odot$ we see that if $M \oplus N$ is balanced, then $M \odot N = 0$. Thus, in the sum (6) all terms are zero, except possibly the ones based entirely on $M, \bar{M} \in T$. Since $M \odot M = \bar{M} \odot \bar{M} = 4$, $M \odot \bar{M} = \bar{M} \odot M = -4$ we see that $M \odot M + M \odot \bar{M} = \bar{M} \odot \bar{M} + M \odot \bar{M} = \cdots = 0$. Let $i \leq k-1$. Without loss of generality, we prove that there is an antidote for $X_1 \odot X_{2^{i-3}+1}$. Since $i \leq k-1$, both $\odot$ factors belong to the same function, in this case, $X_1, X_{2^{i-3}+1}$ belong to g_1^1. Next, to avoid an awkward typing, we make the notation: if X is a block in the affine function

g_1^1, we denote by X' the block in $\mathcal{O}(g_1^1)$ on the same position as X. First, if $X_1 = X_{2^{i-3}+1}$, then from the definition of the operator $\mathcal{O}$, we obtain (at step $i-1$), $X'_1 = \bar{X}'_{2^{i-3}+1}$, therefore $X_1 \odot X_{2^{i-3}+1} + X'_1 \odot X'_{2^{i-3}+1} = 0$. If $X_1 = \bar{X}_{2^{i-3}+1}$, then by the same argument $X'_1 = X'_{2^{i-3}+1}$, and $X_1 \odot X_{2^{i-3}+1} + X'_1 \odot X'_{2^{i-3}+1} = 0$. Now, assume that $k \leq i$. In this case, each function g_s^j has all or none of its blocks in a parenthesis, since the number of terms in a parenthesis is 2^{i-3}, which is now divisible by 2^{k-3} (the number of blocks in each g_s^j). First, consider $k \leq i \leq n-2$. In this case, each portion (*if it exists*) of a parenthesis of (6), based on the same block M is a sum of terms of the form $g_s^j \odot g_r^j$ (with both functions *in the same* quarter of f), which terms are 0, since two affine functions, which are not equal or complementary (see the last condition of Construction 1), have balanced sum, therefore, their $\odot$ is 0. Now, if $i = n-1$, then (6) can be written as $(g_1^1 \odot \bar{g}_1^1 + \mathcal{O}(g_1^1) \odot \mathcal{O}(g_1^1) + \cdots) + (g_1^1 \odot \bar{g}_1^1 + \mathcal{O}(\bar{g}_1^1) \odot \mathcal{O}(\bar{g}_1^1) + \cdots) = ((-2^{k-1}) + 2^{k-1} + \cdots) + \cdots + ((-2^{k-1}) + 2^{k-1} + \cdots) = 0$. If $i = n$, (6) can be written as $(g_1^1 \odot g_1^1 + \mathcal{O}(g_1^1) \odot \mathcal{O}(\bar{g}_1^1) + \cdots + \bar{g}_1^1 \odot \bar{g}_1^1 + \mathcal{O}(g_1^1) \odot \mathcal{O}(\bar{g}_1^1) + \cdots) = (2^{k-1} + (-2^{k-1}) + \cdots) + \cdots + (2^{k-1} + (-2^{k-1}) + \cdots) = 0$.

Now we evaluate the nonlinearity of f. Let l be an arbitrary affine function, which we may assume is made up of $A, \bar{A}$ (since any affine function is based entirely on $A, \bar{A}$; or $B, \bar{B}$; or $C, \bar{C}$; or $D, \bar{D}$). We calculate $wt(f \oplus l)$. From the part of f that does not contain $A, \bar{A}$ we get $3 \cdot 2^{2k-3} = 2^{2k-1} - 2^{2k-3}$ units. We consider now the part of f based on $A, \bar{A}$. Since each segment in l is the same as the previous segment or it is its complement (see Folklore Lemma) and from Lemma 6, we deduce that in the worst case (minimum number of units for the weight of the sum), l cancels at most 2 functions completely (in each half), and in the rest of the function based on A half of the blocks are cancelled. That can also be seen using the following argument: if l does not have a part corresponding to one of the g_i^1's equal to that g_i^1 (or $\bar{g}_i^1$), then the sum of f and l is balanced (if two affine functions are

not equal or complementary, their sum is balanced). So in the worst case, l has the part corresponding to one of g_i^1 equal to g_i^1 and the part corresponding to $\bar{g}_i^1$ equal to $\bar{g}_i^1$. Thus we cancel two blocks in the first half and two blocks in the second half of f. Therefore, we get from the part of f based on A, (*total number of blocks based on* $A-4$ *blocks cancelled (2 from each half)*) $\times$ (*bits left uncancelled in each block*) $= (8\cdot 2^{k-4}-4)\cdot 2^{k-2} = 2^{2k-3}-2^k$ units. Thus $N_f \geq 2^{2k-1}-2^{2k-3}+2^{2k-3}-2^k = 2^{2k-1}-2^k$. The case $n=2k+1$ is similar.

Using the inequality, $N_f \leq 2^{n-1}-\frac{1}{2}\sqrt{\sigma_f/2^n}$, which was obtained in [3], and our bound for the nonlinearity $N_f \geq 2^{n-1}-2^{[n/2]}$, we deduce $2^{n-1}-2^{[n/2]} \leq 2^{n-1}-2^{-\frac{n}{2}-1}\sqrt{\sigma_f}$, which will produce our right side inequality $\sigma_f \leq 2^{2n+2}$, if n is even, and $\sigma_f \leq 2^{2n+1}$, if n is odd.

In order to show the left side of the inequality we use a technique developed by the authors of [4, 5]. The sum-of-squares indicator satisfies

$$\sigma_f = \sum_x \Delta_f^2(x) = 2^6 \sum_x (b_x - 2^{n-3})^2,$$

where $b_x = \frac{1}{2}\sum_y f(y)f(y\oplus x) = 2^{n-2} - \frac{1}{4}\sum_y f(y)\oplus f(y\oplus x)$. It follows that $\sigma_f = 2^{2n} + 2^6 \sum_{wt(x)\geq 2}(b_x - 2^{n-3})^2$. We attempt to find vectors $x = e_i \oplus e_j, i<j$ such that $(b_x - 2^{n-3})^2$ is not zero. For $x = e_i \oplus e_j, i<j$, let

$$\begin{aligned} S_x := \sum_{y\in \mathbf{Z}_2^n} f(y)\oplus f(y\oplus x) = \sum_{s=1}^{2^n} f(v_s)\oplus f(v_s\oplus e_i\oplus e_j) = \\ 2[f(v_1)\oplus f(v_{2^{j-1}+2^{i-1}+1}) + \cdots + f(v_{2^{i-1}})\oplus f(v_{2^{j-1}+2^i}) + \\ f(v_{2^{i-1}+1})\oplus f(v_{2^{j-1}+1}) + \cdots + f(v_{2^{i-1}+2^{i-1}})\oplus f(v_{2^{j-1}+2^{i-1}})] + \cdots . \end{aligned} \tag{7}$$

Using the form of our functions and taking $x = e_{k-1}\oplus e_n$, we get

$$S_{e_{k-1}\oplus e_n} = 2\sum_M (M\oplus M + \bar{M}\oplus \bar{M}) = 0.$$

Thus, $(b_{e_{k-1}\oplus e_n} - 2^{n-3})^2 = 2^{2n-6}$. We obtain $\sigma_f \geq 2^{2n} + 2^6 2^{2n-6} = 2^{2n+1}$. □

Remark 8. *Same result as in Theorem 5 can be obtained, if the transformation* $\mathcal{O}(g)$ *has the first 4-bit block* $Y_1 = \bar{X}_1$, *obtaining another class of functions with the same properties.*

The following theorem gives precise results on the nonlinearity for odd dimensions for our functions, which are PC with respect to all but two vectors.

Theorem 9. *If n is odd, then the nonlinearity is $N_f = 2^{n-1} - 2^{[\frac{n}{2}]}$, $\sigma_f = 2^{2n+1}$, and f satisfies the PC with respect to all but two vectors $\{0, e_{k-1} \oplus e_n\}$. Moreover, $e_{k-1} \oplus e_n$ is a linear structure of f.*

Proof. We proved that if n is odd, then $\sigma_f = 2^{2n+1}$. If f were not PC with respect to $x \notin \{0, e_{k-1} \oplus e_n\}$, then $b_x \neq 2^{n-3}$, argument used in the proof of the previous theorem. If so, then by the same calculation we would get $\sigma_f > 2^{2n+1}$, which is not true. So f is PC with respect to all but two vectors. In [8], Zhang and Zheng proved that, if a function satisfies the PC with respect to all but two vectors, then n must be odd, the nonzero vector, where the propagation criterion is not satisfied, must be a linear structure and $N_f = 2^{n-1} - 2^{[n/2]}$. We have the result. □

3 Examples and Further Research

We give now two examples for $n = 8, 9$ of functions obtained using Construction 1:

$$\begin{aligned} f_8 =& AAA\bar{A}BBB\bar{B}CCC\bar{C}DDD\bar{D}\bar{A}\bar{A}A\bar{A}\bar{B}\bar{B}B\bar{B}\bar{C}\bar{C}C\bar{C}\bar{D}\bar{D}D\bar{D} \\ & AA\bar{A}ABB\bar{B}BCC\bar{C}CDD\bar{D}D\bar{A}\bar{A}\bar{A}A\bar{B}\bar{B}\bar{B}B\bar{C}\bar{C}\bar{C}C\bar{D}\bar{D}\bar{D}D, \end{aligned} \tag{8}$$

with $g_1^1 = AA, g_1^2 = BB, \ldots$, and

$$\begin{aligned} f_9 =& AAA\bar{A}BBB\bar{B}CCC\bar{C}DDD\bar{D}A\bar{A}AAB\bar{B}BBC\bar{C}CCD\bar{D}DD \\ & \bar{A}\bar{A}AA\bar{B}\bar{B}BB\bar{C}\bar{C}CC\bar{D}\bar{D}DD\bar{A}\bar{A}\bar{A}AB\bar{B}\bar{B}B\bar{C}\bar{C}\bar{C}C\bar{D}\bar{D}\bar{D}D \\ & AA\bar{A}ABB\bar{B}BCC\bar{C}CDD\bar{D}DA\bar{A}\bar{A}AB\bar{B}\bar{B}BC\bar{C}\bar{C}CD\bar{D}\bar{D}D \\ & \bar{A}\bar{A}\bar{A}AB\bar{B}\bar{B}BB\bar{C}\bar{C}CC\bar{D}\bar{D}DA\bar{A}AAB\bar{B}BBC\bar{C}CCD\bar{D}DD, \end{aligned} \tag{9}$$

with $g_1^1 = AA, g_1^2 = BB, \ldots, g_2^1 = A\bar{A}, g_2^2 = B\bar{B}, \ldots$. The nonlinearity of f_8 is $2^7 - 2^4 = 112$ and of f_9 is $2^8 - 2^4 = 240$. The algebraic normal form of $f_8 = x_2 + x_7 + x_1x_5 + x_2x_5 +$

$x_3x_8 + x_4x_7 + x_4x_8 + x_5x_6$ and $f_9 = x_2 + x_8 + x_1x_6 + x_2x_3 + x_2x_6 + x_3x_7 + x_4x_9 + x_5x_8 + x_5x_9 + x_6x_7$, the sum-of-square indicator for f_8 is $\sigma_{f_8} = 262,144 = 2^{2\cdot 8+2}$, and for f_9 is $\sigma_{f_9} = 524,288 = 2^{2\cdot 9+1}$ and they are SAC (actually, f_8 satisfies PC with respect to all but $\mathbf{0}, e_3 \oplus e_7, e_3 \oplus e_8, e_7 \oplus e_8$, and f_9 satisfies PC with respect to all but $\mathbf{0}, e_3 \oplus e_9$).

We proved that for our functions, on odd dimensions, $\sigma_f = 2^{2n+1}$ and $N_f = 2^{n-1} - 2^{[\frac{n}{2}]}$. Based on our numerous numerical examples we conjecture that the two indicators (GAC and nonlinearity) are also precisely controlled on even dimension. Assume that f is obtained by Construction 1.

Conjecture 10. *If n is even, then $\sigma_f = 2^{2n+2}$ and f satisfies the propagation criterion for all but 4 vectors.*

The conjecture will imply the identity for nonlinearity on even dimensions, since in [8], the authors prove that if f is PC with respect to all but four vectors, then n must be even, $N_f = 2^{n-1} - 2^{[n/2]}$ and the three nonzero vectors, which do not satisfy the propagation criterion are linear structures for f.

Acknowledgements. The authors would like to thank the anonymous referees for their helpful comments, which improved significantly the presentation of the paper.

References

[1] T.W. Cusick, P. Stănică, Bounds on the number of functions satisfying the Strict Avalanche Criterion, *Inform. Proc. Letters* **60** (1996), pp. 215-219.

[2] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, J. Vandewalle, Propagation characteristics of Boolean functions, in *Adv. in Cryptology – Eurocrypt' 90* **473** (1991), pp. 161-173.

[3] J.J. Son, J.I. Lim, S. Chee, S.H. Sung, Global avalanche characteristics and nonlinearity of balanced boolean functions, *Inform. Proc. Letters* **65** (1998), pp. 139-144.

[4] P. Stănică, Nonlinearity, Local and Global Avalanche Characteristics of Balanced Boolean Functions, to appear (available online at *http://sciences.aum.edu/˜stanpan*).

[5] S.H. Sung, S. Chee, C. Park, Global avalanche characteristics and propagation criterion of balanced boolean functions, *Inform. Proc. Letters* **69** (1999), pp. 21-24.

[6] A.F. Webster, S.E. Tavares, On the design of S-boxes, *Adv. in Cryptology – Crypto' 85* (1986), pp. 523-534.

[7] X-M. Zhang, Y. Zheng, GAC - The criterion for global avalanche characteristics of cryptographic functions, *J. Universal Computer Science* **1** (1995), pp. 320-337.

[8] X-M. Zhang, Y. Zheng, Characterizating the Structures of Cryptographic Functions Satisfying the Propagation Criterion for Almost all Vectors, *Designs, Codes and Cryptography* **7**, No. 1/2 (1996), pp. 111-134.