NONLINEARITY CRITERIA FOR CRYPTOGRAPHIC FUNCTIONS

Willi Meier [1] Othmar Staffelbach [2]

[1] HTL Brugg-Windisch
CH-5200 Windisch, Switzerland

[2] GRETAG Aktiengesellschaft
Althardstr. 70, CH-8105 Regensdorf
Switzerland

Abstract. Nonlinearity criteria for Boolean functions are classified in view of their suitability for cryptographic design. The classification is set up in terms of the largest transformation group leaving a criterion invariant. In this respect two criteria turn out to be of special interest, the distance to linear structures and the distance to affine functions, which are shown to be invariant under all affine transformations. With regard to these criteria an optimum class of functions is considered. These functions simultaneously have maximum distance to affine functions and maximum distance to linear structures, as well as minimum correlation to affine functions. The functions with these properties are proved to coincide with certain functions known in combinatorial theory, where they are called bent functions. They are shown to have practical applications for block ciphers as well as stream ciphers. In particular they give rise to a new solution of the correlation problem.

1. INTRODUCTION

For cryptographic systems the method of confusion and diffusion (as introduced by Shannon [8]) is used as a fundamental technique to achieve security. Confusion is reflected in nonlinearity of certain Boolean functions describing the cryptographic transformation. Nonlinearity is crucial since most linear systems are easily breakable. As a cipher which explicitly follows the principle of confusion and diffusion we mention DES. Likewise, this concept applies to other cryptosystems, block ciphers as well as stream ciphers.

In this context it is important to have criteria which are measures for nonlinearity. A variety of such criteria are known in cryptographic design. Our aim is to contribute to a general theory which classifies these criteria in view of their ability to measure nonlinearity. As a result of this investigation we are led to a class of nonlinear functions with many remarkable properties with regard to this theory.

Our considerations are based on the idea that a useful criterion should remain invariant under a certain group of transformations. This concept is fundamental in pure mathematics, e.g. in algebra. In cryptography it is motivated by the following point of view: A function is considered weak whenever it can be turned into a cryptographically weak function by means of simple (e.g. linear or affine) transformations. This is reminiscent to the situation, where Shannon introduced the notion of similar secrecy systems ([8], Chap. 8), R and S being similar if there is a transformation A such that R = AS. (Then by definition similar systems are cryptanalytically equivalent.)

To further illustrate our concept we consider the Boolean function $f(x_1, x_2, \ldots, x_n)$ whose algebraic normal form is obtained by summing up all possible product terms in

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 549-562, 1990.

$x_1, x_2, \ldots, x_n$. At the first glance this seems to be a good nonlinear function, since it contains all nonlinear terms. However f can be written as the product $f(x_1,,\ldots,x_n) = (1+x_1)(1+x_2)\cdots(1+x_n)$ which transforms into the monomial function $g(x_1,x_2,\ldots,x_n) = x_1x_2\cdots x_n$ by simply complementing all arguments. This turns f into a poor function with respect to the number of nonlinear terms. Thus, from the present point of view, a large number of nonlinear terms taken as a criterion is not suitable since it is not invariant under simple transformations.

It is desirable therefore that a nonlinearity criterion remains invariant under a larger group of transformations. For many applications this symmetry group should contain the group of all affine transformations. In Section 2 we develop a general method (Theorem 2.1) in order to show that several well known criteria satisfy this stronger requirement. Some of these criteria can be expressed in terms of a distance to appropriate sets of (cryptologically weak) functions. (The distance d(f,S) of a function f to any subset S of Boolean functions is defined as the minimum of the Hamming distances of f to all members of S.) In particular the distance $\delta(f)$ to affine functions is defined as $\delta(f) = d(f,S)$, where S is the set of all affine functions (cf. also [7], p. 122). We show that δ is a nonlinearity criterion with the desired property since it remains invariant under the operation of the full affine group (Corollary 2.2).

Depending on the application different sets S of functions have to be considered as cryptographically weak. The set of affine functions may be replaced e.g. by functions of low nonlinear order, like quadratic functions. Therefore, as a design criterion for a Boolean function f, we may introduce its distance $\delta_k(f)$ to all functions with nonlinear order bounded by k. (Note that $\delta_1 = \delta$.) We show that the design criterion δ_k also remains invariant under affine transformations. This is proved as a consequence of the fact that similar invariance properties hold for the nonlinear order of Boolean functions (Theorem 2.4).

In certain applications the class of affine functions has to be extended to another class of cryptographically weak functions. The definition of these functions is motivated by the fact that for a linear (or affine) Boolean function f the values $f(\underline{x}+\underline{a})$ and $f(\underline{x})$, for every fixed $\underline{a}$, are either always equal or always different. Note however that many functions have this property without being linear or affine. The functions characterized by this condition appear to be important in the analysis and design of block ciphers, as has been pointed out by Chaum and Evertse in [1] and [3], where this property is termed a linear structure. We denote by $\sigma(f)$ the distance d(f,S), where S is the set of all Boolean functions with linear structures. Then as for δ, the distance σ is invariant under the operation of the full affine group (Corollary 2.3).

With respect to linear structures, a function f has optimum nonlinearity if for every nonzero vector $\underline{a} \in GF(2)^n$ the values $f(\underline{x}+\underline{a})$ and $f(\underline{x})$ are equal for exactly half of the arguments $\underline{x} \in GF(2)^n$. If a function f satisfies this property we will call it perfect nonlinear with respect to linear structures, or briefly perfect nonlinear. In [3] Evertse has introduced a corresponding notion for DES-like S-boxes where he named it a 50%-linear structure. Furthermore he questioned whether S-boxes with this restrictive property do exist, a question which is settled in this paper.

In a different direction, this notion of perfect nonlinearity is closely related to another design criterion for S-boxes, namely the strict avalanche criterion (SAC). Basicly this is a diffusion criterion and has been investigated in [11] and [4]. Recall that a Boolean function satisfies SAC if the output changes with probability one half whenever a single input bit is complemented. This means that a function satisfies SAC if the condition stated in the definition of perfect nonlinearity merely holds for vec-

tors $\underline{a}$ of weight 1. Therefore perfect nonlinearity effects diffusion, and it is in fact a much stronger requirement than SAC. It is remarkable that in this context diffusion can be linked with nonlinearity.

It turns out that perfect nonlinear functions correspond to certain functions known in combinatorial theory - in combinatorial theory Rothaus ([6]) has investigated a class of functions, which he called 'bent functions'. The coincidence of bent functions with perfect nonlinear functions is derived by using properties of the Walsh transform. The existence of these functions is established in [6] by giving explicit constructions. In particular, for $n = 2m$, the functions of the form $f(x_1,x_2,\ldots,x_n) = g(x_1, \ldots, x_m) + x_1x_{m+1} + x_2x_{m+2} + \ldots + x_mx_n$ are known to be perfect nonlinear, where $g(x_1, \ldots, x_m)$ is a completely arbitrary function. Moreover a systematic method allows to generate a large class of perfect nonlinear functions out of any existing one. However these constructions apply to even dimensions n only, whereas no perfect nonlinear functions exist in odd dimensions. It is furthermore known that the nonlinear order of bent functions is tightly bounded by n/2.

We show that perfect nonlinear functions are optimum with regard to the distances δ and σ. More precisely for an even number n of arguments the class $\pi(n)$ of perfect nonlinear functions simultaneously has maximum distance to all affine functions (Theorem 3.4) as well as maximum distance to linear structures (Theorem 3.2). These maximum values are shown to be $2^{n-1}-2^{(n/2)-1}$ for δ, and 2^{n-2} for σ. Furthermore, perfect nonlinear functions have equal, and in fact minimum correlation to all affine functions (Theorem 3.5). The maximum distance δ to affine functions is of independent interest in coding theory, where it appears to be the covering radius of the Reed-Muller code of order 1 (cf. [2]). In the same context the maximum value of δ_k coincides with the covering radius of the k-th order Reed-Muller code.

These results allow for applications in several directions. In odd dimensions functions can be generated with properties close to those of perfect nonlinear functions (Section 3.3). Thus in every dimension we arrive at constructing Boolean functions with large distances δ and σ, i.e. functions with guaranteed lower bounds on δ and σ. For large n (e.g. $n \approx 64$) an a priori verification of this property may be impossible since even the computation of Hamming distances between functions becomes infeasible.

Notably, our considerations have consequences for the design of block ciphers. Since perfect nonlinear functions are not exactly balanced the question as raised by Evertse can be answered: There are no DES-like S-boxes with maximum distance to linear structures (Corollary 3.6). A search for such S-boxes was motivated by the analysis of DES in [1] where linear structures of the S-boxes are considered.

The above example shows that in general perfect nonlinearity may not be compatible with other cryptographic design criteria, e.g. balance or highest nonlinear order. We indicate a method of finding functions which at the same time are nearly perfect nonlinear (i.e. with large δ and σ) and satisfy other criteria of cryptographic interest.

In particular this procedure is applied to propose functions which are useful in stream cipher design where one or more linear feedback shift registers are combined to produce the key stream. In this design there arise correlation problems, since any Boolean function f has correlation to some linear functions L. Such correlations are shown to lead to correlations to certain LFSR-sequences. For an individual L this correlation is reflected in a nonvanishing cross correlation coefficient c(f,L). The (normalized) correlations to all linear functions L are shown to satisfy

$$\sum_L c(f,L)^2 = 1,$$

which implies that correlations to linear functions do always exist whatever function f is used. However for perfect nonlinear functions the absolute values $|c(f,L)|$ turn out to be uniformly small. This motivates a general method to face the correlation problems in stream cipher design by choosing the combining functions to be (close to) a perfect nonlinear function (which in fact can be done in conjunction with other design criteria). By suitable design the remaining correlations may become as small as to defeat any kind of correlation attack.

This contrasts to the method of facing correlation by choosing correlation immune functions. A correlation immune function (of some order) has zero correlation to certain linear functions. However, as the above formula shows, the strongest correlations (to some other linear functions) are necessarily larger than for perfect (or nearly perfect) nonlinear functions.

2. NONLINEARITY CRITERIA FOR BOOLEAN FUNCTIONS

Cryptographic transformations are often described in terms of functions $GF(2)^n \longrightarrow GF(2)^m$. For small values of n and m these functions are usually given in form of tables. These tables can then be used as building blocks for generating functions in higher dimensions. As examples we mention the S-boxes $S: GF(2)^6 \longrightarrow GF(2)^4$ of DES, or the combining functions used in certain types of stream ciphers. The strength of the resulting algorithms heavily relies on the nonlinearity of these functions.

Most of the known nonlinearity criteria can be reduced to conditions imposed on Boolean functions $f: GF(2)^n \longrightarrow GF(2)$. This is illustrated by the notion of linear structures of S-boxes as introduced by Chaum and Evertse ([1],[3]): An S-box $S: GF(2)^n \longrightarrow GF(2)^m$ is said to have a linear structure if there is a nonzero vector $\underline{a} \in GF(2)^n$ together with a nontrivial linear mapping $L: GF(2)^m \longrightarrow GF(2)$ such that $LS(\underline{x}+\underline{a}) + LS(\underline{x})$ takes the same value (0 or 1) for all $\underline{x} \in GF(2)^n$. Thus linear structures of S can be expressed in terms of linear structures of the Boolean function LS. For this reason we concentrate hereafter on Boolean functions $f: GF(2)^n \longrightarrow GF(2)$. It is common to describe these functions in terms of their algebraic normal form

$$f(x_1,\ldots,x_n) = a_0 + \sum a_i x_i + \sum a_{ij} x_i x_j + \ldots + a_{12..n} x_1 x_2 \ldots x_n \qquad (2.1)$$

A function f is nonlinear (or non-affine) if its algebraic normal form contains terms of degree higher than one.

In this section we compare different criteria in view of their ability to measure nonlinearity of Boolean functions.

2.1. Distance to affine functions

The distance to the nearest affine function is defined as

$$\delta(f) = \min_{L \in A(n)} d(f,L) \qquad (2.2)$$

where $d(f,L)$ is the Hamming distance between f and L, and where the minimum is taken over the set $A(n)$ of all affine functions $L(x_1,\ldots,x_n) = a_0 + a_1 x_1 + \ldots + a_n x_n$. Thus $\delta(f)$ is the distance of f to the set $A(n)$. In order to investigate the properties of δ we introduce some additional notations.

Let $\Omega(n)$ denote the group of all invertible transformations of $GF(2)^n$, and let $AGL(n)$ denote the subgroup of all affine transformations. Recall that the elements of $AGL(n)$ can be described as functions $\alpha(\underline{x}) = A\underline{x} + \underline{a}$ where A is a regular $n \times n$ - matrix and $\underline{a} \in GF(2)^n$ is a vector. Moreover denote by $\Phi(n)$ the set of all Boolean functions $f: GF(2)^n \longrightarrow GF(2)$ of n arguments.

An operation of a group G on a set S means a mapping $G \times S \longrightarrow S$ which is compatible with group multiplication (cf. [5], Ch.I). For the image of a pair (g,s) ($g \in G$ and $s \in S$) the notation $g \cdot s$ is commonly used. In these terms an operation of the group $\Omega(n)$ on the set $\Phi(n)$ is defined by

$$\alpha \cdot f(\underline{x}) = f(\alpha(\underline{x})), \quad \text{where } f \in \Phi(n) \text{ and } \alpha \in \Omega(n) \tag{2.3}$$

With this notion, we can now make some of our considerations in more general and more precise terms. Any design criterion is connected with a function D (valuation)

$$D: \Phi(n) \longrightarrow W \tag{2.4}$$

with values in a suitable set W, and a function f is considered to be "good" if the value $D(f)$ belongs to some well defined subset W_1 of W. It may be essential for a design criterion that the valuation D remains invariant under those transformations of $\Omega(n)$ which are considered "cryptographically weak". This guarantees that a good function cannot be made "worse" by means of weak transformations. For nonlinearity, weak transformations usually include affine transformations. To illustrate our terminology, the number of terms in the algebraic normal form (as exemplified in the introduction) is not invariant even under simple transformations like complementations of variables.

For any design criterion it is therefore of interest to introduce the largest subgroup $I(D)$ of $\Omega(n)$ which leaves D invariant, i.e.

$$I(D) = \{\alpha \in \Omega(n) \mid D(\alpha \cdot f) = D(f) \text{ for all } f \in \Phi(n)\} \tag{2.5}$$

Hereafter $I(D)$ will be called the <u>symmetry group of D</u>. In cryptography it may be essential that $I(D)$ is large. We therefore investigate various design criteria in view of their symmetry groups.

First we show that the distance δ to the nearest affine function remains in fact invariant under the operation of the whole affine group $AGL(n)$ (cf. Corollary 2.2 below.) It appears worthwhile to prove this result in a more general context, which allows to analyze other design criteria with regard to their symmetry group.

Let H be a subset of $\Phi(n)$, and for $f \in \Phi(n)$ let $d_H(f) = d(f,H)$ be the distance of f to the set H. (In applications, this subset will be the class of cryptographically weak functions, and for δ it will be the set $A(n)$ of all affine functions.) Moreover let

$$\Omega(n)^H = \{\alpha \in \Omega(n) \mid \alpha \cdot h \in H \text{ for all } h \in H\} \tag{2.6}$$

which will be called the <u>symmetry group of the set H</u>. This terminology is justified by the following result.

Theorem 2.1. For any subset H of $\Phi(n)$ the symmetry group of d_H coincides with the symmetry group of H

$$I(d_H) = \Omega(n)^H. \tag{2.7}$$

Proof. (a) $\Omega(n)^H$ is contained in $I(d_H)$: Suppose $\alpha \in \Omega(n)^H$ and $f \in \Phi(n)$. Let $h \in H$ such $d_H(f) = d(f,h)$. Then $d_H(f) = d(f,h) = d(\alpha\cdot f,\alpha\cdot h) \geq d_H(\alpha\cdot f)$. Observe that the second equality is a consequence of the fact that the operation of $\Omega(n)$ on $\Phi(n)$ leaves the Hamming distance invariant. Moreover the last inequality holds as $\alpha\cdot h \in H$ by definition (2.6). Therefore

$$d_H(f) \geq d_H(\alpha\cdot f) \tag{2.8}$$

Since $\Omega(n)^H$ is a subgroup (2.8) may be applied with respect to the operation of α^{-1}. This yields $d_H(\alpha\cdot f) \geq d_H(\alpha^{-1}\cdot(\alpha\cdot f)) = d_H(f)$, and consequently $d_H(\alpha\cdot f) = d_H(f)$.

(b) $I(d_H)$ is contained in $\Omega(n)^H$: For any $\alpha \notin \Omega(n)^H$ there exists $h \in H$ such that $\alpha\cdot h$ is not in H. Hence $d_H(h) = 0$ but $d_H(\alpha\cdot h) \neq 0$. Therefore α is not in $I(d_H)$.

Corollary 2.2. The symmetry group $I(\delta)$ of δ is the affine group AGL(n).

Proof. With regard to Theorem 2.1. it remains to show that $\Omega(n)^{A(n)} = AGL(n)$. Obviously AGL(n) is contained in $\Omega(n)^{A(n)}$. In the other direction for any $\alpha \in \Omega(n) - AGL(n)$ there exists an index i such that the i-th component $\alpha_i(x_1,\ldots,x_n)$ of α is not affine. Then for $g(x_1,\ldots,x_n) = x_i$, the function $\alpha\cdot g(x_1,\ldots,x_n) = \alpha_i(x_1,\ldots,x_n)$ is not in A(n), which implies that α is not in $\Omega(n)^{A(n)}$.

2.2. Distance to linear structures

According to the preliminary remarks to this section a general linear structure can be formulated in terms of linear structures of appropriate Boolean functions. Recall that a linear structure of a Boolean function $f: GF(2)^n \longrightarrow GF(2)$ can be identified with a vector $\underline{a} \in GF(2)^n$ such that the expression

$$f(\underline{x} + \underline{a}) + f(\underline{x}) \tag{2.9}$$

takes the same value (0 or 1) for all $\underline{x} \in GF(2)^n$ ([1],[3]). Let LS(n) denote the subset of Boolean functions having linear structures. Observe that LS(n) properly contains the set A(n) of all affine functions.

For a Boolean function f the <u>distance to linear structures</u> is defined as the distance of f to the set LS(n):

$$\sigma(f) = d(f,LS(n)) = \min_{S \in LS(n)} d(f,S) \tag{2.10}$$

The distance to linear structures serves as a useful nonlinearity criterion as follows as a corollary to Theorem 2.1.

Corollary 2.3. The symmetry group $I(\sigma)$ of σ contains the affine group AGL(n).

Proof. In order to apply Theorem 2.1 we show that $\Omega(n)^{LS(n)}$ contains AGL(n). Let $f \in LS(n)$ and let $\underline{a} \in GF(2)^n$ be a linear structure of f, i.e. for all $\underline{x} \in GF(2)^n$ the equation $f(\underline{x}+\underline{a}) + f(\underline{x}) = c$ holds, where $c \in GF(2)$ is a constant. Then for $\alpha \in AGL(n)$

$$f(\alpha(\underline{x} + \alpha^{-1}(\underline{a}))) + f(\alpha(\underline{x})) = c \tag{2.11}$$

is satisfied for all $\underline{x} \in GF(2)^n$. This means that $\alpha^{-1}(\underline{a})$ is a linear structure of $\alpha\cdot f$. Hence $\alpha \in \Omega(n)^{LS(n)}$.

2.3. The nonlinear order

For a Boolean function $f \in \Phi(n)$ let $O(f)$ be the degree of the highest order terms in the algebraic normal form, which is called the nonlinear order of f. This defines another useful nonlinearity criterion O: $\Phi(n) \longrightarrow \{0,\ldots,n\}$ as is demonstrated by the following

Theorem 2.4. The symmetry group $I(O)$ of O is the affine group $AGL(n)$.

Proof. (a) $AGL(n)$ is contained in $I(O)$: Let $\alpha \in AGL(n)$ and $f \in \Phi(n)$ arbitrary. Compute the algebraic normal form of $\alpha \cdot f$ by formal reduction of $f(\alpha(\underline{x}))$. In this procedure existing nonlinear terms of $f(\underline{x})$ may disappear and new terms may be generated in $f(\alpha(\underline{x}))$. However terms of some degree k in $f(\underline{x})$ cannot create terms of degree higher than k in $f(\alpha(\underline{x}))$. This shows

$$O(\alpha \cdot f) \leq O(f) \tag{2.12}$$

Formula (2.12) may be applied also with respect to the operation of α^{-1}. Hence

$$O(f) = O(\alpha^{-1} \cdot (\alpha \cdot f)) \leq O(\alpha \cdot f)$$

and $O(\alpha \cdot f) = O(f)$. Therefore $\alpha \in I(O)$.

(b) $I(O)$ is contained in $AGL(n)$: Suppose that α is not contained in $AGL(n)$. Then α has a nonlinear component $\alpha_i(x_1,\ldots,x_n)$. With $f(x_1,\ldots,x_n) = x_i$ we have $\alpha \cdot f = \alpha_i$. Thus $O(\alpha \cdot f) > 1$ whereas $O(f) = 1$. Therefore α is not contained in $I(O)$.

Theorem 2.4 implies that other nonlinearity criteria, namely the distances δ_k to functions with nonlinear order bounded by k, also remain invariant under the operation of $AGL(n)$.

2.4. Correlation immunity

Refer to the notion of correlation immunity as introduced by Siegenthaler ([9]). It is known that correlation immunity is not a genuine nonlinearity criterion. Indeed the consideration of its symmetry group further illuminates this fact. In view of a later comparison to other design criteria, the study of correlation immunity in the context of symmetry groups is of independent interest. We start by defining a valuation $c: \Phi(n) \longrightarrow \{0,1, \ldots ,n-1\}$ by assigning to every function $f \in \Phi(n)$ its order $c(f)$ of correlation immunity.

Theorem 2.5. The symmetry group $I(c)$ is the group of permutations and complementations of variables, i.e. the group $P(n) = \{\alpha=(A,\underline{a}) \in AGL(n)$ where A is a permutation matrix$\}$.

Proof. First we show that $I(c)$ is contained in $AGL(n)$. Suppose that α is not contained in $AGL(n)$, and let $\alpha(\underline{x}) = (\alpha_1(\underline{x}),\ldots,\alpha_n(\underline{x}))$. For this we claim that there exists a sum of at least n-1 α_i's which is not linear. Suppose to the contrary that all the sums

$$\beta_0 = \alpha_1 + \alpha_2 + \ldots + \alpha_n \qquad \text{and} \qquad \beta_i = \sum_{j \neq i} \alpha_j$$

are linear. Then $\alpha_i = \beta_0 + \beta_i$ is linear for all i, in contradiction to the nonlinearity of α.

In case β_0 is nonlinear take $f(\underline{x}) = x_1 + x_2 + \ldots + x_n$, and in case β_i is nonlinear for some $i > 0$ take $f(\underline{x}) = \sum_{j \neq i} x_j$. Then $\alpha \cdot f = \beta_i$ has nonlinear order at least 2.

Moreover $\alpha \cdot f$ is balanced as α is a permutation of $GF(2)^n$. Therefore by a result of Siegenthaler ([9]), $c(\alpha \cdot f) < n-2$ whereas $c(f) \geq n-2$. Hence α is not contained in $I(c)$.

In a second step we show that $I(c)$ is contained in $P(n)$. Suppose $\alpha \in AGL(n)$ is not contained in $P(n)$. Then there exists a component $\alpha_i(\underline{x}) = b_0 + b_1x_1 + \ldots + b_nx_n$ with weight$(b_1,\ldots,b_n) = t > 1$. Take $f(\underline{x}) = x_i$. Then $c(\alpha \cdot f) = t-1 > 0$ and $c(f) = 0$. Therefore α is not contained in $I(c)$. Alltogether this shows that $I(c)$ is contained in $P(n)$. Since obviously $P(n)$ is contained in $I(c)$, this completes the proof of the theorem.

3. PERFECT NONLINEAR FUNCTIONS

In this section we investigate a class of functions whose definition is motivated by considering linear structures. With respect to linear structures (cf. (2.9)) a Boolean function f has optimum nonlinearity if $f(\underline{x}+\underline{a})$ coincides with $f(\underline{x})$ for exactly half of the arguments $\underline{x}$:

Definition 3.1. A Boolean function $f: GF(2)^n \longrightarrow GF(2)$ is called perfect nonlinear with respect to linear structures (or briefly perfect nonlinear) if for every nonzero vector $\underline{a} \in GF(2)^n$ the values $f(\underline{x}+\underline{a})$ and $f(\underline{x})$ are equal for exactly half of the arguments $\underline{x} \in GF(2)^n$.

The subset of $\Phi(n)$ consisting of the perfect nonlinear functions will be denoted by $\pi(n)$. We first show that these functions are optimum with respect to the distance σ to linear structures.

For an arbitrary function $f: GF(2)^n \longrightarrow GF(2)$ the distance to linear structures can be computed as follows. Let $\underline{a} \in GF(2)^n$ be a nonzero vector. Then the space $GF(2)^n$ can be exhausted by 2^{n-1} pairs $(\underline{x},\underline{x}+\underline{a})$. Denote by n_0 the number of elements in the set W_0 of pairs $(\underline{x},\underline{x}+\underline{a})$ for which $f(\underline{x})$ coincides with $f(\underline{x}+\underline{a})$. Similarly let n_1 be the number of elements in the set W_1 of pairs $(\underline{x},\underline{x}+\underline{a})$ for which $f(\underline{x})$ differs from $f(\underline{x}+\underline{a})$.

Furthermore any Boolean function can be derived from f by modifying an appropriate set of f-values. In this way f can be turned into a function with the linear structure $\underline{a}$ by changing the f-values of either $\underline{x}$ or $\underline{x}+\underline{a}$ for pairs in W_0, or by changing the f-values of either $\underline{x}$ or $\underline{x}+\underline{a}$ for the pairs in W_1. Thus n_0 values are to be changed to get a function g with the linear structure $(g(\underline{x}) \neq g(\underline{x}+\underline{a})$ for all $\underline{x})$, and n_1 values are to be changed to get a function g with the linear structure $(g(\underline{x}) = g(\underline{x}+\underline{a})$ for all $\underline{x})$. In order to generate any other function with these linear structures at least $\min(n_0,n_1)$ modifications are necessary. Therefore $n = \min(n_0,n_1)$ is the distance of f to the nearest functions with the linear structure $\underline{a}$. Observe that this n depends on the vector $\underline{a}$, i.e. $n = n_f(\underline{a}) = \min(n_0(\underline{a}),n_1(\underline{a}))$. Hence the distance of f to linear structures is given by

$$\sigma(f) = \min_{\underline{a} \neq 0} n_f(\underline{a}) \tag{3.1}$$

Since $n_0(\underline{a}) + n_1(\underline{a}) = 2^{n-1}$ the derivation of formula (3.1) also proves that $n_f(\underline{a}) \leq 2^{n-2}$ for all $\underline{a} \neq 0$. This maximum distance is achieved by perfect nonlinear functions, as these functions are characterized by $n_0(\underline{a}) = n_1(\underline{a}) = 2^{n-2}$ for $\underline{a} \neq 0$, or equivalently by the property $\sigma(f) = 2^{n-2}$. This proves

Theorem 3.2. The class $\pi(n)$ of perfect nonlinear functions is the class of functions with maximum distance 2^{n-2} to linear structures.

3.1. Bent functions

We now establish a relationship between perfect nonlinear functions and the 'bent' functions which were introduced by Rothaus ([6]). The relation is expressed in terms of the Walsh transform.

Hereafter, in connection with Walsh transforms, all Boolean functions are considered with values +1 and -1 (i.e. $f(\underline{x})$ is replaced by $(-1)^{f(\underline{x})}$). Recall the definition of the Walsh transform

$$F(\underline{w}) = \sum_{\underline{x} \in GF(2)^n} f(\underline{x})(-1)^{\underline{x}\cdot\underline{w}} \tag{3.2}$$

where $\underline{w} \in GF(2)^n$ and $\underline{x}\cdot\underline{w}$ is the dot-product over GF(2), and where the sum is evaluated over the reals.

For a Boolean function $f: GF(2)^n \longrightarrow \{+1,-1\}$ the condition of Definition 3.1. for given $\underline{a}$ reads as

$$\sum_{\underline{x} \in GF(2)^n} f(\underline{x})f(\underline{x}+\underline{a}) = 0 \tag{3.3}$$

The sum (3.3) equals $f*f(\underline{a})$ where f*f denotes the convolution of f with itself. Thus a ±1-valued function f is perfect nonlinear if and only if $f*f(\underline{a}) = 0$ for every nonzero vector $\underline{a} \in GF(2)^n$, i.e. if and only if f*f is a δ-function. By the convolution theorem the function f*f transforms into F^2, and a δ-function transforms into a constant. Therefore a ±1-valued Boolean function f is perfect nonlinear if and only if $|F(\underline{w})|$ is constant for all $\underline{w}$. Since $f*f(\underline{0}) = 2^n$, this constant is

$$|F(\underline{w})| = 2^{n/2} \tag{3.4}$$

This property has been used by Rothaus to define the bent functions, which implies

Theorem 3.3. The class of perfect nonlinear functions coincides with the class of bent functions.

The following theorems A and B are the main results proved in [6] about bent functions.

Theorem A. Bent functions only exist for even numbers n of arguments, and their nonlinear order is always bounded by n/2.

Theorem B. For an even number n of arguments bent functions are constructed as follows.

(B1) Let $n = 2m$. Then the functions of the form $f(x_1,\ldots,x_n) = g(x_1,\ldots,x_m) + x_1x_{m+1} + x_2x_{m+2} + \ldots + x_mx_n$ are bent, where $g(x_1,\ldots,x_m)$ is a completely arbitrary function of m variables.

(B2) Let $\underline{x} = (x_1,\ldots,x_n)$ and let $a(\underline{x})$, $b(\underline{x})$ and $c(\underline{x})$ be bent functions such $a(\underline{x}) + b(\underline{x}) + c(\underline{x})$ is also bent. Then the function $f(\underline{x},x_{n+1},x_{n+2}) = a(\underline{x})b(\underline{x}) + b(\underline{x})c(\underline{x}) + c(\underline{x})a(\underline{x}) + [a(\underline{x})+b(\underline{x})]x_{n+1} + [a(\underline{x})+c(\underline{x})]x_{n+2} + x_{n+1}x_{n+2}$ is a bent function. The requirement that $a(\underline{x})+b(\underline{x})+c(\underline{x})$ is bent is readily met by taking $a(\underline{x})$, $b(\underline{x})$ and $c(\underline{x})$ from class B1, or by putting $a(\underline{x}) = b(\underline{x})$ or $b(\underline{x}) = c(\underline{x})$.

(B1) leads to an explicit construction of bent functions, whereas (B2) allows to generate new perfect nonlinear or bent functions out of any existing ones. This procedure can be combined with linear operations on given perfect nonlinear functions. In fact formula (2.11) implies that the class $\pi(n)$ of perfect nonlinear functions is in-

variant under the operation of the affine group AGL(n). Moreover addition of an arbitrary affine function does not affect perfect nonlinearity. Therefore assigning to $f \in \Phi(n)$ the function $\underline{x} \longrightarrow f(\alpha(\underline{x})) + L(\underline{x})$ defines an operation of AGL(n) x A(n) on $\Phi(n)$ which leaves $\pi(n)$ invariant. This leads to the following recursive construction of perfect nonlinear functions.

I. For n = 2 take the class C(2) consisting of all functions of nonlinear order 2.

II. For n > 2 take any functions a,b,c in C(n-2) such that their sum is also in C(n-2), and apply construction (B2). This defines a class C'(n) of perfect nonlinear functions. This class C'(n) is enlarged to a class C(n) by letting operate the whole group G = AGL(n) x A(n) on C'(n).

It can be shown that C(n) includes the functions obtained in (B1). It is not clear whether the class C(n) exhausts all functions in $\pi(n)$. But (B1) implies that there are at least $2^{2^{n/2}}$ perfect nonlinear functions among all 2^{2^n} Boolean functions. Thus only a very small fraction of all Boolean functions are perfect nonlinear. Already for n = 6 (i.e. in the input dimension of the DES S-boxes) it is virtually impossible to find perfect nonlinear functions by a pure random search.

3.2. Distance to affine functions and correlation

Let $L_w(\underline{x}) = \underline{w}\cdot\underline{x}$ denote an arbitrary linear function. Thus $(-1)^{\underline{w}\cdot\underline{x}}$ is the corresponding ±1-valued function which is also denoted by $L_w(\underline{x})$. Then the definition (3.2) of the Walsh transform implies

$$F(\underline{w}) = \#\{\underline{x} \mid f(\underline{x})=L_w(\underline{x})\} - \#\{\underline{x} \mid f(\underline{x})\neq L_w(\underline{x})\} = 2^n - 2d(f,L_w)$$

where d denotes the Hamming distance. Therefore

$$d(f,L_w) = 2^{n-1} - \frac{1}{2} F(\underline{w}) \tag{3.5}$$

For the corresponding affine function $L_w' = 1 + L_w$ the distance d is computed as $d(f,L_w') = 2^{n-1} + (1/2)F(\underline{w})$. Formula (3.5) can be used to find the best affine approximation to a given function by finding $\underline{w}$ such that $|F(\underline{w})|$ is maximum (cf. also Rueppel ([7], p. 122)), i.e.

$$\delta(f) = 2^{n-1} - \frac{1}{2} \max_{w} |F(\underline{w})| \tag{3.6}$$

Thus by property (3.4) the perfect nonlinear functions always have distance

$$\delta(f) = 2^{n-1} - 2^{n/2-1} \tag{3.7}$$

to the nearest affine functions. Suppose now that f is not perfect nonlinear. Then by Parseval's theorem

$$\sum_{w} F(\underline{w})^2 = 2^n \sum_{x} f(\underline{x})^2 = 2^{2n} \tag{3.8}$$

there exists a $\underline{w}$ with $|F(\underline{w})| > 2^{n/2}$. This implies $\delta(f) < 2^{n-1} - 2^{n/2-1}$ and therefore f is closer to the set of all affine functions than are perfect nonlinear functions.

This shows that the perfect nonlinear functions are not only optimum with respect to the distance to linear structures but also with respect to the distance to all affine functions.

Theorem 3.4. The class $\pi(n)$ of perfect nonlinear functions is the class of functions with maximum distance $2^{n-1} - 2^{(n/2)-1}$ to affine functions.

As formula (3.5) shows this result can be refined to the statement that the distance of a perfect nonlinear function f to any affine function is either $2^{n-1} + 2^{n/2-1}$ or $2^{n-1} - 2^{n/2-1}$. This fact can be expressed in terms of correlations of f to affine functions. In general the Hamming distance between two Boolean functions $f,g: GF(2)^n \longrightarrow \{+1,-1\}$ is tied up with the cross correlation between f and g which is defined as

$$c(f,g) = \frac{\#\{\underline{x} \mid f(\underline{x}) = g(\underline{x})\} - \#\{\underline{x} \mid f(\underline{x}) \neq g(\underline{x})\}}{2^n}$$

For $g = L_w$ we have by definition of the Walsh transform (see also (3.5))

$$c(f,L_w) = \frac{F(\underline{w})}{2^n} \tag{3.9}$$

Therefore the absolute value of the cross correlation between a perfect nonlinear function and any affine function is a constant equal to $2^{-n/2}$. Moreover for a function g which is not perfect nonlinear there is always an affine function L with cross correlation c(g,L) larger than $2^{-n/2}$ in absolute value. This is summarized in the following

Theorem 3.5. The perfect nonlinear functions are the class of functions with minimum correlation to all affine functions.

This property contrasts to correlation immunity. Recall that a *m-th order correlation immune* function f satisfies $F(\underline{w}) = 0$ for all $\underline{w}$ with Hamming weight less or equal m (cf. [12]). Hence for these vectors $\underline{w}$ the cross correlation $c(f,L_w)$ vanishes. On the other hand Parseval's theorem implies

$$\sum_{w \in GF(2)^n} c(f,L_w)^2 = 1 \tag{3.10}$$

for an arbitrary Boolean function f, which means that the "global correlation" to all linear (or affine) functions does not depend on the function f. Thus for correlation immune functions the vanishing of certain cross correlations necessarily leads to larger correlations to other affine functions.

The cross correlation c(f,0) to the all zero function measures the deviation from ±1-balance of a Boolean function f. Therefore a perfect nonlinear function is never balanced. However its deviation from balance is given by $2^{-n/2}$ which rapidly tends to 0 as n grows larger. The same holds for the correlation to any other affine function. The fact that there exist no balanced perfect nonlinear functions answers a question raised by Evertse (cf. [3]).

Corollary 3.6. *There are no DES-like S-boxes which are perfect nonlinear, or equivalently, S-boxes with maximum distance to linear structures.*

3.3. Boolean functions with an odd number of arguments

Recall that there are no perfect nonlinear functions with an odd number of arguments. This relies on the fact that the absolute value of the Walsh transform of a perfect nonlinear function has to be constant (cf. formula (3.4)). However for odd dimensions we can construct functions with the property that the absolute value of their Walsh transform is two-valued. Such functions may be obtained by the following construction.

For $f \in \Phi(n)$, n odd, denote by f_0 the lower half of f, i.e. the function $f_0 \in \Phi(n-1)$ defined by $f_0(x_1, \ldots, x_{n-1}) = f(0,x_1,\ldots,x_{n-1})$, and by $f_1 \in \Phi(n-1)$ the upper half, $f_1(x_1, \ldots, x_{n-1}) = f(1,x_1,\ldots,x_{n-1})$. Similarly denote by F_0 and F_1 the lower and upper half of the Walsh transform F. Moreover let F_0' and F_1' be the Walsh transforms of f_0 and f_1, respectively. Then definition (3.2) implies

$$\begin{aligned} F_0 &= F_0' + F_1' \\ F_1 &= F_0' - F_1' \end{aligned} \tag{3.11}$$

Suppose now that f_0 and f_1 are perfect nonlinear. Then the values of F_0' and F_1' are $\pm 2^{(n-1)/2}$, which implies that the values of F_0 and F_1 are either 0 or $\pm 2^{(n+1)/2}$. Thus for any pair of perfect nonlinear functions $f_0, f_1 \in \pi(n-1)$ we can construct a function $f \in \Phi(n)$ such that the function $|F|$ takes two values (0 or $2^{(n+1)/2}$). More precisely, by Parseval's theorem (cf. (3.8)), half of the values of $|F|$ are 0 and the other half $2^{(n+1)/2}$.

For n odd denote by $\pi'(n)$ the class of all functions f such that $|F|$ takes the 2 values 0 and $2^{(n+1)/2}$. These classes π' of functions in odd dimensions are related to the classes π in even dimensions. This is reflected by similar properties of the two classes with regard to nonlinear order and distance to affine functions. In analogy to Theorem A it can be shown that the nonlinear order of a function $f \in \pi'(n)$ is always bounded by (n+1)/2. Moreover the distance of a function $f \in \pi'(n)$ to affine functions is obtained as

$$\delta(f) = 2^{n-1} - 2^{(n+1)/2-1}. \tag{3.12}$$

This shows that in odd dimensions the elements of $\pi'(n)$ are nearly as far from affine functions as are the perfect nonlinear functions in even dimensions. Note however that it is possible to generate functions f in odd dimensions with larger distance $\delta(f)$. In general the maximum value of δ coincides with the covering radius of the Reed-Muller code R(1,n). This covering radius is unknown if n is an arbitrary odd number (cf. [2]).

4. CONCLUSIONS AND APPLICATIONS

The theory of perfect nonlinear (or bent) functions has interesting implications to the design of block ciphers as well as stream ciphers. We have already observed (cf. Corollary 3.6) that perfect nonlinearity may not be compatible with other cryptographic design criteria. For example perfect nonlinearity cannot be achieved in conjunction with balance or highest nonlinear order. However a reasonable strategy will be to find nearly perfect nonlinear functions which satisfy additional design criteria. This is illustrated by the following example of finding nearly perfect nonlinear functions which are balanced.

Recall that a function $f \in \pi(n)$ has distance $2^{n-1} \pm 2^{n/2-1}$ to each affine function. Suppose e.g. that f has distance $2^{n-1} + 2^{n/2-1}$ to the all zero function. Then com-

plementing an arbitrary set of $2^{n/2-1}$ f-values 1 yields a balanced function f'. With regard to distance to affine functions this modified function f' still has desirable properties, since the triangle inequality implies

$$\delta(f') \geq 2^{n-1} - 2^{n/2}. \tag{4.1}$$

To illustrate this procedure take n = 8. In this case it is easy to generate balanced functions with distance δ at least 112 (compared to 120 for perfect nonlinear functions). Instead one could randomly try balanced functions until a function with $\delta = 112$ has been found. However it has appeared (cf. Section 3) that perfect (or nearly perfect) nonlinear functions are very rare in the set of all Boolean functions. Therefore an exhaustive search in the set of balanced functions has virtually zero probability to succeed in reasonable time.

A similar method can be applied to other design criteria, e.g. nonlinear order or correlation immunity. This leads to the following general procedure, where we use a systematic approach to satisfy first those properties which cannot be achieved by a pure random search.

1. Generate a random perfect nonlinear function f using the recursive algorithm as described in Section 3.
2. Find a random function f' as close as possible to f which satisfies all the other desired criteria.

In this way we can construct functions which are useful in stream cipher design where one or more linear feedback shift registers (LFSRs) are combined to produce the key stream.

We start by considering the case where n different taps of one LFSR are nonlinearly combined by some Boolean function $f \in \Phi(n)$ (a situation which was originally treated in [10]). Denote by $\underline{a}_1, \underline{a}_2, \ldots, \underline{a}_n$ the output sequences of these taps. Now suppose that f is correlated to the linear function L_w, $\underline{w} \in GF(2)^n$. Then the generator output sequence is correlated to the sum

$$\underline{x} = w_1\underline{a}_1 + w_2\underline{a}_2 + \ldots + w_n\underline{a}_n \tag{4.2}$$

which is a sequence (another phase) produced by the same LFSR. The corresponding cross correlation is obtained by (3.9)

$$c_f(\underline{w}) = \frac{F(\underline{w})}{2^n}$$

In this situation the use of correlation immune functions (of any order) is not adequate. To the contrary, correlation immunity of functions is equivalent to the vanishing of certain Walsh coefficients (or cross correlations to certain phases). But in this case Parseval's equality (cf. also (3.10))

$$\sum_{w \in GF(2)^n} c_f(\underline{w})^2 = 1$$

implies that cross correlations to other phases are necessarily larger. In this context it is best to face the correlation problem by choosing f as close as possible to a perfect nonlinear function (where all cross correlations are minimum). This treatment also applies to the situation where taps of different LFSR's are combined.

Suppose that a Boolean function $f \in \Phi(n)$ combines a total number of n taps from k different LFSRs. Again, correlation will occur to sequences of the form (4.2) which is caused by correlation of f to the corresponding linear functions L_w. In this more general setting the sequence (4.2) can be expressed as

$$\underline{x} = \underline{b}_1 + \underline{b}_2 + \ldots + \underline{b}_k \qquad (4.3)$$

by collecting terms coming from the same LFSR (i.e. $\underline{b}_i = \Sigma\, w_j \underline{a}_j$, summed over the set S_i of all indices j corresponding to tap positions belonging to LFSR i). It may happen that some of the $\underline{b}_i$'s in (4.3) are zero, in which case the generator is vulnerable to a divide and conquer attack by exploiting the correlation. Otherwise stated, if all summands $\underline{b}_i$ are nonzero, a divide and conquer correlation attack is not possible. To this aim maximum order correlation immunity has been postulated in [7]. In our terminology the generator is maximum order correlation immune if the combining function f satisfies the following condition MCI (expressed in terms of the Walsh transform):

$$\text{MCI:} \quad \left[\begin{array}{l}\text{For every } \underline{w} \\ \text{with } F(\underline{w}) \neq 0\end{array}\right] \Longrightarrow \left[\begin{array}{l}\text{For every } i,\ 1 \le i \le k, \text{ there is at least} \\ \text{one index } \ j \in S_i \ \text{ such that } w_j = 1.\end{array}\right]$$

In fact MCI is equivalent to the condition that all $\underline{b}_i$'s in (4.3) are nonzero.

In addition to MCI the combining function f may be designed such that the remaining correlations are uniformly small. This can be achieved e.g. by choosing f close to a perfect nonlinear function. By appropriate design these correlations may become as small as to defeat any kind of correlation attack.

Acknowledgement.

We wish to thank Bert den Boer for helpful discussions.

References

[1] D. Chaum, J.-H. Evertse, "Cryptanalysis of DES with a reduced number of rounds", Proceedings of Crypto'85, pp. 192-211.

[2] G.D. Cohen, M.G. Karpovsky, H.F. Mattson, J.R. Schatz, "Covering radius - Survey and recent results", IEEE Trans. Inform. Theory, Vol. IT-31, pp. 328-343, 1985.

[3] J.-H. Evertse, "Linear structures in block ciphers", Proceedings of Eurocrypt'87, pp. 249-266.

[4] R. Forré, "The strict avalanche criterion: Spectral properties of Boolean functions and an extended definition", Proceedings of Crypto'88.

[5] S. Lang, "Algebra", Addison-Wesley Publishing Company, 1971.

[6] O.S. Rothaus, "On bent functions", Journal of Combinatorial Theory (A), Vol. 20, pp. 300-305, 1976.

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

[8] C.E. Shannon, "Communications theory of secrecy systems", Bell Sys. Tech. Journal, Vol. 28, pp. 656-715, 1949.

[9] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications", IEEE Trans. Inform. Theory, Vol. IT-30, pp. 776-780, 1984.

[10] T. Siegenthaler, "Cryptanalysts representation of nonlinearly filtered ML-sequences", Proceedings of Eurocrypt'85, pp. 103-110.

[11] A.F. Webster, S.E. Tavares, "On the design of S-boxes", Proceedings of Crypto'85, pp. 523-534.

[12] G.Z. Xiao, J.L. Massey, "A spectral characterization of correlation-immune combining functions", IEEE Trans. Inform. Theory, Vol IT-34, pp. 569-571, 1988.