Highly Nonlinear Balanced Boolean Functions Satisfying High Degree Propagation Criterion *

Jennifer Seberry
Xian-Mo Zhang
Yuliang Zheng

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

E-mail: {jennie,xianmo,yuliang}@cs.uow.edu.au
Phone: +61 42 21 4327
Fax: +61 42 21 4329

November 2, 1993

Abstract

Three of the most important nonlinearity criteria for cryptographically strong functions are balancedness, nonlinearity and propagation criterion. In this paper we study systematic methods for constructing highly nonlinear balanced Boolean functions satisfying the high degree propagation criterion. In particular, we present a method for constructing highly nonlinear balanced Boolean functions on V_{2k+1} satisfying the propagation criterion with respect to *all but one* vectors in V_{2k+1}, and a method for constructing highly nonlinear balanced Boolean functions on V_{2k} satisfying the propagation criterion with respect to *all but three* vectors in V_{2k}. We then show that the vectors where the propagation criterion is not satisfied can be moved upward in such a way that the functions constructed on V_{2k+1} satisfy the propagation criterion of degree $2k$, while the function constructed on V_{2k} satisfy the propagation criterion of degree $\frac{4}{3}k$. The moving technique does not alter the balancedness and nonlinearity of the functions. The methods are illustrated by concrete constructions of such cryptographically strong functions. The algebraic degrees of the functions are also discussed.

Key Words

Propagation Criterion, Strict Avalanche Criterion, Nonlinearity, S-box, Hadamard Matrix, Bent Functions, Boolean Functions.

1 Introduction

The propagation criterion is one of the most important nonlinearity criteria for the design of cryptographically strong Boolean functions [15]. A Boolean function of n input coordinates

*Preprint No. 93-1. Supported in part by the Australian Research Council (ARC) under the reference numbers A49130102, A9030136, A49131885 and A49232172.

is said to satisfy *the propagation criterion with respect to a non-zero vector* if complementing input coordinates according to the vector results in the output of the function being complemented 50% of the time over all possible input vectors, and to satisfy *the propagation criterion of degree k* if complementing k or less input coordinates results in the output of the function being complemented 50% of the time over all possible input vectors. It is well known that bent functions possess the highest nonlinearity and satisfy the propagation criterion with respect to *all* non-zero vectors [16]. However two drawbacks of bent functions prohibit their direct applications in practice. The first drawback is that they are not balanced, and the second drawback is that they exist only when the number of input coordinates is even. Cryptographic applications often require that when input coordinates of a Boolean function are selected independently, at random, the output of the function must behave as a uniformly distributed random variable. In other words, the function has to be balanced. Some practical applications need Boolean functions with an odd number of input coordinates.

This paper initiates the research into highly nonlinear balanced functions satisfying the propagation criterion. We present two methods, one for odd n and the other for even n, for constructing balanced functions satisfying the high degree propagation criterion, where n is the number of input coordinates. More precisely, when n is odd, we construct balanced functions that satisfy the propagation criterion with respect to *all but one* non-zero vectors, and when n is even, functions we construct are balanced and also satisfy the propagation criterion with respect to all but three non-zero vectors. We also show that the vectors where the propagation criterion is not satisfied can be transformed into other vectors. In particular, they can be transformed into vectors with a high Hamming weight. As a consequence, we obtain balanced functions satisfying the propagation criterion of degree $n-1$ when n is odd, and balanced functions satisfying the propagation criterion of degree $\frac{2}{3}n$ when n is even. It turns out that the non-linearity of the functions thus constructed is very high and comparable to the nonlinearity obtainable by any balanced functions (whether they satisfy the propagation criterion or not). In summary, we have the following results:

1. For any non-zero vector $\gamma^* \in V_{2k+1}$ ($k \geqq 1$), there exist balanced functions on V_{2k+1} satisfying the propagation criterion with respect to all non-zero vectors $\gamma \in V_{2k+1}$ with $\gamma \neq \gamma^*$. The nonlinearities of the functions are at least $2^{2k} - 2^k$.

   In particular, when $\gamma = (1, \ldots, 1, 1)$, g^* satisfies the propagation criterion of degree $2k$.

2. For any non-zero vector $\gamma_1^*, \gamma_2^* \in V_{2k}$ ($k \geqq 2$) with $\gamma_1^* \neq \gamma_2^*$, there exist balanced functions on V_{2k} satisfying the propagation criterion with respect to *all but three* non-zero vectors in V_{2k}. The three vectors where the propagation criterion is not satisfied are γ_1^*, γ_2^* and $\gamma_1^* \oplus \gamma_2^*$. The nonlinearities of the functions are at least $2^{2k-1} - 2^k$.

   When γ_1^* and γ_2^* are selected properly, g^* satisfies the propagation criterion of degree $\frac{4}{3}k$.

The organization of the rest part of the paper is as follows: in Section 2 we introduce notations and definitions used in this paper. In Section 3 we prove two results on the nonlinearity of certain forms of functions. Our construction methods for highly nonlinear balanced functions satisfying the propagation criterion with respect to all but one or three vectors are presented in Section 4, this is followed by the explanation of the vector-moving technique in Section 5. The technique allows us to move vectors where the propagation

criterion is not satisfied in such a way that the resulting functions may be used for some special cryptographic purposes or satisfy the high degree propagation criterion. The algebraic degrees of the functions constructed using our methods are discussed in the same section. To illustrate the methods, two concrete constructions are presented in Section 6. The paper is closed by a discussion of future work in Section 7.

2 Notations and Definitions

We consider functions from V_n to $GF(2)$ (or simply functions on V_n), where V_n is the vector space of n tuples of elements from $GF(2)$. These functions are also called Boolean functions. Let f be a function on V_n. The $(1,-1)$-sequence defined by $((-1)^{f(\alpha_0)},(-1)^{f(\alpha_1)},\ldots,(-1)^{f(\alpha_{2^n-1})})$ is called the *sequence* of f, and the $(0,1)$-sequence defined by $(f(\alpha_0),f(\alpha_1),\ldots,f(\alpha_{2^n-1}))$ is called the *truth table* of f, where $\alpha_0=(0,\ldots,0,0)$, $\alpha_1=(0,\ldots,0,1)$, ..., $\alpha_{2^{n-1}-1}=(1,\ldots,1,1)$. f is said *balanced* if its truth table has 2^{n-1} zeros (ones).

Obviously if $(a_0,\ldots,a_{2^n-1})$ and $(b_0,\ldots,b_{2^n-1})$ are the sequences of functions f_1 and f_2 on V_n respectively, then $(a_0b_0,\ldots,a_{2^n-1}b_{2^n-1})$ is the sequence of $f(x)\oplus g(x)$, where $x=(x_1,x_2,\ldots,x_n)$. In particular, $-(a_0,\ldots,a_{2^n-1})=(-a_0,\ldots,-a_{2^n-1})$ is the sequence of $1\oplus f_1(x)$.

An *affine* function f on V_n is a function that takes the form of $f(x)=a_1x_1\oplus\cdots\oplus a_nx_n\oplus c$, where $a_j,c\in GF(2)$, $j=1,2,\ldots,n$. Furthermore f is called a *linear* function if $c=0$. The sequence of an affine (or linear) function is called an *affine (or linear) sequence*. The *Hamming weight* of a vector $\alpha\in V_n$, denoted by $W(\alpha)$, is the number of ones in its truth table. Given two functions f and g on V_n, the *Hamming distance* between them is defined as $d(f,g)=W(f(x)\oplus g(x))$. The *nonlinearity* of f, denoted by N_f, is the minimal Hamming distance between f and all affine functions on V_n, i.e., $N_f=\min_{i=0,1,\ldots,2^{n+1}-1}d(f,\varphi_i)$ where φ_0, φ_1, ..., $\varphi_{2^{n+1}-1}$ denote the affine functions on V_n.

The following notation will be used in this paper. Let $\alpha=(a_1,\cdots,a_n)$ and $\beta=(b_1,\cdots,b_n)$ be two vectors (or sequences), the *scalar product* of α and β, denoted by $\langle\alpha,\beta\rangle$, is defined as the sum of the component-wise multiplications. In particular, when α and β are from V_n, $\langle\alpha,\beta\rangle=a_1b_1\oplus\cdots\oplus a_nb_n$, where the addition and the multiplication are over $GF(2)$, and when α and β are $(1,-1)$-sequences, $\langle\alpha,\beta\rangle=\sum_{i=1}^{n}a_ib_i$, where the addition and the multiplication are over the reals.

A $(1,-1)$-matrix H of order m is called a *Hadamard* matrix if $HH^t=mI_m$, where H^t is the transpose of H and I_m is the identity matrix of order m. It is well known that the order of a Hadamard matrix is 1, 2 or divisible by 4 [18]. A special kind of Hadamard matrix, called *Sylvester-Hadamard matrix* or *Walsh-Hadamard matrix*, will be relevant to this paper. A Sylvester-Hadamard matrix of order 2^n, denoted by H_n, is generated by the following recursive relation

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

The following notation will be used in the rest of the paper. Let $\delta=(i_1,i_2,\ldots,i_p)$ be a constant vector in V_p. Then D_δ is a function on V_p defined by

$$D_\delta(y_1,y_2,\ldots,y_p)=(y_1\oplus\bar{i_1})\cdots(y_p\oplus\bar{i_p})$$

where $\bar{x}$ denotes $1\oplus x$, the binary complement of x. This notation is very useful in obtaining the functional representation of a concatenated sequence. Let $f_{0\cdots0}(x_1,\ldots,x_q)$,

$f_{0\cdots1}(x_1,\ldots,x_q)$, ..., $f_{1\cdots1}(x_1,\ldots,x_q)$ be 2^p functions on V_q, each indexed by a vector in V_p, and let $\xi_{0\cdots0}$, $\xi_{0\cdots1}$, ..., $\xi_{1\cdots1}$ be their sequences. Let ξ be the concatenation of $\xi_{0\cdots0}$, $\xi_{0\cdots1}$, ..., $\xi_{1\cdots1}$ (i.e., $\xi = (\xi_{0\cdots0}, \xi_{0\cdots1}, \ldots, \xi_{1\cdots1})$). Then ξ is the sequence of the following function on V_{p+q}

$$f(y,x) = \bigoplus_{\delta \in V_p} D_\delta(y) f_\delta(x)$$

where $y = (y_1,\ldots,y_p)$ and $x = (x_1,\ldots,x_q)$. (See also Lemma 9 of [17]).

In particular, if ξ_1, ξ_2 are the sequences of functions f_1, f_2 on V_n, then $\eta = (\xi_1, \xi_2)$ is the sequence of the following function on V_{n+1}

$$g(u,x_1,\ldots,x_n) = (1 \oplus u) f_1(x_1,\ldots,x_n) \oplus u f_2(x_1,\ldots,x_n).$$

We now introduce the concept of bent functions.

Definition 1 *A function f on V_n is called a* bent *function if*

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

for all $\beta \in V_n$. Here $f(x) \oplus \langle \beta, x \rangle$ is regarded as a real-valued function.

From [1, 21, 17] we know that the following three statements are equivalent

(i) f is bent.

(ii) $\langle \xi, \ell \rangle = \pm 2^{\frac{1}{2}n}$ for any affine sequence ℓ of length 2^n, where ξ is the sequence of f.

(iii) $f(x) \oplus f(x \oplus \alpha)$ is balanced for any non-zero vector $\alpha \in V_n$.

From the definition we can see that bent functions on V_n exist only when n is even. It was Rothaus who first introduced and studied bent functions [16]. Other issues related to bent functions, such as properties, constructions and counting, can be found in [1, 5, 7, 12, 21]. Kumar, Scholtz and Welch [6] defined and studied bent functions from Z_q^n to Z_q, where q is a positive integer. Applications of bent functions to digital communications, coding theory and cryptography can be found in such as [2, 3, 7, 8, 9, 10, 11, 12].

Now we introduce the definition of propagation criterion.

Definition 2 *Let f be a function on V_n. We say that f satisfies*

1. *the* propagation criterion with respect to α *if $f(x) \oplus f(x \oplus \alpha)$ is a balanced function, where $x = (x_1, x_2, \ldots, x_n)$ and α is a non-zero vector in V_n.*

2. *the* propagation criterion of degree k *if it satisfies the propagation criterion with respect to all $\alpha \in V_n$ with $1 \leqq W(\alpha) \leqq k$.*

The above definition for propagation criterion is from in [15]. Further work on the topic can be found in [14] where a nonsystematic method for obtaining balanced functions satisfying the propagation criterion was suggested. Note that the strict avalanche criterion (SAC) introduced by Webster and Tavares [19, 20] is equivalent to the propagation criterion of degree 1 and that the perfect nonlinearity studied by Meier and Staffelbach [10] is equivalent to the propagation criterion of degree n where n is the number of coordinates.

From above discussion it becomes clear that when n is even, only bent functions fulfill the propagation criterion of the maximal degree n. Another property of bent functions is that they possess the highest possible nonlinearity ($2^{n-1} - 2^{\frac{1}{2}n-1}$ for any bent function on V_n when n is even). However, since bent functions are not balanced and they exist only for even n, they can not be directly employed in many practical applications. Therefore it is an interesting topic to study functions that are balanced and satisfy the propagation criterion of high degree. Since a balanced function can not satisfy the propagation criterion of degree n, the first question that has to be answered is how high a degree of the propagation criterion of a balanced function can be achieved. In this paper we show that when n is odd, there are balanced functions that achieve the propagation criterion of degree $n-1$, and that when n is even, there are balanced functions that achieve the propagation criterion of degree $\frac{2}{3}n$. In fact, we obtain a stronger result: for odd n we present a method for constructing balanced functions that satisfy the propagation criterion with respect to *all but one* non-zero vectors in V_n, and for even n we present a method for constructing balanced functions that satisfy the propagation criterion with respect to *all but three* non-zero vectors in V_n. Note that for odd n our result is optimal in the sense that no balanced functions can satisfy the propagation criterion with respect to all non-zero vectors.

Before going into detailed discussion, we first present, in the next section, two results about nonlinearity. These results will be used in a later part of the paper. We present these results in a separate section since they are of independent interest.

3 Two Results on Nonlinearity

Lemma 1 *Let $f(x_1, x_2, \ldots, x_{2k})$ be a bent function on V_{2k} and let η_0 be the sequence of $f(0, x_2, \ldots, x_{2k})$. Then for any affine sequence ℓ of length 2^{2k-1}, we have $-2^k \leqq \langle \eta_0, \ell \rangle \leqq 2^k$.*

Proof. Let η_1 be the sequence of $f(1, x_2, \ldots, x_{2k})$. Since $f(x_1, x_2, \ldots, x_{2k}) = (1 \oplus x_1) f(0, x_2, \ldots, x_{2k}) \oplus x_1 f(1, x_2, \ldots, x_{2k})$, $\eta = (\eta_0, \eta_1)$ is the sequence of $f(x_1, x_2, \ldots, x_{2k})$. On the other hand, by Lemma 10 of [17], both $L = (\ell, \ell)$ and $L' = (\ell, -\ell)$ are affine sequences of length 2^{2k}.

Now we prove the lemma by contradiction. Suppose the lemma is not true. Without loss of generality assume that $\langle \eta_0, \ell \rangle > 2^k$. There are two cases that have to be considered: $\langle \eta_1, \ell \rangle > 0$ and $\langle \eta_1, \ell \rangle < 0$. In the first case we have $\langle \eta, L \rangle \geqq \langle \eta_0, \ell \rangle + \langle \eta_1, \ell \rangle > 2^k$, and in the second case we have $\langle \eta, L' \rangle \geqq \langle \eta_0, \ell \rangle + \langle \eta_1, -\ell \rangle = \langle \eta_0, \ell \rangle + (-1)\langle \eta_1, \ell \rangle > 2^k$, both of which contradict the fact that $\langle \eta, M \rangle = \pm 2^{\frac{1}{2}n}$ for any affine sequence M (see the remark following Definition 1). This completes the proof. □

Lemma 2 *Let f_1 and f_2 be bent functions on V_n and let ξ_1 and ξ_2 be the sequences of f_1 and f_2 respectively. Let P_1 and P_2 be positive numbers and let g be a function on V_{n+1} defined by*

$$g(u, x_1, \ldots, x_n) = (1 \oplus u) f_1(x_1, \ldots, x_n) \oplus u f_2(x_1, \ldots, x_n).$$

For any affine sequence ℓ of length 2^n, if $\langle \xi_1, \ell \rangle \leqq P_1$ and $\langle \xi_2, \ell \rangle \leqq P_2$, then $N_g \geqq 2^n - \frac{1}{2}(P_1 + P_2)$.

Proof. Note that $\xi = (\xi_1, \xi_2)$ is the sequence of g (see the comment before Definition 1. Let ψ be an arbitrary affine function on V_{n+1} and let L be the sequence of ψ. From properties of

Sylvester-Hadamard matrices we know that L must take the form of $L = (\ell, \pm\ell)$ where ℓ is an affine sequence of length 2^n. Note that $\langle \xi, L \rangle = \langle \xi_1, \ell \rangle \pm \langle \xi_2, \ell \rangle$ and thus $|\langle \xi, L \rangle| \leqq P_1 + P_2$. On the other hand, by Lemma 11 of [17] we have $d(g, \psi) = 2^n - \frac{1}{2}\langle \xi, L \rangle$. From these discussions we have $d(g, \psi) \geqq 2^n - \frac{1}{2}(P_1 + P_2)$. Since ψ is arbitrary we have $N_g \geqq 2^n - \frac{1}{2}(P_1 + P_2)$, and this completes the proof. □

4 Basic Constructions

This section presents two methods for constructing highly nonlinear balanced functions satisfying the propagation criterion. For odd n, we construct balanced functions that satisfy the propagation criterion with respect to all non-zero vectors except $\gamma = (1, 0, \ldots, 0)$. And for even n, we construct balanced functions that satisfy the propagation criterion with respect to *all but three* non-zero vectors. The three vectors where the propagation criterion is not satisfied are $\gamma_1 = (1, 0, 0, \ldots, 0)$, $\gamma_2 = (0, 1, 0, \ldots, 0)$, and $\gamma_3 = \gamma_1 \oplus \gamma_2 = (1, 1, 0, \ldots, 0)$. The two methods both start with bent functions, and hence are similar from a technical point of view. In the next section we will show how γ, γ_1 and γ_2, can be transformed into any other non-zero vectors.

4.1 On V_{2k+1}

Let f be a bent function on V_{2k}, and let g be a function on V_{2k+1} defined by

$$g(x_1, x_2, \ldots, x_{2k+1}) = x_1 \oplus f(x_2, \ldots, x_{2k+1}). \tag{1}$$

Lemma 3 *The function g defined in (1) satisfies the propagation criterion with respect to all non-zero vectors $\gamma \in V_{2k+1}$ with $\gamma \neq (1, 0, \ldots, 0)$.*

Proof. Let $\gamma = (a_1, a_2, \ldots, a_{2k+1}) \neq (1, 0, \ldots, 0)$ and let $x = (x_1, x_2, \ldots, x_{2k+1})$. Then $g(x) \oplus g(x \oplus \gamma) = a_1 \oplus f(x_2, \ldots, x_{2k+1}) \oplus f(x_2 \oplus a_2, \ldots, x_{2k+1} \oplus a_{2k+1})$. Since f is a bent function, $f(x_2, \ldots, x_{2k+1}) \oplus f(x_2 \oplus a_2, \ldots, x_{2k+1} \oplus a_{2k+1})$ is balanced for all $(a_2, \ldots, a_{2k+1}) \neq (0, \ldots, 0)$ (see (iii) after Definition 1). Thus $g(x) \oplus g(x \oplus \gamma)$ is balanced for all $\gamma = (a_1, a_2, \ldots, a_{2k+1}) \neq (1, 0, \ldots, 0)$. □

Lemma 4 *The nonlinearity N_g of the function g defined by (1) satisfies $N_g \geqq 2^{2k} - 2^k$.*

Proof. Note that $g(x_1, x_2, \ldots, x_{2k+1}) = (1 \oplus x_1) f(x_2, \ldots, x_{2k+1}) \oplus x_1 (1 \oplus f(x_2, \ldots, x_{2k+1}))$. Let ξ be the sequence of f. Then $\eta = (\xi, -\xi)$ is the sequence of g (see the comment before Definition 1). Since f is bent we have $\langle \xi, \ell \rangle = \pm 2^k$ for any affine sequence ℓ of length 2^{2k}. By Lemma 2 we have $N_g \geqq 2^{2k} - \frac{1}{2}(2^k + 2^k) \geqq 2^{2k} - 2^k$. □

The following lemma is a special case of Lemma 20 of [17], which says that if f_1 is balanced on V_s or f_2 is balanced on V_t, then $f_1(x_1, x_2, \ldots, x_s) \oplus f_2(y_1, y_2, \ldots, y_t)$ is a balanced function on V_{s+t}.

Lemma 5 *The function g defined by (1) is balanced.*

Combining these three lemmas we have

Corollary 1 *The function g defined by (1) is balanced and satisfies the propagation criterion with respect to all non-zero vectors $\gamma \in V_{2k+1}$ with $\gamma \neq (1, 0, \ldots, 0)$. The nonlinearity of g satisfies $N_g \geqq 2^{2k} - 2^k$.*

4.2 On V_{2k}

Let f be a bent function on V_{2k-2} and let g be a function on V_{2k} obtained from f in the following way:

$$g(x_1, x_2, x_3, \ldots, x_{2k}) = x_1 \oplus x_2 \oplus f(x_3, \ldots, x_{2k}). \tag{2}$$

Lemma 6 *The function g defined in (2) satisfies the propagation criterion with respect to* all but three *non-zero vectors in V_{2k}. The three vectors where the propagation criterion is not satisfied are $\gamma_1 = (1,0,0,\ldots,0)$, $\gamma_2 = (0,1,0,\ldots,0)$, and $\gamma_3 = \gamma_1 \oplus \gamma_2 = (1,1,0,\ldots,0)$.*

Proof. Let $\gamma = (a_1, a_2, \ldots, a_{2k})$ be a non-zero vector in V_{2k} differing from γ_1, γ_2 and γ_3. Also let $x = (x_1, \ldots, x_{2k})$. Then we have $g(x) \oplus g(x \oplus \gamma) = a_1 \oplus a_2 \oplus f(x_3, \ldots, x_{2k}) \oplus f(x_3 \oplus a_3, \ldots, x_{2k} \oplus a_{2k})$. Since f is a bent function on V_{2k-2} and $(a_3, \ldots, a_{2k}) \neq (0, \ldots, 0)$, by (iii) after Definition 1 we know that $f(x_3, \ldots, x_{2k}) \oplus f(x_3 \oplus a_3, \ldots, x_{2k} \oplus a_{2k})$ is balanced, from which it follows that $g(x) \oplus g(x \oplus \gamma)$ is balanced for any non-zero vector γ in V_{2k} differing from γ_1, γ_2 and γ_3. This proves the lemma. □

Lemma 7 *The nonlinearity of the function g defined by (2) satisfies $N_g \geqq 2^{2k-1} - 2^k$.*

Proof. Note that

$$g(x_1, x_2, \ldots, x_{2k}) = (1 \oplus x_1) f_1(x_2, \ldots, x_{2k}) \oplus x_1 (1 \oplus f_1(x_2, \ldots, x_{2k}))$$

where $f_1(x_2, \ldots, x_{2k}) = x_2 \oplus f(x_3, \ldots, x_{2k})$. Let ξ be the sequence of $f_1(x_2, \ldots, x_{2k})$. Then $\eta = (\xi, -\xi)$ is the sequence of g (see the comment before Definition 1). By Lemma 4 we have $N_{f_1} \geqq 2^{2k-2} - 2^{k-1}$. Now let ψ be an affine function on V_{2k-1} and let ℓ be the sequence of ψ. Then the distance between f_1 and ψ can be calculated by $d(f_1, \psi) = 2^{2k-2} - \frac{1}{2}\langle \xi, \ell \rangle$ (see Lemma 11 of [17]). Note that $d(f_1, \psi) \geqq N_{f_1}$. This implies that $\langle \xi, \ell \rangle \leqq 2^k$. Using Lemma 2 we have $N_g \geqq 2^{2k-1} - 2^k$. □

Again the following lemma is a special case of Lemma 20 of [17]:

Lemma 8 *The function g defined by (2) is balanced.*

Thus we have the following result:

Corollary 2 *The function g defined by (2) is balanced and satisfies the propagation criterion with respect to all non-zero vectors $\gamma \in V_{2k}$ with $\gamma \neq (c_1, c_1, 0, \ldots, 0)$, where $c_1, c_2 \in GF(2)$. The nonlinearity of g satisfies $N_g \geqq 2^{2k-1} - 2^k$.*

5 Moving Vectors Around

Though functions constructed according to (1) or (2) satisfy the propagation criterion with respect to all but one or three non-zero vectors, they are not interesting in practical applications. This section shows that through linear transformation of input coordinates, the vectors where the propagation criterion is not satisfied can be moved while the balancedness and nonlinearity of the functions are maintained. In particular, the vectors can be transformed into vectors having a high Hamming weight. In this way we obtain highly nonlinear balanced functions satisfying the high degree propagation criterion.

5.1 On V_{2k+1}

Theorem 1 *For any non-zero vector $\gamma^* \in V_{2k+1}$ ($k \geqq 1$), there exist balanced functions on V_{2k+1} satisfying the propagation criterion with respect to all non-zero vectors $\gamma \in V_{2k+1}$ with $\gamma \neq \gamma^*$. The nonlinearities of the functions are at least $2^{2k} - 2^k$.*

Proof. Let f be a bent function and let g be the function constructed by (1). From linear algebra we know that for any bases B_1 and B_2 of the vector space V_{2k+1}, where $B_1 = \{\alpha_j | j = 1, \ldots, 2k+1\}$ and $B_2 = \{\beta_j | j = 1, \ldots, 2k+1\}$, there exists a unique nondegenerate matrix A of order $2k+1$ with entries from $GF(2)$ such that $\alpha_j A = \beta_j$, $j = 1, \ldots, 2k+1$. In particular, this is true when $\alpha_1 = \gamma^*$ and $\beta_1 = (1, 0, \ldots, 0)$. Let $x = (x_1, x_2, \ldots, x_n)$ and let g^* be the function obtained from g by employing linear transformation on the input coordinates of g:

$$g^*(x) = g(xA).$$

Now we show that g^* is balanced, has the same nonlinearity as that of g and satisfies the propagation criterion with respect to all non-zero vectors except γ^*. First, since A is nondegenerate, xA is an one-to-one mapping on V_{2k+1}. The balancedness of g^* follows from the fact that xA is an one-to-one mapping, that g is balanced, and that $g^*(x) = 0$ if and only if $g(xA) = 0$.

Let φ be an affine function on V_{2k+1} and let $\varphi_A(x) = \varphi(xA)$. It is easy to verify that $d(g, \varphi) = d(g^*, \varphi_A)$. Since A is nondegenerate, φ_A will run through all affine functions on V_{2k+1} while φ runs through all affine functions on V_{2k+1}. This proves that $N_{g^*} = N_g$.

Let γ be a non-zero vector in V_{2k+1} with $\gamma \neq \gamma^*$. Consider the following function $g^*(x) \oplus g^*(x \oplus \gamma) = g(xA) \oplus g(xA \oplus \gamma A) = g(y) \oplus g(y \oplus \gamma A)$ where $y = xA$. Note that A is nondegenerate and thus y runs through V_{2k+1} while x runs through V_{2k+1}. Since $\gamma \neq \gamma^*$ we have $\gamma A \neq (1, 0, \ldots, 0)$. From (iii) after Definition 1, $g(y) \oplus g(y \oplus \gamma A)$ is balanced and hence $g^*(x) \oplus g^*(x \oplus \gamma)$ is balanced. Consequently, g^* satisfies the propagation criterion with respect to all non-zero vectors in V_{2k+1} but γ^*. This completes the proof. □

As a consequence of Theorem 1, we obtain, by letting $\gamma^* = (1, 1, \ldots, 1)$, highly nonlinear balanced functions on V_{2k+1} satisfying the propagation criterion of degree $2k$. This is described in the following:

Corollary 3 *Let f be a bent function on V_{2k} and let $g^*(x_1, \ldots, x_{2k+1}) = x_1 \oplus f(x_1 \oplus x_2, x_1 \oplus x_3, \ldots, x_1 \oplus x_{2k+1})$. Then g^* is a balanced function on V_{2k+1} and satisfies the propagation criterion of degree $2k$. The nonlinearity of g^* satisfies $N_{g^*} \geqq 2^{2k} - 2^k$.*

Proof. Let e_j, $j = 1, 2, \ldots, 2k+1$, be a vector in V_{2k+1} whose jth coordinate is 1 and all other coordinates are 0. In the proof of Theorem 1, we let $\alpha_1 = \gamma_0 = (1, \ldots, 1)$, $\alpha_j = e_j$, $j = 2, \ldots, 2k+1$ and $\beta_j = e_j$, $j = 1, \ldots, 2k+1$. Then there is a unique nondegenerate matrix A of order $2k+1$ such that $\alpha_j A = \beta_j$, $j = 1, \ldots, 2k+1$. It is easy to verify that A has the following form:

$$A = \begin{bmatrix} \gamma_0 \\ e_2 \\ \vdots \\ e_{2k+1} \end{bmatrix}.$$

Thus we have $g^*(x) = g(xA) = g(x_1, x_1 \oplus x_2, \ldots, x_1 \oplus x_{2k+1}) = x_1 \oplus f(x_1 \oplus x_2, x_1 \oplus x_3, \ldots, x_1 \oplus x_{2k+1})$, where $g(x) = x_1 \oplus f(x_2, \ldots, x_{2k+1})$, and $x = (x_1, x_2, \ldots, x_{2k+1})$. By

Theorem 1 g^* satisfies the propagation criterion with respect to all non-zero vectors in V_{2k+1} except the all-one vector $\gamma^* = (1, 1, \ldots, 1)$. Consequently g^* satisfies the propagation criterion of degree $2k$. □

5.2 On V_{2k}

Theorem 2 *For any non-zero vectors $\gamma_1^*, \gamma_2^* \in V_{2k}$ ($k \geqq 2$) with $\gamma_1^* \neq \gamma_2^*$, there exist balanced functions on V_{2k} satisfying the propagation criterion with respect to* all but three *non-zero vectors in V_{2k}. The three vectors where the propagation criterion is not satisfied are γ_1^*, γ_2^* and $\gamma_1^* \oplus \gamma_2^*$. The nonlinearities of the functions are at least $2^{2k-1} - 2^k$.*

Proof. The proof is essentially the same as that for Theorem 1. The major difference lies in the selection of bases $B_1 = \{\alpha_j | j = 1, \ldots, 2k\}$ and $B_2 = \{\beta_j | j = 1, \ldots, 2k\}$. By linear algebra, we can let $\alpha_1 = \gamma_1^*$, $\alpha_2 = \gamma_2^*$, $\beta_1 = (1,0,0,\ldots,0)$, and $\beta_2 = (0,1,0,\ldots,0)$. By the same reasoning as in the proof of Theorem 1, we can see that g^* defined by $g^*(x) = g(xA)$ satisfies the propagation criterion with respect to all but the following three non-zero vectors in V_{2k}: γ_1^*, γ_2^* and $\gamma_1^* \oplus \gamma_2^*$. Here $x = (x_1, x_2, \ldots, x_{2k})$, $g(x) = x_1 \oplus x_2 \oplus f(x_3, \ldots, x_{2k})$, and f, a bent function on V_{2k-2}, are all the same as in (2), and A is the unique nondegenerate matrix such that $\alpha_j A = \beta_j$, $j = 1, \ldots, 2k$. □

Similarly to the case on V_{2k+1}, we can obtain highly nonlinear balanced functions satisfying the high degree propagation criterion, by properly selecting vectors γ_1^* and γ_2^*. Unlike the case on V_{2k+1}, however, the degree of propagation criterion the functions can achieve is $\frac{4}{3}k$, but not $2k - 1$. The construction method is described in the following corollary.

Corollary 4 *Suppose that $2k = 3t + c$ where $c = 0, 1$ or 2. Then there exist balanced functions on V_{2k} that satisfy the propagation criterion of degree $2t - 1$ (when $c = 0$ or 1), or $2t$ (when $c = 2$). The nonlinearities of the functions are at least $2^{2k-1} - 2^k$.*

Proof. Set $c_1 = 0$, $c_2 = 1$ if $c = 1$ and set $c_1 = c_2 = \frac{1}{2}c$ otherwise. Let $\gamma_1^* = (a_1, \ldots, a_{3t+c})$ and $\gamma_2^* = (b_1, \ldots, b_{3t+c})$, where

$$a_j = \begin{cases} 1 & \text{for } j = 1, \ldots, 2t + c_1, \\ 0 & \text{for } j = 2t + c_1 + 1, \ldots, 3t + c. \end{cases}$$

$$b_j = \begin{cases} 0 & \text{for } j = 1, \ldots, t + c_1, \\ 1 & \text{for } j = t + c_1 + 1, \ldots, 3t + c. \end{cases}$$

By Theorem 2 there exists a balanced function g^* on V_{2k} satisfying the propagation criterion with respect to all but three non-zero vectors in V_{2k}. The three vectors are γ_1^*, γ_2^* and $\gamma_1^* \oplus \gamma_2^*$. The nonlinearity of g^* satisfies $N_{g^*} \geqq 2^{2k-1} - 2^k$.

Note that $W(\gamma_1^*) = 2t + c_1$, $W(\gamma_2^*) = 2t + c_2$, and $W(\gamma_1^* \oplus \gamma_2^*) = 2t + 2c_1 = 2t + c$. The minimum among the three weights is $2t + c_1$. Therefore, for any nonzero vector $\gamma \in V_{2k}$ with $W(\gamma) \leqq 2t + c_1 - 1$, we have $\gamma \neq \gamma_1^*, \gamma_2^*$ or $\gamma_1^* \oplus \gamma_2^*$. By Theorem 2, $g^*(x) \oplus g^*(x \oplus \gamma)$ is balanced. From this we conclude that g^* satisfies the propagation criterion of order $2t + c_1 - 1$. The proof is completed by noting that $c_1 = 0$ if $c = 0$ or 1 and $c_1 = 1$ if $c = 2$. □

5.3 Algebraic Degrees

The product of coordinates in a function is called a term. The degree of a term is the number of coordinates in the term, and the algebraic degree of a function is the degree of the longest term in it. The algebraic degree is also a nonlinearity criterion and it becomes important in certain practical applications where linear approximation of a nonlinear function needs to be avoided. In our constructions (1) and (2), the algebraic degree of a resulting function g is the same as that of the starting bent function f.

The simplest bent function on V_{2k} is the following quadratic function:

$$f(x_1, x_2, \ldots, x_{2k}) = x_1 x_{k+1} \oplus x_2 x_{k+2} \oplus \cdots \oplus x_k x_{2k}.$$

Bent functions with higher algebraic degrees exist and there are many methods for constructing such functions [4]. The following is a method discovered by Dillon and Maiorana [4, 6] for constructing a bent function f on V_{2k}:

$$f(x) = \langle x', \pi(x'') \rangle \oplus r(x'')$$

where $x = (x', x'')$, $x' = (x_1, \ldots, x_k)$, $x'' = (x_{k+1}, \ldots, x_{2k})$, r is an arbitrary function on V_k and $\pi = (\pi_1(x''), \pi_2(x''), \ldots, \pi_k(x''))$ is a permutation on the vector space V_k. Due to the arbitrariness of r, the algebraic degree of f can be any integer between 2 and k. From these discussions it becomes clear that functions obtained by (1) and (2) can achieve a wide range of algebraic degrees, namely $2, \ldots, k$ and $2, \ldots, k-1$ respectively.

Recently, Detombe and Tavares obtained, while studying the design of S-boxes, balanced *quadratic* functions on V_{2k+1} that satisfy the propagation criterion with respect to all but one vectors in V_{2k+1}. (They called these functions *near bent* functions.) They obtained the functions by the use of the *cubing* technique suggested by Pieprzyk [13]. Applicability of these quadratic functions in practice is limited by the following two facts:

1. Their algebraic degree is only 2.
2. They are all equivalent in structure in the sense that they can be transformed into one another by linear transformation of input coordinates.

6 Examples

This section provides two concrete examples to illustrate our methods for constructing highly nonlinear balanced functions satisfying the high degree propagation criterion.

Our first example is concerned with odd n. We consider balanced functions on V_7. Note that $f(x_1, x_2, x_3, x_4, x_5, x_6) = x_1 x_2 \oplus x_3 x_4 \oplus x_5 x_6 \oplus x_2 x_4 x_6$ is a bent function on V_6. It is obtained by the use of Dillon and Maiorana's construction [4, 6]. Now let

$$\begin{aligned} & g(x_1, x_2, x_3, x_4, x_5, x_6, x_7) \\ = \;& x_1 \oplus f(x_2, x_3, x_4, x_5, x_6, x_7) \\ = \;& x_1 \oplus x_2 x_3 \oplus x_4 x_5 \oplus x_6 x_7 \oplus x_3 x_5 x_7. \end{aligned}$$

By Corollary 3, the following function

$$\begin{aligned} g^*(x_1, x_2, x_3, x_4, x_5, x_6, x_7) &= x_1 \oplus f(x_1 \oplus x_2, x_1 \oplus x_3, x_1 \oplus x_4, x_1 \oplus x_5, x_1 \oplus x_6, x_1 \oplus x_7) \\ &= x_1 \oplus (x_1 \oplus x_2)(x_1 \oplus x_3) \oplus (x_1 \oplus x_4)(x_1 \oplus x_5) \oplus \\ &\quad (x_1 \oplus x_6)(x_1 \oplus x_7) \oplus (x_1 \oplus x_3)(x_1 \oplus x_5)(x_1 \oplus x_7) \end{aligned}$$

satisfies the propagation criterion of degree 6. The propagation criterion is not satisfied only by the all-one vector $(1,1,1,1,1,1,1)$.

On the other hand, assume that $\gamma^* = (0,0,1,0,1,1,0)$. Let e_j be a vector on V_7 whose jth coordinate is 1 and other coordinates are 0, where $j = 1,2,\ldots,7$. Let $\alpha_1 = \gamma_0$, $\alpha_2 = e_2$, $\alpha_3 = e_1$ and $\alpha_j = e_j$, $j = 4,5,6,7$. And let $\beta_j = e_j$, $j = 1,\ldots 7$. Thus $\{\alpha_1,\ldots,\alpha_7\}$ and $\{\beta_1,\ldots,\beta_7\}$ are two bases of V_7. By matrix manipulation we can find the following matrix

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

that satisfies $\alpha_j A = \beta_j$, $j = 1,\ldots,7$. By Theorem 1

$$\begin{aligned} & h^*(x_1,x_2,x_3,x_4,x_5,x_6,x_7) \\ &= g((x_1,x_2,x_3,x_4,x_5,x_6,x_7)A) \\ &= g(x_3,x_2,x_1,x_4,x_3 \oplus x_5, x_3 \oplus x_6, x_7) \\ &= x_3 \oplus x_2x_1 \oplus x_4(x_3 \oplus x_5) \oplus (x_3 \oplus x_6)x_7 \oplus x_1(x_3 \oplus x_5)x_7 \end{aligned}$$

is a balanced function on V_7 satisfying the propagation criterion with respect to all $\gamma \in V_7$ with $\gamma \neq (0,0,1,0,1,1,0)$.

Note that $N_{g^*} = N_{h^*} \geqq 2^6 - 2^3 = 56$. This nonlinearity is very high, since according to Corollary 17 of [17], the nonlinearity of balanced functions on V_7 is upper-bounded by $\lfloor\lfloor 2^{7-1} - 2^{\frac{1}{2}7-1}\rfloor\rfloor = \lfloor\lfloor 64 - 4 \cdot 2^{\frac{1}{2}}\rfloor\rfloor = 58$, where $\lfloor\lfloor x\rfloor\rfloor$ denotes the maximum even integer less than or equal to x.

Our second example is for even n. We consider balanced functions on V_{12}. Note that n can be written as $n = 2k = 3t + c$, where $k = 6$, $t = 4$ and $c = 0$. Again by using Dillon and Maiorana's construction we have the following bent function on V_{10}:

$$\begin{aligned} & f(x_3,x_4,x_5,x_6,x_7,x_8,x_9,x_{10},x_{11},x_{12}) \\ &= x_3x_4 \oplus x_5x_6 \oplus x_7x_8 \oplus x_9x_{10} \oplus x_{11}x_{12} \oplus x_4x_6x_8x_{10}x_{12}. \end{aligned}$$

By Corollary 1

$$\begin{aligned} & g(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8,x_9,x_{10}) \\ &= x_1 \oplus x_2 \oplus f(x_3,x_4,x_5,x_6,x_7,x_8,x_9,x_{10},x_{11},x_{12}) \\ &= x_1 \oplus x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8 \oplus x_9x_{10} \oplus x_{11}x_{12} \oplus x_4x_6x_8x_{10}x_{12} \end{aligned}$$

is balanced and satisfies the propagation criterion with respect all non-zero vectors $\gamma \in V_{12}$ with $\gamma \neq (c_1,c_2,0,0,0,0,0,0,0,0,0,0)$, where $c_1,c_2 \in GF(2)$. The nonlinearity of g satisfies $N_g \geqq 2^{11} - 2^6 = 1984$, which is comparable to $2^{11} - 2^5 - 2 = 2014$, the upper-bound of the nonlinearity of a balanced function on V_{12} (see Corollary 17 of [17]).

Let e_j be the vector in V_{12}, whose the jth coordinate is 1 and other coordinates are all 0, where $j = 1,\ldots,12$.

Let $\gamma_1^* = (1,1,1,1,1,1,1,1,0,0,0,0)$, $\gamma_2^* = (0,0,0,0,1,1,1,1,1,1,1,1)$ and set

$$\begin{aligned} B_1 &= \{\gamma_1^*, \gamma_2^*, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_{10}, e_{11}, e_{12}\}, \\ B_2 &= \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9, e_{10}, e_{11}, e_{12}\}. \end{aligned}$$

Now let A be a matrix defined by

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

It is not hard to check that $\gamma_1^* A = e_1$, $\gamma_2^* A = e_2$, $e_2 A = e_3$, $e_3 A = e_4$, $e_4 A = e_5$, $e_5 A = e_6$, $e_6 A = e_7$, $e_7 A = e_8$, $e_8 A = e_9$, $e_{10} A = e_{10}$, $e_{11} A = e_{11}$, $e_{12} A = e_{12}$. Let

$$\begin{aligned} & g^*(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}) \\ &= g((x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12})A) \\ &= g(x_1,\ x_9,\ x_1 \oplus x_2,\ x_1 \oplus x_3,\ x_1 \oplus x_4,\ x_1 \oplus x_5 \oplus x_9,\ x_1 \oplus x_6 \oplus x_9, \\ &\quad x_1 \oplus x_7 \oplus x_9,\ x_1 \oplus x_8 \oplus x_9,\ x_9 \oplus x_{10},\ x_9 \oplus x_{11},\ x_9 \oplus x_{12}). \end{aligned}$$

By Theorem 2 the function g^* is balanced and its nonlinearity satisfies $N_g \geqq 2^{11} - 2^6 = 1984$. In addition, g^* satisfies the propagation criterion with respect all but three non-zero vectors in V_{12}. The three non-zero vectors are $\gamma_1^* = (1,1,1,1,1,1,1,1,0,0,0,0)$, $\gamma_2^* = (0,0,0,0,1,1,1,1,1,1,1,1)$ and $\gamma_3^* = \gamma_1^* \oplus \gamma_2^* = (1,1,1,1,0,0,0,0,1,1,1,1)$. By Corollary 4, g^* satisfies the propagation criterion of degree $2t - 1 = 7$.

7 Concluding Remarks

We have presented systematic methods for constructing balanced functions satisfying the propagation criterion with respect to all but one or three vectors. We have also developed a technique that allows us to transform vectors where the propagation criterion is not satisfied into other vectors, while maintaining the nonlinearity and balancedness of the functions. As a consequence, we obtain highly nonlinear balanced functions on V_{2k+1} satisfying the propagation criterion of the maximum degree, namely $2k$, and highly nonlinear balanced functions on V_{2k} satisfying the propagation criterion of degree $\frac{4}{3}k$. We believe that the vector transformation technique has applications in other research areas such as the design of cryptographically strong S-boxes. It is also interesting to note that functions constructed on V_{2k+1} are optimal in the sense that they achieve the maximum degree of propagation criterion. It is left as future work to examine whether there are highly nonlinear balanced functions on V_{2k} satisfying the propagation criterion of degree $2k - 1$, and if there are, to find methods for constructing such functions.

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. Technical Report, TR 90-013, Department of Electrical Engineering, Queen's University, 1990.

[3] J. Detombe and S. Tavares. Constructing large cryptographically strong S-boxes. In *Advances in Cryptology - AUSCRYPT'92*. Springer-Verlag, Berlin, Heidelberg, New York, 1993. to appear.

[4] J. F. Dillon. *Elementary Hadamard Difference Sets*. Ph.D. dissertation, University of Maryland, 1974.

[5] 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.

[6] 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.

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

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

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

[10] W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology - EUROCRYPT'89*, volume 434, Lecture Notes in Computer Science, pages 549–562. Springer-Verlag, Berlin, Heidelberg, New York, 1990.

[11] K. Nyberg. Perfect nonlinear S-boxes. In *Advances in Cryptology - EUROCRYPT'91*, volume 547, Lecture Notes in Computer Science, pages 378–386. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[12] 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.

[13] J. Pieprzyk. Bent permutations. In *Proceeding of the International Conference on Finite Fields, Coding Theory, and Advances in Communications and Computing*, Las Vegas, 1991.

[14] B. Preneel, R. Govaerts, and J. Vandewalle. Boolean functions satisfying higher order propagation criteria. In *Advances in Cryptology - EUROCRYPT'91*, volume 547, Lecture Notes in Computer Science, pages 141–152. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[15] B. Preneel, W. V. Leekwick, L. V. Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, volume 437, Lecture Notes in Computer Science, pages 155–165. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

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

[17] J. Seberry and X. M. Zhang. Highly nonlinear 0-1 balanced functions satisfying strict avalanche criterion. In *Advances in Cryptology - AUSCRYPT'92*. Springer-Verlag, Berlin, Heidelberg, New York, 1993. to appear.

[18] 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.

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

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

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