Highly Nonlinear 0-1 Balanced Boolean Functions Satisfying Strict Avalanche Criterion (Extended Abstract)

Jennifer Seberry *
Xian-Mo Zhang †

Department of Computer Science
The University of Wollongong
Wollongong, NSW 2522, AUSTRALIA

Abstract

Nonlinearity, 0-1 balancedness and strict avalanche criterion (SAC) are important criteria for cryptographic functions. Bent functions have maximum nonlinearity and satisfy SAC however they are not 0-1 balanced and hence cannot be directly used in many cryptosystems where 0-1 balancedness is needed. In this paper we construct

(i) 0-1 balanced boolean functions on V_{2k+1} ($k \geqq 1$) having nonlinearity $2^{2k} - 2^k$ and satisfying SAC,

(ii) 0-1 balanced boolean functions on V_{2k} ($k \geqq 2$) having nonlinearity $2^{2k-1} - 2^k$ and satisfying SAC.

We demonstrate that the above nonlinearities are very high not only for the 0-1 balanced functions satisfying SAC but also for all 0-1 balanced functions.

1 Basic Definitions

Let V_n be the vector space of n tuples of elements from $GF(2)$. Let α, $\beta \in V_n$. Write $\alpha = (a_1 \cdots a_n)$, $\beta = (b_1 \cdots b_n)$, where $a_i, b_i \in GF(2)$. Write $\langle \alpha, \beta \rangle = \sum_{j=1}^{n} a_j b_j$ for the scalar product of α and β. We write $\alpha = (a_1 \cdots a_n) < \beta = (b_1 \cdots b_n)$ if there exists k, $1 \leqq k \leqq n$, such that $a_1 = b_1, \ldots, a_{k-1} = b_{k-1}$ and $a_k = 0$, $b_k = 1$. Hence we can order all vectors in V_n by the relation $<$

$$\alpha_0 < \alpha_1 < \cdots < \alpha_{2^n - 1},$$

where

$$\alpha_0 = (0 \cdots 00), \ \ldots, \ \alpha_{2^{n-1}-1} = (01 \cdots 1),$$

$$\alpha_{2^{n-1}} = (10 \cdots 0), \ \ldots, \ \alpha_{2^n - 1} = (11 \cdots 1).$$

Definition 1 *Let $f(x)$ be a function from V_n to $GF(2)$ (simply, a function on V_n). We call the (1 -1)-sequence $\eta_f = ((-1)^{f(\alpha_0)} \ (-1)^{f(\alpha_1)} \ \ldots \ (-1)^{f(\alpha_{2^n-1})})$ the* sequence *of $f(x)$. $f(x)$ is called the* function *of η_f. The (0, 1)-sequence $(f(\alpha_0) \ f(\alpha_1) \ \ldots \ f(\alpha_{2^n-1}))$ is called the* truth table *of $f(x)$. In particular, if the truth table of $f(x)$ has 2^{n-1} zeros (ones) $f(x)$ is called* 0-1 balanced.

Let $\xi = (a_1 \cdots a_{2^n})$ and $\eta = (b_1 \cdots b_{2^n})$ be (1 , -1)-sequences of length 2^n. The operation $*$ between ξ and η, denoted by $\xi * \eta$, is the sequence $(a_1 b_1 \cdots a_{2^n} b_{2^n})$. Obviously if ξ and η are the sequences of functions $f(x)$ and $g(x)$ on V_n respectively then $\xi * \eta$ is the sequence of $f(x) + g(x)$.

Definition 2 *We call the function $h(x) = a_1 x_1 + \cdots + a_n x_n + c$, $a_j, c \in GF(2)$, an* affine function, *in particular, $h(x)$ will be called a* linear function *if the constant $c = 0$. The sequence of an affine function (a linear function) will be called an* affine sequence *(a* linear sequence*).*

*Supported in part by the Australian Research Council under the reference numbers A49130102, A9030136, A49131885 and A49232172.
†Supported in part by the Australian Research Council under the reference number A49130102.

Definition 3 *Let f and g be functions on V_n. $d(f,g) = \sum_{f(x)\neq g(x)} 1$ is called the* Hamming distance *between f and g. Let $\varphi_1, \ldots, \varphi_{2^n}, \varphi_{2^n+1}, \ldots, \varphi_{2^{n+1}}$ be all affine functions on V_n. $N_f = min_{i=1,\ldots,2^{n+1}} d(f, \varphi_i)$ is called the* nonlinearity *of $f(x)$.*

The nonlinearity is a crucial criterion for a good cryptographic design. It prevents the cryptosystems from being attacked by a set of linear equations. The concept of nonlinearity was introduced by Pieprzyk and Finkelstein [16].

Definition 4 *Let $f(x)$ be a function on V_n. If $f(x)+f(x+\alpha)$ is 0-1 balanced for every $\alpha \in V_n$, $W(\alpha)=1$, where $W(\alpha)$ denotes the number of nonzero coordinates of α (*Hamming weight*) of α, we say that $f(x)$ satisfies the* strict avalanche criterion *(SAC).*

We can give an equivalent description of SAC: let f be a function on V_n. If if we change any single input the probability that the output changes is $\frac{1}{2}$ (see [2]). The strict avalanche criterion was originally defined in [20], [21], later it has been generalized in many ways [2], [3], [6], [10], [13], [18]. The SAC is relevant to the completeness and the avalanche effect. The 0-1 balancedness, the nonlinearity and the avalanche criterion are important criteria for cryptographic functions [1], [3], [4], [13].

Definition 5 *A (1, -1)-matrix H of order h will be called an* Hadamard matrix *if $HH^T = hI_h$.*

If h is the order of an Hadamard matrix then h is 1, 2 or divisible by 4 [19]. A special kind of Hadamard matrix, defined as follows will be relevant:

Definition 6 *The* Sylvester-Hadamard matrix *(or* Walsh-Hadamard matrix*) of order 2^n, denoted by H_n, is generated by the recursive relation*

$$H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}, \quad n = 1, 2, \ldots, \quad H_0 = 1.$$

Definition 7 *Let $f(x)$ be a function from V_n to $GF(2)$. If*

$$2^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(x)+\langle \beta, x \rangle} = \pm 1,$$

for every $\beta \in V_n$. We call $f(x)$ a bent function *on V_n.*

¿From Definition 7, bent functions on V_n only exist for even n. Bent functions were first introduced and studied by Rothaus [17]. Further properties, constructions and equivalence bounds for bent functions can be found in [1], [7], [9], [15], [22]. Kumar, Scholtz and Welch [8] defined and studied the bent functions from Z_q^n to Z_q. Bent functions are useful for digital communications, coding theory and cryptography [2], [4], [9], [11], [12], [13], [14], [15]. Bent functions on V_n (n is even) not only attain the upper bound of nonlinearity, $2^{n-1} - 2^{\frac{1}{2}n-1}$, but also satisfy SAC. However 0-1 balancedness is often required in cryptosystems and bent functions are not 0-1 balanced since the Hamming weight of bent functions on V_n is $2^{n-1} \pm 2^{\frac{1}{2}n-1}$ [17]. In this paper we construct 0-1 balanced functions with high nonlinearity satisfying high-order SAC from bent functions.

Notation 1 *Let X be an indeterminant. We give X a binary subscript that is $X_{i_1 \cdots i_n}$ where $i_1, \ldots, i_n \in GF(2)$. For any sequence of constants $i_1, \ldots, i_p$ from $GF(2)$ define a function $D_{i_1 \cdots i_p}$ from V_p to $GF(2)$ by*

$$D_{i_1 \cdots i_p}(y_1, \ldots, y_p) = (y_1 + \bar{i_1}) \cdots (y_p + \bar{i_p})$$

where $\bar{i} = 1 + i$ is the complement of i modulo 2.

2 The Properties of Balancedness and Nonlinearity

Lemma 1 *Let $\xi_{i_1 \cdots i_p}$ be the sequence of a function $f_{i_1 \cdots i_p}(x_1, \cdots, x_q)$ from V_q to $GF(2)$. Write $\xi = (\xi_{0\cdots 00}\ \xi_{0\cdots 01}\ \cdots\ \xi_{1\cdots 11})$ for the concatenation of $\xi_{0\cdots 00}$, $\xi_{0\cdots 01}$, $\cdots$, $\xi_{1\cdots 11}$. Then ξ is the sequence of the function from V_{q+p} to $GF(2)$ given by*

$$f(y_1, \ldots, y_p, x_1, \ldots, x_q) = \sum_{(i_1 \cdots i_p) \in V_p} D_{i_1 \cdots i_p}(y_1, \ldots, y_p) f_{i_1 \ldots i_p}(x_1, \cdots, x_q).$$

Proof. It is obvious that:

$$D_{i_1\cdots i_p}(y_1,\dots,y_p) = \begin{cases} 1 & \text{if } (y_1\cdots y_p) = (i_1\cdots i_p)\ , \\ 0 & \text{otherwise.}\end{cases}$$

Hence, by exhaustive choice,

$$f(i_1,\dots,i_p,x_1,\dots,x_q) = D_{i_1\cdots i_p}(i_1,\dots,i_p)f_{i_1\dots i_p}(x_1,\cdots,x_q) = f_{i_1\dots i_p}(x_1,\cdots,x_q).$$

By the definition of sequence of functions (Definition 1) the lemma is true. □
□

Lemma 2 *Write* $H_n = \begin{bmatrix} l_0 \\ l_1 \\ \vdots \\ l_{2^n-1}\end{bmatrix}$ *where l_i is a row of H_n. Then l_i is the sequence of $h_i(x) = \langle \alpha_i, x\rangle$ where α_i is defined before Definition 1.*

Proof. By induction on n. Let $n = 1$. Since $H_1 = \begin{bmatrix} + & + \\ + & - \end{bmatrix}$, $l_0 = (+\,+)$, the sequence of $\langle 0, x\rangle$ and $l_1 = (+\,-)$, the sequence of $\langle 1, x\rangle$ where $x \in V_1$, $+$ and $-$ stand for 1 and -1 respectively. Suppose the lemma is true for $n = 1, 2, \dots, k-1$.

Since $H_k = H_1 \times H_{k-1}$, where $\times$ is the Kronecker product, each row of H_n can be expressed as $\delta \times l$ where $\delta = (+\,+)$ or $(+\,-)$, and l is a row of H_{n-1}. By the assumption l is the sequence of a function, say $h(x) = \langle \alpha, x\rangle$, where $\alpha, x \in V_{k-1}$. Thus $\delta \times l$ is the sequence of $\langle \beta, y\rangle$ where $y \in V_k$, $\beta = (0\ \alpha)$ or $(1\ \alpha)$ according as $\delta = (+\,+)$ or $(+\,-)$. Thus the lemma is true for $n = k$. □
□

¿From Lemma 10 all the rows of H_n comprise all the sequences of linear functions on V_n and hence all the rows of $\pm H_n$ comprise all the sequences of affine functions on V_n.

Lemma 3 *Let f and g be functions on V_n whose sequences are η_f and η_g respectively. Then $d(f,g) = 2^{n-1} - \frac{1}{2}\langle \eta_f, \eta_g\rangle$.*

Proof. $\langle \eta_f, \eta_g\rangle = \sum_{f(x)=g(x)} 1 - \sum_{f(x)\neq g(x)} 1 = 2^n - 2\sum_{f(x)\neq g(x)} 1 = 2^n - 2d(f,g)$. This proves the lemma. □
□

Let $H_n = (h_{ij})$ and $L_i = (h_{i1}\cdots h_{i2^n})$ i.e. the i-th row of H_n. Write $L_{i+2^n} = -L_i$, $i = 1,\dots,2^n$. Since L_i, $i = 1,\dots,2^n$, is a linear sequence L_1, …, L_{2^n}, L_{2^n+1}, …, $L_{2^{n+1}}$ comprise all affine sequences. Let f be a function on V_n whose sequence is η_f and φ_i be the function of L_i.

Write $\eta_f = (a_1 \cdots a_{2^n})$. Since $\langle \eta_f, L_i\rangle = \sum_{j=1}^{2^n} a_j h_{ij}$

$$\langle \eta_f, L_i\rangle^2 = 2^n + 2\sum_{j<t} a_j a_t h_{ij} h_{it}. \tag{1}$$

and

$$\sum_{i=1}^{2^n}\langle \eta_f, L_i\rangle^2 = 2^{2n} + 2\sum_{i=1}^{2^n}\sum_{j<t} a_j a_t h_{ij} h_{it} = 2^{2n} + 2\sum_{j<t} a_j a_t \sum_{i=1}^{2^n} h_{ij} h_{it}.$$

Since H_n is an Hadamard matrix $\sum_{i=1}^{2^n} h_{ij}h_{it} = 0$ for $j \neq t$ and hence

$$\sum_{i=1}^{2^n}\langle \eta_f, L_i\rangle^2 = 2^{2n}. \tag{2}$$

Thus there exists an integer, say i_0, such that $\langle \eta_f, L_{i_0}\rangle^2 = \langle \eta_f, L_{i_0+2^n}\rangle^2 \geqq 2^n$ and hence $\langle \eta_f, L_{i_0}\rangle \geqq 2^{\frac{1}{2}n}$ or $\langle \eta_f, L_{i_0+2^n}\rangle \geqq 2^{\frac{1}{2}n}$. Without any loss of generality suppose $\langle \eta_f, L_{i_0}\rangle \geqq 2^{\frac{1}{2}n}$. By Lemma 11 $d(f, \varphi_{i_0}) \leqq 2^{n-1} - 2^{\frac{1}{2}n-1}$. This proves

Lemma 4 *$N_f \leqq 2^{n-1} - 2^{\frac{1}{2}n-1}$ for any function on V_n.*

Lemma 5 *If both (0, 1)-sequences ξ and η of length $2t$ consist of an even number of ones and an even number of minus ones then $d(\xi, \eta)$ is even.*

Proof. Write $\xi = (a_1 \cdots a_{2t})$ and $\eta = (b_1 \cdots b_{2t})$. Let n_1 denote the number of pairs (a_i, b_i) such that $a_i = 1$, $b_i = 1$; let n_2 denote the number of pairs (a_i, b_i) such that $a_i = 1$, $b_i = 0$; let n_3 denote the number of pairs (a_i, b_i) such that $a_i = 0$, $b_i = 1$; and let n_4 denote the number of pairs (a_i, b_i) such that $a_i = 0$, $b_i = 0$. Hence $n_1 + n_2$, $n_3 + n_4$, $n_1 + n_3$ and $n_2 + n_4$ are all even and hence $2n_1 + n_2 + n_3$ is even. Thus $n_2 + n_3 = d(\xi, \eta)$ is even. □

□

The following result can be found in [5]

Lemma 6 *Let $f(x)$ be a function from V_n to $GF(2)$. $f(x)$ and ξ be the sequence of $f(x)$. Then the following four statements are equivalent*

(i) $f(x)$ is bent,

(ii) for any affine sequence of length 2^n, denoted by l, $\langle \xi, l \rangle = \pm 2^{\frac{1}{2}n}$,

(iii) $f(x) + f(x + \alpha)$ is 0-1 balanced for every nonzero $\alpha \in V_n$,

(iv) $f(x) + \langle \alpha, x \rangle$ contains $2^{n-1} \pm 2^{\frac{1}{2}n-1}$ zeros for every $\alpha \in V_n$.

Let L_j and φ, $j = 1, \ldots, 2^{n+1}$, be the same as in the proof of Lemma 12. If f is a bent function then $\langle \eta_f, L_i \rangle^2 = 2^n$ and hence $\langle \eta_f, L_i \rangle = 2^{\frac{1}{2}n}$ or $\langle \eta_f, L_{i+2^n} \rangle = 2^{\frac{1}{2}n}$ for each fixed i, $1 \leqq i \leqq 2^n$. By Lemma 11 $d(f, \varphi_i) = 2^{n-1} - 2^{\frac{1}{2}n-1}$ or $d(f, \varphi_{i+2^n}) = 2^{n-1} - 2^{\frac{1}{2}n-1}$ for each fixed i, $1 \leqq i \leqq 2^n$. Thus $N_f = 2^{n-1} - 2^{\frac{1}{2}n-1}$. In other words, bent functions attain the upper bound for nonlinearities given in Lemma 12. Conversely, if a function f on V_n attains the upper bound for nonlinearities, $2^{n-1} - 2^{\frac{1}{2}n-1}$, then $\langle \eta_f, L_i \rangle^2 = 2^n$ for $i = 1, \ldots, 2^{n+1}$ i.e. f is bent, otherwise $\langle \eta_f, L_i \rangle^2 = 2^n$ does not hold for some i, $1 \leqq i \leqq 2^{n+1}$. Note that $L_{i+2^n} = -L_i$. ¿From (2) there exist i_1 and i_2, $1 \leqq i_1, i_2, \leqq 2^n$, such that $\langle \eta_f, L_{i_1} \rangle^2 > 2^n$ and $\langle \eta_f, L_{i_2} \rangle^2 < 2^n$. Thus $\langle \eta_f, L_{i_1} \rangle > 2^{\frac{1}{2}n}$ or $\langle \eta_f, L_{i_1+2^n} \rangle > 2^{\frac{1}{2}n}$. Without any loss generality, suppose $\langle \eta_f, L_{i_1} \rangle > 2^{\frac{1}{2}n}$. By using Lemma 11 $d(f, \varphi_{i_1}) < 2^{n-1} - 2^{\frac{1}{2}n-1}$ and hence $N_f < 2^{n-1} - 2^{\frac{1}{2}n-1}$. This is a contradiction to the assumption that f attains the maximum nonlinearity $2^{n-1} - 2^{\frac{1}{2}n-1}$. Hence we have proved

Corollary 1 *A function on V_n attains the upper bound for nonlinearities, $2^{n-1} - 2^{\frac{1}{2}n-1}$, if and only if it is bent.*

¿From (1) we have

Corollary 2 *Let f be a function on V_n whose sequence is $\eta_f = (a_1 \cdots a_{2^n})$. Then f is bent if and only if $\sum_{j<t} a_j a_t h_{ij} h_{it} = 0$ for $i = 1, \ldots, 2^n$ where $(h_{ij}) = H_n$.*

¿From Corollary 15 0-1 balanced functions cannot attain the upper bound for nonlinearities $2^{n-1} - 2^{\frac{1}{2}n-1}$. However we can construct a class of 0-1 balanced functions with high nonlinearity by using bent functions.

Corollary 3 *Let f be a 0-1 balanced function on V_n ($n \geqq 3$). Then $N_f \leqq 2^{n-1} - 2^{\frac{1}{2}n-1} - 2$ if n is even number and $N_f \leqq \lfloor\lfloor 2^{n-1} - 2^{\frac{1}{2}n-1} \rfloor\rfloor$ if n is odd where $\lfloor\lfloor x \rfloor\rfloor$ denotes the maximum even number less than or equal to x.*

Proof. Note that f and each φ_i, where φ_i is the same as in Definition 3, have an even number of ones and an even of number of zeros. By Lemma 13 $d(f, \varphi_i)$ is even. By corollary 15 $d(f, \varphi_i) < 2^{n-1} - 2^{\frac{1}{2}n-1}$. This proves the corollary. □

□

Lemma 7 *Let $f_j(x_1, \ldots, x_{2k})$ be a bent function on V_{2k}, $j = 1, 2$. Set*

$$g(u, x_1, \ldots, x_{2k}) = (1 + u) f_1(x) + u f_2(x).$$

Then $N_g \geqq 2^{2k} - 2^k$.

Proof. Write ξ_j for the sequence of f_j, $j = 1, 2$. By Lemma 9 $\gamma = (\xi_1\ \xi_2)$ is the sequence of g, of length 2^{2k+1}. Let L be the sequence of an affine function, say φ. By Lemma 10 L is a row of $\pm H_{2k+1}$. Since $H_{2k+1} = H_1 \times H_{2k}$ and $H_1 = \begin{bmatrix} + & + \\ + & - \end{bmatrix}$, where $\times$ is the Kronecker product, L can be expressed as $L = (l'\ l')$ or $L = (l'\ \ -l')$, by Lemma 10, where l' is a row of $\pm H_{2k}$. Since both f_j and $f_j + h$ are bent, by (ii) of Lemma 14, $\langle \xi_j, l' \rangle = \pm 2^k$. $\langle \gamma, L \rangle = \langle \xi_1, l' \rangle \pm \langle \xi_2, l' \rangle$. Thus $|\langle \gamma, L \rangle| \leqq 2^{k+1}$. By Lemma 11 $d(g, \varphi) \geqq 2^{2k} - 2^k$. Since φ is arbitrary $N_g \geqq 2^{2k} - 2^k$. □

□

Lemma 8 *Let $f_j(x_1, \ldots, x_{2k-2})$ be a bent function on V_{2k-2}, $j = 1, 2, 3, 4$. Set*

$$g(u, v, x_1, \ldots, x_{2k-2}) = (1 + u)(1 + v)f_1(x) + (1 + u)vf_2(x) + u(1 + v)f_3(x) + uvf_4(x).$$

Then $N_g \geqq 2^{2k-1} - 2^k$.

Proof. Let ξ_j be the sequence of $f_j(x)$, $j = 1, 2, 3, 4$ and $\eta = (\xi_1\ \xi_2\ \xi_3\ \xi_4)$ be the sequence of g. Let L be an affine sequence of length 2^{2k} whose function is $h(z)$, an affine function. By Lemma 10 L is a row of $\pm H_{2k}$. Since $H_{2k} = H_2 \times H_{2k-2}$ and L can be expressed as $L = l_2 \times l_{k-2}$ where l_2 is a row of $\pm H_2$ and l_{2k-2} is a row of $\pm H_{2k-2}$. Since each ξ_i is bent, by (ii) of Lemma 14, $\langle \xi_i, l \rangle = \pm 2^{k-1}$. Note that $|\langle \eta, L \rangle| \leqq \sum_{i=1}^{4} |\langle \xi_i, l \rangle|$ and hence $|\langle \eta, L \rangle| \leqq 4 \cdot 2^{k-1}$. By Lemma 11 $d(g, h) \geqq 2^{2k-1} - 2^k$. Since h is an arbitrary affine function $N_g \geqq 2^{2k-1} - 2^k$. □

□

Lemma 9 *$f_1(x_1, \ldots, x_n) + f_2(u_1, \ldots, u_t)$ is a 0-1 balanced function on V_{n+t} if f_1 is a 0-1 balanced function on V_n or f_2 is a 0-1 balanced function on V_t.*

Proof. Set $g(x_1, \ldots, x_n, u_1, \ldots, u_t) = f_1(x_1, \ldots, x_n) + f_2(u_1, \ldots, u_t)$. Without any loss of generality, suppose f_1 is a 0-1 balanced function on V_n. Note that for every fixed $(u_1^0 \cdots u_t^0) \in V_t$, $g(x_1, \ldots, x_n, u_1^0, \ldots, u_t^0) = f_1(x_1, \ldots, x_n) + f_2(u_1^0, \ldots, u_t^0)$ is a 0-1 balanced function on V_n thus $g(x_1, \ldots, x_n, u_1, \ldots, u_t)$ is a 0-1 balanced function on V_{n+t}. □

□

3 Construction

3.1 On V_{2k+1}

Let $k \geqq 1$ and $f(x_1, \ldots, x_{2k})$ be a bent function on V_{2k}. Write $x = (x_1 \cdots x_{2k})$. Let $h(x)$ be a non-constant affine function on V_{2k}. Note that $f(x) + h(x)$ is also bent (see Property 2, p95, [8]) and hence $f + h$ assumes the value zero $2^{2k-1} \pm 2^{k-1}$ times and assumes the value one $2^{2k-1} \mp 2^{k-1}$ times.

Without any loss of generality we suppose $f(x)$ assumes the value zero $2^{2k-1} + 2^{k-1}$ times (if $f(x)$ assumes the value zero $2^{2k-1} - 2^{k-1}$ times, the bent function $f(x) + 1$ assumes the value zero $2^{2k-1} + 2^{k-1}$ times and hence we can replace $f(x)$ by $f(x) + 1$). Also we suppose $f(x) + h(x)$ assumes the value zero $2^{2k-1} - 2^{k-1}$ times (if $f(x) + h(x)$ assumes the value zero $2^{2k-1} + 2^{k-1}$ times, the bent function $f(x) + h(x) + 1$ assumes the value zero $2^{2k-1} - 2^{k-1}$ times so we can replace $f(x) + h(x)$ by $f(x) + h(x) + 1$). Set

$$g(u, x_1, \ldots, x_{2k}) = f(x_1, \ldots, x_{2k}) + uh(x_1, \ldots, x_{2k}). \tag{3}$$

Lemma 10 *$g(u, x_1, \ldots, x_{2k})$ defined by (3) is a 0-1 balanced function on V_{2k+1}.*

Proof. Note that $g(0, x_1, \ldots, x_{2k}) = f(x_1, \ldots, x_{2k})$ assumes the value zero $2^{2k-1} + 2^{k-1}$ times and $g(1, x_1, \ldots, x_{2k}) = f(x_1, \ldots, x_{2k}) + h(x_1, \ldots, x_{2k})$ assumes the value zero $2^{2k-1} - 2^{k-1}$ times. Thus $g(u, x_1, \ldots, x_{2k})$ assumes the value zero 2^k times (one 2^k times). □

□

Lemma 11 *$N_g \geqq 2^{2k} - 2^k$ where g is defined by (3).*

Proof. $g = f + uh = (1+u)f + u(f+h)$. Note that both f and $f+h$ are bent functions on V_{2k}. By Lemma 18 $N_g \geqq 2^{2k} - 2^k$. □

□

Lemma 12 *$g(u, x_1, \ldots, x_{2k})$ defined by (3) satisfies the strict avalanche criterion.*

Proof. Let $\gamma = (b\ a_1 \cdots a_{2k})$ with $W(\gamma) = 1$. Write $\alpha = (a_1 \cdots a_{2k})$, $z = (u\ x_1 \ldots x_{2k})$ and $x = (x_1 \ldots x_{2k})$. $g(z+\gamma) = f(x+\alpha) + (u+b)h(x+\alpha)$ and hence $g(z) + g(z+\gamma) = f(x) + f(x+\alpha) + u(h(x) + h(x+\alpha)) + bh(x+\alpha)$.

Case 1: $b = 0$ and hence $W(\alpha) = 1$. $g(z) + g(z+\gamma) = f(x) + f(x+\alpha) + u(h(x) + h(x+\alpha))$. Since h is a non-constant affine function $h(x) + h(x+\alpha) = c$ where c is a constant. Thus $g(z) + g(z+\gamma) = f(x) + f(x+\alpha) + cu$. By (iii) of Lemma 14 $f(x) + f(x+\alpha)$ is a 0-1 balanced function on V_{2k} and hence by Lemma 20 $g(z) + g(z+\gamma)$ is a 0-1 balanced function on V_{2k+1}.

Case 2: $b = 1$ and hence $W(\alpha) = 0$ i.e. $\alpha = 0$. $g(z) + g(z+\gamma) = h(x)$. Since $h(x)$ is a non-constant affine function on V_{2k} $h(x)$ is a 0-1 balanced and hence by Lemma 20 $g(z) + g(z+\alpha)$ is a 0-1 balanced function on V_{2k+1}. □

□

Summarizing Lemmas 21, 22, 23 we have

Theorem 1 *For $k \geqq 1$, $g(u, x_1, \ldots, x_{2k})$ defined by (3) is a 0-1 balanced function on V_{2k+1} having $N_g \geqq 2^{2k} - 2^k$ and satisfying the strict avalanche criterion.*

3.2 On V_{2k}

Let $k \geqq 2$ and $f(x_1, \ldots, x_{2k-2})$ be bent function on V_{2k-2}. Write $x = (x_1 \cdots x_{2k-2})$. Let $h_j(x)$, $j = 1, 2, 3$, be three non-constant affine functions on V_{2k-2} such that $h_i(x) + h_j(x)$ is non-constant for any $i \neq j$. Such $h_1(x)$, $h_2(x)$, $h_3(x)$ exist for $k \geqq 2$. Note that each $f(x) + h_j(x)$ is also bent (see Property 2, p95, [8]) and hence $f + h_j$ assumes the value zero $2^{2k-3} \pm 2^{k-2}$ times and assumes the value one $2^{2k-3} \mp 2^{k-2}$ times.

Without any loss of generality we suppose both $f(x)$ and $f(x) + h_1(x)$ assume the value zero $2^{2k-3} + 2^{k-2}$ times and both $f(x) + h_2(x)$ and $f(x) + h_3(x)$ assume the value zero $2^{2k-3} - 2^{k-2}$ times. This assumption is reasonable because $f(x) + h_j(x)$ assumes the value zero $2^{2k-3} - 2^{k-2}$ times if and only if $f(x) + h_j(x) + 1$ assumes the value zero $2^{2k-3} + 2^{k-2}$ times and $h_j(x) + 1$ is also a non-constant affine function thus we can choose one of $f(x) + h_j(x)$ and $f(x) + h_j(x) + 1$ so that the assumption is satisfied. Set

$$\begin{aligned} & g(u, v, x_1, \ldots, x_{2k-2}) = \\ & \qquad f(x) + vh_1(x) + uh_2(x) + uv(h_1(x) + h_2(x) + h_3(x)). \end{aligned} \tag{4}$$

Lemma 13 *$g(u, v, x_1, \ldots, x_{2k-2})$ defined by (4) is a 0-1 balanced function on V_{2k}.*

Proof. Note that $g(0, 0, x_1, \ldots, x_{2k-2}) = f(x)$, $g(0, 1, x_1, \ldots, x_{2k-2}) = f(x) + h_1(x)$, $g(1, 0, x_1, \ldots, x_{2k-2}) = f(x) + h_2(x)$, $g(1, 1, x_1, \ldots, x_{2k-2}) = f(x) + h_1(x) + h_2(x) + (h_1(x) + h_2(x) + h_3(x)) = f(x) + h_3(x)$. By the assumption the first two functions assume the value zero $2^{2k-2} + 2^{k-1}$ times in total and the second two functions assume the value zero $2^{2k-2} - 2^{k-1}$ times in total. Hence $g(u, v, x_1, \ldots, x_{2k-2})$ assumes the value zero 2^{2k-1} times in total and thus it is a 0-1 balanced function on V_{2k}. □

□

Lemma 14 *$N_g \geqq 2^{2k-1} - 2^k$ where g is defined by (4).*

Proof. Note that $g = f(x) + vh_1(x) + uh_2(x) + uv(h_1(x) + h_2(x) + h_3(x)) = (1+u)(1+v)f(x) + (1+u)v(f(x) + h_1(x)) + u(1+v)(f(x) + h_2(x)) + uv(f(x) + h_3(x))$. By Lemma 19 $N_g \geqq 2^{2k-1} - 2^k$. □

□

Lemma 15 *$g(u, v, x_1, \ldots, x_{2k-2})$ defined by (4) satisfies the strict avalanche criterion.*

Proof. Let $\gamma = (b\ c\ a_1 \cdots a_{2k-2})$ with $W(\gamma) = 1$. Write $\alpha = (a_1 \cdots a_{2k-2})$, $z = (u\ v\ x_1 \ldots x_{2k-2})$ and $x = (x_1 \ldots x_{2k-2})$.

Note that $g(z+\gamma) = f(x+\alpha)+(v+c)h_1(x+\alpha)+(u+b)h_2(x+\alpha)+(u+b)(v+c)(h_1(x+\alpha)+h_2(x+\alpha)+h_3(x+\alpha))$.

Case 1: $b = 1$ and hence $c = 0$, $W(\alpha) = 0$ i.e. $\alpha = 0$. $g(z) + g(z+\gamma) = h_2(x) + v(h_1(x) + h_2(x) + h_3(x))$ will be $h_2(x)$ when $v = 0$ and $h_1(x) + h_3(x)$ when $v = 1$. Both $h_2(x)$ and $h_1(x) + h_3(x)$ are non-constant affine functions on V_{2k-2} and hence $g(z) + g(z+\gamma)$ is 0-1 balanced on V_{2k}.

Case 2: $c = 1$ and hence $b = 0$, $W(\alpha) = 0$ i.e. $\alpha = 0$. The proof is similar to Case 1.

Case 3: $W(\alpha) \neq 0$ and hence $b = c = 0$. Since h_j is an affine function we can write $h_j(x) + h_j(x+\alpha) = a_j$ where a_j is a constant. Hence $g(z) + g(z+\gamma) = f(x) + f(x+\alpha) + va_1 + ua_2 + uv(a_1 + a_2 + a_3)$. By (iii) of Lemma 14 $f(x) + f(x+\alpha)$ is a 0-1 balanced function on V_{2k-2} and hence by Lemma 20 $g(z) + g(z+\gamma)$ is a 0-1 balanced function on V_{2k}. This proves that $g(u, v, x_1, \ldots, x_{2k-2})$ satisfies the strict avalanche criterion. □

□

Summarizing Lemmas 25, 26, 27 we have

Theorem 2 *For $k \geqq 2$, $g(u, v, x_1, \ldots, x_{2k-2})$ defined by (4) is a 0-1 balanced function on V_{2k} having $N_g \geqq 2^{2k-2} - 2^k$ and satisfying the strict avalanche criterion.*

4 Remarks

We note that the nonlinearities of 0-1 balanced functions satisfying SAC in Theorems 24 and 28 are the same as those for ordinary 0-1 balanced functions (see [13]). Next we give two examples of the theorems.

Example 1 *In Theorem 24 let $k = 2$. Consider V_5. As we know, $f(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4$ is a bent function in V_4. Choose the non-constant affine function $h(x_1, x_2, x_3, x_4) = 1 + x_1 + x_2 + x_3 + x_4$. Note f assumes the value zero $2^{4-1} + 2^{2-1} = 10$ times and $f + h$ assumes the value zero $2^{4-1} - 2^{2-1} = 6$ times. Hence we set $g(u, x_1, x_2, x_3, x_4) = f(x_1, x_2, x_3, x_4) + uh(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4 + u(1 + x_1 + x_2 + x_3 + x_4)$. By Theorem 24 $g(u, x_1, x_2, x_3, x_4)$ is a 0-1 balanced function with $N_g \geqq 2^4 - 2^2 = 12$, satisfying the strict avalanche criterion. On the other hand, by Corollary 17 the bound for nonlinearly 0-1 balanced functions on V_5 is $\lfloor\lfloor 2^4 - 2^{2-\frac{1}{2}} \rfloor\rfloor = \lfloor\lfloor 13.1818\cdots \rfloor\rfloor = 12$ where $\lfloor\lfloor x \rfloor\rfloor$ denotes the maximum even number no larger than x. This means that $N_g = 12$ attains the upper bound for nonlinearly 0-1 balanced functions on V_5.*

Example 2 *In Theorem 28 let $k = 3$. Consider V_6. Choose $f(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4$, a bent function in V_4. Also choose non-constant affine functions $h_1(x_1, x_2, x_3, x_4) = x_1$, $h_2(x_1, x_2, x_3, x_4) = 1 + x_2$, $h_3(x_1, x_2, x_3, x_4) = 1 + x_3$. Note both f and $f + h_1$ assume the value zero $2^{4-1} + 2^{2-1} = 10$ times and both $f + h_3$ and $f + h_4$ assume the value zero $2^{4-1} - 2^{2-1} = 6$ times. Hence we set $g(u, v, x_1, x_2, x_3, x_4) = f + vh_1 + uh_2 + uv(h_1 + h_2 + h_3)$. By Theorem 28 $g(u, v, x_1, x_2, x_3, x_4)$ is a 0-1 balanced function with $N_g \geqq 2^5 - 2^3 = 24$, satisfying the strict avalanche criterion. On the other hand, by Corollary 17 the upper bound for nonlinearly 0-1 balanced functions on V_6 is $2^5 - 2^2 - 2 = 26$. This means that $N_g = 24$ is very high.*

Recently Zheng, Pieprzyk and Seberry [23] constructed a very efficient one way hashing algorithm using boolean functions constructed by the method given in Theorem 24. These functions have further cryptographically useful properties.

References

[1] C. M. Adams and S. E. Tavares. Generating and counting binary bent sequences. *IEEE Transactions on Information Theory*, IT-36 No. 5:1170–1173, 1990.

[2] C. M. Adams and S. E. Tavares. The use of bent sequences to achieve higher-order strict avalanche criterion. to appear, 1990.

[3] M. H. Dawson and S. E. Tavares. An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks. In *Advances in Cryptology-EUROCRYPT'91*, volume 547, Lecture Notes in Computer Science, pages 352–367. Springer-Verlag, 1991.

[4] John Detombe and Stafford Tavares. Constructing large cryptographically strong S-boxes. Presented in AUSCRYPT'92, 1992.

[5] J. F. Dillon. A survey of bent functions. *NSA Mathematical Meeting*, pages 191–215, 1972.

[6] R. Forre. The strict avalanche criterion: Special properties of boolean functions and extended definition. In *Advances in Cryptology: Crypto'88 Proceedings*, volume 403, Lecture Notes in Computer Science, pages 450–468. Springer-Verlag, New York, 1989.

[7] P. V. Kumar and R. A. Scholtz. Bounds on the linear span of bent sequences. *IEEE Transactions on Information Theory*, IT-29 No. 6:854–862, 1983.

[8] P. V. Kumar, R. A. Scholtz, and L. R. Welch. Generalized bent functions and their properties. *Journal of Combinatorial Theory*, Ser. A, 40:90–107, 1985.

[9] A. Lempel and M. Cohn. Maximal families of bent sequences. *IEEE Transactions on Information Theory*, IT-28 No. 6:865–868, 1982.

[10] S Lloyd. Couting functions satisfying a higher order strict avalanche criterion. In *Advances in Cryptology-EUROCRYPT'89*, volume 434, Lecture Notes in Computer Science, pages 64–74. Springer-Verlag, New York, 1990.

[11] V. V. Losev. Decoding of sequences of bent functions by means of a fast Hadamard transform. *Radiotechnika i elektronika*, 7:1479–1492, 1987.

[12] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. New York: North-Holland, 1977.

[13] Willi Meier and Othmar Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology-EUROCRYPT'89*, volume 434, Lecture Notes in Computer Science, pages 549–562. Springer-Verlag, 1990.

[14] Kaisa Nyberg. Perfect nonlinear S-boxes. In *Advances in Cryptology-EUROCRYPT'91*, volume 547, Lecture Notes in Computer Science, pages 378–386. Springer-Verlag, 1991.

[15] J. D. Olsen, R. A. Scholtz, and L. R. Welch. Bent-function sequences. *IEEE Transactions on Information Theory*, IT-28 No. 6:858–864, 1982.

[16] J. Pieprzyk and G. Finkelstein. Towards effective nonlinear cryptosystem design. *IEE Proceedings (Part E)*, 135:325–335, 1988.

[17] O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.

[18] S. E. Tavares, M. Sivabalan, and L. E. Peppard. On the designs of SP networks from an information theoretic point of view. In *Advances in Cryptology: Crypto'92 Proceedings*, 1992.

[19] W. D. Wallis, A. Penfold Street, and J. Seberry Wallis. *Combinatorics: Room Squares, sum-free sets, Hadamard Matrices*, volume 292 of Lecture Notes in Mathematics. Springer-Verlag, Berlin- Heidelberg- New York, 1972.

[20] A. F. Webster. *Plaintext/Ciphertext Bit Dependencies in Cryptographic System*. Master's Thesis, Department of Electrical Engineering, Queen's University, 1985.

[21] A. F. Webster and S. E. Tavares. On the designs of S-boxes. In *Advances in Cryptology: Crypto'85 Proceedings*, volume 219, Lecture Notes in Computer Science, pages 523–534. Springer-Verlag, New York, 1986.

[22] R. Yarlagadda and J. E. Hershey. Analysis and synthesis of bent sequences. *IEE Proceeding (Part E)*, 136:112–123, 1989.

[23] Yuliang Zheng, Josef Pieprzyk, and Jennifer Seberry. Haval — one-way hashing algorithm with variable length of output. Presented in AUSCRYPT'92, 1992.