Propagation Characteristics of Boolean Functions

Bart Preneel[1], Werner Van Leekwijck, Luc Van Linden,
René Govaerts and Joos Vandewalle

Katholieke Universiteit Leuven, Laboratorium ESAT
Kardinaal Mercierlaan, 94, B–3030 Heverlee, Belgium

Abstract

The relation between the Walsh-Hadamard transform and the autocorrelation function of Boolean functions is used to study propagation characteristics of these functions. The Strict Avalanche Criterion and the Perfect Nonlinearity Criterion are generalized in a Propagation Criterion of degree k. New properties and constructions for Boolean bent functions are given and also the extension of the definition to odd values of n is discussed. New properties of functions satisfying higher order SAC are derived. Finally a general framework is established to classify functions according to their propagation characteristics if a number of bits is kept constant.

1 Introduction

The design and evaluation of cryptographic functions requires the definition of design criteria. It is known that the security of schemes based on a combination of permutations and substitutions strongly depends on the characteristics of the substitution tables or S-boxes. The relevance of the criteria can be based on information theoretic grounds or on specific attacks that are possible if certain conditions are not fulfilled. It is possible to define characteristics for individual output bits of S-boxes as well as for the relation between the different functions. In this paper, only individual functions of n bits to 1 bit are studied, but it is certainly possible to extend the scope.

In the past following criteria have been proposed: the function must have a high nonlinear order (no affine functions are allowed), must be 0/1 balanced, complete, satisfy a strict avalanche criterion or be perfect non-linear (with respect to linear structures). These criteria can be extended by imposing the requirement that the functions created by *fixing a number of input bits* of the original function still satisfy certain criteria. A second extension is possible by not only specifying the average values but also the *extreme values*. It is clear that no function can satisfy all these criteria: a good function will be the golden mean.

[1] NFWO aspirant navorser, sponsored by the National Fund for Scientific Research (Belgium).

I.B. Damgard (Ed.): Advances in Cryptology - EUROCRYPT '90, LNCS 473, pp. 161-173, 1991.

An example of the study of the design principles of the Data Encryption Standard can be found in [BMP86]. The analysis of key clustering for a limited number of rounds of the DES also used intensively properties of the S-boxes when two input bits are fixed [DQD84]. An attack on the same cipher uses linear structures [Eve87] and can be thwarted if the S-boxes are perfect non-linear [MS89]. The price paid is that perfect non-linear functions are not balanced.

In this paper, we will not attempt to study the link between design criteria and the cryptographic functions, but we will try to generalize certain criteria and to study the functions that satisfy them. In a first section, the importance of the autocorrelation function of a Boolean function will be stressed and a new propagation criterion will be defined. Next the bent functions will be studied, followed by the functions satisfying higher order SAC. These criteria are further generalized and functions satisfying these criteria are studied.

2 Definitions

2.1 Boolean functions

A Boolean function $f(\underline{x})$ is a function whose domain is the vector space $\mathbb{Z}_2^n$ of binary n-tuples $(x_1, x_2, \ldots, x_n)$ that takes the values 0 and 1. In some cases it will be more convenient to work with functions that take the values $\{-1, 1\}$. The functions $\hat{f}(\underline{x})$ is defined as $\hat{f}(\underline{x}) = 1 - 2 \cdot f(\underline{x})$.

The Hamming weight *hwt* of an element of $\mathbb{Z}_2^n$ is the number of components equal to 1. The Hamming distance $d(f,g)$ between two Boolean functions f and g is the number of function values in which they differ:

$$d(f,g) = hwt(f \oplus g) = 2^{n-1} - \frac{1}{2} \sum_{\underline{x}} \hat{f}(\underline{x}) \cdot \hat{g}(\underline{x}).$$

Here $\sum_{\underline{x}}$ denotes the summation over all $\underline{x} \in \mathbb{Z}_2^n$. The correlation $c(f,g)$ is closely related to the Hamming distance: $c(f,g) = 1 - d(f,g)/2^{n-1}$.

A Boolean function is said to be linear if there exists a $\underline{w} \in \mathbb{Z}_2^n$ such that it can be written as $L_{\underline{w}}(\underline{x}) = \underline{x} \cdot \underline{w}$ or $\hat{L}_{\underline{w}}(\underline{x}) = (-1)^{\underline{x} \cdot \underline{w}}$. Here $\underline{x} \cdot \underline{w}$ denotes the dot product of $\underline{x}$ and $\underline{w}$, defined as $\underline{x} \cdot \underline{w} = x_1 w_1 \oplus x_2 w_2 \oplus \ldots \oplus x_n w_n$. The set of affine functions $A_{\underline{w}, w_0}(\underline{x})$ is the union of the set of the linear functions and their complement: $A_{\underline{w}, w_0}(\underline{x}) = L_{\underline{w}}(\underline{x}) \oplus w_0$, $w_0 \in \mathbb{Z}_2$.

2.2 The Walsh-Hadamard transform

Definition 1 *Let $f(\underline{x})$ be any real-valued function with domain the vector space $\mathbb{Z}_2^n$. The* **Walsh-Hadamard transform** *of $f(\underline{x})$ is the real-valued function over the vector space $\mathbb{Z}_2^n$ defined as*

$$F(\underline{w}) = \sum_{\underline{x}} f(\underline{x}) \cdot (-1)^{\underline{x} \cdot \underline{w}}.$$

The function $f(\underline{x})$ *can be recovered by the* **inverse Walsh–Hadamard transform:**

$$f(\underline{x}) = \frac{1}{2^n} \sum_{\underline{w}} F(\underline{w}) \cdot (-1)^{\underline{x} \cdot \underline{w}}.$$

The relationship between the Walsh-Hadamard transform of $f(\underline{x})$ and $\hat{f}(\underline{x})$ is given by [For88] $\hat{F}(\underline{w}) = -2F(\underline{w}) + 2^n\ \delta(\underline{w})$ and $F(\underline{w}) = -\frac{1}{2}\hat{F}(\underline{w}) + 2^{n-1}\ \delta(\underline{w})$, where $\delta(\underline{w})$ denotes the Kronecker delta $(\delta(\underline{0}) = 1, \delta(\underline{k}) = 0\ \ \forall \underline{k} \neq \underline{0})$.

As the Walsh-Hadamard transform is linear, an alternative definition based on a matrix product is possible. The function values of $f(\underline{x})$ and $F(\underline{x})$ are written in the column matrices $[f]$ and $[F]$ respectively

$$[F] = H_n \cdot [f] \,,$$

where H_n is the Walsh-Hadamard matrix of order n that can be recursively defined as

$$H_n = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes H_{n-1} \,, \qquad H_0 = [1] \,.$$

Here $\otimes$ denotes the Kronecker product between matrices. It is easily seen that $H_n^2 = 2^n \cdot I_n$.

In case of the Fourier transform, the energy spectrum (the square modulus of the Fourier transform) is used in a wide range of applications. A very important relation, known as the *Wiener-Khintchine theorem*, is that the inverse transform of the energy spectrum results in the autocorrelation function. A similar relation can be established in case of the Walsh-Hadamard transform. The autocorrelation function $\hat{r}(\underline{a})$ is defined as

$$\hat{r}(\underline{a}) = \sum_{\underline{x}} \hat{f}(\underline{x}) \cdot \hat{f}(\underline{x} \oplus \underline{a}).$$

Note that $\hat{r}(\underline{0})$ equals 2^n. The Walsh-Hadamard energy spectrum of any real-valued function is defined as $\hat{F}^2(\underline{w})$. The Walsh-Hadamard transform of $\hat{r}(\underline{a})$ will be denoted with $\hat{R}(\underline{w})$.

Theorem 1 *The Walsh-Hadamard transform of the autocorrelation function of any real-valued function is equal to the Walsh-Hadamard energy spectrum of that function:* $\hat{R}(\underline{w}) = \hat{F}^2(\underline{w}), \quad \forall \underline{w} \in \mathbb{Z}_2^n$.

In case $\hat{f}(\underline{x})$ is Boolean, the importance of the autocorrelation function can be seen as follows:

$$\Pr\left(\hat{f}(\underline{x}) \neq \hat{f}(\underline{x} \oplus \underline{a})\right) = \frac{1}{2} - \frac{\hat{r}(\underline{a})}{2^{n+1}}.$$

For large values of n this theorem allows for an efficient computation of these probabilities, requiring $O(n2^n)$ operations (in stead of $O(2^{2n})$ for a straightforward computation). Summing these probabilities for all $\underline{a} \neq \underline{0}$ yields:

$$\sum_{\underline{a} \neq \underline{0}} \Pr\left(\hat{f}(\underline{x}) \neq \hat{f}(\underline{x} \oplus \underline{a})\right) = 2^{n-1} - \frac{\hat{F}^2(0)}{2^{n+1}}$$

If all probabilities are equal to $\frac{1}{2}$, then $\mid \hat{F}(0) \mid = 2^{\frac{n}{2}}$. If $f(\underline{x})$ is 0/1 balanced then $\hat{F}(0) = 0$ and the average of the probabilities is $(2^{n-1})/(2^n - 1) > \frac{1}{2}$.

2.3 The algebraic normal transform

The Walsh-Hadamard transform writes a Boolean function $\hat{f}(\underline{x})$ as a sum of linear functions of the form $(-1)^{\underline{x} \cdot \underline{w}}$. It can also be of interest to write a Boolean function as the sum of all products of the variables:

$$f(\underline{x}) = a_0 \oplus \sum_{1 \leq i \leq n} a_i x_i \oplus \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 x_n .$$

This form is called the algebraic normal form of a Boolean function f, denoted with $\mathcal{F}$ and the corresponding transformation is called the algebraic normal transform [Rue86]. When the natural order of the variables is used, namely 1, x_1, x_2, $x_1 x_2$, x_3, $x_1 x_3$, $\ldots$, $x_1 x_2 \ldots x_n$ following definition can be stated [Jan89]:

Definition 2 *The* **algebraic normal transform** *of a Boolean function f is a linear transformation (with respect to addition modulo 2) defined as*

$$[\mathcal{F}] = A_n \cdot [f]$$

$$\textit{with} \quad A_n = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \otimes A_{n-1} , \qquad A_0 = [1] .$$

The transform is an involution: $A_n^2 = I_n$.

Definition 3 *The* **nonlinear order** *of a Boolean function (notation:* ord(f)*) is defined as the degree of the highest order term in the algebraic normal form.*

The affine Boolean functions are thus the functions with nonlinear order < 2.

2.4 Definition of propagation properties

The definitions of strict avalanche criterion and of perfect non-linearity can be formulated with the help of the autocorrelation function.

A Boolean function $f(\underline{x})$ satisfies the *strict avalanche criterion (SAC)* if and only if $f(\underline{x})$ changes with a probability of one half whenever a single input bit of $\underline{x}$ is complemented [WT85], i.e.

$$\hat{r}(\underline{a}) = 0 \;\text{ for }\; hwt(\underline{a}) = 1.$$

As a consequence, theorem 1 in [For88], stating that $\hat{f}(\underline{x})$ fulfills the SAC if and only if

$$\sum_{\underline{w}} \hat{F}^2(\underline{w}) \cdot (-1)^{w_i} = 0 \quad 1 \leq i \leq n$$

is a special case of our theorem 1.

A Boolean function $f(\underline{x})$ is *perfect non-linear (with respect to linear structures)* if $f(\underline{x})$ changes with a probability of one half whenever i $(1 \leq i \leq n)$ bits of $\underline{x}$ are complemented [MS89]:

$$\hat{r}(\underline{a}) = 0 \ \text{ for } \ 1 \leq hwt(\underline{a}) \leq n.$$

The perfect non-linear functions or bent functions will be studied in section 3. Note that if functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ are considered, the definition of perfect non-linear and bent can be extended. Only if q is prime both concepts coincide [Nyb90].

These definitions can be generalized in a natural way as follows. A Boolean function $f(\underline{x})$ satisfies the *propagation criterion of degree k (PC of degree k)* if $f(\underline{x})$ changes with a probability of one half whenever i $(1 \leq i \leq k)$ bits of $\underline{x}$ are complemented:

$$\hat{r}(\underline{a}) = 0 \ \text{ for } \ 1 \leq hwt(\underline{a}) \leq k.$$

Note that SAC is equivalent to PC of degree 1 and perfect non-linear is PC of degree n.

When we are interested in propagation properties, it is important to be able to construct different functions that satisfy the same property starting from one function. A trivial example of such a construction is a complementation. The following theorem shows that other constructions are possible for functions satisfying PC of degree k by means of a dyadic shift in the Walsh-Hadamard domain.

Theorem 2 *Let $f(\underline{x})$ be a Boolean function. Then the function $g(\underline{x})$ defined as $\hat{G}(\underline{w}) = \hat{F}(\underline{w} \oplus \underline{s})$ is also Boolean for all $\underline{s}$. Moreover, the autocorrelation function of $\hat{g}(\underline{x})$ has the same absolute values (and thus the same zeroes) as the autocorrelation function of $\hat{f}(\underline{x})$ and for $\underline{s} \neq \underline{0}$ the distance $d(f,g)$ equals 2^{n-1}.*

Corollary 1 *A dyadic shift and a complementation in the Walsh-Hadamard domain generate all 2^{n+1} possible changes of terms in the algebraic normal form with degree smaller than 2.*

Note that a dyadic shift in the original domain generates a Boolean function with the same autocorrelation function, inducing only changes of terms of degree $< ord(f)$. However, the maximal distance condition is only fulfilled if the original function is bent.

3 Properties and constructions of bent functions

In [Rot76] bent functions are first defined and the importance for cryptographic applications was explained in [MS89]. In this section we give a brief overview of the known properties of bent functions. Some new properties will be stated without proof. A new construction method for bent functions is derived, and upper and lower bounds on the number of bent functions are computed accordingly. Finally, an extension of the definition for odd n is considered.

3.1 Properties of bent functions

In the following, unless mentioned explicitly, we will consider only Boolean bent functions. Bent functions only exist for even values of n. They have a flat energy spectrum with value 2^n. As a consequence bent functions are never balanced and the difference between the number of ones and the number of zeroes equals $\pm 2^{\frac{n}{2}}$. This also implies that their autocorrelation function is an impulse function. In [MS89] it is shown that bent functions have maximum distance 2^{n-2} to all linear structures and maximum distance $2^{n-1} - 2^{\frac{n}{2}-1}$ to all affine functions and thus they have minimum correlation $\pm 2^{-\frac{n}{2}}$ to all affine functions. The nonlinear order of bent functions is bounded from above by $\frac{n}{2}$ for $n > 2$.

A first important property is based on the similarity of the Walsh-Hadamard transform and its inverse. A bent function has a constant energy spectrum, but not all functions with a constant energy spectrum are Boolean (i.e. have an absolute value of 1). The conditions for a function to be Boolean or bent are dual, as shown by the following theorem.

Theorem 3 *Any real-valued function over $\mathbb{Z}_2^n$ is* **Boolean** *if and only if*

$$| \hat{f}(\underline{x}) | = 1 \quad \Longleftrightarrow \quad \sum_{\underline{w}} \hat{F}(\underline{w})\hat{F}(\underline{w} \oplus \underline{a}) = 2^{2n}\delta(\underline{a}).$$

Any real-valued function over $\mathbb{Z}_2^n$ is **bent** *if and only if*

$$\sum_{\underline{x}} \hat{f}(\underline{x})\hat{f}(\underline{x} \oplus \underline{a}) = 2^n\delta(\underline{a}) \quad \Longleftrightarrow \quad | \hat{F}(\underline{w}) | = 2^{\frac{n}{2}}.$$

It is easily seen that the number of all (non necessarily Boolean) bent functions over $\mathbb{Z}_2^n$ equals the number of Boolean functions over $\mathbb{Z}_2^n$, namely 2^{2^n}. On the other hand, the number of Boolean bent functions for n even remains an open problem. This duality leads to following theorem [Rot76] and definition:

Theorem 4 *Let $\hat{f}(\underline{x})$ be a Boolean bent function. Then $\hat{g}(\underline{x})$ and $\hat{h}(\underline{x})$, defined as $\hat{g}(\underline{x}) = 2^{-\frac{n}{2}}\hat{F}(\underline{x})$ and $\hat{h}(\underline{x}) = -2^{-\frac{n}{2}}\hat{F}(\underline{x})$ are also Boolean bent functions.*

Definition 4 *The* **dual** *and* **anti-dual** *bent functions are the Boolean eigenvectors of the Walsh-Hadamard matrix of order n with eigenvalues $2^{\frac{n}{2}}$ and $-2^{\frac{n}{2}}$ respectively.* Hence these bent functions are the Boolean solutions of the equation $H_n[\hat{f}] = \pm 2^{n/2}[\hat{f}]$, that is studied in more detail in [YH82].

The alternative formula for the distance $d(f,g) = 2^{n-1} - 2^{-n-1}\sum_{\underline{w}} \hat{F}(\underline{w})\hat{G}(\underline{w})$ shows that the minimum distance to affine functions equals $2^{n-1} - 1/2 \max_{\underline{w}} | \hat{F}(\underline{w}) |$. The maximal value of the spectrum is thus a measure for the minimum distance to affine functions. The degree of nonlinearity with respect to linear structures is defined to be 0 for affine functions and 1 for bent functions.

Definition 5 *The* **degree of nonlinearity with respect to linear structures DNL** *is defined as*

$$DNL = \frac{2^{n-1} - 1/2 \max_{\underline{w}} |\hat{F}(\underline{w})|}{2^{n-1} - 2^{\lfloor n/2 \rfloor - 1}}$$

For $n = 4$, this results in following distribution, where abstraction is made of constant and linear terms. Every function in the table corresponds to 32 different functions.

number of functions	1	16	120	560	875	448	28
DNL	0	1/6	2/6	3/6	4/6	5/6	1

The sum of all the values of the Walsh-Hadamard transform of a Boolean function is restricted to two distinct values. This observation can be extended in case l bits of $\underline{w}$ are fixed through considering the sum over the 2^{n-l} remaining possibilities (notation: $\sum_{\underline{w}}[l]$). Following theorem gives the values that these sums can take.

Theorem 5 *Let $\hat{f}(\underline{x})$ be any Boolean function. Then*

$$\sum_{\underline{w}}[l]\ \hat{F}(\underline{w}) = -2^n + k \cdot 2^{n+1-l} \quad \textit{with}\ 0 \le k \le 2^l.$$

Let $\hat{f}(\underline{x})$ be any bent function (non necessarily Boolean). Then

$$\sum_{\underline{w}}[l]\ \hat{F}(\underline{w}) = -2^{3n/2-l} + k \cdot 2^{n/2+1} \quad \textit{with}\ 0 \le k \le 2^{n-l}.$$

Let $\hat{f}(\underline{x})$ be any Boolean bent function. Then $\sum_{\underline{w}}[l]\ \hat{F}(\underline{w}) = 2^{n/2} \sum_{\underline{x}}[l] \hat{f}(\underline{x}) =$

$$\begin{cases} -2^n + k \cdot 2^{n+1-l} \ \ \textit{with}\ 0 \le k \le 2^l, & \textit{if}\ 0 \le l \le \frac{n}{2} \\ -2^{3n/2-l} + k \cdot 2^{n/2+1} \ \ \textit{with}\ 0 \le k \le 2^{n-l}, & \textit{if}\ \frac{n}{2} \le l \le n. \end{cases}$$

The previous theorem makes it theoretically possible to construct *all* bent functions of n variables without performing an exhaustive search. The Walsh spectrum of a (Boolean) bent function has $2^{n-1} \pm 2^{n/2-1}$ positive values. Starting from the previous theorem, this can be extended for the case that l bits are kept constant.

Lemma 1 *The number of positive entries of the Walsh-Hadamard transform of a Boolean bent function when l bits of $\underline{w}$ are fixed equals*

$$P_+(l) = 2^{n-l-1} + 2^{-n/2-1} \cdot \sum_{\underline{w}}[l]\ \hat{F}(\underline{w}).$$

For $n = 4$, this results in following values for $\{P_+(0)\} = \{6, 10\}$, $\{P_+(1)\} = \{2, 4, 6\}$. For $l \ge n/2$ no additional restrictions are imposed. With a recursive construction starting from $l = 0$ the number of positive entries at level l can be composed of the combination of two entries of level $l + 1$. Additional restrictions have to be imposed, and for the time being it is only feasible for $n = 4$ to construct all bent functions in this way.

3.2 Construction of bent functions

Most known constructions are enumerated in [YH89]: the two Rothaus constructions [Rot76], the eigenvectors of Walsh-Hadamard matrices [YH82], constructions based on Kronecker algebra, concatenation, dyadic shifts and linear transformations of variables. The generalization of the Rothaus construction by Maiorana and McFarland is discussed in [Nyb90]. In this section new constructions will be given based on Walsh-Hadamard matrices and concatenation. Conditions are stated for a function of nonlinear order 2 to be bent.

Theorem 6 *For $n = 2m$, consider the rows of the Walsh-Hadamard matrix H_m. The concatenation of the 2^m rows or their complement in arbitrary order results in $(2^m)!\,2^{2^m}$ different Boolean bent functions of n variables.*

This construction results in the same lower bound as the Maiorana construction. An upper bound for $n > 2$ can be computed based on the restriction on the nonlinear order:

$$2^{2^{n-1}+d(n)} \text{ with } d(n) = \frac{1}{2}\binom{n}{n/2}.$$

Following table gives the lower bound, the number of bent functions (if known), the upper bound and the number of Boolean functions. For $n = 6$, the number of bent functions equals 5,425,430,528.

n	lower bound	# bent	upper bound	# Boolean
2	8	8	8	16
4	384	896	2048	65536
6	$2^{23.3}$	$2^{32.3}$	2^{42}	2^{64}
8	$2^{60.3}$	?	2^{163}	2^{256}

The construction of a Boolean function $\hat{f}(\underline{x})$ through concatenation implies that the vector $[\hat{f}]$ is obtained as a concatenation of different vectors $[\hat{g}_i]$.

Theorem 7 *The concatenation $\hat{f}$ of dimension $n+2$ of 4 bent functions $\hat{g}_i$ of dimension n is bent if and only if*

$$\hat{G}_1(\underline{w}) \cdot \hat{G}_2(\underline{w}) \cdot \hat{G}_3(\underline{w}) \cdot \hat{G}_4(\underline{w}) = -2^{2n}, \quad \forall \underline{w} \in \mathbb{Z}_2^n.$$

Corollary 2 *If $\hat{f}$, $\hat{g}_1$, $\hat{g}_2$ and $\hat{g}_3$ are bent then $\hat{g}_4$ is also bent.*

- The order of the $\hat{g}_i$ has no importance.
- In case $\hat{g}_1 = \hat{g}_2$, the theorem reduces to $\hat{g}_4 = -\hat{g}_3$, and if $\hat{g}_1 = \hat{g}_2 = \hat{g}_3$, then $\hat{g}_4 = -\hat{g}_1$. These special cases are considered in [YH89].

Theorem 8 *If the concatenation of 4 arbitrary vectors of dimension n is bent, then the concatenation of all 4! permutations of these vectors is bent.*

Note that through dyadic shifting of f only 4 of the 24 permutations can be obtained. This theorem is best possible in the sense that if the function is split up in 8 vectors, all permutations will in general not result in a bent function.

When the nonlinear order is restricted to 2, counting and construction of all functions is possible. In that case the autocorrelation function can take only the values $\{0, \pm 2^n\}$. Following theorem was stated in chapter 15 of [MWS78].

Theorem 9 *Let $\hat{f}(\underline{x})$ be a Boolean function with* $\mathrm{ord}(f) = 2$ *and second order coefficients of the algebraic normal form denoted by a_{ij}. Then $\hat{f}(\underline{x})$ is bent if and only if the matrix V, defined as $v_{ij} = a_{ij}$ for $i \neq j$ and $v_{ii} = 0$, has full rank. For n even, the number of second order bent functions equals $\prod_{i=0}^{(n/2)-1}(2^{2i+1} - 1)2^{2i}$. For odd n, no bent functions exist.*

3.3 Extension of bent functions for odd n

As there exist no bent functions for odd n, it is interesting to extend the concept. In [MS89], following proposal for extension was made:

$$f(\underline{x}) = \overline{x}_n f_0(x_1, \ldots, x_{n-1}) \oplus x_n f_1(x_1, \ldots, x_{n-1}), \quad \text{with } f_0, f_1 \text{ bent.}$$

It is clear that *ord(f)* $\leq (n+1)/2$. It is also shown that for half of the values of $\underline{w}$, $\hat{F}(\underline{w}) = 0$ and for the other half $|\hat{F}(\underline{w})| = 2^{(n+1)/2}$. The maximum distance to affine functions equals $2^{n-1} - 2^{(n+1)/2-1}$. However, these functions do not necessarily satisfy PC of degree 1: e.g. if $f_0 = f_1$, then $\hat{r}(0\ldots01) \neq 0$, but for all other values of $\underline{a} \neq \underline{0}$, $\hat{r}(\underline{a}) = \underline{0}$. It is clear that $\hat{r}(\underline{a}) = 0$ if the most significant bit of $\underline{a}$ equals zero. If the right choice for f_0 and f_1 is made, $\hat{r}(\underline{a})$ will also be zero for $\underline{a} = 10\ldots0$, and only in these cases f will satisfy PC of degree 1. Other constructions that will be discussed in a forthcoming paper result in functions that satisfy PC of degree $n-1$. A second observation is that f will be balanced if and only if f_0 and f_1 have a different number of zeroes and ones. An example of a function satisfying both properties will be given in section 5.

4 Higher order SAC

Higher order SAC is defined in [For88]. In [Llo89] the definition is simplified and it is shown that exactly 2^{n+1} functions satisfy the SAC of maximal order $n-2$.

Definition 6 *A Boolean function $f(\underline{x})$ satisfies the* **strict avalanche criterion of order** *m (SAC of order m) if any function obtained from $f(\underline{x})$ by keeping m of its input bits constant satisfies the SAC.*

A first theorem gives an upper bound on the non-linear order of functions satisfying SAC of order m.

Theorem 10 *Let f be a Boolean function of n variables, $n > 2$.*

1. *if f satisfies SAC of order $n-2$, then* $\mathrm{ord}(f) = 2$.
2. *if f satisfies SAC of order m $(0 \leq m < n-2)$, then* $\mathrm{ord}(f) \leq n - m - 1$.

This results in following table:

m (order of SAC)	0	1	...	$n-4$	$n-3$	$n-2$
non-linear order $\leq$	$n-1$	$n-2$	...	3	2	2

The next theorem gives a characterization of all second order functions satisfying SAC.

Theorem 11 *Let f be a Boolean function of n variables, with $n > 2$ and* $\mathrm{ord}(f) = 2$. *f satisfies SAC of order m $(0 \leq m \leq n-2)$, if and only if every variable x_i occurs in at least $m+1$ second order terms of the algebraic normal form.*

Definition 7 *The function $s_n(\underline{x})$ is defined as the function with the algebraic normal form containing all second order terms:*

$$s_n(\underline{x}) = \sum_{1 \leq i < j \leq n} x_i x_j .$$

It is clear from theorem 10 and 11 that if abstraction is made of affine terms, this is the only function satisfying SAC of order $n-2$. Hence the sum modulo 2 of 2 functions satisfying SAC of order $n-2$ is always affine. The observations in this paragraph were independently made by Bert den Boer [dBo90].

Theorem 10 and 11 characterize all functions satisfying SAC of order $n-3$ and enable to count them. A different characterization and counting method is explained in [Llo90].

5 Propagation characteristics

It seems plausible to study what happens if m bits are kept constant in functions that satisfy PC of degree k, as was done for the strict avalanche criterion. This allows for a more general classification of propagation characteristics of Boolean functions. We impose the restriction $k+m \leq n$: if m bits are kept constant at most $n-m$ bits can be changed.

Definition 8 *A Boolean function $f(\underline{x})$ of n variables satisfies the* **propagation criterion of degree k and order m** *(PC of degree k and order m) if any function obtained from $f(\underline{x})$ by keeping m input bits constant satisfies PC of degree k.*

Definition 9 *The* **propagation matrix** *N_n for all Boolean functions of n variables is the $n \times n$ matrix: $N_n(k,m) = \# \{f \mid f$ satisfies PC of degree k and order $m\} / 2^{n+1}$. with f a Boolean function and $k+m \leq n$.*

The division by 2^{n+1} implies that abstraction is made of linear and constant terms, that have no influence on propagation properties. It is clear that $N_n(k,m) \leq N_n(k,l)$ for $m \geq l$, $N_n(k,m) \leq N_n(l,m)$ for $k \geq l$, and $N_n(1,n-1) = 0$. The entry $N_n(n,0)$ contains the number of bent functions divided by 2^{n+1}. Note that theorem 10 also imposes restrictions on the nonlinear order of functions for values of $k > 1$.

The functions satisfying PC of degree 1 (= higher order SAC) were studied in section 4. Theorems 9 and 11 can be generalized resulting in a classification of the functions $s_n(\underline{x})$.

Theorem 12 *The functions $s_n(\underline{x})$ satisfy PC of degree k and order m if $k+m \leq n-1$ and also if $k+m=n$ and k is even. The functions $s_n(\underline{x})$ are the only functions satisfying PC of degree 2 and order $n-2$.*
For n even the functions $s_n(\underline{x})$ are bent (theorem 9), while for n odd these functions are an example of balanced functions that satisfy PC of degree $n-1$.

The matrices $N_3(k,m)$, $N_4(k,m)$ and $N_5(k,m)$ are given in Table 1. The entries $N_4(2\text{-}4,0)$ contain only the bent functions. The entry $N_4(1,0)$ contains 88 third order functions. The entries $N_4(1,2)$, $N_4(2,1)$ and $N_4(2,2)$ consist of the function s_4.

m k	0	1	2
1	4	1	0
2	1	1	–
3	0	–	–

m k	0	1	2	3
1	129	10	1	0
2	28	1	1	–
3	28	0	–	–
4	28	–	–	–

m k	0	1	2	3	4
1	430040	813	26	1	0
2	3568	28	1	1	–
3	168	28	0	–	–
4	28	28	–	–	–
5	0	–	–	–	–

Table 1: The matrices $N_3(k,m)$, $N_4(k,m)$ and $N_5(k,m)$

The concept of PC can be extended if the restriction $k+m \leq n$ is removed. This means that a certain value is given to m bits and subsequently k bits are changed. However, the set of bits that are given a certain value and the set of those that are changed can have common elements. This leads to a definition based on information theoretic grounds.

Definition 10 *A Boolean function $f(\underline{x})$ of n variables satisfies the* **extended propagation criterion of degree** k **and order** m *(EPC of degree k and order m) if knowledge of m bits of $\underline{x}$ gives no information on $f(\underline{x}) \oplus f(\underline{x} \oplus \underline{a})$, $\forall$ $\underline{a}$ with* $1 \leq \text{hwt}(\underline{a}) \leq k$.

Definition 11 *The* **extended propagation matrix** N_n^* *for all Boolean functions of n variables is the $n \times n$ matrix:*
$N_n^*(k,m) = \#\{f \mid f \textit{ satisfies EPC of degree } k \textit{ and order } m\}/2^{n+1}$.

The definition can be restated in terms of balancedness and correlation immunity [Sie84] of the directional derivative of a Boolean function.

Definition 12 *The* **directional derivative** *of a Boolean function f in direction $\underline{a}$ is defined as:*

$$d_{f,\underline{a}}(\underline{x}) = f(\underline{x}) \oplus f(\underline{x} \oplus \underline{a}).$$

The relation between the directional derivative and the autocorrelation function is given by:

$$\hat{r}(\underline{a}) = \sum_{\underline{x}} \hat{d}_{f,\underline{a}}(\underline{x}).$$

This results in an equivalent formulation of the EPC.

Theorem 13 *Let f be a Boolean function of n variables.*

1. *f satisfies EPC of degree k and order 0 if and only if the directional derivative $\hat{d}_{f,\underline{a}}(\underline{x})$ of f is balanced $\forall\ \underline{a} : 1 \leq \mathrm{hwt}(\underline{a}) \leq k$.*
2. *f satisfies EPC of degree k and order $m > 0$ if and only if the directional derivative $\hat{d}_{f,\underline{a}}(\underline{x})$ of f is balanced and mth order correlation immune $\forall\ \underline{a}$: $1 \leq \mathrm{hwt}(\underline{a}) \leq k$.*

The relation between PC and EPC is given in following theorem:

Theorem 14 *Let f be a Boolean function of n variables.*

1. *If f satisfies EPC of degree k and order m then f satisfies PC of degree k and order m.*
2. *If f satisfies PC of degree k and order 0 or 1 then f satisfies EPC of degree k and order 0 or 1.*
3. *If f satisfies PC of degree 1 and order m then f satisfies EPC of degree 1 and order m.*

Following example shows that this theorem is tight. Consider the function $s_n(\underline{x})$. The directional derivative of this function for a vector $\underline{a}$ with a 1 in position i and j is equal to $x_i \oplus x_j \oplus 1$. This function is balanced and correlation immune of order 1, but not of order 2. Hence $s_n(\underline{x})$ does not satisfy EPC of degree 2 and order 2. In this particular example, it is clear that if $x_i = x_j$, then $f(\underline{x} \oplus \underline{a}) \neq f(\underline{x}), \forall \underline{x}$ and if $x_i \neq x_j$, then $f(\underline{x} \oplus \underline{a}) = f(\underline{x}), \forall \underline{x}$. For the ordinary PC the average of both cases is considered: $f(\underline{x})$ changes on average with a probability of 0.5. For $n \leq 5$, the functions $s_n(\underline{x})$ are the only functions for which PC and EPC are not equivalent.

6 Summary

The importance of the relation between the autocorrelation function and the Walsh-Hadamard energy spectrum has been shown. This concept can be extended in the case of S-boxes to crosscorrelation properties. Existing propagation criteria were generalized to the propagation criterion PC of degree k and order m and an extended propagation criterion EPC. Functions satisfying these criteria were studied, especially the bent functions, the functions satisfying higher order SAC and the functions s_n consisting of all second order terms. The results show that functions satisfying PC of highest order and degree are only second order functions that clearly have some other weaknesses. Further research is necessary to characterize and count functions that satisfy the propagation criteria, to construct functions that are a compromise between different criteria and to extend the concepts to the design of S-boxes.

Acknowledgement

We would like to thank the people that showed interest in our work and especially Antoon Bosselaers, Kaisa Nyberg and Herman J. Tiersma for their helpful comments.

References

[BMP86] E.F. Brickell, J.H. Moore and M.R. Purtill, "Structures in the S-boxes of the DES", *Advances in Cryptology, Proc. Crypto 86*, Springer Verlag, 1987, p. 3–8.

[dBo90] B. den Boer, personal communication.

[DQD84] Y. Desmedt, J.-J. Quisquater and M. Davio, "Dependence of output on input in DES: small avalanche characteristics", *Advances in Cryptology, Proc. Crypto 84*, Springer Verlag, 1985, p. 359–376.

[Eve87] J.-H. Evertse, "Linear Structures in block ciphers", *Advances in Cryptology, Proc. Eurocrypt 87*, Springer Verlag, 1988, p. 249–266.

[For88] R. Forré, "The strict avalanche criterion: spectral properties of Boolean functions and an extended definition", *Advances in Cryptology, Proc. Crypto 88*, Springer Verlag, 1990, p. 450–468.

[Jan89] C.J.A. Jansen, *"Investigations on nonlinear streamcipher systems: construction and evaluation methods"*, PhD. Thesis, Technical University Delft, 1989.

[Llo89] S. Lloyd, "Counting functions satisfying a higher order strict avalanche criterion", *Advances in Cryptology, Proc. Eurocrypt 89*, Springer Verlag, to appear.

[Llo90] S. Lloyd, "Characterising and counting functions satisfying the strict avalanche criterion of order $(n-3)$".

[MWS78] F.J. MacWilliams and N.J.A. Sloane, *"The theory of error-correcting codes"*, North-Holland Publishing Company, Amsterdam, 1978.

[MS89] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions", *Advances in Cryptology, Proc. Eurocrypt 89*, Springer Verlag, to appear.

[Nyb90] K. Nyberg, "Constructions of bent functions and difference sets", *These Proceedings*.

[Rot76] O.S. Rothaus, "On bent functions", *Journal of Combinatorial Theory (A)*, Vol. 20, p. 300–305, 1976.

[Rue86] R.A. Rueppel, *"Analysis and design of stream ciphers"*, Springer Verlag, 1986.

[Sie84] T. Siegenthaler, "Correlation immunity of non-linear combining functions for cryptographic applications", *IEEE Trans. Inform. Theory*, Vol. IT-30, p. 776–780, Oct. 1984.

[WT85] A.F. Webster and S.E. Tavares, "On the design of S-boxes", *Advances in Cryptology, Proc. Crypto 85*, Springer Verlag, 1986, p. 523–534.

[GM88] X. Guo-Zhen and J.L. Massey, "A spectral characterization of correlation-immune combining functions", *IEEE Trans. Inform. Theory*, Vol. IT-34, p. 569–571, May 1988.

[YH82] R. Yarlagadda and J.E. Hershey, "A note on the eigenvectors of Hadamard matrices of order 2^n", *Linear Algebra & Appl.*, Vol. 45, p. 43–53, 1982.

[YH89] R. Yarlagadda and J.E. Hershey, "Analysis and synthesis of bent sequences", *Proc. IEE*, Vol. 136, Pt. E, p. 112–123, March 1989.