Structures of highly nonlinear cryptographic functions

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Xian-Mo Zhang
University of Wollongong, xianmo@uow.edu.au

Yuliang Zheng
University of Wollongong, yuliang@uow.edu.au

Publication Details
Structures of highly nonlinear cryptographic functions

Abstract
This paper studies the properties and constructions of nonlinear Boolean functions, which are a core component of cryptographic primitives including data encryption algorithms and one-way hash functions. A main contribution of this paper is to completely characterise the structures of cryptographic functions that satisfy the propagation criterion with respect to all but six or less vectors.

Disciplines
Physical Sciences and Mathematics

Publication Details

This conference paper is available at Research Online: http://ro.uow.edu.au/infopapers/1106
Structures of Highly Nonlinear Cryptographic Functions

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

Summary  This paper studies the properties and constructions of nonlinear Boolean functions, which are a core component of cryptographic primitives including data encryption algorithms and one-way hash functions. A main contribution of this paper is to completely characterise the structures of cryptographic functions that satisfy the propagation criterion with respect to all but six or less vectors.

1 Introduction

Cryptographic techniques for information authentication and data encryption require Boolean functions with a number of critical properties that distinguish them from linear (or affine) functions. Among the properties are high nonlinearity, high degree of propagation, few linear structures, high algebraic degree etc. These properties are often called nonlinearity criteria. An important topic is to investigate relationships among the various nonlinearity criteria. Progress in this direction has been made in [7], where connections have been revealed among the strict avalanche characteristic (SAC), differential characteristics, linear structures and nonlinearity, of quadratic functions.

In this paper we carry on the investigation initiated in [7] and bring together nonlinearity and propagation characteristic of a Boolean function (quadratic or non-quadratic). We further extend our investigation into the structures of cryptographic functions.

Due to the limit in space, proofs of the main results are left to the full version of the paper.

2 Basic Definitions

We consider Boolean functions from $V_n$ to $GF(2)$ (or simply functions on $V_n$), $V_n$ is the vector space of $n$ tuples of elements from $GF(2)$. The truth table of a function $f$ on $V_n$ is a $(0,1)$-sequence defined by $(f(α_0), f(α_1), . . . , f(α_{2^n-1}))$, and the sequence of $f$ is a $(1,-1)$-sequence defined by $((-1)^{f(α_0)}, (-1)^{f(α_1)}, . . . , (-1)^{f(α_{2^n-1})})$, where $α_0 = (0, . . . , 0, 0), α_1 = (0, . . . , 0, 1), . . . , α_{2^n-1} = (1, . . . , 1, 1)$. The matrix of $f$ is a $(1,-1)$-matrix of order $2^n$ defined by $M = ((-1)^{f(α_i⊕α_j)})$. $f$ is said to be balanced if its truth table contains an equal number of ones and zeros.

An affine function $f$ on $V_n$ is a function that takes the form of $f(x_1, . . . , x_n) = a_1x_1⊕···⊕a_nx_n⊕c$, where $a_j, c ∈ GF(2), j = 1, 2, . . . , n$. Furthermore $f$ is called a linear function if $c = 0$.

Definition 1 Let $s$ be a $(0,1)$-sequence. The Hamming weight of $s$, denoted by $W(s)$, is the number of ones in the sequence. Given two functions $f$ and $g$ on $V_n$, the Hamming distance $d(f,g)$ between them is defined as the Hamming weight of the truth table of $f(x) ⊕ g(x)$, where $x = (x_1, . . . , x_n)$. The nonlinearity of $f$, denoted by $N_f$, is the minimal Hamming distance between $f$ and all affine functions on $V_n$, i.e., $N_f = \min_{i=1,2, . . . ,2^n+1} d(f,φ_i)$ where $φ_1, φ_2, . . . , φ_{2^n+1}$ are all the affine functions on $V_n$.

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 $f(x) ⊕ f(x ⊕ α)$ is a balanced function, where $x = (x_1, . . . , x_n)$ and $α$ is a vector in $V_n$.

2. the propagation criterion of degree $k$ if it satisfies the propagation criterion with respect to all $α$ in $V_n$ with $1 ≤ W(α) ≤ k$.

The above definition for propagation criterion is from [5]. Note that the strict avalanche criterion (SAC) introduced by Webster and Tavares [9, 8] is equivalent to the propagation criterion of degree 1.

While the propagation characteristic measures the avalanche effect of a function, the linear structure is a concept that in a sense complements the former, namely, it indicates the straightness of a function.

Definition 3 Let $f$ be a function on $V_n$. A vector $α ∈ V_n$ is called a linear structure of $f$ if $f(x) ⊕ f(x ⊕ α)$ is a constant.

By definition, the zero vector in $V_n$ is a linear structure of all functions on $V_n$. It is not hard to see that the linear structures of a function $f$ form a linear subspace of $V_n$. The dimension of the subspace is called the linearity dimension of $f$. We note that it was Evertse who first introduced the notion of linear structure (in a sense broader than
ours) and studied its implication on the security of encryption algorithms [3].

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 $m$. A Sylvester-Hadamard matrix of order $2^n$, denoted by $H_n$, is generated by the following recursive relation

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

**Definition 4** 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 $\langle \beta, x \rangle$ is the scalar product of $\beta$ and $x$, namely, $\langle \beta, x \rangle = \sum_{i=1}^n b_i x_i$, and $f(x) \oplus \langle \beta, x \rangle$ is regarded as a real-valued function.

Bent functions can be characterized in various ways [1, 2, 6]. In particular the following four statements are equivalent:

(i) $f$ is bent.

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

(iii) $f$ satisfies the propagation criterion with respect to all non-zero vectors in $V_n$.

(iv) $M$, the matrix of $f$, is a Hadamard matrix.

Bent functions on $V_n$ exist only when $n$ is even. Another important property of bent functions is that they achieve the highest possible nonlinearity $2^{n-1} - 2^{\frac{n}{2} - 1}$.

### 3 Propagation Characteristic and Nonlinearity

Given two sequences $a = (a_1, \ldots, a_m)$ and $b = (b_1, \ldots, b_m)$, their component-wise product is defined by $a \ast b = (a_1 b_1, \ldots, a_m b_m)$. Let $f$ be a function on $V_n$. For a vector $\alpha \in V_n$, denote by $\xi(\alpha)$ the sequence of $f(x \oplus \alpha)$. Thus $\xi(0)$ is the sequence of $f$ itself and $\xi(0) \ast \xi(\alpha)$ is the sequence of $f(x) \oplus f(x \oplus \alpha)$.

Set

$$\Delta(\alpha) = (\xi(0), \xi(\alpha)),$$

the scalar product of $\xi(0)$ and $\xi(\alpha)$. Obviously, $\Delta(\alpha) = 0$ if and only if $f(x) \oplus f(x \oplus \alpha)$ is balanced, i.e., $f$ satisfies the propagation criterion with respect to $\alpha$. On the other hand, if $|\Delta(\alpha)| = 2^n$, then $f(x) \oplus f(x \oplus \alpha)$ is a constant and hence $\alpha$ is a linear structure of $f$.

Let $M = ((-1)^{f(\alpha_i \oplus \alpha_j)})$ be the matrix of $f$ and $\xi$ be the sequence of $f$. Due to a very pretty result by R. L. McFarland (see Theorem 3.3 of [2]), $M$ can be decomposed into

$$M = 2^{-n}H_n \text{diag}(\xi, \ell_0, \ldots, (\xi, \ell_{2^n-1}))H_n$$

where $\ell_i$ is the $i$th row of $H_n$, a Sylvester-Hadamard matrix of order $2^n$. By Lemma 2 of [6], $\ell_i$ is the sequence of a linear function defined by $\psi_i(x) = \langle \alpha_i, x \rangle$, where $\alpha_i$ is the $i$th vector in $V_n$ according to the ascending alphabetical order.

Clearly

$$M M^T = 2^{-n}H_n \text{diag}(\xi, \ell_0^2, \ldots, (\xi, \ell_{2^n-1})^2)H_n. \quad (1)$$

On the other hand, we always have

$$M M^T = (\Delta(\alpha_{i+j})).$$

where $i, j = 0, 1, \ldots, 2^n - 1$.

Let $S$ be a set of vectors in $V_n$. The rank of $S$ is the maximum number of linearly independent vectors in $S$. Note that when $S$ forms a linear subspace of $V_n$, its rank coincides with its dimension.

Lemma 6 of [6] states that the distance between two functions $f_1$ and $f_2$ on $V_n$ can be expressed as $d(f_1, f_2) = 2^{n-1} - \frac{1}{2}(\xi f_1, \xi f_2)$, where $\xi f_1$ and $\xi f_2$ are the sequences of $f_1$ and $f_2$ respectively. As an immediate consequence we have:

**Lemma 1** The nonlinearity of a function $f$ on $V_n$ can be calculated by

$$N_f = 2^{n-1} - \frac{1}{2} \max\{|\langle \xi, \ell_i \rangle|, 0 \leq i \leq 2^n - 1\}$$

where $\xi$ is the sequence of $f$ and $\ell_0, \ldots, \ell_{2^n-1}$ are the sequences of the linear functions on $V_n$.

Now we prove a central result of this paper:

**Theorem 1** Let $f$ be a function on $V_n$ that satisfies the propagation criterion with respect to all but a subset $\mathcal{R}$ of vectors in $V_n$. Then the nonlinearity of $f$ satisfies $N_f \geq 2^{n-1} - 2^{\frac{n}{2}(n+1)-1}$, where $t$ is the rank of $\mathcal{R}$.

It was observed by Nyberg in Proposition 3 of [4] (see also a detailed discussion in [7]) that knowing the linearity dimension, say $t$, of a function $f$ on $V_n$, the nonlinearity of the function can be expressed as $N_f = 2^t N_t$, where $N_t$ is the nonlinearity of a function obtained by restricting $f$ on an $(n-t)$-dimensional subspace of $V_n$. Therefore, in a sense Theorem 1 is complementary to Proposition 3 of [4].

In the next section we discuss an interesting special case where $|\mathcal{R}| = 2$. More general cases where $|\mathcal{R}| > 2$, which need very different proof techniques, will be fully discussed in the later part of the paper.
4 Functions with $|\mathbb{R}| = 2$

Since $\mathbb{R}$ consists of two vectors, a zero and a nonzero, it forms a one-dimensional subspace of $V_n$. The following result on splitting a power of 2 into two squares will be used in later discussions.

**Lemma 2** Let $n \geq 2$ be a positive integer and $2^n = p^2 + q^2$ where both $p \geq 0$ and $q \geq 0$ are integers. Then $p = 2^{\frac{n}{2}}$ and $q = 0$ when $n$ is even, and $p = q = 2^{\frac{n}{2}(n-1)}$ when $n$ is odd.

Now we can prove

**Theorem 2** If $f$, a function on $V_n$, satisfies the propagation criterion with respect to all but two (a zero and a nonzero) vectors in $V_n$, then

(i) $n$ must be odd,

(ii) the nonzero vector where the propagation criterion is not satisfied must be a linear structure of $f$ and

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

A further examination of the proof for Theorem 2 reveals that a function with $|\mathbb{R}| = 2$ has a very simple structure as described below.

**Corollary 1** A function $f$ on $V_n$ satisfies the propagation criterion with respect to all but two (a zero and a nonzero) vectors in $V_n$, if and only if there exists a nonsingular linear matrix of order $n$ over $GF(2)$, say $B$, such that $g(x) = f(xB)$ can be written as

$$g(x) = cx_n \oplus h(x_1, \ldots, x_{n-1})$$

where $h$ is a bent function on $V_{n-1}$ and $c$ is a constant in $GF(2)$.

By Theorem 2 and Corollary 1, functions on $V_n$ that satisfy the propagation criterion with respect to all but two vectors in $V_n$ exist only if $n$ is odd, and such a function can always be (informally) viewed as being obtained by repeating twice a bent function on $V_{n-1}$ (subject to a nonsingular linear transformation on the input coordinates).

When $\mathbb{R}$ has more than two vectors, it does not necessarily form a linear subspace of $V_n$. Therefore discussions presented in this section do not directly apply to the more general case. Nevertheless, using a different technique, we show in the next section a significant result on the structure of $\mathbb{R}$, namely, the nonzero vectors in $\mathbb{R}$ with $|\mathbb{R}| > 2$ are linearly dependent.

5 Linear Dependence in $\mathbb{R}$

**Theorem 3** Suppose that $f$, a function on $V_n$, satisfies the propagation criterion with respect to all but $k + 1$ vectors $0, \beta_1, \ldots, \beta_k$ in $V_n$, where $k > 1$. Then $\beta_1, \ldots, \beta_k$ are linearly dependent, namely, there exist $k$ constants $c_1, \ldots, c_k \in GF(2)$, not all of which are zeros, such that $c_1\beta_1 \oplus \cdots \oplus c_k\beta_k = 0$.

We believe that Theorem 3 is of significant importance, as it reveals for the first time the interdependence among the vectors where the propagation criterion is not satisfied by $f$. Of particular interest is the case when $\mathbb{R} = \{0, \beta_1, \ldots, \beta_k\}$ forms a linear subspace of $V_n$. Recall that linear structures form a linear subspace. Therefore, when $\mathbb{R}$ is a subspace, a nonzero vector in $\mathbb{R}$ is a linear structure if and only if all other nonzero vectors are linear structures of $f$.

In the following sections we examine the cases when $|\mathbb{R}| = 3, 4, 5, 6$.

6 Functions with $|\mathbb{R}| = 3$

When $|\mathbb{R}| = 3$, the two distinct nonzero vectors in $\mathbb{R}$ can not be linearly dependent. By Theorem 3 we have

**Theorem 4** There exists no function that does not satisfy the propagation criterion with respect to only three vectors.

7 Functions with $|\mathbb{R}| = 4$

Next we consider the case when $|\mathbb{R}| = 4$. Similarly to the case of $|\mathbb{R}| = 2$, the first step we take is to introduce a result on splitting a power of 2 into four, but not two, squares.

**Lemma 3** Let $n \geq 3$ be a positive integer and $2^n = \sum_{j=1}^4 p_j^2$ where each $p_j \geq 0$ is an integer. Then

(i) $p_1^2 = p_2^2 = 2^{n-1}$, $p_3 = p_4 = 0$, if $n$ is odd;

(ii) $p_1^2 = 2^n$, $p_2 = p_3 = p_4 = 0$ or $p_1^2 = p_2^2 = p_3^2 = p_4^2 = 2^{n-1}$, if $n$ is even.

Now we can prove a key result on the case of $|\mathbb{R}| = 4$.

**Theorem 5** If $f$, a function on $V_n$, satisfies the propagation criterion with respect to all but four vectors $(0, \beta_1, \beta_2, \beta_3)$ in $V_n$, Then

(i) $\mathbb{R} = \{0, \beta_1, \beta_2, \beta_3\}$ forms a two-dimensional linear subspace of $V_n$,

(ii) $n$ must be even,
(iii) $\beta_1, \beta_2$ and $\beta_3$ must be linear structures of $f$, 
(iv) the nonlinearity of $f$ satisfies $N_f = 2^{n-1} - 2^{\frac{n}{2}}$.

As a result we have

**Corollary 2** A function $f$ on $V_n$ satisfies the propagation criterion with respect to all but four vectors in $V_n$ if and only if there exists a nonsingular linear matrix of order $n$ over $GF(2)$, say $B$, such that

$$g(x) = f(xB)$$

where $c_1$ and $c_2$ are constants in $GF(2)$, and $h$ is a bent function on $V_{n-2}$.

The proof of Corollary 2 is similar to that of Corollary 1.

In [6], it has been shown that repeating twice a bent function on $V_n$, $n$ even, results in a function on $V_{n-1}$ or $V_{n-2}$ that satisfies the propagation criterion with respect to all but two or four vectors in $V_{n-1}$ or $V_{n-2}$. Combining Corollaries 2 and 1 with results shown in [6], we conclude that the methods of repeating bent functions presented in [6] generate all the functions that satisfy the propagation criterion with respect to all but two or four vectors.

## 8 Functions with $|\mathcal{R}| = 5$ 

Let $f$ be a function on $V_n$ with $|\mathcal{R}| = 5$ and let $\mathcal{R} = \{0, \beta_1, \beta_2, \beta_3, \beta_4\}$. First we discuss properties of and relationship among the four nonzero vectors. This is followed by a method showing how to construct functions with $|\mathcal{R}| = 5$.

### 8.1 $\beta_1, \beta_2, \beta_3$ and $\beta_4$ Are Not Linear Structures

By Theorem 3, $\beta_1, \beta_2, \beta_3, \beta_4$ are linearly dependent. As $\beta_1, \beta_2, \beta_3, \beta_4$ are distinct nonzero vectors, the rank of $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ must be 3.

Without loss of generality, we assume that $\beta_1, \beta_2, \beta_3$ are linearly independent. As a nonsingular linear transformation on the input coordinates does not affect the total number of vectors where the propagation criterion is satisfied by $f$, we can further assume that $\beta_1 = \alpha_1 = (0, \ldots, 0, 0, 0, 1)$, $\beta_2 = \alpha_2 = (0, \ldots, 0, 1, 0, 0)$ and $\beta_3 = \alpha_3 = (0, \ldots, 0, 1, 0, 0)$.

Our goal is to prove that $\beta_1, \beta_2, \beta_3$ and $\beta_4$ are related by $\beta_1 \oplus \beta_2 \oplus \beta_3 \oplus \beta_4 = 0$; that is, $\beta_4 = \beta_1 \oplus \beta_2 \oplus \beta_3$. We achieve this by showing that there exist no “shorter” relations than $\beta_4 = \beta_1 \oplus \beta_2 \oplus \beta_3$, namely, none of the three shorter equations $\beta_4 = \beta_1 \oplus \beta_2$, $\beta_4 = \beta_2 \oplus \beta_3$ and $\beta_4 = \beta_1 \oplus \beta_3$. We can show that $\beta_4 \neq \beta_1 \oplus \beta_2$. In addition, $\beta_4 \neq \beta_2 \oplus \beta_3$ and $\beta_4 \neq \beta_1 \oplus \beta_3$ can be proved in the same way. Hence we have proved the following result:

**Lemma 4** Let $f$ be a function on $V_n$ that satisfies the propagation criterion with respect to all but five vectors $\mathcal{R} = \{0, \beta_1, \beta_2, \beta_3, \beta_4\}$ in $V_n$. Then $\beta_1 \oplus \beta_2 \oplus \beta_3 \oplus \beta_4 = 0$.

### 8.2 $\beta_1, \beta_2, \beta_3$ and $\beta_4$ Are Not Linear Structures

In the full paper the following result is established.

**Theorem 6** Let $f$ be a Boolean function on $V_n$ that satisfies the propagation criterion with respect to all but a subset $\mathcal{R} = \{0, \beta_1, \beta_2, \beta_3, \beta_4\}$. Then

(i) $n$ is odd,

(ii) $\beta_1 \oplus \beta_2 \oplus \beta_3 \oplus \beta_4 = 0$,

(iii) $|\Delta(\beta_j)| = 2^{n-1}$, $j = 1, 2, 3, 4$, and three $\Delta(\beta_j)$ have the same sign while the remaining has a different sign, and

(iv) the nonlinearity of $f$ satisfies $N_f = 2^{n-1} - 2^{\frac{n}{2}}(n-1)$.

Recall that when $|\mathcal{R}| = 2$ or 4, all nonzero vectors in $\mathcal{R}$ are linear structures of $f$, and the structure of $f$ is very simple — it can be (informally) viewed as the two- or four-repetition of a bent function on $V_{n-1}$ or $V_{n-2}$. In contrast, when $|\mathcal{R}| = 5$, none of the nonzero vectors in $\mathcal{R}$ is a linear structure of $f$. Thus if a non-bent function does not possess linear structures, then $|\mathcal{R}|$ must be at least 5. In this sense, functions with $|\mathcal{R}| = 5$ occupy a very special position in our understanding of the structures of functions.

### 8.3 Constructing Functions with $|\mathcal{R}| = 5$

The structure of a function with $|\mathcal{R}| = 5$ is not as simple as the cases when $|\mathcal{R}| < 5$. Unlike the case with $|\mathcal{R}| = 2$ or 4, there seem to be a number of different ways to construct functions with $|\mathcal{R}| = 5$. The purpose of this section is to demonstrate one of such construction methods.

We start with $n = 5$. Let $\omega(y)$ be a mapping from $V_2$ into $V_3$, defined as follows

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

$$\omega(1, 0) = (1, 1, 0), \omega(1, 1) = (0, 1, 1).$$

Set

$$f_5(z) = f_5(y, x) = \langle \omega(y), x \rangle \quad (2)$$
where $y \in V_2$ and $x \in V_3$, $z = (y, x)$. $f_5$ can be explicitly expressed as

$$f_5(y_1, y_2, x_1, x_2, x_3) = (1 \oplus y_1)(1 \oplus y_2)x_1 \oplus (1 \oplus y_1)y_2x_2 \oplus y_1(1 \oplus y_2)(x_1 \oplus x_2) \oplus y_1y_2(x_2 \oplus x_3)$$

To further discuss the properties of $f_5$, let $\ell_{100}, \ell_{010}, \ell_{110}, \ell_{011}$ denote the sequences of $\varphi_{100}(x_1, x_2, x_3) = x_1, \varphi_{010}(x_1, x_2, x_3) = x_2, \varphi_{110}(x_1, x_2, x_3) = x_1 \oplus x_2,$ and $\varphi_{011}(x_1, x_2, x_3) = x_2 \oplus x_3$ respectively, where each $\varphi$ is regarded as a linear function on $V_3$. By Lemma 1 of [6], $\ell_{100}, \ell_{010}, \ell_{110}, \ell_{011}$ are different rows of $H_3$. By Lemma 2 of [6], the sequence of $f_5$ is

$$\xi = (\ell_{100}, \ell_{010}, \ell_{110}, \ell_{011}).$$

Let $\xi(\gamma)$ denote the sequence of

$$f_5(z \oplus \gamma) = \langle \omega(y \oplus \beta), x \oplus \alpha \rangle$$

where $\beta \in V_2$ and $\alpha \in V_3$, $\gamma = (\beta, \alpha)$. We now consider $D(\gamma) = (\xi(\gamma), \xi(\gamma)).$

Case 1: $\beta \neq 0$. In this case we have

$$f_5(z) \oplus f_5(z \oplus \gamma) = \langle \omega(y \oplus \beta), x \oplus \alpha \rangle$$

Note that $\omega(y \oplus \beta)$ is a nonzero constant vector in $V_2$ for any fixed $y \in V_2$. Thus $f_5(z) \oplus f_5(z \oplus \gamma)$ is a nonzero linear function on $V_3$ for any fixed $y \in V_2$ and hence it is balanced. This proves that $D(\gamma) = 0$ with $\gamma = (\beta, \alpha)$ and $\beta \neq 0$.

Case 2: $\beta = 0$. In this case

$$f_5(z) \oplus f_5(z \oplus \gamma) = \langle \omega(y), \alpha \rangle$$

is balanced for $\alpha = (0, 1, 1), (1, 0, 0)$ and $(1, 1, 1)$. In other words, $D(\gamma) = 0$, if $\gamma = (0, \alpha)$ and $\alpha = (0, 1, 1), (1, 0, 0)$ or $(1, 1, 1)$. It is straightforward to verify that $D(\gamma) = 2^4, -2^4, -2^4$ with $\gamma = (0, \alpha)$ and $\alpha = (0, 0, 1), (0, 1, 0), (1, 0, 1)$ and $(1, 1, 0)$ respectively. Obviously $D(0) = 2^4$. Thus $f_5$ satisfies the propagation criterion with respect to all but five vectors in $V_2$.

With $f_5$ as a basis, we now construct functions with $|R| = 5$ over higher dimensional spaces. Let $t \geq 5$ be odd and $s$ be even. And let $g$ be a function on $V_t$ that satisfies the propagation criterion with respect to all but five vectors in $V_t$, and $h$ be a bent function on $V_s$. Set

$$f(w) = g(v) \oplus h(u)$$

where $w = (v, u), v \in V_t$ and $u \in V_s$. Then we have

**Lemma 5** A function constructed by (7) satisfies $|R| = 5$.

A function $f$ constructed by (5) is balanced if $g$ is balanced. As the function $f_5$ on $V_4$ defined in (4) is balanced, we have

**Theorem 7** For any odd $n \geq 5$, there exists a balanced function satisfying the propagation criterion with respect to all but five vectors in $V_n$.

As an example, set $h(x_6, x_7) = x_6x_7$ and

$$f_7(x_1, x_2, x_3, x_4, x_5, x_6, x_7) = f_5(x_1, x_2, x_3, x_4, x_5) \oplus h(x_6, x_7)$$

where $f_5$ is defined in (4). Note that $h(x_6, x_7)$ is a bent function on $V_4$, by Theorem 7, $f_7$ is a balanced function on $V_7$ that satisfies $|R| = 5$.

To close this section we note that one can also start with constructing a function $f_7$ on $V_7$ with $|R| = 5$ by using the same method as that for designing $f_5$.

**9 Functions with $|R| = 6$**

Careful analysis which will be presented in the final paper shows that:

**Theorem 8** There exists no function on $V_n$ such that $|R| = 6$.

**10 Degrees of Propagation**

In [6] it has been shown that if $f$ is a function on $V_n$ with $|R| = 2$, then, through a nonsingular linear transformation on input coordinates, $f$ can be converted into a function satisfying the propagation criterion of degree $n - 1$. Similarly, when $|R| = 4$, the degree can be $\approx \frac{2}{3}n$. In this section we show that with $|R| = 5$, the degree can be $n - 3$.

Assume that the four nonzero vectors in $R$ are $\beta_1, \beta_2, \beta_3$ and $\beta_4$, and that $\beta_1, \beta_2$ and $\beta_3$ are a basis of $R = \{0, \beta_1, \beta_2, \beta_3, \beta_4\}$. Let $B$ be an $n \times n$ nonsingular matrix on $GF(2)$ with the property that

$$\beta_1B = (1, 0, 1, 0, 0, 1)$$
$$\beta_2B = (1, 0, 0, 1, 0, 0)$$
$$\beta_3B = (1, 0, 1, 0, 0, 0)$$

As $\beta_4 = \beta_1 + \beta_2 + \beta_3$, we have

$$\beta_4B = (\beta_1 + \beta_2 + \beta_3)B = (1, 1, 1, 1, 1, 1).$$

Now let $g(x) = f(xB)$. Then $g$ satisfies the propagation criterion of degree $n - 3$, as the only exceptional vectors are $(0, \ldots, 0, 0, 0, 0), (1, \ldots, 1, 0, 0, 0), (1, \ldots, 1, 0, 1, 0), (1, \ldots, 1, 1, 0, 0)$ and $(1, \ldots, 1, 1, 1, 1)$.

These discussions, together with Theorem 7, show that for any odd $n \geq 5$, there exist balanced functions on $V_n$ that satisfy the propagation criterion of degree $n - 3$ and do not possess a nonzero linear structure.

Table 1 shows structural properties of functions with $|R| \leq 6$. 


\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|c|}
\hline
$R$ & $\{0\}$ & $\{0, \beta\}$ & $\{0, \beta_1, \beta_2, \beta_3\}$ & $\{0, \beta_1, \beta_2, \beta_3, \beta_4\}$ \\
\hline
Dimension $n$ & even & odd & even & odd \\
\hline
Form of function & bent & $c_0x_n \oplus h(x_1, \ldots, x_{n-1})$, $h$ is bent. & $c_1x_n \oplus c_2x_{n-1} \oplus h(x_1, \ldots, x_{n-2})$, $h$ is bent. & e.g. \ $f_5(x_1, \ldots, x_5) \oplus h(x_6, \ldots, x_n)$, $f_5$ is defined in (4), $h$ is bent. \\
\hline
Nonzero linear structure(s) & No & $\beta$ & $\beta_1, \beta_2, \beta_3$ & No \\
\hline
Nonlinearity & $2^{n-1} - 2^{\frac{2}{n-1}} n - 1$ & $2^{n-1} - 2^{\frac{n-1}{2}} n - 1$ & $2^{n-1} - 2^{\frac{n-1}{2}} n$ & $2^{n-1} - 2^\frac{n-1}{2}$ \\
\hline
Degree of propagation & $n$ & $n-1$ & $\approx \frac{2}{n}$ & $n - 3$ \\
\hline
Is $R$ a subspace? & Yes & Yes & Yes & No, however, $\beta_1 \oplus \beta_2 \oplus \beta_3 \oplus \beta_4 = 0.$ \\
\hline
Rank of $R$ & 0 & 1 & 2 & 3 \\
\hline
\end{tabular}
\caption{Structural Properties of Highly Nonlinear Functions (Functions with three or six exceptional vectors do not exist.)}
\end{table}

11 Final Remarks

We have presented a quantitative relationship between propagation characteristic and nonlinearity. We have shown that no functions satisfy the propagation criterion with respect to all but three or six vectors. We have also completely decided the structures and construction methods of cryptographic functions that satisfy the propagation criterion with respect to all but two, four or five vectors. An interesting topic for future research is to investigate the structures of functions with seven or more exceptional vectors.

Acknowledgments

The first author was supported in part by ARC (A49130102, A4913185 and A49232172) and ATERB (C010/058), the second author by ARC (A49130102), and the third author by ARC (A49232172) and ATERB (N069/412).

References


Thesis, Department of Electrical Engineering, Queen’s University, Ontario, 1985.