Hadamard Matrices, Bent Functions and Cryptography

Jennifer Seberry and Xian-Mo Zhang
Department of Computer Science
The University of Wollongong
Wollongong, NSW 2522, AUSTRALIA

E-mail: {j.seberry,xianmo}@cs.uow.edu.au

November 23, 1995

Abstract

The recent incorporation of the *HAVAL (Hashing Algorithm with Variable Lengths)* into the *Tripwire* security package for SUN workstations and research for the latest LOKI family of algorithms, both of which use bent functions, have led many to ask us "What are bent functions?".

This article is to help introduce bent functions to those who work in Combinatorial Theory.

1 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 $GF(2)$, $V_n = (0,1)^n$. These functions are also called Boolean functions.

Example 1 (Vector Space) $V_2 = (0,1)^2$, therefore $00, 01, 10, 11$ are all the vectors in V_2.

Notation 1 (Vectors) We use the notation:

$$\alpha_0 = (0,\ldots,0,0),\ \alpha_1 = (0,\ldots,0,1),\ \ldots\ ,\alpha_{2^n-1-1} = (1,\ldots,1,1).$$

Definition 1 (Sequence, Truth Table and Matrix of a Function) Let f be a function on V_n. Use α_i as in Notation 1. 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. 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. The $(1,1)$-matrix of order 2^n defined by $((-1)^{f(\alpha_i \oplus \alpha_j)})$ is called the *matrix* of f.

Example 2 (Truth Table, Sequence and Matrix of a Function) Let $f(x) = x_1x_2x_3 \oplus x_1x_3 \oplus x_2 \oplus x_3 \oplus 1$ be a function on V_3.

The truth table of f

$$f(000) = 1,\ f(001) = 0,\ f(010) = 0,\ f(011) = 1,\ f(100) = 1,\ f(101) = 1,\ f(110) = 0,\ f(111) = 1.$$

The sequence of f is $-1,\ 1,\ 1,\ -1,\ -1,\ -1,\ 1,\ -1$.

The matrix of f is

$$\begin{bmatrix} - & + & + & - & - & - & + & - \\ + & - & - & + & - & - & - & + \\ + & - & - & + & + & - & - & - \\ - & + & + & - & - & + & - & - \\ - & - & + & - & - & + & + & - \\ - & - & - & + & + & - & - & + \\ + & - & - & - & + & - & - & + \\ - & + & - & - & - & + & + & - \end{bmatrix}.$$

Definition 2 (Balanced Functions) A function f on V_n is said to be *balanced* if its truth table has 2^{n-1} zeros (ones).

Example 3 (Balance) $f = x_1x_2 \oplus x_3$, a function on V_3, is balanced since the truth table of f is

$$0,\ 1,\ 0,\ 1,\ 0,\ 1,\ 1,\ 0.$$

f takes the value zero $2^{3-1} = 4$ times.

Definition 3 (Affine and Linear Functions) An *affine* function f on V_n is a function that takes the form of $f = a_1x_1 \oplus \cdots \oplus a_nx_n \oplus c$, where $a_j, c \in GF(2)$, $j = 1, 2, \ldots, n$. Furthermore f is called a *linear* function if $c = 0$.

Example 4 (Affine and Linear Functions) An affine function is one like

$$f = x_3 \oplus x_1 \oplus 1$$

and a linear function is one like

$$f = x_3 \oplus x_1.$$

Note: There are no terms such as x_1x_2 or $x_1^2x_3$.

Definition 4 (Affine Sequence) The sequence of an affine (or linear) function is called an *affine (or linear) sequence.*

Definition 5 (Hamming Weight and Hamming Distance) 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 $d(f, g) = W(f(x) \oplus g(x))$, where $x = (x_1, x_2, \ldots, x_n)$.

Example 5 (Hamming Weight) If $\alpha = (101)$ than $W(\alpha) = 2$.

Example 6 (Hamming Distance) If $f(x) = x_1x_2$ and $g(x) = x_1 \oplus x_2$ then

$$d(f,g) = W(f(x) \oplus g(x)) = W(x_1x_2 \oplus x_1 \oplus x_2).$$

Hence for $x = (x_1, x_2) = \{(0,0),(0,1),(1,0),(1,1)\}$

$d(f,g) = 0,1,1,3$ respectively.

Notation 2 (Scalar Product) 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 multiplication are over $GF(2)$. If α and β are $(1,-1)$-sequences, $\langle \alpha, \beta \rangle = \sum_{i=1}^{n} a_ib_i$, and the addition and multiplication is taken over the reals.

Lemma 1 *If $\xi = (a_1, \ldots, a_{2^n})$ and $\eta = (b_1, \ldots, b_{2^n})$ are the sequences of functions f_1 and f_2 on V_n respectively, then*

$$\xi * \eta = (a_1b_1, a_2b_2, \ldots, a_{2^n}b_{2^n})$$

is the sequence of $f_1(x) \oplus f_2(x)$, where $x = (x_1, x_2, \ldots, x_n)$.

Proof. The two sequences are given by

$a_i = (-1)^{f_1(\alpha_i)}$ and $b_i = (-1)^{f_2(\alpha_i)}$, for α_i as before.

Then $a_ib_i = (-1)^{f_1(\alpha_i)}(-1)^{f_2(\alpha_i)} = (-1)^{f_1(\alpha_i) \oplus f_2(\alpha_i)}$ □

Example 7 (Sequence of The Sum of Two Functions) We use the notation $-$ to represent -1. Let $f_1(x) = x_1x_2$, which has sequence

$$\xi = (-1)^{f_1(0,0)}, (-1)^{f_1(0,1)}, (-1)^{f_1(1,0)}, (-1)^{f_1(1,1)} = 1\ 1\ 1\ -$$

and $f_2(x) = x_2$, which has sequence

$$\eta = (-1)^{f_2(0,0)}, (-1)^{f_2(0,1)}, (-1)^{f_2(1,0)}, (-1)^{f_2(1,1)} = 1\ -\ 1\ -\ .$$

Now $f_1(x) \oplus f_2(x) = x_1x_2 \oplus x_2$ has the sequence $1\ -\ 1\ 1$, which is $\xi * \eta = (a_0b_0, a_1b_1, a_2b_2, a_3b_3)$.

Definition 6 (Walsh-Hadamard Matrix) 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 [24]. 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

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

Lemma 2 *The ith row of H_n is the sequence of linear function $\varphi_i(x) = \langle \alpha_i, x \rangle$, where $x \in V_n$ and α_i is the binary representation of i, $i = 0, 1, \ldots, 2^n - 1$.*

Proof. By induction on n. Let $n = 1$. Since $H_1 = \begin{bmatrix} + & + \\ + & - \end{bmatrix}$, $\ell_0 = (+\ +)$, the sequence of $\langle 0, x \rangle$ and $\ell_1 = (+\ -)$, 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 $n = 1, 2, \ldots, k-1$.

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

Example 8 (Walsh-Hadamard Matrices) The first few *Walsh-Hadamard matrices* are:

$$H_0 = [1],$$

$$H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$H_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix},$$

$$H_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

Notation 3 Let $\delta = (i_1, i_2, \ldots, i_p)$ be a constant vector in V_p. Then D_δ, the D-function of δ, is a function on V_p defined by

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

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 functions on V_q, 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}

$$f(y, x) = \bigoplus_{\delta \in V_p} D_\delta(y) f_\delta(x) \tag{1}$$

where $y = (y_1, \ldots, y_p)$ and $x = (x_1, \ldots, x_q)$. (See also Lemma 9 of [20]).

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}

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

Example 9 (Finding Polynomial from Truth Table) Consider the sequence

$$-, \ -, \ +, \ +,$$

which corresponds to the binary sequence 0, 0, 1, 1. In order to find the equivalent sequence we consider

$$a \ \oplus \ bx_1 \ \oplus \ cx_2 \ \oplus \ dx_1x_2$$

for 00, 10, 01, 11 respectively, obtaining upon substitution the equations

$$0 = a, \ 0 = a \oplus b, \ 1 = a \oplus c, \ 1 = a \oplus b \oplus c \oplus d$$

which have solution $a = 0$, $b = 0$, $c = 1$ and $d = 0$, so the associated boolean function is $f(x) = x_2$, which is linear. We note that the matrix

$$[abcd] \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} = [0011]$$

gives the same equations and so the solution is

$$[abcd] = [0011] \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}^{-1} = [0011] \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Because $[abcd] = [0010]$ the boolean function is $f(x) = x_2$.

Example 10 (Formula (1)) To find the boolean function associated with the sequence 0 0 1 0 1 0 0 1 for a three variable solution, we consider

$$[00101001]\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ x_1 \\ x_2 \\ x_1x_2 \\ x_3 \\ x_1x_3 \\ x_2x_3 \\ x_1x_2x_3 \end{bmatrix}$$ obtaining $x_2 \oplus x_1x_2 \oplus x_3 \oplus x_1x_3 \oplus x_1x_2x_3$.

Lemma 3 *In general if* $G_0 = 1$ *and*

$$G_n = \begin{bmatrix} G_{n-1} & G_{n-1} \\ 0 & G_{n-1} \end{bmatrix}$$

the boolean function associated with the binary sequence $\alpha = (a_0a_1 \ldots a_{2^n-1})$ *is* $\alpha G_n x^T$, *where* $x^T = (1, x_1, x_2, x_1x_2, x_3, x_1x_3, x_2x_3, x_1x_2x_3, x_4, \ldots,)$.

Example 11 (Application of Lemma 3) Now we consider the balanced sequences (01101001) and (10011001) respectively, which give

$$(01101001)G_3x^T = (01101000)x^T$$

and

$$(10011001)G_3x^T = (11100000)x^T,$$

which are the boolean functions $f(x) = x_1 \oplus x_2 \oplus x_3$ and $f(x) = 1 \oplus x_1 \oplus x_2$.

2 Cryptographically Desirable Properties

We list these and then give more details and discussion of each. The art of cryptography has led practitioner to believe that cryptographically desirable properties are:

- Balance,
- Nonlinearity,
- SAC, propagation,
- Correlation immunity,
- Algebraic degree.

2.1 Balance

Definition 7 (Balanced Functions) A function f on V_n is said to be *balanced* if its truth table has 2^{n-1} zeros (ones).

Example 12 (Balance) $f = x_1x_2 \oplus x_3$, a function on V_3, is balanced since the truth table of f is

$$0,\ 1,\ 0,\ 1,\ 0,\ 1,\ 1,\ 0.$$

f takes the value zero $2^{3-1} = 4$ times.

We noted before, in Definition 7, that a function, say f on Vn is balanced if f takes the value zero 2^{n-1} times.

We now explore further properties of balanced functions.

Lemma 4 (Nondegenerate Transformation) *Let*

$$g(x) = f(xB \oplus \beta)$$

where B is any nonsingular matrix of order n and β is any vector in V_n. Then g is balanced if and only if f is balanced.

Proof. We note that if B is nonsingular, then x runs through all vectors $\alpha_0 = (0, \ldots, 0)$ to $\alpha_{2^n-1} = (1, \ldots, 1)$, so $y = xB \oplus \beta$.

Hence if $f(x)$ is balanced so is

$$g(x) = f(xB \oplus \beta).$$

□

Example 13 (For Lemma 4) Set

$$g(x) = f(xB \oplus \beta)$$

where

$$B = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix},$$

$$\beta = (1, 1, 1).$$

Thus

$$g(x_1, x_2, x_3) = f(x_1 \oplus x_2 \oplus 1,\ x_1 \oplus x_3 \oplus 1,\ x_2 \oplus 1).$$

g is also balanced since $g(x_0) = 0$, if and only if $f(x_0B \oplus \beta) = 0$.

Lemma 5 (Sum of Functions) *Let f and g be functions on V_n and V_m respectively. Then $f(x) \oplus g(y)$ is balanced if f is balanced.*

Proof. Since $g(y')$ is constant for given y' and since the truth table of $f(x)$ is zero (one) half the time the truth table of $f(x) \oplus g(y')$ is zero (one) half the time. □

2.2 Nonlinearity

We recall from Definition 5 the Hamming distance $d(f, g)$. The following definition is given by Pieprzyk and Finkelstein [16]:

Definition 8 (N_f or nonlinearity of a function f)

$$N_f = min\{d(f, \varphi) | \varphi \text{ is affine}\}$$

is called the *nonlinearity* of f.

Example 14 (Nonlinearity) To show a calculation using this definition we consider

x	$f(x) = x_1x_2$	$\phi_1(x) = 1 \oplus x_1$	$\phi_2(x) = 1 \oplus x_2$	$\phi_3(x) = 1 \oplus x_1 \oplus x_2$
00	0	1	1	1
01	0	0	1	0
10	0	1	0	0
11	1	0	0	1

So that $d(f, \phi_i) = \sum_{f(x) \neq g(x)} = 1$ gives

$$d(f, \phi_1) = 3, \quad d(f, \phi_2) = 3, \quad d(f, \phi_3) = 1$$

and the nonlinearity or $\min d(f, \phi_i) = 1$.

Lemma 6

$$d(f, g) = 2^{n-1} - \frac{1}{2}\langle \xi, \eta \rangle$$

where ξ, η are the sequences of f and g respectively.

Proof. Write $\xi = a_0, a_1, \ldots, a_{2^n-1}$ and $\eta = b_0, b_1, \ldots, b_{2^n-1}$. Let $\rho(+)$ ($\rho(-)$) denote the number of j, such that $a_j = b_j$ ($a_j \neq b_j$). Hence $\langle \xi, \eta \rangle = \rho(+) - \rho(-) = 2^n - 2\rho(-)$ and hence $\rho(-) = 2^{n-1} - \frac{1}{2}\langle \xi, \eta \rangle$. Obviously, $\rho(-) = d(f, g)$. This proves the lemma. □

Example 15 (For Lemma 6) The sequences of $f, \phi_1, \phi_2, \phi_3$, are $\xi = (1,1,1,-1)$, $\eta_1 = (-1,1,-1,1)$, $\eta_2 = (-1,-1,1,1)$ and $\eta_3 = (-1,1,1,-1)$ respectively, so

$$\langle \xi,\ \eta_1 \rangle = -2, \quad \langle \xi,\ \eta_2 \rangle = -2, \quad \langle \xi,\ \eta_3 \rangle = 2$$

and so

$$d(f, \phi_1) = 3, \quad d(f, \phi_2) = 3, \quad d(f, \phi_3) = 1$$

and the nonlinearity or $\min d(f, \phi_i) = 1$.

Lemma 7 *Any nonzero affine function is balanced.*

Proof. The lemma immediately follows Lemma 5. □

Lemma 8 (Nonlinearity Inequality) *Let f be an arbitrary function on V_n. Then the nonlinearity of f, N_f, satisfies*

$$N_f \leqq 2^{n-1} - 2^{\frac{1}{2}n-1}.$$

Proof. There exist many proofs for this lemma. We now give a direct proof.

Let f be any function on V_n and ξ be the sequence of f. Let ℓ_j be the jth row (column) of H_n, $j = 0, 1, \ldots, 2^n - 1$. Note that

$$\xi H_n = \langle \xi, \ell_0 \rangle, \langle \xi, \ell_1 \rangle, \ldots, \langle \xi, \ell_{2^n-1} \rangle.$$

Hence $\xi H_n H_n \xi^T = \sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^2$ and hence $2^n \xi \xi^T = \sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^2$. This proves

$$\sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^2 = 2^{2n}. \tag{2}$$

(2) is called *Parseval's equation* (see P. 416 of [11]). Thus there exist a j_0, $0 \leqq j_0 \leqq 2^n - 1$, such that $\langle \xi, \ell_{j_0} \rangle^2 \geqq 2^n$ and thus $\langle \xi, \ell_{j_0} \rangle \geqq 2^{\frac{1}{2}n}$ or $\langle \xi, \ell_{j_0} \rangle \leqq -2^{\frac{1}{2}n}$.

From Lemma 2, ℓ_{j_0} is the sequence of a linear function, denoted by φ_{j_0}. In the first case, by using Lemma 6, $d(f, \varphi_{j_0}) \leqq 2^{n-1} - 2^{\frac{1}{2}n-1}$. In the second case, $\langle \xi, -\ell_{j_0} \rangle \geqq 2^{\frac{1}{2}n}$. Note that $-\ell_{j_0}$ is the sequence of affine function $1 \oplus \varphi_{j_0}$. By using Lemma 6, $d(f, 1 \oplus \varphi_{j_0}) \leqq 2^{n-1} - 2^{\frac{1}{2}n-1}$. By the definition of the nonlinearity, we have proved $N_f \leqq 2^{n-1} - 2^{\frac{1}{2}n-1}$. □

Lemma 9 *Let*

$$g(x) = f(xB \oplus \beta)$$

where B is any nonsingular matrix of order n and β is any vector in V_n. Then

$$N_g = N_f.$$

Proof. Let φ be an arbitrary affine function on V_n. By the definition of the nonlinearity, there exists an affine function on V_n, say φ, such that $d(f,\varphi) = N_f$. Set $\psi(x) = \varphi(xB \oplus \beta)$. Obviously $d(g,\psi) = d(f,\varphi)$. Note that ψ is also an affine function. By the definition of nonlinearity, $N_g \leqq d(g,\psi)$. This proves that $N_g \leqq N_f$. Since B is nonsingular, the deduction can be reversed and thus $N_f \leqq N_g$. The proof is completed. □

2.3 Propagation Criterion

Now we introduce the definition of the propagation criterion.

Definition 9 (Propagation and SAC) 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 $1 \leqq W(\alpha) \leqq k$,
3. *strict avalanche criterion (SAC)* if the propagation criterion degree of f is 1.

The above definition of the propagation criterion is from in [18]. Further work on the topic can be found in [17] 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 [25, 26] is equivalent to the propagation criterion of degree 1 whereas the perfect nonlinearity studied by Meier and Staffelbach [12] is equivalent to the propagation criterion of degree n where n is the number of the coordinates of the function.

Example 16 (Propagation Criterion) Consider $f = x_1x_2 \oplus x_3$, a function on V_3. Let $\alpha = (1,1,0)$. Hence

$$f(x) \oplus f(x \oplus \alpha) = (x_1x_2 \oplus x_3) \oplus ((x_1 \oplus 1)(x_2 \oplus 1) \oplus x_3) = x_1 \oplus x_2 \oplus 1$$

is balanced. Thus f satisfies the propagation criterion with respect to $\alpha = (1,1,0)$.

Example 17 (Propagation Criterion) Consider the following function on V_5

$$f(x_1,x_2,x_3,x_4,x_5) = x_1 \oplus x_1x_5 \oplus x_2x_4 \oplus x_2x_5 \oplus x_2x_4x_5 \oplus x_3x_4x_5.$$

Let $\alpha = (0,0,1,0,0)$ then

$$f(x) \oplus f(x \oplus \alpha) = x_3x_4x_5 \oplus (x_3 \oplus 1)x_4x_5 = x_4x_5$$

which is not balanced. In fact, f does not satisfy the propagation criterion with respect to any vector in the subset of vectors

$$\Re = \{(0,0,0,0,0),(0,0,0,0,1),(0,0,0,1,0),(0,0,1,0,0),(0,0,1,1,1)\}.$$

Theorem 1 *Let f be a function on V_n and A be a* nonsingular *matrix of order n over $GF(2)$. If $f(x) \oplus f(x \oplus \gamma)$ is balanced for each row γ of A. Then $\psi(x) = f(xA)$ satisfies the strict avalanche criterion (SAC).*

Theorem 2 *Let $f_1, \ldots, f_m$ be functions on V_n Set*

$$\Re = \{\gamma | f_j(x) \oplus f_j(x \oplus \alpha), \textit{is not balanced for a } j,\ 1 \leqq j \leqq m\}.$$

If $|\Re| < 2^{n-1}$ then there exists a nonsingular *matrix of order n over $GF(2)$ such that each $\psi_j(x) = f_j(xA)$ satisfies the SAC.*

Example 18 (For Theorem 1) $f = x_1x_2 \oplus x_3$ does not satisfy SAC as

$$f(x) \oplus f(x \oplus e_3) = x_1x_2 \oplus x_3 \oplus x_1x_2 \oplus (x_3 \oplus 1) = 1$$

is not balanced, for $e_3 = (001)$. On the other hand, for $e_1 = (100)$, $e_2 = (010)$, $\gamma = (111)$

$$f(x) \oplus f(x \oplus e_1) = x_2,\ f(x) \oplus f(x \oplus e_2) = x_1,\ f(x) \oplus f(x \oplus \gamma) = x_1 \oplus x_2 \oplus 1$$

are balanced.

Consider

$$A = \begin{bmatrix} e_1 \\ e_2 \\ \gamma \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

Then

$$g(x) = f(xA)$$

satisfies the SAC.

Example 19 (For Theorem 2) Let $f_1 = x_1 \oplus x_3 \oplus x_2x_3$, $f_2 = x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2x_3$ and $f_3 = x_1x_2 \oplus x_2x_3 \oplus x_1x_3$. Since f_1 does not satisfy the propagation criterion with respect to only $(1,0,0)$, f_2 does not satisfy the propagation criterion with respect to only $(1,0,1)$, and f_3 does not satisfy the propagation criterion with respect to only $(1,1,1)$. Hence $\Re = \{(1,0,0), (1,0,1), (1,1,1)\}$ and $|\Re| = 3 < 2^{n-1}$, where $n = 3$. By Theorem 2, there exists a nonsingular there exists a matrix of order 3 over $GF(2)$ such that each $\psi_j(x) = f_j(xA)$ satisfies the SAC. In fact, by using Theorem 1, A can be chosen as

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

2.4 Linear Structure

Definition 10 Let f be a function on V_n. A vector, α, is called a *linear structure* of f if $f(x) \oplus f(x \oplus \alpha)$ is constant.

Every function has at least one linear structure because of the zero vector.

Example 20 (Linear Structure) Consider the function $f = x_1x_2 \oplus x_3$ on V_3. Now $\beta = (0,0,1)$ is a linear structure of f, since

$$f(x) \oplus f(x \oplus \beta) = (x_1x_2 \oplus x_3) \oplus (x_1x_2 \oplus x_3 \oplus 1) = 1.$$

Note: a linear structure is not good for cryptographic purposes and it will be avoided or minimized in cryptographic design.

2.5 Bent Functions

We now introduce the concept of bent functions.

Definition 11 (Bent Functions) 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.

Let f be a function on V_n. We know that the following seven 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) $2^{-\frac{1}{2}n} H_n \xi^T$ is a $(1,-1)$ vector,

(iv) $f(x) \oplus f(x \oplus \alpha)$ is balanced for any non-zero vector $\alpha \in V_n$, where $x = (x_1, x_2, \ldots, x_n)$,

(v) M, the matrix of f, is an Hadamard matrix,

(vi) the nonlinearity N_f satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}n-1}$,

(vii) $D = \{x | f(x) = 1\}$ is an Hadamard difference set in V_n,

$$D = (2^n,\ 2^{n-1} \pm 2^{\frac{1}{2}n-1},\ 2^{n-2} \pm 2^{\frac{1}{2}n-1}).$$

The proof can be found in many literatures, for example, [1, 20, 27]. As examples, we now prove that bent functions can be defined as mentioned in (v), (vi) or (vii) by supposing the equivalence of (i), (ii), (iii) and (iv).

Proof. [(v) $\Leftrightarrow$ (ii)] From a very pretty result by R. L. McFarland (see Theorem 3.3 of [5])

$$M = 2^{-n} H_n diag(\langle \xi, \ell_0 \rangle, \cdots, \langle \xi, \ell_{2^n-1} \rangle) H_n, \tag{3}$$

the equivalence of (v) and (ii) is obvious. □

Proof. [(vi) ⇔ (ii)] Suppose (ii) holds i.e. $\langle \xi, \ell_j \rangle = \pm 2^{\frac{1}{2}n}$ for each linear sequence of length 2^n, say ℓ_j, that is the sequence of linear function, say φ_j. Note that $\langle \xi, 1 + \ell_j \rangle = \mp 2^{\frac{1}{2}n}$ for each linear sequence of length 2^n, ℓ_j. Note that $1+\ell_j$ is the sequence of affine function $1 \oplus \varphi_j$. From Lemma 6, for any linear φ_j, either $d(f, \varphi_j) = 2^{n-1} - 2^{\frac{1}{2}n}$ or $d(f, 1 \oplus \varphi_j) = 2^{n-1} - 2^{\frac{1}{2}n}$. This proves (vi).

Conversely, suppose (vi) holds. We prove that (ii) must hold. Otherwise, from (2), there exists a linear sequence of length 2^n, say ℓ, that is the sequence of a linear function, say φ, such that $|\langle \xi, \ell \rangle| > 2^{\frac{1}{2}n}$. Hence $\langle \xi, \ell \rangle > 2^{\frac{1}{2}n}$ or $\langle \xi, \ell \rangle < -2^{\frac{1}{2}n}$. In the first case, by Lemma 6, $d(f, \varphi_j) < 2^{n-1} - 2^{\frac{1}{2}n}$ hence $N_f < 2^{n-1} - 2^{\frac{1}{2}n}$. The second case can be rewritten as $\langle \xi, -\ell \rangle > 2^{\frac{1}{2}n}$. Note that $-\ell$ is the sequence of affine function $1 \oplus \varphi$. By the same reasoning, $d(f, 1 \oplus \varphi_j) < 2^{n-1} - 2^{\frac{1}{2}n}$ hence $N_f < 2^{n-1} - 2^{\frac{1}{2}n}$. This contradicts the assumption that $N_f = 2^{n-1} - 2^{\frac{1}{2}n}$. Hence (ii) holds. □

Proof. [(vii) ⇔ (v)] Before the proof, we introduce the concepts of difference sets and Hadamard difference sets. Let G be an Abelian group of order v and let D be a k-subset of G. D is a (v, k, λ)-*difference set* in G if for each nonzero element $g \in G$ the equation $g = d_i - d_j$ has exactly λ solutions (d_i, d_j) with $d_i, d_j \in D$. In particular, a (v, k, λ)-difference set is called an *Hadamard difference set* if $v = 4(k - \lambda)$.

Let $[D]$ be a $(0, 1)$ (real value) matrix of order $v \times v$, whose entries are label by (α, β), where $\alpha, \beta \in G$ and entry on (α, β) position is 1 if and only if $\alpha - \beta \in D$. From [6], D is a (v, k, λ)-difference set if and only if $[D]^2 = (k - \lambda)I - \lambda J$, where I is the identity matrix and J is the all-one matrix. Set $[D^*] = J - 2[D]$. Equivalently, D is a (v, k, λ)-difference set if and only if $[D^*]^2 = 4(k - \lambda)I + (v - 4(k - \lambda))J$. Hence D is a (v, k, λ)- Hadamard difference set if and only if $[D^*]$ is an Hadamard matrix.

We now prove the equivalence between (vii) and (v). Specialize G as the set of all the vectors in V_n and regard the operation of G as the boolean addition of the vectors. Hence G is an Abelian group. Specialize D as $D = \{x | f(x) = 1\}$. It is not hard to find that $[D^*]$ is identified with M, the matrix of f. From last paragraph, M is an Hadamard matrix if and only if D is a (v, k, λ)-Hadamard difference set, where $v = 2^n$ thus k must be $2^{n-1} \pm 2^{\frac{1}{2}n-1}$ and λ must be $2^{n-2} \pm 2^{\frac{1}{2}n-1}$ (see [6]). □

It was Rothaus who first introduced and studied bent functions [19]. Other issues related to bent functions, such as their properties, construction and enumeration, can be found in [1, 7, 9, 15, 27]. Kumar, Scholtz and Welch [8] 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 [2, 4, 9, 10, 11, 12, 13, 15].

Example 21 (for Hadamard Difference Set) $f = x_1x_2 \oplus x_3x_4$ is a bent function on V_4. Hence, from (vii), $D = \{x | f(x) = 1\} = \{(0011), (0111), (1011), (1100), (1101), (1110)\}$ is an Hadamard difference set.

Basic Properties of Bent Functions

Let f be a bent function on V_n then

1. n must be even,
2. the degree of f is less than or equal to $\frac{1}{2}n$, except for $n = 2$,
3. for any affine function φ, $f \oplus \varphi$ is also bent,
4. $f(xA \oplus \alpha)$ is also bent where A is any nonsingular matrix of order n, and α is any vector in V_n,
5. f takes the value zero $2^{n-1} \pm 2^{\frac{1}{2}n-1}$ times,
6. $2^{-\frac{1}{2}n} H_n \xi^T$ is also a bent sequence.

Example 22 (Bent Function) We now prove that $f(x) = x_1 x_2$ is a bent function on V_2.

1. *Proof* (using sequences).
   The truth table of f is

   $$f(0,0) = 0,\ f(0,1) = 0,\ f(1,0) = 0, f(1,1) = 1$$

   Now consider the Sylvester-Hadamard matrix of order 2^2

   $$H_2 = \begin{bmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{bmatrix} = \begin{bmatrix} \ell_1 \\ \ell_2 \\ \ell_3 \\ \ell_4 \end{bmatrix}.$$

   We consider

   $$\langle \xi, \ell_1 \rangle = 2, \langle \xi, \ell_2 \rangle = 2, \langle \xi, \ell_3 \rangle = 2, \langle \xi, \ell_4 \rangle = -2,$$

   thus the sequence of f is

   $$\xi = + \ + \ + \ - .$$

   Hence the statement (ii) is satisfied.

2. *Proof* (using matrices).
   The matrix of f is

   $$M = \begin{bmatrix} + & + & + & - \\ + & + & - & + \\ + & - & + & + \\ - & + & + & + \end{bmatrix},$$

   which is an Hadamard matrix as $MM^T = 4I_4$.

3. *Proof* (using balance).
   Let $\alpha = (a_1, a_2) \neq (0,0)$.
   $f(x) \oplus f(x \oplus \alpha) = x_1 x_2 \oplus (x_1 \oplus a_1)(x_2 \oplus a_2) = a_1 x_2 \oplus a_2 x_1 \oplus a_1 a_2$ is a nonconstant affine function thus 0-1 balanced.

Example 23 (Bent Functions Are Not Balanced) $f = x_1x_2 \oplus x_3x_4$ is a bent function on V_4. The truth table of f is

$$0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 1,\ 1,\ 1,\ 0.$$

f takes the value zero $2^{4-1} + 2^{\frac{1}{2}4-1} = 8 + 2 = 10$ times Therefore this function is not balanced.

3 The Relationship Between Avalanche Effect and Nonlinearity

Let f be a function on V_n, $\xi(\alpha)$ be the sequence of $f(x \oplus \alpha)$. Thus $\xi(0) * \xi(\alpha)$ is the sequence of $f(x) \oplus f(x \oplus \alpha)$.

Define $\Delta(\alpha)$, the *excess* of α, to be $\Delta(\alpha) = \langle \xi(0), \xi(\alpha) \rangle$.

Let ℓ_i be the ith row of H_n. By Lemma 2 of [23], ℓ_i is the sequence of linear function $\varphi_i = \langle \alpha_i, x \rangle$, where α_i is defined as in Definition 1.

Lemma 10 *Let f be a function on V_n. Then the Hamming weight of $f(x) \oplus f(x \oplus \alpha)$ is equal to $2^{n-1} - \frac{1}{2}\Delta(\alpha)$.*

Proof. Let e_+ (e_-) denote the number of ones (minus ones) in the sequence of $\xi(0) * \xi(\alpha)$. Thus $e_+ - e_- = \Delta(\alpha)$ and $(2^n - e_-) - e_- = \Delta(\alpha)$ and $e_- = 2^{n-1} - \frac{1}{2}\Delta(\alpha)$. Note that e_- is also the number of ones in the truth table of $f(x) \oplus f(x \oplus \alpha)$. Thus the lemma holds. □

Obviously, by Lemma 10,

Lemma 11 *$\Delta(\alpha) = 0$ if and only if $f(x) \oplus f(x \oplus \alpha)$ is balanced i.e. f satisfies the propagation criterion with respect to α.*

If $|\Delta(\alpha)| = 2^n$ then $f(x) \oplus f(x \oplus \alpha)$ is constant and then α is a linear structure (see [14]).

However the propagation criterion is not satisfied by every function. In most cases, $\Delta(\alpha) \neq 0$ but is relatively small, thus $f(x) \oplus f(x \oplus \alpha)$ is nearly balanced, and thus f has good avalanche effects.

To measure the avalanche effect of a function, say f, with respect to every vector we consider

$$\sum_{\alpha \in V_n} \Delta^2(\alpha),$$

which we hope will be as small as possible. In fact, it is smallest for bent functions and largest for affine functions.

Let M be the matrix of f (see Section 1), ξ be the sequence of f. From (3), the first row of MM^T is

$$(\Delta(\alpha_0), \Delta(\alpha_1), \cdots, \Delta(\alpha_{2^n-1})).$$

The first row of

$$2^{-n} H_n diag(\langle \xi, \ell_0 \rangle^2, \cdots, \langle \xi, \ell_{2^n-1} \rangle^2) H_n$$

can be expressed as

$$2^{-n}(\langle \xi^*, \ell_0 \rangle, \cdots, \langle \xi^*, \ell_{2^n-1} \rangle) = 2^{-n} \xi^* H_n$$

where

$$\xi^* = (\langle \xi, \ell_0 \rangle^2, \cdots, \langle \xi, \ell_{2^n-1} \rangle^2).$$

Thus

$$(\Delta(\alpha_0), \Delta(\alpha_1), \cdots, \Delta(\alpha_{2^n-1})) = 2^{-n}(\langle \xi, \ell_0 \rangle^2, \cdots, \langle \xi, \ell_{2^n-1} \rangle^2) H_n.$$

We have now constructed infinite balanced functions with nonlinearity greater than the lower bounds.

Theorem 3 *Let f be a function on V_n. Then*

$$(\Delta(\alpha_0), \Delta(\alpha_1), \cdots, \Delta(\alpha_{2^n-1})) H_n = (\langle \xi, \ell_0 \rangle^2, \cdots, \langle \xi, \ell_{2^n-1} \rangle^2).$$

Theorem 3 shows the relationship between the nonlinearity and the avalanche effect. This can be seen from Lemma 10 and the following fact (see Lemma 4 of [23])

$$d(g_1, g_2) = 2^{n-1} - \frac{1}{2} \langle \eta_1, \eta_2 \rangle$$

where each η_i is the sequence of function g_i on V_n.

Write $\eta = (\Delta(\alpha_0), \Delta(\alpha_1), \cdots, \Delta(\alpha_{2^n-1}))$. Since

$$\langle \xi^*, \xi^* \rangle = \langle \eta H_n, \eta H_n \rangle = \eta H_n H_n^T \eta^T = 2^n \langle \eta, \eta \rangle$$

$$\sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^4 = 2^n \sum_{\alpha \in V_n} \Delta^2(\alpha).$$

Thus we have

Corollary 1 *Let f be a function on V_n. Then*

$$\sum_{\alpha \in V_n} \Delta^2(\alpha) = 2^{-n} \sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^4.$$

From Corollary 1, we can unite the nonlinearity and the difference of a function on V_n, say f, by a new criterion, denoted by $\sigma(f)$, defined as follows

$$\sigma(f) = \sum_{\delta \in V_n} \Delta^2(\alpha) = 2^{-n} \sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^4.$$

From Theorem 1, the larger the nonlinearity of a function is the better the avalanche effect is.

Theorem 4 *Let f be a function on V_n. Then*

(i) $2^{2n} \leqq \sigma(f) \leqq 2^{3n}$,

(ii) $\sigma(f) = 2^{2n}$ *if and only if f is a bent function,*

(iii) $\sigma(f) = 2^{3n}$ *if and only if f is an affine function.*

Proof. (i) By Theorem 1,

$$\sigma(f) = 2^{-n} \sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^4 = 2^{-n} (\sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^2)^2.$$

From (2), we have

$$\sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^2 = 2^{2n}.$$

Thus

$$\sigma(f) \leqq 2^{-n} 2^{4n} = 2^{3n}.$$

(ii) Note that $\Delta(0) = 2^n$.

$$\sigma(f) = \sum_{\alpha \in V_n} \Delta^2(\alpha) = \Delta^2(0) = 2^{2n}. \tag{4}$$

From (4), $\sigma(f) = 2^{2n}$ if and only if $\Delta(\alpha) = 0$ for any $\alpha \neq 0$ i.e. f is bent (see 1).

(iii) Set $y_j = \langle \xi, \ell_j \rangle^2$. By Parseval's equation, $\sum_{j=0}^{2^n-1} y_j = 2^n$.

It is not hard to see $\sigma(f) = 2^{3n} \Longleftrightarrow 2^{-n} \sum_{j=0}^{2^n-1} y_j^2 = 2^{3n} \Longleftrightarrow \sum_{j=0}^{2^n-1} y_j^2 = 2^{4n} \Longleftrightarrow \sum_{j=0}^{2^n-1} y_j^2 = (\sum_{j=0}^{2^n-1} y_j)^2 \Longleftrightarrow y_i y_j = 0$ if $j \neq i \Longleftrightarrow$ there exists a j_0 such that $y_{j_0} = 2^{2n}$ and $y_j = 0$ if $j \neq j_0 \Longleftrightarrow$ there exists a j_0 such that $\langle \xi, \ell_{j_0} \rangle = \pm 2^n$ and $\langle \xi, \ell_j \rangle = 0$ if $j \neq j_0 \Longleftrightarrow$ there exists a j_0 such that $\xi = \pm \ell_{j_0}$ i.e. f is an affine function. □

4 Some Balanced Functions

Bent functions have the largest nonlinearity and the smallest difference but are not balanced thus they cannot be used in most cryptographic designs. In [22, 20, 21, 23] the authors constructed balanced functions having high nonlinearity and satisfying the propagation criterion. We now analyze $\delta(f)$ for each construction.

4.1 Concatenating Bent Functions

4.1.1 On V_{2k+1}

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

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

Set

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

where A is any nonsingular matrix of order $2k+1$ over $GF(2)$. By Corollary 6 of [23], g^* is a balanced function on V_{2k+1} and satisfies the propagation criterion with respect to all non-zero vectors except for γ^* where γ^* is the first row of A. The nonlinearity of g^* satisfies $N_{g^*} \geqq 2^{2k} - 2^k$.

For any nonzero vector $\alpha \in V_{2k+1}$, Consider $g(x) \oplus g(x \oplus \alpha)$.

Case 1: $\alpha \neq (1,0,\ldots,0)$. From the definition of g, $g(x) \oplus g(x \oplus \alpha)$ is balanced thus $\Delta(\alpha) = 0$.

Case 2: $\alpha = (1,0,\ldots,0) = \alpha_1$. From the definition of g, $g(x) \oplus g(x \oplus \alpha) = 1$, for all $x \in V_{2k+1}$. Thus $\Delta(\alpha_1) = -2^{2k+1}$.

Hence

$$\sigma(g) = \sum_{\alpha \in V_{2k+1}} \Delta^2(\alpha) = \Delta^2(0) + \Delta^2(\alpha_1) = 2 \cdot 2^{4k+2} = 2^{4k+3}.$$

Note that $\sigma(g)$ is invariant under any nondegenerate linear transformation on the variables. Thus $\sigma^*(g^*) = 2^{4k+3}$. By Theorem 4, the lower bound of $\sigma(f)$, where f is a function on V_{2k+1}, is 2^{2k+1}. However this bound cannot be reached as this bound is only attained by bent functions and bent functions only exist in even dimension vector spaces.

By Lemma 10 of [23], the nonlinearity and the number of vectors for which the propagation criterion is satisfied, is the same for g^* and g.

Unfortunately, g has a linear structure although it satisfies the propagation criterion with respect to other nonzero vectors.

4.1.2 On V_{2k}

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

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

Set

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

where A is any nonsingular matrix of order $2k$ over $GF(2)$. By Corollary 7 of [23], g^* is a balanced function on V_{2k} and satisfies the propagation criterion with respect to all but three non-zero vectors. The nonlinearity of g^* satisfies $N_{g^*} \geqq 2^{2k-1} - 2^k$.

For any nonzero vector $\alpha \in V_{2k}$, Consider $g(x) \oplus g(x \oplus \alpha)$.

Write $\alpha_1 = (1, 0, \ldots, 0)$, $\alpha_2 = (0, 1, \ldots, 0)$, $\alpha_3 = (1, 1, \ldots, 0)$.

Case 1: $\alpha \neq \alpha_1, \alpha_2, \alpha_3$. From the definition of g, $g(x) \oplus g(x \oplus \alpha)$ is balanced thus $\Delta(\alpha) = 0$.

Case 2: $\alpha = \alpha_j$, $j = 1, 2, 3$. From the definition of g, $g(x) \oplus g(x \oplus \alpha_j) = 1$, $j = 1, 2$, for all $x \in V_{2k+1}$. Thus $\Delta(\alpha_j) = -2^{2k}$, $j = 1, 2$. $g(x) \oplus g(x \oplus \alpha_3) = 0$, since $\Delta(\alpha_3) = 2^{2k}$.

Thus

$$\sigma(g) = \sum_{\alpha \in V_{2k}} \Delta^2(\alpha) = \Delta^2(0) + \sum_{j=1}^{3} \Delta^2(\alpha_j) = 4 \cdot 2^{4k} = 2^{4k+2}.$$

Note that $\sigma(g)$ is invariant under any nondegenerate linear transformation on the variables. Thus $\sigma(g^*) = 2^{4k+2}$. By Theorem 4, the lower bound of $\sigma(f)$, where f is a function on V_{2k}, is 2^{2k}. But this bound is reached only by bent functions and not by balanced functions.

By Lemma 10 of [23], the nonlinearity and the number of vectors to which the propagation criterion is satisfied, is the same for g^* and g.

Unfortunately, g has three linear structures although it satisfies the propagation criterion with respect to other nonzero vectors.

4.2 Concatenating Linear Functions

Let $p < q$, $y = (y_1, \ldots, y_p)$ and $x = (x_1, \ldots, x_q)$. Since there exist 2^q distinct linear functions on V_q, we can choose 2^p different those and give each a subscript δ, $\delta \in V_p$. Write the set of the 2^p linear functions as $\Re$.

We can construct balanced, highly nonlinear functions satisfying the propagation criterion by the following method

$$g(z) = g(y, x) = \bigoplus_{\delta \in V_p} D_\delta(y) \varphi_\delta(x) \tag{5}$$

where $z = (y, x)$.

By Lemma 3 of [21],

(i) g is balanced,

(ii) the nonlinearity of g satisfies $N_g \geqq 2^{p+q-1} - 2^{q-1}$,

(iii) g satisfies the propagation criterion with respect to any $\gamma = (\beta, \alpha)$ with $\beta \neq 0$, where $\beta \in V_p$ and $\alpha \in V_q$,

(iv) the degree of g can be $p + 1$ if $\Re$ is appropriate.

Let ξ_δ is the sequence of φ_δ and η is the sequence of g. By Lemma 1 of [20], η is a concatenation of 2^p distinct ξ_δ.

Note that $H_{p+q} = H_p \times H_q$. and hence any row of H_{p+q}, say L, can be represented as $L = \ell' \times \ell''$, where ℓ' is a row of H_p and ℓ'' is a row of H_q.

Since different rows of H_p is orthogonal

$$\langle \eta, L \rangle = \begin{cases} 2^q & \text{if } f \in \Re, \text{ where} L = \ell' \times \ell'' \\ 0 & \text{if } f \notin \Re, \text{ where } L = \ell' \times \ell'' \end{cases}$$

where f is the corresponding linear function of ℓ''.

Note that there exist $2^p \cdot 2^p$ L such that the corresponding linear function of ℓ'' belongs to $\Re$, where $L = \ell' \times \ell''$.

By Theorem 1,

$$\sigma(g) = 2^{-p-q} 2^p \cdot 2^p \cdot 2^{4q} = 2^{p+3q}.$$

Note that $\sigma(g)$ is invariable under any nondegenerate linear transformation on the variables. Thus $\sigma(g^*) = 2^{p+3q}$. By Theorem 4, the lower bound of $\sigma(f)$, where f is a function on V_{p+q}, is 2^{2p+2q}. But this bound is reached only by bent functions instead of balanced functions.

By Lemma 10 of [23], the nonlinearity and the number of vectors to which the propagation criterion is satisfied, of g^* is the same with g.

We now prove the following conclusion.

If there exists $\delta_0 \in V_p$ such that

$$rank \ \ of \ \ \{\varphi_\delta \oplus \varphi_{\delta_0} | \delta \in V_p\} = q$$

then g, defined in (5), has no linear structures.

Consider

$$g(z) \oplus g(z \oplus \gamma) = g(y, x) \oplus g(y \oplus \beta, x \oplus \alpha). \tag{6}$$

(iii) of Lemma 3 of [21] (see a previous paragraph in this subsection) (6) is balanced for $\beta \neq 0$.

Thus to find a linear structure of g we only need to discuss (6) for $\beta = 0$. In this case (6) is specialized as

$$\begin{aligned} g(z) \oplus g(z \oplus \gamma) &= g(y, x) \oplus g(y, x \oplus \alpha) \\ = \bigoplus_{\delta \in V_p} D_\delta(y)(\varphi_\delta(x) \oplus \varphi(x \oplus \alpha) &= \bigoplus_{\delta \in V_p} D_\delta(y)\varphi_\delta(\alpha). \end{aligned} \tag{7}$$

Clearly, $\gamma = (0, \alpha)$ is a linear structure if and only if (7) is constant if and only if

$$\varphi_\delta(\alpha) = c \tag{8}$$

for every $\delta \in V_p$, where $c \in GF(2)$. (8) is equivalent to

$$\varphi_\delta(\alpha) \oplus \varphi_{\delta_0}(\alpha) = 0 \tag{9}$$

for each $\delta \in V_p$. Since the rank of $\{\varphi_\delta \oplus \varphi_{\delta_0} | \delta \in V_p\} = q$, also $\alpha \in V_q$, there exists no nonzero α satisfying (9), a set of linear equations about α. This proves that g has no linear structures.

The condition in this conclusion is easy to satisfy. For example, $h_1(x) = x_1$, $h_2(x) = x_2$, ..., $h_q(x) = x_q$ are linearly independent functions on V_q. Let φ_0 be an arbitrary linear function on V_q. Write $\varphi_j = h_j \oplus \varphi_0$, $j = 1, 2, \ldots, q$. Thus $\varphi_1 \oplus \varphi_0$, ..., $\varphi_q \oplus \varphi_0$ are linearly independent. To construct function g, defined by (5), we need 2^p linear functions on V_q, whose collection is denoted by $\mho = \{\varphi_\delta, | \delta \in V_p\}$. Count $\varphi_1 = h_1 \oplus \varphi_0$, ... $\varphi_q = h_q \oplus \varphi_0$ and φ_0, as $q+1$ linear functions in $\mho$ and choose any $2^p - q - 1$ linear functions on V_q as the rest we construct $\mho$. Clearly $\mho$ satisfies the condition in the above conclusion.

Also, g still satisfies (i), (ii), (iii), (iv), mentioned in the beginning of this subsection. We only need to expline (iv). Since $2^p - p - 1$ linear functions can be chosen arbitrarily after $q+1$ linear functions are fixed, we can make $\bigoplus_{\delta \in V_p} \varphi_\delta \neq 0$. By the proof of Lemma 3 of [21], the degree of g is $p+1$.

The request that a function has no linear structures is an important criterion for cryptographic function as a linear structure shows the function has an unnecessary variable that will be identified by cryptographic attack.

It is impossible to calculate the maximum Δ_γ of functions constructed in (5) unless further request or information are given. However we guarantee that we can easily construct functions without linear structures using (5).

5 New Construction of Cryptographic Functions with Small Difference

In this section we construct balanced functions having high nonlinearity and satisfying the propagation criterion with respect to many vectors. Furthermore we require the functions to have small $\sigma(f)$ and difference. Big difference with respect to a nonzero vector implies the avalanche effect of the function is week. In particular, if the difference with respect to a nonzero vector reaches the maxmun value i.e. the vector is a linear structure, the function contains an unnecessary variable. In this paper we are concerned with the difference as well as other criteria and make the difference as small as possible. At least, we require the functions to have no linear structure.

5.1 On V_{2k}

For $z \in V_{2k}$, write $z = (y, x)$, $y \in V_k$, $x \in V_k$. Set

$$g(z) = g(y, x) = \begin{cases} \langle y, x \rangle & \text{if } y \neq 0 \\ \langle \alpha_1, x \rangle & \text{if } y = 0 \end{cases} \tag{10}$$

where where $\alpha_0, \alpha_1, \ldots, \alpha_{2^k-1}$ are defined as at beginning of Section 1.

Obviously, for any fixed $\alpha \in V_k$, $g(\alpha, x)$ is a nonzero linear function and thus balanced. Hence we have

Lemma 12 *g, a function on V_{2k}, defined as in (10), is balanced.*

Let $\gamma = (\beta, \alpha)$ be a nonzero vector in V_{2k}, where $\beta, \alpha \in V_k$. By the definition of $\Delta(\gamma)$

$$\Delta(\gamma) = \sum_{y \in V_k} \sum_{x \in V_k} (-1)^{g(y,x) \oplus g(y \oplus \beta, x \oplus \alpha)}.$$

Case 1: $\beta \neq 0$.

$$\Delta(\gamma) = \sum_{y=0,\beta} \sum_{x \in V_k} (-1)^{g(y,x) \oplus g(y \oplus \beta, x \oplus \alpha)} + \sum_{y \neq 0,\beta} \sum_{x \in V_k} (-1)^{g(y,x) \oplus g(y \oplus \beta, x \oplus \alpha)}.$$

For $y = 0$,

$$g(0, x) \oplus g(\beta, x \oplus \alpha) = \langle \alpha_1, x \rangle \oplus \langle \beta, x \oplus \alpha \rangle = \langle \alpha_1 \oplus \beta, x \rangle \oplus \langle \beta, \alpha \rangle. \tag{11}$$

For $y = \beta$,

$$g(\beta, x) \oplus g(0, x \oplus \alpha) = \langle \beta, x \rangle \oplus \langle \alpha_1, x \oplus \alpha \rangle = \langle \alpha_1 \oplus \beta, x \rangle \oplus \langle \alpha_1, \alpha \rangle. \tag{12}$$

For $y \neq 0, \beta$,

$$g(y, x) \oplus g(y \oplus \beta, x \oplus \alpha) = \langle y, x \rangle \oplus \langle y \oplus \beta, x \oplus \alpha \rangle = \langle \beta, \alpha \rangle \oplus \langle \beta, x \rangle \oplus \langle y, \alpha \rangle. \tag{13}$$

Case1.1: $\beta = \alpha_1$. In this case, (11) becomes $\langle \beta, \alpha \rangle$, (12) becomes $\langle \alpha_1, \alpha \rangle$ and (13) is a nonzero linear function of x for fixed y and thus balanced. Hence

$$\Delta(\gamma) = \sum_{x \in V_k} [(-1)^{\langle \alpha_1, \alpha \rangle} + (-1)^{\langle \alpha_1, \alpha \rangle}] =$$

$$2 \cdot 2^k \cdot c = 2^{k+1} c$$

where $c = (-1)^{\langle \alpha_1, \alpha \rangle} = \pm 1$.

Case 1.2: $\beta \neq \alpha_1$. (11), (12) and (13) are all nonzero linear functions and thus balanced. Hence $\Delta(\gamma) = 0$.

Case 2: $\beta = 0$. In this case, $\alpha \neq 0$ is necessary. (10) is specialized as

$$\Delta(\gamma) = \sum_{x \in V_k} (-1)^{g(0,x) \oplus g(0, x \oplus \alpha)} + \sum_{y \neq 0} \sum_{x \in V_k} (-1)^{g(y,x) \oplus g(y \oplus \beta, x \oplus \alpha)}.$$

For $y = 0$,

$$g(0,x) \oplus g(0, x \oplus \alpha) = \langle \alpha_1, x \rangle \oplus \langle \alpha_1, x \oplus \alpha \rangle = \langle \alpha_1, \alpha \rangle. \tag{14}$$

For $y \neq 0$,

$$g(y,x) \oplus g(y, x \oplus \alpha) = \langle y, x \rangle \oplus \langle y, x \oplus \alpha \rangle = \langle y, \alpha \rangle. \tag{15}$$

$$\Delta(\gamma) = \sum_{x \in V_k} (-1)^{\langle \alpha_1, \alpha \rangle} + \sum_{y \neq 0} \sum_{x \in V_k} (-1)^{\langle y, \alpha \rangle} =$$

$$\sum_{x \in V_k} (-1)^{\langle \alpha_1, \alpha \rangle} + \sum_{y \in V_k} \sum_{x \in V_k} (-1)^{\langle y, \alpha \rangle} - \sum_{x \in V_k} (-1)^{\langle 0, \alpha \rangle}.$$

Note that $\langle y, \alpha \rangle$ is a nonzero linear function and thus balanced.

$$\Delta(\gamma) = \sum_{x \in V_k} (-1)^{\langle \alpha_1, \alpha \rangle} - \sum_{x \in V_k} (-1)^{\langle 0, \alpha \rangle} = \sum_{x \in V_k} [(-1)^{\langle \alpha_1, \alpha \rangle} - 1] =$$

$$\begin{cases} 0 & \text{if } \langle \alpha_1, \alpha \rangle = 0 \\ 2^{k+1} & \text{if } \langle \alpha_1, \alpha \rangle = 1 \end{cases}$$

Summarize Cases 1 and 2, we conclude

Lemma 13 *Let g, be the function on V_{2k}, defined as in (10). Then*

$$|\Delta(\gamma)| \leqq 2^{k+1}$$

for any nonzero vector $\gamma \in V_{2k}$.

Lemma 13 shows that function g has no linear structure furthermore the difference with respect to any nonzero vector is bounded by a small value.

In Case 1.2, $\Delta(\gamma) = 0$, $\beta \neq 0$, $\beta \neq \alpha_1$, α is arbitrary. There exist $(2^k - 2)2^k = 2^{2k} - 2^{k+1}$ such $\gamma = (\beta, \alpha)$.

In Case 2, $\Delta(\gamma) = 0$, $\beta = 0$. α satisfies $\alpha \neq 0$ and $\langle \alpha_1, \alpha \rangle = 0$, that has $2^{k-1} - 1$ nonzero solutions of α.

Hence there exist $2^{2k} - 2^{k+1} + 2^{k-1} - 1$ $\gamma = (\beta, \alpha)$ such that $\Delta(\gamma) = 0$. Since $\Delta(\gamma) = 0$ if and only if $g(z) \oplus g(z \oplus \gamma)$ is balanced, we have the following conclusion

Lemma 14 *g, a function on V_{2k}, defined as in (10) satisfies the propagation criterion with respect to $2^{2k} - 2^{k+1} + 2^{k-1} - 1$ nonzero vectors.*

Let ℓ_i be the sequence of linear function, on V_k, $\langle \alpha_i, x\rangle$. By Lemma 2 of [20], ℓ_i is the ith row of H_k, $i = 0, 1, \ldots, 2^k - 1$.

Let ξ be the sequence of g, defined as in (10). From Lemma 1 of [20],

$$\xi = (\ell_1, \ell_1, \ell_2, \ldots, \ell_{2^k-1}).$$

Let L_s be the sth row of H_{2k}. By Lemma 2 of [20], L_s is a linear sequence of length 2^{2k}. Since $H_{2k} = H_k \times H_k$, L_s can be rewritten as $L_s = \ell_p \times \ell_q$, for some p and q, $0 \leqq p, q, \leqq 2^k - 1$.

Write $\ell_p = (c_0, c_1, \ldots, c_{2^k-1})$ thus

$$L_s = (c_0\ell_q, c_1\ell_q, \ldots, c_{2^k-1}\ell_q).$$

Since H_k is a Hadamard matrix, $\langle \ell_i, \ell_j\rangle = 0$, if $j \neq i$.

Hence

$$\langle \xi, L_s\rangle = \begin{cases} (c_0 + c_1)\langle \ell_1, \ell_1\rangle = (c_0 + c_1)2^k & \text{if } q = 1 \\ \pm 2^k & \text{if } q \neq 0, 1 \\ 0 & \text{if } q = 0 \end{cases}$$

Note that $c_0 = 1$ and $c_1 = \pm 1$. There exist 2^{k-1} ℓ_p such that $c_1 = 1$. Hence there exist 2^{k-1} L_s such that $L_s = \ell_p \times \ell_q$ with $c_1 = 1$ and $q = 1$. For such L_s $\langle \xi, L_s\rangle = 2^{k+1}$.

For $c_1 = -1$, $\langle \xi, L\rangle = 0$.

There exits $2^k \cdot (2^k - 2)$ L_s such that $L_s = \ell_p \times \ell_q$ with $q \neq 0, 1$. For such L_s $\langle \xi, L_s\rangle = \pm 2^k$.

Hence

$$\begin{aligned} \sigma(g) &= 2^{-2k} \sum_{s=0}^{2^{2k}-1} \langle \xi, L_s\rangle^4 = 2^{k-1} \cdot 2^{4(k+1)} + 2^k \cdot (2^k - 2) \cdot 2^{4k} \\ &= 2^{4k} + 2^{3k+3} - 2^{3k+1}. \end{aligned}$$

This proves that the following conclusion

Lemma 15 *g, a function on V_{2k}, defined as in (10) satisfies $\sigma(g) = 2^{4k} + 2^{3k+3} - 2^{3k+1}$.*

Note that $|\langle \xi, L_s\rangle| \leqq 2^{k+1}$ for any L_s, that is a row of H_{2k}, also a linear sequence of length 2^{2k}. By using Lemma 3 of [20], we have

Lemma 16 *g, a function on V_{2k}, defined as in (10) satisfies $N_g \geqq 2^{2k-1} - 2^k$.*

Summarize Lemmas 12, 13, 14, 15 and 16 we have

Theorem 5 *Let g be the function on V_{2k}, defined as in (10). Then*

(i) g *is balanced;*

(ii) $N_g \geqq 2^{2k-1} - 2^k$,

(iii) g *satisfies the propagation criterion with respect to* $2^{2k} - 2^{k+1} + 2^{k-1} - 1$ *nonzero vectors,*

(iv) $\sigma(g) = 2^{4k} + 2^{3k+3} - 2^{3k+1}$,

(v) $|\Delta(\gamma)| \leqq 2^{k+1}$ *for any nonzero vector* $\gamma \in V_{2k}$.

Furthermore, since g does not satisfies the propagation criterion with respect to $2^{2k} - (2^{2k} - 2^{k+1} + 2^{k-1} - 1) = 2^{k+1} - 2^{k-1} + 1 < 2^{2k-1}$ vectors, by Theorem 2 of [22], there exists a nonsingular matrix of order $2k$ over $GF(2)$, say A, such that $h(z) = f(zA)$ satisfies the strict avalanche criterion (SAC).

5.2 On V_{2k+1}

Lemma 17 *There exists a permutation on* V_k, *say* $m(u)$, *such that* $u \oplus m(u)$ *runs through all the vectors in* V_k *while* u *runs through* V_k *once.*

Proof. There are many proofs of this lemma. For example, from Section 4, [21], there exists a matrix, say E, of order 2^k with entries linear functions on V_k such that each row (except for the top row) is a listing of all the linear functions on V_k and the sum of any two distinct rows is a listing of all linear functions on V_k.

Let the second and the third rows be

$$\varphi_{2,0}, \varphi_{2,1}, \ldots, \varphi_{2,2^k-1}$$

and

$$\varphi_{3,0}, \varphi_{3,1}, \ldots, \varphi_{3,2^k-1}$$

respectively, where each φij is a linear function on V_k. Define a permutation m on all linear functions on V_k by the following regulation

$$m(\varphi_{2,j}) = \varphi_{3,j}$$

$j = 0, 1, \ldots, 2^k - 1$. By the property of matrix E,

$$\varphi_{2,j} \oplus m(\varphi_{2,j}) = \varphi_{2,j} \oplus \varphi_{3,j}$$

runs through all the linear functions on V_k while j runs through $0, 1, \ldots, 2^k - 1$. Since all the linear functions on V_k is also a vector space isomorphic to V_k the lemma has been proved. □

Write $W_1 = \{(0, u) | u \in V_k\}$, $W_2 = \{(1, u) | u \in V_k\}$, where $0, 1 \in GF(2)$. Obviously, $V_{k+1} = W_1 \cup W_2$.

For any $y \in V_{k+1}$, write $y = (y_1, u)$, $y_1 \in GF(2)$, $u \in V_k$.

For $z \in V_{2k+1}$, write $z = (y, x)$, $y \in V_{k+1}$, $x \in V_k$. Set

$$g(z) = g(y,x) = \begin{cases} 1 \oplus \langle u, x \rangle & \text{if } y \in W_1 \\ \langle m(u), x \rangle & \text{if } y \in W_2 \end{cases} \tag{16}$$

For any fixed $\alpha \in V_k$, there exists a unique $\alpha' \in V_k$, such that $m(\alpha') = \alpha$. Write $y' = (0, \alpha)$, $y'' = (1, \alpha')$. By the definition in (16), $g(y', x) = 1 \oplus \langle \alpha, x \rangle$ and $g(y'', x) = \langle m(\alpha'), x \rangle = \langle \alpha, x \rangle$. This proves the following lemma

Lemma 18 *g, a function on V_{2k+1}, defined as in (16), is balanced.*

Let $\gamma = (\beta, \alpha)$ be a nonzero vector in V_{2k+1}, where $\beta \in V_{k+1}$, $\alpha \in V_k$. By the definition of $\Delta(\gamma)$

$$\Delta(\gamma) = \sum_{y \in W_1} \sum_{x \in V_k} (-1)^{g(y,x) \oplus g(y \oplus \beta, x \oplus \alpha)} + \sum_{y \in W_2} \sum_{x \in V_k} (-1)^{g(y,x) \oplus g(y \oplus \beta, x \oplus \alpha)}.$$

Case 1: $\beta \neq 0$.

Case 1.1: $\beta \in W_1$ thus $y \in W_1$ implies $y \oplus \beta \in W_1$ and $y \in W_2$ implies $y \oplus \beta \in W_2$.

Write $\beta = (0, \tau)$. Since $\beta \neq 0$, $\tau \neq 0$. For $y \in W_1$,

$$g(y,x) \oplus g(y \oplus \beta, x \oplus \alpha) = \langle u, x \rangle \oplus \langle u \oplus \beta, x \oplus \alpha \rangle = \langle u, \alpha \rangle \oplus \langle \tau, x \rangle \oplus \langle \tau, \alpha \rangle$$

is a nonzero linear function of x for a fixed y.

$$g(y,x) \oplus g(y \oplus \beta, x \oplus \alpha) = \langle m(u), x \rangle \oplus \langle m(u \oplus \beta), x \oplus \alpha \rangle =$$

$$\langle m(u) \oplus m(u \oplus \tau), x \rangle \oplus \langle m(u \oplus \beta), \alpha \rangle$$

is a nonzero linear function and thus balanced since $m(u) \oplus m(u \oplus \tau) \neq 0$ for $\tau \neq 0$. Hence $\Delta(\gamma) = 0$.

Case 1.2: $\beta \in W_2$ thus $y \in W_1$ implies $y \oplus \beta \in W_2$ and $y \in W_2$ implies $y \oplus \beta \in W_1$.

For $y \in W_1$,

$g(y,x) \oplus g(y \oplus \beta, x \oplus \alpha) = \langle u, x \rangle \oplus \langle m(u \oplus \tau), x \oplus \alpha \rangle = \langle u \oplus m(u \oplus \tau), x \rangle \oplus \langle m(u \oplus \tau), \alpha \rangle$.

By the properties of permutation $m(u)$, there exists a unique u_0 such that

$$m(u_0) \oplus m(u_0 \oplus \tau) = 0. \tag{17}$$

Thus $g(y,x) \oplus g(y \oplus \beta, x \oplus \alpha)$ is a nonzero linear function and thus balanced for any fixed $y = (0, u) \neq (0, u_0)$.

For $y \in W_2$,

$$g(y,x) \oplus g(y \oplus \beta, x \oplus \alpha) = \langle m(u), x\rangle \oplus \langle u \oplus \tau, x \oplus \alpha\rangle =$$

$$\langle m(u) \oplus u \oplus \tau, x\rangle \oplus \langle u \oplus \tau, \alpha\rangle.$$

By the properties of permutation $m(u)$, there exists a unique u_* such that

$$m(u_*) \oplus u_* \oplus \tau = 0. \tag{18}$$

Thus $g(y,x) \oplus g(y \oplus \beta, x \oplus \alpha)$ is a nonzero linear function and thus balanced for any fixed $y \neq (1,u), (1,u_*)$.

$$\Delta(\gamma) = \sum_{x \in V_k} (-1)^{\langle m(u_0 \oplus \tau), \alpha\rangle} + \sum_{x \in V_k} +(-1)^{\langle u_* \oplus \tau, \alpha\rangle}.$$

Rewrite (17) and (18) as

$$m(u_0 \oplus \tau) \oplus u_0 \oplus \tau = \tau$$

and

$$m(u_*) \oplus u_* = \tau$$

respectively. By the properties of permutation $m(u)$, $m(u_*) = u \oplus \tau$. This causes $m(u_0 \oplus \tau) = u_* \oplus \tau$. Hence

$$\Delta(\gamma) = 2^k[(-1)^{\langle m(u_0 \oplus \tau), \alpha\rangle} + (-1)^{\langle u_* \oplus \tau, \alpha\rangle}] = \pm 2^{k+1}.$$

Case 2: $\beta = 0$. In this case, $\alpha \neq 0$ is necessary.

$$\Delta(\gamma) = \sum_{y \in W_1} \sum_{x \in V_k} (-1)^{g(y,x) \oplus g(y, x \oplus \alpha)} + \sum_{y \in W_2, \beta} \sum_{x \in V_k} (-1)^{g(y,x) \oplus g(y, x \oplus \alpha)}.$$

For $y \in W_1$,

$$g(y,x) \oplus g(y, x \oplus \alpha) = \langle u, x\rangle \oplus \langle u, x \oplus \alpha\rangle = \langle u, \alpha\rangle$$

is a nonzero linear function of x, and thus balanced.

For $y \in W_2$,

$$g(y,x) \oplus g(y, x \oplus \alpha) = \langle m(u), x\rangle \oplus \langle m(u), x \oplus \alpha\rangle = \langle m(u), \alpha\rangle.$$

Since $m(u)$ is a permutation on V_n, $m(u)$ will run through V_k once while u runs through V_k once. On the other hand, $\langle u, \alpha\rangle$ is balanced hence $\langle m(u), \alpha\rangle$ is balanced.

This proves that $\Delta(\gamma) = 0$ in Case 2.

Summarize Cases 1 and 2, we conclude

Lemma 19 *Let g, be the function on V_{2k+1}, defined as in (16). Then*

$$|\Delta(\gamma)| \leqq 2^{k+1}$$

for any nonzero vector $\gamma \in V_{2k+1}$.

Lemma 19 shows that function g has no linear structure furthermore the difference with respect to any nonzero vector is bounded by a small value.

In Case 1.1, $\Delta(\gamma) = 0$, $\beta \neq 0$, and $\beta \in W_1$ while α is arbitrary. There exist $(2^k - 1)2^k = 2^{2k} - 2^k$ such $\gamma = (\beta, \alpha)$.

In Case 2, $\Delta(\gamma) = 0$, $\beta = 0$. $\alpha \neq$ is arbitrary. There exist $2^k - 1$ such $\gamma = (\beta, \alpha)$.

Summarize Cases 1.1 and 2 we have

Lemma 20 *g, a function on V_{2k+1}, defined as in (16) satisfies the propagation criterion with respect to $2^{2k} - 1$ nonzero vectors.*

Let ℓ_i be the ith row of H_{k+1}, $i = 0, 1, \ldots, 2^{k+1} - 1$. By Lemma 2 of [20], each ℓ_i is is a linear sequence of length 2^{k+1}.

Similarly, denote ith row of H_k by e_i. this is the sequence. By Lemma 2 of [20], e_i is the sequence of linear function $\langle \alpha_i, x \rangle = 0$, where $\alpha_0, \alpha_1, \ldots, \alpha_{2^k-1}$ are defined as at beginning of Section 1.

Recall (16), for fixed $\beta = (y_1, \tau)$, $y_1 \in GF(2)$, $\tau \in V_k$.

$$g(\beta, x) = \begin{cases} 1 \oplus \langle \tau, x \rangle & \text{if } \beta \in W_1 \\ \langle m(\tau), x \rangle & \text{if } \beta \in W_2 \end{cases} \tag{19}$$

Clearly, for any fixed $\beta \in V_{k+1}$, $g(\beta, x)$ is a linear function on V_k.

Let ξ be the sequence of g, defined as in (10). From Lemma 1 of [20], ξ is a concatenation of 2^{k+1} linear sequences of length 2^k. Furthermore, from (19), each linear sequence of length 2^k appear in this concatenation (20). Write

$$\xi = -e_0, -e_1, \ldots, -e_{2^k-1}, e'_0, e'_1, \ldots, e'_{2^k-1} \tag{20}$$

where $e'_0, e'_1, \ldots, e'_{2^k-1}$ is a permutation of $e_0, e_1, \ldots, e_{2^k-1}$, this permutation depends on permutation $m(u)$.

Let L_s be the sth row of H_{2k+1}. By Lemma 2 of [20], L_s is a linear sequence of length 2^{2k+1}. Since $H_{2k} = H_{k+1} \times H_k$, L_s can be rewritten as $L_s = \ell_p \times e_q$, for some p and q, $0 \leqq p \leqq 2^{k+1} - 1$, $0 \leqq q \leqq 2^k - 1$.

Write $\ell_p = (c_0, c_1, \ldots, c_{2^{k+1}-1})$ thus

$$L_s = (c_0 e_q, c_1 e_q, \ldots, c_{2^{k+1}-1} e_q).$$

Since H_k is a Hadamard matrix, $\langle e_i, e_j \rangle = 0$, if $j \neq i$.

Let e_q appear the ith entry and jth ($j > 2^k - 1$) entry in the sequence (20), whose entries come from linear sequences of length 2^k. Hence

$$\langle \xi, L_s \rangle = \langle \xi, \ell_p \times e_q \rangle = (-c_i + c_j)\langle e_q, e_q \rangle = (-c_i + c_j)2^k$$

$$= \begin{cases} \pm 2^{k+1} & \text{if } c_j = -c_i \\ 0 & \text{if } c_j = c_i \end{cases}$$

There exist 2^{2k} $L_s = \ell_p \times e_q$ such that $c_j = -c_i$ and 2^{2k} $L_s = \ell_p \times e_q$ such that $c_j = c_i$ and $q = 1$.

Hence

$$\sigma(g) = 2^{-2k-1} \sum_{s=0}^{2^{2k+1}-1} \langle \xi, L_s \rangle^4 = 2^{-2k-1} \cdot 2^{2k} \cdot 2^{4(k+1)} = 2^{4k+3}.$$

This proves that the following conclusion

Lemma 21 *g, a function on V_{2k+1}, defined as in (16) satisfies $\sigma(g) = 2^{4k+3}$.*

Note that $|\langle \xi, L_s \rangle| \leqq 2^{k+1}$ for any L_s, that is a row of H_{2k+1}, also a linear sequence of length 2^{2k+1}. By using Lemma 3 of [20], we have

Lemma 22 *g, a function on V_{2k+1}, defined as in (16) satisfies $N_g \geqq 2^{2k} - 2^k$.*

Summarize Lemmas 18, 19, 20, 21 and 22 we have

Theorem 6 *Let g be the function on V_{2k+1}, defined as in (16). Then*

(i) g is balanced;

(ii) $N_g \geqq 2^{2k} - 2^k$,

(iii) g satisfies the propagation criterion with respect to $2^{2k} - 1$ nonzero vectors,

(iv) $\sigma(g) = 2^{4k+3}$,

(v) $|\Delta(\gamma)| \leqq 2^{k+1}$ for any nonzero vector $\gamma \in V_{2k}$.

We indicate that g does not satisfies the SAC even we use any nonsingular linear transformation on the variables, since there exists no $2k + 1$ linearly independent vectors which g satisfies the propagation criterion with respect to.

6 Group Hadamard Matrices and Bent Functions

The properties of *Group Hadamard Matrices* are:

1. Let G be a group. Define a vector, say $p = (p_1, \ldots, p_n)$, where each $p_j \in G$.
2. The product $*$ of two vectors, say p and q, is $p * q = (p_1 q_1, \ldots, p_n q_n)$, where $q = (q_1, \ldots, q_n)$.
3. The inverse of p is $p^{-1} = (p_1^{-1}, \ldots, p_n^{-1})$, where p_j^{-1} is the inverse of p_j in G.
4. p and q are *s-orthogonal* if $p * q^{-1} = (p_1 q_1^{-1}, \ldots, p_n q_n^{-1})$ is s listings of G. In this case $n = s|G|$.

Definition 12 A square matrix with elements from G is called a generalized Hadamard matrix of type s for group G if its rows are mutually s-orthogonal (Butson, Drake).

A $(1, -1)$ Hadamard matrix of order n is a generalized Hadamard matrix of type $\frac{1}{2}n$ for the group $G = \{1, -1\}$.

Example 24 (Generalized Hadamard Matrix) Let ε be the root of a primitive equation on $GF(2^3)$, say $1 \oplus x \oplus x^3 = 0$.

List

$$1,\ \varepsilon,\ \varepsilon^2,\ \varepsilon^3,\ \varepsilon^4,\ \varepsilon^5,\ \varepsilon^6.$$

$$1,\ \varepsilon,\ \varepsilon^2,\ 1 \oplus \varepsilon,\ \varepsilon \oplus \varepsilon^2,\ 1 \oplus \varepsilon \oplus \varepsilon^2,\ 1 \oplus \varepsilon^2.$$

For convenience, write $a \oplus b\varepsilon \oplus c\varepsilon^2$ as $(abc) \in V_3$. Correspondingly, the above sequence becomes

$$(100),\ (010),\ (001),\ (110),\ (011),\ (111),\ (101).$$

Set

$$N = \begin{bmatrix} (000) & (000) & (000) & (000) & (000) & (000) & (000) & (000) \\ (000) & (100) & (010) & (001) & (110) & (011) & (111) & (101) \\ (000) & (010) & (001) & (110) & (011) & (111) & (101) & (100) \\ (000) & (001) & (110) & (011) & (111) & (101) & (100) & (010) \\ (000) & (110) & (011) & (111) & (101) & (100) & (010) & (001) \\ (000) & (011) & (111) & (101) & (100) & (010) & (001) & (110) \\ (000) & (111) & (101) & (100) & (010) & (001) & (110) & (011) \\ (000) & (101) & (100) & (010) & (001) & (110) & (011) & (111) \end{bmatrix}$$

The second row of N is the above sequence with (000). The third row is the left shifting the second and keeping (000). The fourth row is the left shifting the third and keeping (000) ....

N is a generalized Hadamard matrix of type 1 for group $G = V_3$.

Changing each (abc) in N into $ax_1 \oplus bx_2 \oplus cx_3$ gives matrix M whose second row is

$$0,\ x_1,\ x_2,\ x_3,\ x_1 \oplus x_2,\ x_2 \oplus x_3,\ x_1 \oplus x_2 \oplus x_3,\ x_1 \oplus x_3.$$

M is a generalized Hadamard matrix of type 1 for group

$$G = \{0,\ x_1,\ x_2,\ x_3,\ x_1 \oplus x_2,\ x_2 \oplus x_3,\ x_1 \oplus x_3,\ x_1 \oplus x_2 \oplus x_3\}.$$

Any (1, -1) Hadamard matrix of order n is type $\frac{1}{2}n$ for group $G = \{1, -1\}$.

Definition 13 Let M be a generalized Hadamard matrix of type s for group G. M is called a *group Hadamard matrix* if the rows of M and the columns form a group under the operation $*$ (Butson, Drake and de Launey).

If G is cyclic then any row group Hadamard matrix for G is also a column group Hadamard matrix.

Example 25 (Group Hadamard Matrix) The matrix N in a previous example is a group Hadamard matrix of type 1 for $G = V_3$.

$$\{1,\ \varepsilon,\ \varepsilon^2,\ 1 \oplus \varepsilon,\ \varepsilon \oplus \varepsilon^2,\ 1 \oplus \varepsilon,\ \varepsilon \oplus \varepsilon^2,\ 1 \oplus \varepsilon \oplus \varepsilon^2,\ 1 \oplus \varepsilon^2\}.$$

Example 26 (Group Hadamard Matrix) M in a previous example is a group Hadamard matrix of type 1 for

$$G = \{0,\ x_1,\ x_2,\ x_3,\ x_1 \oplus x_2,\ x_2 \oplus x_3,\ x_1 \oplus x_3,\ x_1 \oplus x_2 \oplus x_3\}.$$

Example 27 (Group Hadamard Matrix)

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

is a group Hadamard matrix of type 4 for group $G = GF(2)$.

Example 28 (Group Hadamard Matrix) Replace elements 0 and 1 in M by 1 and -1 respectively a group Hadamard matrix of type 4 for group $G = \{1, -1\}$.

Sylvester-Hadamard matrix H_n is a group Hadamard matrix of type 2^{n-1} for the group $G = \{1, -1\}$. For example,

$$H_3 = \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{bmatrix}$$

is a group Hadamard matrix of type $2^2 = 4$ for the group $G = \{1, -1\}$.

Example 29 (A Set of Bent Functions) Let ℓ_0, ℓ_1, ℓ_2, ℓ_3, ℓ_4, ℓ_5, ℓ_6, ℓ_7 be the truth table of the linear functions on V_3:

$$\{0,\ x_1,\ x_2,\ x_3,\ x_1 \oplus x_2,\ x_2 \oplus x_3,\ x_1 \oplus x_3,\ x_1 \oplus x_2 \oplus x_3\}$$

respectively.

Construct seven $(0,1)$-sequences (truth tables) of length 2^6:

$$\begin{array}{llllllll} \eta_1 = \ell_0 & \ell_1 & \ell_2 & \ell_3 & \ell_4 & \ell_5 & \ell_6 & \ell_7 \\ \eta_2 = \ell_0 & \ell_2 & \ell_3 & \ell_4 & \ell_5 & \ell_6 & \ell_7 & \ell_1 \\ \eta_3 = \ell_0 & \ell_3 & \ell_4 & \ell_5 & \ell_6 & \ell_7 & \ell_1 & \ell_2 \\ \eta_4 = \ell_0 & \ell_4 & \ell_5 & \ell_6 & \ell_7 & \ell_1 & \ell_2 & \ell_3 \\ \eta_5 = \ell_0 & \ell_5 & \ell_6 & \ell_7 & \ell_1 & \ell_2 & \ell_3 & \ell_4 \\ \eta_6 = \ell_0 & \ell_6 & \ell_7 & \ell_1 & \ell_2 & \ell_3 & \ell_4 & \ell_5 \\ \eta_7 = \ell_0 & \ell_7 & \ell_1 & \ell_2 & \ell_3 & \ell_4 & \ell_5 & \ell_6 \end{array} .$$

Since M is a group Hadamard matrix, for any $j \neq i$ there exists a unique t such that $\eta_j \oplus \eta_i = \eta_t$.

Thus if we let η_j be the truth table of a (bent) function V_6, say g_j, for any $j \neq i$ there exists a unique t such that $g_j \oplus g_i = g_t$.

g_1, g_2 and g_3 are linearly independent. Thus any nonzero linear combination of f_1, f_2, f_3 is also a bent function on V_6.

This construction can be extended to any dimension i.e. for any even number, say n there exist $\frac{1}{2}n$ bent functions on V_n such that any nonzero linear combination of them is also a bent function on V_n. Since bent functions are not balanced we must modify them.

Example 30 (Independent Set of Bent Functions) Let g_1, g_2, ..., g_k be bent functions on V_{2k} whose any nonzero linear combination of them is also a bent function on V_{2k}.

Let η_j be the truth table of g_j. Write

$$\begin{array}{lccccc}
\eta_1 = \ell_0 & \ell_1 & \ell_2 & \cdots & \ell_{2^k} \\
\eta_2 = \ell_0 & \ell_2 & \ell_3 & \cdots & \ell_1 \\
 & & \vdots & & \\
\eta_k = \ell_0 & \ell_k & \ell_{k+1} & \cdots & \ell_{k-1},
\end{array}$$

where each ℓ_j is the truth table ℓ_0 is the truth table of the zero linear functions.

Example 31 (Modifying A Set of Independent Functions) Select any 2^t $(t < k)$ columns of the above array excluding the first column. We have

$$\begin{array}{lccc}
\xi_1 = \ell_{j_1} & \ell_{j_2} & \cdots & \ell_{j_{2^t}} \\
\eta_2 = \ell_{j_1+1} & \ell_{j_2+1} & \cdots & \ell_{j_{2^t}+1} \\
 & \vdots & & \\
\eta_k = \ell_{j_1+k-1} & \ell_{j_2+k-1} & \cdots & \ell_{j_{2^t+k-1}}.
\end{array}$$

Each ξ_j is of length 2^{k+t}, thus it is the truth table of a function on V_{k+t}, say f_j.

Set

$$F(x) = (f_1(x), \ldots, f_k(x)),$$

where $x \in V_{k+t}$. Then F is a mapping from V_{k+t} to V_k.

Select any 2^t $(t < k)$ columns of the above array excluding the first column. We have

$$\begin{array}{lccc}
\xi_1 = \ell_{j_1} & \ell_{j_2} & \cdots & \ell_{j_{2^t}} \\
\eta_2 = \ell_{j_1+1} & \ell_{j_2+1} & \cdots & \ell_{j_{2^t}+1} \\
 & \vdots & & \\
\eta_k = \ell_{j_1+k-1} & \ell_{j_2+k-1} & \cdots & \ell_{j_{2^t+k-1}}.
\end{array}$$

Each ξ_j is of length 2^{k+t}, thus it is the truth table of a function on V_{k+t}, say f_j.
Set

$$F(x) = (f_1(x), \ldots, f_k(x)),$$

where $x \in V_{k+t}$. Then F is a mapping from V_{k+t} to V_k.

Example 32 (A Set of Bent Functions) Let ε be the root of a primitive equation on $GF(2^3)$, say $1 \oplus x \oplus x^3 = 0$.

Consider

$$1,\ \varepsilon,\ \varepsilon^2,\ \varepsilon^3,\ \varepsilon^4,\ \varepsilon^5,\ \varepsilon^6$$

and rewrite as

$$1,\ \varepsilon,\ \varepsilon^2,\ 1 \oplus \varepsilon,\ \varepsilon \oplus \varepsilon^2,\ 1 \oplus \varepsilon \oplus \varepsilon^2,\ 1 \oplus \varepsilon^2.$$

Change 1, ε, ε^2 into x_1, x_2, x_3 respectively. We have

$$x_1,\ x_2,\ x_3,\ x_1 \oplus x_2,\ x_2 \oplus x_3,\ x_1 \oplus x_2 \oplus x_3,\ x_1 \oplus x_3.$$

Shifting this sequence six times gives seven sequences which form the core of M. From M we construct seven $(0,1)$ sequences (truth tables) $\eta_1, \ldots, \eta_7$, as mentioned previously. Let η_1, η_2, η_3 be the truth tables of g_1, g_2, g_3. Then any nonzero linear combination of g_1, g_2, g_3 is bent.

7 S-Box Design

Definition 14 A $n \times k$ *S-box* is a mapping from V_n to V_k:

$$F(x) = (f_1(x), \ldots, f_k(x))$$

where $n \geqq k$, each $f_j(x)$ is a function on V_n.

We require:

(i) Any nonzero linear combination of $f_1, \ldots, f_k$, say $f = c_1 f_1 \oplus \cdots \oplus c_k f_k$, $(c_1, \ldots, c_k) \neq (0, \ldots, 0)$, to be balanced,

(ii) any nonzero linear combination of $f_1, \ldots, f_k$ to be highly nonlinear,

(iii) any nonzero linear combination of $f_1, \ldots, f_k$ to satisfy SAC,

(iv) $F(x)$ to be *regular* run through each vector in V_k 2^{n-k} times while x runs through V_n once,

(v) $F(x)$ to have *good differential distribution* i.e. $F(x) \oplus F(x \oplus \alpha)$ runs through some 2^{k-1} vectors in V_k each 2^{n-k+1} times while x runs through V_n once, but does not take another 2^{k-1} vectors at all (Biham and Shamir) [3].

Note : (ii) and (iv) are equivalent and some criteria have to be weakened if they cannot be satisfied completely.

Example 33 (S-Box properties) Consider the 3×3 *S-box* mapping from V_3 to V_3:

$$F(x) = (f_1(x), f_2(x), f_3(x))$$

where

$$f_1 = x_1 \oplus x_3 \oplus x_2 x_3,\ f_2 = x_1 \oplus x_2 \oplus x_1 x_2 \oplus x_2 x_3,\ f_3 = x_1 x_2 \oplus x_2 x_3 \oplus x_1 x_3.$$

Then

(i) Any nonzero linear combination of f_1, f_2, f_3, say $f = c_1 f_1 \oplus c_2 f_2 \oplus c_3 f_3$, $(c_1, c_2, c_3) \neq (0,0,0)$, is balanced,

(ii) any nonzero linear combination of f_1, f_2, f_3, say f, has nonlinearity 2 i.e. $N_f \geqq 2$ (maximum for balanced functions on V_3),

(iii) any nonzero linear combination of f_1, f_2, f_3, say f, satisfies the propagation criterion except for a single nonzero vector related to the particular combination, f,

(iv) $F(x)$ is regular, in this case, it is a permutation,

(v) $F(x)$ has *good differential distribution* i.e. $F(x) \oplus F(x \oplus \alpha)$ runs through some 2^2 vectors in V_3 each 2^1 times while x runs through V_3 once, but does not assume another 2^2 vectors at all.

Example 34 (Difference Distribution) For example, let $\alpha = (001)$. $F(x) \oplus F(x \oplus \alpha)$ runs through some (010), (011), (100), (101) each 2^1 times while x runs through V_3 once.

Let $\alpha = (111)$. $F(x) \oplus F(x \oplus \alpha)$ runs through some (001), (011), (101), (111) each 2^1 times while x runs through V_3 once.

Example 35 (Polynomial Permutation) Note that any element in $GF(2^n)$, say α, can be expressed as $\alpha = a_1 \oplus a_2 \varepsilon \oplus \cdots \oplus a_n \varepsilon^{n-1}$, where each $a_j \in GF(2)$ and ε is a primitive element of $GF(2^n)$. Thus we have establish a relationship between V_n and $GF(2^n)$, this is isomorphism under the operation, this is boolean addition. Let n be odd. Hence $F(x) = x^3$, where $x \in V_n$, can be regarded a permutation on V_n. It has been proved that

(i) Any nonzero linear combination of the coordinate functions, say f, is balanced (i.e. regular, a permutation),

(ii) any nonzero linear combination of the coordinate function, say f, has nonlinearity $N_f \geqq 2^{n-1} - 2^{\frac{1}{2}(n-1)}$,

(iii) any nonzero linear combination of the coordinate function, say f, satisfies the propagation criterion except for a single nonzero vector related to the particular combination, f,

(iv) $F(x)$ has *good differential distribution* i.e. $F(x) \oplus F(x \oplus \alpha)$ runs through some 2^{n-1} vectors in V_n each 2^1 times while x runs through V_3 once, but does not assume another 2^{n-1} vectors at all (Pieprzyk, Tavares and Nyberg).

Example 36 (A Counterexample for S-box Design) (i) Let

$$F(x) = (f_1(x), \ldots, f_k(x))$$

is a regular mapping with good differential distribution from V_n to V_k. Then

$$F(x) = (f_1(x), \ldots, f_t(x)),$$

where $t < k$, is regular but does not have good differential distribution.

(ii) Let

$$F(x) = (f_1(x), \ldots, f_k(x))$$

be a regular mapping from V_n to V_k and F have good differential distribution. Then there exist functions on V_n, say

$$f_{k+1}(x), \ldots, f_s(x)$$

such that

$$F(x) = (f_1(x), \ldots, f_k(x),\ f_{k+1}(x), \ldots, f_s(x))$$

be a regular mapping from V_n to V_s but cannot have good differential distribution.

There exist a nonsingular matrix of order $k + t$ such that $F^*(x) = F(xA)$, another mapping from V_{k+t} to V_k, has the following properties:

(i) any nonzero linear combination of the coordinates of F^* is balanced,

(ii) any nonzero linear combination of the coordinates of F^* has the nonlinearity no less than $2^{k+t-1} - 2^{k-1}$,

(iii) any nonzero linear combination of the coordinates of F^* satisfies SAC,

(iv) any nonzero linear combination of the coordinates of F^* has the algebraic $t + 1$.

F^* does not satisfy the good differential distribution. However we can add other special functions, for example, those we saw in the above examples, to F^* as some more coordinate functions and obtain a new mapping with better differential distribution.

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] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, Vol. 4, No. 1:3–72, 1991.

[4] J. Detombe and S. Tavares. Constructing large cryptographically strong S-boxes. In *Advances in Cryptology - AUSCRYPT'92*, volume 718, Lecture Notes in Computer Science, pages 165–181. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[5] J. F. Dillon. A survey of bent functions. *The NSA Technical Journal*, pages 191–215, 1972. (unclassified).

[6] M. Hall, Jr. *Combinatorial Theory.* Ginn-Blaisdell, Waltham, 1967.

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

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

[12] 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.

[13] 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.

[14] K. Nyberg. On the construction of highly nonlinear permutations. In *Advances in Cryptology - EUROCRYPT'92*, volume 658, Lecture Notes in Computer Science, pages 92–98. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[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] 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.

[18] B. Preneel, W. V. Leekwijck, 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.

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

[20] J. Seberry, X. M. Zhang, and Y. Zheng. Highly nonlinear 0-1 balanced functions satisfying strict avalanche criterion. In *Advances in Cryptology - AUSCRYPT'92*, volume 718, Lecture Notes in Computer Science, pages 145–155. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[21] J. Seberry, X. M. Zhang, and Y. Zheng. Systematic generation of cryptographically robust S-boxes. In *Proceedings of the first ACM Conference on Computer and Communications Security*, pages 172 – 182. The Association for Computing Machinery, New York, 1993.

[22] J. Seberry, X. M. Zhang, and Y. Zheng. Improving the strict avalanche characteristics of cryptographic functions. *Information Processing Letters*, 50:37–41, 1994.

[23] J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearly balanced boolean functions and their propagation characteristics. In *Advances in Cryptology - CRYPTO'93*, volume 773, Lecture Notes in Computer Science, pages 49–60. Springer-Verlag, Berlin, Heidelberg, New York, 1994.

[24] 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.

[25] A. F. Webster. Plaintext/ciphertext bit dependencies in cryptographic system. Master's Thesis, Department of Electrical Engineering, Queen's University, Ontario, 1985.

[26] A. F. Webster and S. E. Tavares. On the design 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.

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