Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions

Anne Canteaut[1], Claude Carlet[2], Pascale Charpin[1], and Caroline Fontaine[3]

[1] INRIA projet CODES
B.P. 105
78153 Le Chesnay Cedex - France.
{Anne.Canteaut,Pascale.Charpin}@inria.fr
[2] GREYC, Université de Caen
14032 Caen Cedex - France.
Claude.Carlet@info.unicaen.fr
[3] LIFL, Université des Sciences et Technologies de Lille
59655 Villeneuve d'Ascq Cedex - France.
Caroline.Fontaine@lifl.fr

Abstract. We investigate the link between the nonlinearity of a Boolean function and its propagation characteristics. We prove that highly nonlinear functions usually have good propagation properties regarding different criteria. Conversely, any Boolean function satisfying the propagation criterion with respect to a linear subspace of codimension 1 or 2 has a high nonlinearity. We also point out that most highly nonlinear functions with a three-valued Walsh spectrum can be transformed into 1-resilient functions.

1 Introduction

The design of conventional cryptographic systems relies on two fundamental principles introduced by Shannon [25]: confusion and diffusion. Confusion aims at concealing any algebraic structure in the system. Diffusion consists in spreading out the influence of a minor modification of the input data over all outputs. Most conventional primitives are concerned with these essential principles: secret-key ciphers (block ciphers and stream ciphers) as well as hash functions. Confusion and diffusion can be quantified by some properties of the Boolean functions describing the system. Confusion corresponds to the nonlinearity of the involved functions, *i.e.*, to their Hamming distances to the set of affine functions. Diffusion is related to the propagation characteristics of the considered Boolean function f: these properties describe the behaviors of the derivatives $x \mapsto f(x+a)+f(x)$. The relevant cryptographic quantities are the biases of the output probability distributions of the derivatives relatively to the uniform distribution; they are measured by the auto-correlation coefficients of the function. Diffusion is therefore estimated by complementary indicators: propagation

criterion, distance to the set of all Boolean functions with a linear structure and sum-of-squares indicator. All these quantities will be here considered in a unified approach.

A major link between diffusion and confusion criteria was pointed out by Meier and Staffelbach [18]. They proved that maximal nonlinearity and perfect propagation characteristics are equivalent requirements for Boolean functions with an even number of variables. Unfortunately those functions which achieve perfect diffusion and perfect confusion (called bent functions) are not balanced; that means that they do not have a uniform output distribution. The construction of balanced Boolean functions having a high nonlinearity and good propagation characteristics then remains an open problem although such functions are essential components of cryptographic primitives.

In this paper we further investigate the link between diffusion and confusion criteria for Boolean functions. We show that highly nonlinear functions usually coincide with the functions having remarkable propagation characteristics. In this context, we point out the major role played by the highly nonlinear functions whose Walsh spectrum takes three values. We exhibit general constructions of such functions and we prove that they can easily be transformed into balanced first-order correlation-immune functions. They are therefore well-suited combining functions for pseudo-random generators since they ensure a high resistance to fast correlation attacks.

2 Cryptographic criteria for Boolean functions

A Boolean function with n variables is a function from the set of n-bit vectors, $\mathbf{F}_2^n$, into $\mathbf{F}_2$. Such a function f can be expressed as a unique polynomial in $x_1, \ldots, x_n$ called its *algebraic normal form* (see e.g. [14]). Some cryptographic applications require that this polynomial has a high degree. For instance, when f is used as a combining function in a pseudo-random generator, its degree conditions the linear complexity of the produced running-key. The following notation will be intensively used in the paper. The usual dot product between two vectors x and y is denoted by $x \cdot y$. For any $\alpha \in \mathbf{F}_2^n$, ϕ_α is the linear function with n variables defined by $\phi_\alpha(x_1, \ldots, x_n) = \alpha \cdot x = \sum_{i=1}^{n} \alpha_i x_i$. The *Walsh transform* of a Boolean function f refers to the Fourier transform of the corresponding sign function $x \mapsto (-1)^{f(x)}$. In this context we denote by $\mathcal{F}(f)$ the value in 0 of the Walsh transform of f:

$$\mathcal{F}(f) = \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)} = 2^n - 2wt(f)$$

where $wt(f)$ is the Hamming weight of f, *i.e.*, the number of $x \in \mathbf{F}_2^n$ such that $f(x) = 1$.

The *Walsh spectrum* of a Boolean function f with n variables therefore consists of all values $\{\mathcal{F}(f + \phi_\alpha), \alpha \in \mathbf{F}_2^n\}$. Since linear attacks on blocks ciphers and correlation attacks on stream ciphers equally search for a linear or an affine approximation of the involved function, the signs of the Walsh coefficients have

no cryptographic relevance. We then often consider the set $\{\mathcal{F}(f+\phi_\alpha+\varepsilon), \alpha \in \mathbf{F}_2^n, \varepsilon \in \mathbf{F}_2\}$. The values of this spectrum, called the *extended Walsh spectrum*, are symmetric with respect to 0 since $\mathcal{F}(f+\phi_\alpha+1) = -\mathcal{F}(f+\phi_\alpha)$.

We now recall the main cryptographic criteria for Boolean functions and we express all of them in terms of Walsh spectrum. A first obvious requirement in most applications is that the output of the used Boolean function be uniformly distributed. This corresponds to *balancedness*:

Definition 1. *A Boolean function f is balanced if $\mathcal{F}(f) = 0$.*

A second usual criterion is that f should be far from all affine functions (regarding Hamming distance). In stream ciphers applications, when f is used in a pseudo-random generator as a combining function or as a filtering function, the existence of a "good" approximation of f by an affine function makes fast correlation attacks feasible [17, 13, 12]. Similarly, if f is used in a block cipher as an S-box component, this would lead to successful linear attacks [15].

Definition 2. *The* nonlinearity *of a Boolean function f with n variables is its Hamming distance to the set of affine functions. It can be expressed as*

$$\mathcal{NL}(f) = 2^{n-1} - \frac{1}{2}\mathcal{L}(f) \text{ where } \mathcal{L}(f) = \max_{\alpha \in \mathbf{F}_2^n} |\mathcal{F}(f+\phi_\alpha)| \ .$$

Any Boolean function f with n variables satisfies $\mathcal{L}(f) \geq 2^{n/2}$; the functions for which equality holds are called *bent functions* [23]. This lower bound can only be achieved for even values of n. When n is odd, the lowest achievable value of $\mathcal{L}(f)$ is unknown in the general case: there always exist some functions with $\mathcal{L}(f) = 2^{(n+1)/2}$ and this value corresponds to the minimum possible nonlinearity for any $n \leq 7$. On the other hand some functions with $\mathcal{L}(f) = \frac{27}{32}2^{(n+1)/2}$ are known for any odd $n \geq 15$ [20, 21]. From now on, we will focus on highly nonlinear Boolean functions in the following sense:

Definition 3. *Let f be a Boolean function with n variables. Then f is said to be* almost optimal *if $\mathcal{L}(f) \leq 2^{(n+1)/2}$ when n is odd, and $\mathcal{L}(f) \leq 2^{(n+2)/2}$ when n is even.*

Besides its maximum value, the whole Walsh spectrum of a Boolean function has a great cryptographic significance. When f is used in a combining pseudo-random generator, the distribution probability of its output should be unaltered when any t of its inputs are fixed [27]. This property, called *t-th order correlation-immunity* [26], is characterized by the set of zero values in the Walsh spectrum [29]:

Definition 4. *Let f be a Boolean function with n variables.*

- *f is* correlation-immune with respect to a subset *E of $\mathbf{F}_2^n$ if $\mathcal{F}(f+\phi_\alpha) = 0$ for all $\alpha \in E$.*
- *f is* t-th order correlation-immune (t-CI) *if it is correlation-immune with respect to $\{x \in \mathbf{F}_2^n, 1 \leq wt(x) \leq t\}$, where $wt(x)$ denotes the Hamming weight of the n-bit vector x,* i.e.*, the number of its nonzero components.*

Balanced t-th order correlation-immune functions are called t-resilient *functions.*

These criteria may not be compatible in general: there are necessary tradeoffs between the degree, the nonlinearity and the correlation-immunity order of a function.

Some other criteria consider the probability distribution of the output difference of the Boolean function for a fixed input difference. They then focus on the properties of the functions $D_a f : x \mapsto f(x+a) + f(x)$ for $a \in \mathbf{F}_2^n$. The function $D_a f$ is called the *derivative of f with respect to direction a.* The *auto-correlation function of f* refers to the function $\alpha \mapsto \mathcal{F}(D_\alpha f)$. The auto-correlation coefficient $\mathcal{F}(D_\alpha f)$ then measures the statistical bias of the output distribution of $D_\alpha f$ relatively to the uniform distribution. The propagation characteristics of a Boolean function can then be estimated by several indicators. Some applications require that the output difference of a function be uniformly distributed for low-weight input differences. This property, referred as *propagation criterion* [22], is notably important when the function is used in a hash function or in a block cipher.

Definition 5. *Let f be a Boolean function with n variables.*

- *f satisfies the* propagation criterion with respect to a subset E *of* $\mathbf{F}_2^n$ *if* $\mathcal{F}(D_\alpha f) = 0$ *for all* $\alpha \in E$.
- *f satisfies the* propagation criterion of degree k (PC(k)) *if it satisfies the propagation criterion with respect to* $\{x \in \mathbf{F}_2^n, 1 \leq wt(x) \leq k\}$.

The strict avalanche criterion (SAC) [28] actually corresponds to the propagation criterion of degree 1. It is also recommended that the output distribution of all derivatives be close to the uniform distribution: the existence of a derivative whose output takes a constant value with a high probability leads to differential attacks [3, 2]. This means that $|\mathcal{F}(D_\alpha f)|$ should be small for all nonzero $\alpha \in \mathbf{F}_2^n$. Recall that the *linear space* of f is the subspace of those α such that $D_\alpha f$ is a constant function. Such $\alpha \neq 0$ is said to be a *linear structure* for f. The maximum value $|\mathcal{F}(D_\alpha f)|$ over all nonzero α, called the *absolute indicator* [30], then quantifies the distance of f to the set of all Boolean functions with a linear structure [18]. The only functions whose absolute indicator equals 0 are the bent functions.

The output distributions of the derivatives can also be studied in average through the second moment of the auto-correlation coefficients, called the *sum-of-squares indicator* [30]:

Definition 6. *The* sum-of-squares indicator *of a Boolean function f with n variables, denoted by $\mathcal{V}(f)$, is defined by*

$$\mathcal{V}(f) = \sum_{\alpha \in \mathbf{F}_2^n} \mathcal{F}^2(D_\alpha f) \ .$$

The above presented criteria are invariant under certain transformations.

Proposition 1. *The degree, the extended Walsh spectrum (and the nonlinearity), the absolute indicator and the sum-of-squares indicator are invariant under addition of an affine function.*

The invariance of the propagation characteristics is derived from $\mathcal{F}(D_\alpha(f + \phi_\beta)) = (-1)^{\alpha\cdot\beta}\mathcal{F}(D_\alpha f)$ for any α and β in $\mathbf{F}_2^n$. Most notably, this proposition implies that if there exists $\alpha \in \mathbf{F}_2^n$ such that $\mathcal{F}(f + \phi_\alpha) = 0$, then $f + \phi_\alpha$ is a balanced function having the same degree, extended Walsh spectrum, absolute indicator and sum-of-squares indicator as f.

Proposition 2. *The weight, the degree, the Walsh spectrum (and the nonlinearity), the absolute indicator and the sum-of-squares indicator are invariant under right composition by a linear permutation of* $\mathbf{F}_2^n$.

Both of these types of transformations change neither the size nor the rank of the sets $E_{CI}(f) = \{\alpha \in \mathbf{F}_2^n,\ \mathcal{F}(f+\phi_\alpha) = 0\}$ and $E_{PC}(f) = \{\alpha \in \mathbf{F}_2^n,\ \mathcal{F}(D_\alpha f) = 0\}$. The first-order correlation immunity and the propagation criterion of degree 1 can therefore be studied up to the previous equivalences:

Proposition 3. *Let f be a Boolean function with n variables. If $E_{CI}(f)$ (resp., $E_{PC}(f)$) has rank n, then there exists a linear permutation π of $\mathbf{F}_2^n$ such that the Boolean function $f \circ \pi$ is first-order correlation-immune (resp., satisfies the propagation criterion of degree 1).*

The rest of the paper is organized as follows. We observe in Section 3 that the nonlinearity of a Boolean function provides an upper bound on its sum-of-squares indicator. Moreover, we completely characterize the functions achieving this bound: their extended Walsh spectra take at most 3 values. In Section 4 we derive a lower bound on the number of zero auto-correlation coefficients of a function from its nonlinearity. Section 5 is devoted to the nonlinearity of Boolean functions with a linear structure. We essentially show that these functions are not almost optimal when the dimensions of their linear spaces exceed 1 for odd n, and 2 for even n. Conversely, Section 6 focuses on the functions which satisfy the propagation criterion with respect to a linear subspace of codimension 1 or 2. We prove that these functions are almost optimal and that they have a three-valued extended Walsh spectrum when n is odd. For even n we obtain new characterizations of bent functions. In the last section we study the correlation-immunity order of Boolean functions with a three-valued Walsh spectrum. Such functions are 1-resilient (up to a linear permutation) unless n is odd and they satisfy PC$(n-1)$. We deduce that for any odd n and any degree $d \leq (n+1)/2$, there exist 1-resilient functions of degree d, with n variables, and with nonlinearity $2^{n-1} - 2^{(n-1)/2}$.

3 Relation between the sum-of-squares indicator and the Walsh spectrum

The auto-correlation coefficients of a Boolean function are related to its Walsh spectrum through the following formulas. Proofs of these results can notably be found in [5] and [30].

Lemma 1. *Let f be a Boolean function with n variables. For any $\alpha \in \mathbf{F}_2^n$,*

$$\mathcal{F}^2(f+\phi_\alpha) = \sum_{\beta \in \mathbf{F}_2^n} (-1)^{\alpha \cdot \beta} \mathcal{F}(D_\beta f) \ .$$

Lemma 2. *Let f be a Boolean function with n variables. Then*

$$\sum_{\alpha \in \mathbf{F}_2^n} \mathcal{F}^4(f+\phi_\alpha) = 2^n \mathcal{V}(f) \ .$$

We now point out that the nonlinearity of a function obviously provides an upper bound on its sum-of-squares indicator, $\mathcal{V}(f)$. Moreover, some further information on the Walsh spectrum of a function can be derived from the value of $\mathcal{V}(f)$. The following result was proved independently in [32, Theorem 5]. We give here a much simpler proof.

Theorem 1. *Let f be a Boolean function with n variables and let $\mathcal{L}(f) = \max_{\alpha \in \mathbf{F}_2^n} |\mathcal{F}(f+\phi_\alpha)|$. Then we have*

$$\mathcal{V}(f) \leq 2^n \mathcal{L}(f)^2$$

with equality if and only if the extended Walsh spectrum of f takes at most three values, 0, $\mathcal{L}(f)$ and $-\mathcal{L}(f)$.

Proof: Let us consider the following quantity

$$\mathcal{I}(f) = \sum_{\alpha \in \mathbf{F}_2^n} \mathcal{F}^2(f+\phi_\alpha) \left[\mathcal{F}^2(f+\phi_\alpha) - \mathcal{L}(f)^2 \right] \ .$$

By Parseval's relation we have $\sum_{\alpha \in \mathbf{F}_2^n} \mathcal{F}^2(f+\phi_\alpha) = 2^{2n}$. It then follows from Lemma 2 that $\mathcal{I}(f) = 2^n(\mathcal{V}(f) - 2^n \mathcal{L}(f)^2)$. By definition $\mathcal{I}(f)$ consists of a sum of terms T_α, $\alpha \in \mathbf{F}_2^n$, which satisfy $T_\alpha \leq 0$ if and only if $|\mathcal{F}(f+\phi_\alpha)| \leq \mathcal{L}(f)$. Since $|\mathcal{F}(f+\phi_\alpha)| \leq \mathcal{L}(f)$ for any α, all terms T_α in $\mathcal{I}(f)$ are non positive, and thus $\mathcal{I}(f) \leq 0$. The equality holds if and only if all terms T_α in $\mathcal{I}(f)$ vanish. This only occurs if $|\mathcal{F}(f+\phi_\alpha)| \in \{0, \mathcal{L}(f)\}$ for all α. □

Following Definition 3, the sum-of-squares indicator of an almost optimal function f with n variables then satisfies $\mathcal{V}(f) \leq 2^{2n+1}$ if n is odd, and $\mathcal{V}(f) \leq 2^{2n+2}$ if n is even.

Example 1. We consider the following function of degree 5 with 7 variables:

$$f(x_1, \ldots, x_7) = x_1x_2x_3x_4x_5 + x_1x_3x_7 + x_1x_2 + x_3x_4 + x_5x_6 \ .$$

This function is almost optimal and its extended Walsh spectrum takes exactly 5 values, $0, \pm 8, \pm 16$. Let A_i denote the number of α such that $|\mathcal{F}(f+\phi_\alpha)| = i$. We have $A_0 = 40$, $A_8 = 32$ and $A_{16} = 56$. It follows that $\mathcal{V}(f) = 29696 < 2^{15}$.

This function f can be added to a bent function with $(n-7)$ variables for any odd $n \geq 7$. This provides an almost optimal function g with n variables whose extended Walsh spectrum takes the following 5 values: $0, \pm 2^{(n-1)/2}, \pm 2^{(n+1)/2}$. Moreover, we have $A_0 = 5 \cdot 2^{n-4}$, $A_{2^{(n-1)/2}} = 2^{n-2}$ and $A_{2^{(n+1)/2}} = 7 \cdot 2^{n-4}$; thus $\mathcal{V}(g) = 2^{2n+1} - 3 \cdot 2^{2n-4}$.

The functions whose extended Walsh spectra take at most three values are very specific since their extended Walsh spectrum is completely determined by their nonlinearity. In this case the values of the Walsh transform belong to $0, \pm\mathcal{L}(f)$.

Theorem 2. *Let f be a Boolean function with n variables. Assume that the extended Walsh spectrum of f takes at most three values, 0 and $\pm\mathcal{L}(f)$. Then $\mathcal{L}(f) = 2^i$ with $i \geq n/2$ and*

$$\#\{\alpha \in \mathbf{F}_2^n,\ |\mathcal{F}(f+\phi_\alpha)| = \mathcal{L}(f)\} = \frac{2^{2n}}{\mathcal{L}(f)^2} = 2^{2n-2i}\ ;$$

$$\#\{\alpha \in \mathbf{F}_2^n,\ |\mathcal{F}(f+\phi_\alpha)| = 0\} = \frac{2^n(\mathcal{L}(f)^2 - 2^n)}{\mathcal{L}(f)^2} = 2^n - 2^{2n-2i}\ .$$

Moreover, the degree of f is less than or equal to $n - i + 1$.

Proof: Since $\mathcal{F}^2(f+\phi_\alpha)$ lies in $\{0, \mathcal{L}(f)^2\}$ for all $\alpha \in \mathbf{F}_2^n$, we have from Parseval's relation

$$\sum_{\alpha \in \mathbf{F}_2^n} \mathcal{F}^2(f+\phi_\alpha) = \mathcal{L}(f)^2 A_{\mathcal{L}(f)} = 2^{2n}$$

where $A_{\mathcal{L}(f)} = \#\{\alpha \in \mathbf{F}_2^n,\ |\mathcal{F}(f+\phi_\alpha)| = \mathcal{L}(f)\}$. It follows that $\mathcal{L}(f) = 2^i$. Since $A_{\mathcal{L}(f)} \leq 2^n$, we deduce that $i \geq n/2$. The upper-bound on the degree of f comes from the divisibility of the Walsh coefficients [6, Lemma 3]. □

Note that any Boolean function of degree 2 satisfies the hypotheses of the previous theorem [14, p. 441]. Theorem 2 now implies that the only almost optimal functions having a three-valued extended Walsh spectrum satisfy $\mathcal{L}(f) = 2^{(n+1)/2}$ when n is odd and $\mathcal{L}(f) = 2^{(n+2)/2}$ when n is even (bent functions have a two-valued extended Walsh spectrum).

4 Propagation criterion on highly nonlinear functions

We have pointed out that the nonlinearity of a Boolean function provides an upper bound on its sum-of-squares indicator, *i.e.*, on the second moment of the auto-correlation coefficients. We now show that it also gives a lower bound on the number of zero auto-correlation coefficients.

Proposition 4. *Let f be a Boolean function of degree d with n variables and let $E_{PC}(f) = \{\alpha \in \mathbf{F}_2^n,\ \mathcal{F}(D_\alpha f) = 0\}$. Then*

$$|E_{PC}(f)| \geq 2^n - 1 - 2^{n-4-2\lfloor \frac{n-2}{d-1} \rfloor} \left(\mathcal{L}(f)^2 - 2^n\right)\ .$$

Proof: Since any derivative $D_\alpha f$ of f is a function of degree $(d-1)$ with a linear structure, $\mathcal{F}(D_\alpha f)$ is divisible by $2^{\lfloor \frac{n-2}{d-1} \rfloor + 2}$ [16]. We then deduce

$$\begin{aligned}\mathcal{V}(f) &= \sum_{\alpha \notin E_{PC}(f)} \mathcal{F}^2(D_\alpha f) = 2^{2n} + \sum_{\alpha \notin E_{PC}(f), \alpha \neq 0} \mathcal{F}^2(D_\alpha f) \\ &\geq 2^{2n} + (2^n - 1 - |E_{PC}(f)|) 2^{2\lfloor \frac{n-2}{d-1} \rfloor + 4}\end{aligned}$$

We know from Theorem 1 that $\mathcal{V}(f) \leq 2^n \mathcal{L}(f)$. We therefore deduce the expected result. □

This bound is essentially relevant for functions having a high nonlinearity and a low degree. For instance we deduce that almost optimal functions of degree 3 satisfy $|E_{PC}(f)| \geq 2^{n-2} - 1$ when n is even and $|E_{PC}(f)| \geq 2^{n-1} - 1$ when n is odd.

Corollary 1. *Let n be an odd integer. Let f be an almost optimal function of degree 3 with n variables. Then there exists a permutation π of $\mathbf{F}_2^n$ such that $f \circ \pi$ satisfies PC(1) unless there exists an affine subspace $\overline{H}$ of $\mathbf{F}_2^n$ of codimension 1 such that $\mathcal{F}^2(D_\alpha f) = 2^{n+1}$ for any $\alpha \in \overline{H}$.*

Proof: It follows from Proposition 3 that f can be transformed into a function satisfying PC(1) if $E_{PC}(f)$ has rank n. Since the previous theorem implies that $|E_{PC}(f) \cup \{0\}| \geq 2^{n-1}$, $E_{PC}(f)$ has full rank except if $E_{PC}(f) \cup \{0\}$ is an hyperplane of $\mathbf{F}_2^n$, *i.e.*, a linear subspace of codimension 1. In this case, the lower bound on the size of $E_{PC}(f)$ is achieved. It is clear from the proof of the previous theorem that this occurs if and only if $\mathcal{V}(f) = 2^{2n+1}$ and $\mathcal{F}^2(D_\alpha f) = 2^{n+1}$ for any nonzero $\mathbf{F}_2^n \setminus E_{PC}(f)$. □

This corollary therefore provides a fast algorithm for obtaining almost optimal functions of degree 3 which satisfy PC(1) when the number of variables is odd.

5 Walsh spectrum of Boolean functions with a linear structure

Theorem 1 also enables us to characterize almost optimal functions which have a linear structure.

Theorem 3. *Let f be a Boolean function with n variables. Assume that f has a linear space V of dimension $k \geq 1$. Then*

$$\mathcal{L}(f) \geq 2^{\frac{n+k}{2}}$$

with equality if and only if f satisfies the propagation criterion with respect to $\mathbf{F}_2^n \setminus V$.

In this case, k and n have the same parity and f has a three-valued extended Walsh spectrum.

Proof: If f has a linear space of dimension k, the sum-of-squares indicator satisfies

$$\mathcal{V}(f) = 2^{2n+k} + \sum_{\alpha \notin V} \mathcal{F}^2(D_\alpha f) \geq 2^{2n+k} \ .$$

Thus $\mathcal{L}(f) \geq 2^{(n+k)/2}$ according to Theorem 1 with equality if and only f has a three-valued extended Walsh spectrum and $\mathcal{L}(f) = 2^{(n+k)/2}$. This implies that n and k have the same parity. □

Corollary 2. *Let n be an odd integer and let f be a Boolean function with n variables. The following assertions are equivalent:*

(i) *f is almost optimal and it has a linear structure.*
(ii) *there exists a linear permutation π of $\mathbf{F}_2^n$ such that $f \circ \pi$ satisfies PC($n-2$).*
(iii) *there exists a linear permutation π of $\mathbf{F}_2^n$ such that $f \circ \pi$ satisfies PC($n-1$).*

Proof: Carlet [7, Prop. 1] proved that the second and third assertions are equivalent. Moreover, any function satisfying PC($n-1$) has a linear structure e and all its derivatives with respect to direction $\alpha \notin \{0, e\}$ are balanced. The previous theorem then proves the equivalence with the first assertion. □

The extended Walsh spectrum of an almost optimal function which has a linear structure is then completely determined unless the number of variables is even and the linear space has dimension 1. We now give an example of this situation:

Example 2. Let f_1 and f_2 be the following almost optimal functions with 8 variables:

$$f_1(x_1, \ldots, x_8) = x_1x_2x_3x_4x_5 + x_1x_3x_7 + x_1x_2 + x_3x_4 + x_5x_6 + x_8 \ ,$$
$$f_2(x_1, \ldots, x_8) = x_1x_3x_4x_6 + x_4x_6x_7 + x_1x_2 + x_3x_4 + x_5x_6 + x_8 \ .$$

Both of these functions have a linear space of dimension 1. From Example 1 we know that f_1 has a 5-valued extended Walsh spectrum and $\mathcal{V}(f_1) = 2^{2n+2} - 3 \cdot 2^{2n-3}$. On the other hand f_2 has a 3-valued extended Walsh spectrum and satisfies $\mathcal{V}(f_2) = 2^{2n-2}$.

6 Functions satisfying the propagation criterion with respect to a linear subspace

The previous 3 sections have shown that almost optimal functions generally have good propagation characteristics regarding all indicators. We now conversely focus on the Walsh spectra of the Boolean functions f which have the following remarkable propagation property: f satisfies the propagation criterion with respect to any nonzero element of a linear subspace of $\mathbf{F}_2^n$ of codimension 1 or 2.

Proposition 5. *Let V be a linear subspace of $\mathbf{F}_2^n$ of dimension k. Let $V^\perp$ denote its dual,* i.e., *$V^\perp = \{x \in \mathbf{F}_2^n, x \cdot y = 0$ for all $y \in V\}$. For any Boolean function f with n variables, we have*

$$\sum_{\alpha \in V} \mathcal{F}^2(f + \phi_\alpha) = 2^k \sum_{\beta \in V^\perp} \mathcal{F}(D_\beta f) \ .$$

Proof: We deduce from Lemma 1:

$$\begin{aligned} \sum_{\alpha \in V} \mathcal{F}^2(f + \phi_\alpha) &= \sum_{\alpha \in V} \sum_{\beta \in \mathbf{F}_2^n} (-1)^{\alpha \cdot \beta} \mathcal{F}(D_\beta f) \\ &= \sum_{\beta \in \mathbf{F}_2^n} \mathcal{F}(D_\beta f) \left(\sum_{\alpha \in V} (-1)^{\alpha \cdot \beta} \right) = 2^k \sum_{\beta \in V^\perp} \mathcal{F}(D_\beta f) \end{aligned}$$

since $\sum_{\alpha \in V}(-1)^{\alpha \cdot \beta}$ equals 2^k if $\beta \in V^\perp$ and it equals 0 otherwise. □

We first consider the case where a function f with n variables satisfies the propagation criterion with respect to any $\beta \neq 0$ belonging to an hyperplane. We will use the following well-known lemma due to Jacobi (see [8, Ch. VI]):

Lemma 3. *Let n be an integer, $n > 2$, and let X and Y be two even integers. Then the condition $X^2 + Y^2 = 2^{n+1}$ implies*

- *if n is even, then $X^2 = Y^2 = 2^n$;*
- *if n is odd, then $X^2 = 2^{n+1}$ and $Y = 0$ – or vice-versa.*

For odd values of n, the functions with n variables having balanced derivatives $D_\beta f$ for every nonzero β in an hyperplane can be characterized as follows:

Theorem 4. *Let n be an odd integer, $n > 2$, and f be a Boolean function with n variables. Then the following properties are equivalent.*

(i) *There is an hyperplane $H \subset \mathbf{F}_2^n$ such that f satisfies the propagation criterion with respect to $H \setminus \{0\}$.*

(ii) *f has a three-valued extended Walsh spectrum, $\mathcal{L}(f)$ equals $2^{(n+1)/2}$ and there is some $a \in \mathbf{F}_2^n$ such that*

$$\forall \beta \in \mathbf{F}_2^n, \quad \mathcal{F}^2(f + \phi_\beta) \neq \mathcal{F}^2(f + \phi_{\beta+a}) \ .$$

(iii) *There is a linear permutation π of $\mathbf{F}_2^n$ such that $f \circ \pi(x_1, \ldots, x_n) = (1 + x_n)g + x_n h$ where both g and h are bent functions with $(n-1)$ variables.*

Proof: (i) ⇒ (ii) . Let $a \in \mathbf{F}_2^n$ be such that $H = \{x \in \mathbf{F}_2^n, a \cdot x = 0\}$. Proposition 5 gives for any $\beta \in H$

$$\mathcal{F}^2(f + \phi_\beta) + \mathcal{F}^2(f + \phi_{\beta+a}) = 2 \sum_{\alpha \in H} \mathcal{F}(D_\alpha(f + \phi_\beta)) \ .$$

Since $D_\alpha(f + \phi_\beta) = D_\alpha(f) + \alpha \cdot \beta$, we have

$$\mathcal{F}^2(f + \phi_\beta) + \mathcal{F}^2(f + \phi_{\beta+a}) = 2 \sum_{\alpha \in H} (-1)^{\alpha \cdot \beta} \mathcal{F}(D_\alpha f) = 2\mathcal{F}(D_0 f) = 2^{n+1} \ .$$

From Lemma 3, we deduce that, for any $\beta \in H$, $\mathcal{F}^2(f + \phi_\beta) = 2^{n+1}$ and $\mathcal{F}^2(f + \phi_{\beta+a}) = 0$, or vice-versa. It then follows that, for any $\beta \in \mathbf{F}_2^n$, $\mathcal{F}(f + \phi_\beta)$ belongs to $\{0, \pm 2^{(n+1)/2}\}$ and that $\mathcal{F}^2(f + \phi_\beta) \neq \mathcal{F}^2(f + \phi_{\beta+a})$.

(ii) ⇒ (iii). Let $(e_1, \ldots, e_n)$ denote the canonical basis of $\mathbf{F}_2^n$. Let π be a linear permutation of $\mathbf{F}_2^n$ such that $\pi^{-1}(a) = e_n$. Assertion **(ii)** gives for any $\beta \in \mathbf{F}_2^n$,

$$\mathcal{F}^2(f \circ \pi + \phi_\beta) + \mathcal{F}^2(f \circ \pi + \phi_{\beta+e_n}) = 2^{n+1} \ . \tag{1}$$

For any β in the hyperplane spanned by $e_1, \ldots, e_{n-1}$, ϕ_β does not depend on x_n. We then have $\phi_\beta(x_1, \ldots, x_n) = \phi(x_1, \ldots, x_{n-1})$ where ϕ describes the set of all

linear functions with $(n-1)$ variables when β varies. Using the decomposition $f \circ \pi(x_1, \ldots, x_n) = (1 + x_n)g + x_n h$, we obtain

$$\mathcal{F}(f \circ \pi + \phi_\beta) = \mathcal{F}(g + \phi) + \mathcal{F}(h + \phi) \text{ and}$$
$$\mathcal{F}(f \circ \pi + \phi_{\beta + e_n}) = \mathcal{F}(g + \phi) - \mathcal{F}(h + \phi) \ .$$

Equation (1) now gives

$$\mathcal{F}^2(g + \phi) + \mathcal{F}^2(h + \phi) = \frac{1}{2}\left(\mathcal{F}^2(f \circ \pi + \phi_\beta) + \mathcal{F}^2(f \circ \pi + \phi_{\beta + e_n})\right) = 2^n \ .$$

We deduce from Lemma 3 that, for any linear function ϕ, both $\mathcal{F}^2(g + \phi)$ and $\mathcal{F}^2(h + \phi)$ equal 2^{n-1}, and thus that g and h are bent.

(iii) $\Rightarrow$ (i). Let H' be the hyperplane spanned by $e_1, \ldots, e_{n-1}$. For any $\alpha \in H'$, $D_\alpha(f \circ \pi)$ can be decomposed as

$$D_\alpha(f \circ \pi)(x_1, \ldots, x_n) = (1 + x_n) D_\alpha g(x_1, \ldots, x_{n-1}) + x_n D_\alpha h(x_1, \ldots, x_{n-1}) \ .$$

If g and h are bent, the derivatives $D_\alpha g$ and $D_\alpha h$ are balanced for any $\alpha \in H'$, $\alpha \neq 0$. It follows that $D_\alpha(f \circ \pi)$ is balanced and thus $D_\alpha f$ is balanced for any nonzero α in $\pi(H')$. □

Remark 1. Assertion **(iii)** can actually be generalized. For any vector $\alpha \in \mathbf{F}_2^n$, the restrictions of a Boolean function with n variables to $H_\alpha = \{x \in \mathbf{F}_2^n,\ \alpha \cdot x = 0\}$ and to its complementary set can be identified with Boolean functions with $(n-1)$ variables. Moreover, $\alpha \notin H_\alpha$ if and only if $\sum_{i=1}^n \alpha_i$ is odd. In this case, $\mathbf{F}_2^n$ is the direct sum of H_α and $H_\alpha^\perp$. Exactly as in the previous theorem, we can prove that if f satisfies **(i)** then for any $\alpha \in \mathbf{F}_2^n$ such that $\sum_{i=1}^n \alpha_i$ is odd, there exists a linear permutation π of $\mathbf{F}_2^n$ such that both restrictions of f to H_α and to its complementary set are bent.

When the number of variables is even, we obtain a similar result which provides new characterizations of bent functions. The detailed proof, which relies on the same arguments as the previous one, can be found in [4].

Theorem 5. *Let n be an even integer, $n > 2$, and f be a Boolean function with n variables. Then the following properties are equivalent.*

- **(i)** *There is an hyperplane $H \subset \mathbf{F}_2^n$ such that f satisfies the propagation criterion with respect to $H \setminus \{0\}$.*
- **(ii)** *For any hyperplane $H \subset \mathbf{F}_2^n$, f satisfies the propagation criterion with respect to $H \setminus \{0\}$.*
- **(iii)** *f is bent.*
- **(iv)** *$f(x_1, \ldots, x_n) = (1 + x_n)g + x_n h$ where both g and h are almost optimal functions with $(n-1)$ variables having a three-valued extended Walsh spectrum and, for any linear function ϕ with $(n-1)$ variables, we have*

$$\mathcal{F}^2(g + \phi) \neq \mathcal{F}^2(h + \phi) \ .$$

As pointed out in the remark following Theorem 4, Property **(iv)** also holds if we consider the decomposition of a bent function with respect to any vector α such that $\sum_{i=1}^{n} \alpha_i$ is odd. Note that this theorem is of interest for effective purposes: for checking that a function f is bent it is sufficient to compute the $\mathcal{F}(D_\alpha f)$ for α in some hyperplane.

Similar techniques provide the following result for functions satisfying the propagation criterion with respect to a linear subspace of codimension 2.

Theorem 6. *Let f be a Boolean function with n variables, $n > 2$. Assume that there exists a linear subspace $V \subset \mathbf{F}_2^n$ of codimension 2 such that f satisfies the propagation criterion with respect to $V \setminus \{0\}$.*

- *If n is odd, then f is an almost optimal function with a three-valued extended Walsh spectrum and there is a linear permutation π of $\mathbf{F}_2^n$ such that*

$$f \circ \pi(x_1, \ldots, x_n) = (1 + x_{n-1})(1 + x_n)g_{00} + x_{n-1}(1 + x_n)g_{10} + (1 + x_{n-1})x_n g_{01} + x_{n-1}x_n g_{11}$$

  where all g_{ij} are almost optimal functions with $(n-2)$ variables having a three-valued extended Walsh spectrum.
- *If n is even, then f is either bent or it satisfies $\mathcal{L}(f) = 2^{(n+2)/2}$ and its Walsh coefficients belong to $\{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}$. Moreover, there is a linear permutation π of $\mathbf{F}_2^n$ such that*

$$f \circ \pi(x_1, \ldots, x_n) = (1 + x_{n-1})(1 + x_n)g_{00} + x_{n-1}(1 + x_n)g_{10} + (1 + x_{n-1})x_n g_{01} + x_{n-1}x_n g_{11}$$

  where the Walsh coefficients of all g_{ij} belong to $\{0, \pm 2^{(n-2)/2}, \pm 2^{n/2}\}$.

Converses are not valid in Theorem 6: for odd n, there exist some functions which are not almost optimal and whose restrictions are almost optimal and have a three-valued extended Walsh spectrum. Moreover, the set of all functions satisfying the propagation criterion with respect to a subspace of codimension 2 does not contain all almost optimal functions with a three-valued extended Walsh spectrum.

Example 3. Let $f(x_1, \ldots, x_7) = x_1x_2x_3x_4 + x_1x_3x_5x_6 + x_1x_2x_3 + x_1x_3x_7 + x_1x_2 + x_3x_4 + x_5x_6$. This almost optimal function has a three-valued extended Walsh spectrum but the set $\{\alpha \in F_2^7, \mathcal{F}(D_\alpha f) = 0\} \cup \{0\}$ does not contain any linear space of dimension 5.

Theorems 4 and 6 can be used for generalizing some results given in [31]: any Boolean function with an odd number of variables which has at most 7 nonzero auto-correlation coefficients is almost optimal and it has a three-valued extended Walsh spectrum. This result does not hold anymore when f has 8 nonzero auto-correlation coefficients:

Example 4. For any odd $n \geq 5$, the function

$$f(x_1, \ldots, x_n) = x_2x_3x_4x_5 + x_1x_4x_5 + x_3x_5 + x_2x_4 + g(x_6, \ldots, x_n) \qquad (2)$$

where g is any bent function with $(n–5)$ variables, is such that $\{\alpha \in \mathbf{F}_2^n, \mathcal{F}(D_\alpha f) \neq 0\} = Span(e_1, e_2, e_3)$. This function satisfies $\mathcal{L}(f) = 2^{(n+1)/2}$ but its extended Walsh spectrum has exactly 5 values, $0, \pm 2^{(n-1)/2}, \pm 2^{(n+1)/2}$. Moreover, its sum-of-squares indicator is $\mathcal{V}(f) = 2^{2m-3}$ [1]. Since the bent function g can take any degree less than or equal to $(n-5)/2$, the function defined in (2) can be obtained for any degree d, $4 \leq d \leq (n-5)/2$. Other almost optimal functions whose extended Walsh spectra have more than 3 values can be found in [10, 11].

7 Correlation-immunity of Boolean functions with a three-valued extended Walsh spectrum

We now show that most functions with a three-valued extended Walsh spectrum can be easily transformed into a 1-resilient function, *i.e.* into a function which is balanced and first-order correlation-immune. Since the values of the extended Walsh spectrum are symmetric with respect to 0, if the extended Walsh spectrum of a function has exactly three values, then one of these values is 0. Such a function can therefore be transformed (by addition of a linear function) into a balanced function which have the same extended Walsh spectrum.

Theorem 7. *Let f be balanced Boolean function with n variables. Assume that its extended Walsh spectrum takes three values. Then there exists a linear permutation of $\mathbf{F}_2^n$ such that $f \circ \pi$ is 1-resilient if and only if there is no linear permutation π' of $\mathbf{F}_2^n$ such that $f \circ \pi'$ satisfies PC$(n-1)$.*

Proof: Recall that Proposition 3 asserts that f can be transformed into a 1-resilient function if and only if $E_{CI}(f)$ has rank n. We know from Theorem 2 that $\mathcal{L}(f) = 2^i$ for some $i \geq n/2$ and that the number of zero Walsh coefficients of f is $|E_{CI}(f)| = 2^n - 2^{2n-2i}$. Since f is balanced, it can not be bent and thus $i \geq (n+1)/2$. It follows that $|E_{CI}(f)| \geq 2^{n-1}$ with equality if and only if $i = (n+1)/2$. We obviously deduce that $E_{CI}(f)$ has full rank when $\mathcal{L}(f) > 2^{(n+1)/2}$. Let us now assume that n is odd and $\mathcal{L}(f) = 2^{(n+1)/2}$. The only case where $E_{CI}(f)$ does not have full rank is when it is an hyperplane of $\mathbf{F}_2^n$. Let $\{0, a\} = E_{CI}(f)^\perp$. Proposition 5 applied to $E_{CI}(f)$ leads to

$$0 = \sum_{\alpha \in E_{CI}(f)} \mathcal{F}^2(f + \phi_\alpha) = 2^{n-1}\left(\mathcal{F}(D_0 f) + \mathcal{F}(D_a f)\right) = 2^{n-1}(2^n + \mathcal{F}(D_a f)) \ .$$

Thus $\mathcal{F}(D_a f) = -2^n$; f is then an almost optimal function which has a linear structure. From Corollary 2 we deduce that f can be transformed into a function satisfying PC$(n-1)$.

Conversely, if there is a linear permutation π such $f \circ \pi$ satisfies PC$(n-1)$ then $\mathcal{L}(f) = 2^{(n+1)/2}$ and f has a linear structure a. We now apply Proposition 5

to $H = \{0, a\}^\perp$:

$$\sum_{\alpha \in H} \mathcal{F}^2(f + \phi_\alpha) = 2^{n-1}(2^n + \mathcal{F}(D_a f)) = 0 \text{ or } 2^{2n} \ .$$

Since by hypothesis $f \circ \pi$ is balanced, we have that

$$\sum_{\alpha \in H} \mathcal{F}^2(f + \phi_\alpha) \leq \mathcal{L}(f)^2(2^{n-1} - 1) < 2^{2n} \ .$$

Thus $\sum_{\alpha \in H} \mathcal{F}^2(f + \phi_\alpha) = 0$. It follows that $\mathcal{F}(f + \phi_\alpha) = 0$ for all $\alpha \in H$. Since $|E_{CI}(f)| = 2^{n-1}$, we deduce that $E_{CI}(f) = H$ and thus it has rank $n - 1$. □

For any odd n, 1-resilient functions with n variables having nonlinearity $2^{n-1} - 2^{(n-1)/2}$ can then be easily constructed. According to Theorem 5 it is sufficient to consider the restriction of a bent function with $(n + 1)$ variables to any hyperplane $\{x \in \mathbf{F}_2^{n+1},\ \alpha \cdot x\}$ where $\sum_{i=1}^{n+1} \alpha_i$ is odd. We then only have to check that this function has no linear structure and we transform it by addition of an appropriate linear function and by composition with a linear permutation.

Corollary 3. *Let n be an odd integer. For any integer d, $2 \leq d \leq (n+1)/2$, there exists a 1-resilient function with n variables having degree d and nonlinearity $2^{n-1} - 2^{(n-1)/2}$.*

Proof: We consider the following bent function with $(n + 1)$ variables which belongs to the Maiorana-McFarland class [9]:

$$\forall (x, y) \in \mathbf{F}_2^{\frac{n+1}{2}} \times \mathbf{F}_2^{\frac{n+1}{2}},\ \ f(x, y) = x \cdot \pi(y) + h(y)$$

where h is any Boolean function with $(n+1)/2$ variables and π is the permutation of $\mathbf{F}_2^{\frac{n+1}{2}}$ identified with the power function $x \mapsto x^s$ over $\mathbf{F}_{2^{\frac{n+1}{2}}}$. We choose for example $s = 2^k + 1$ with $k < (n + 1)/2$ and $\frac{n+1}{2\gcd(k,(n+1)/2)}$ odd, or $s = 7$ when $(n + 1)$ is power of 2. Let g be the restriction of f to the hyperplane $\{x \in \mathbf{F}_2^{n+1}, x_1 = 0\}$. The restriction of f has no linear structure when all derivatives of f have degree at least 2. Here we have for any (α, β),

$$D_{(\alpha,\beta)} f(x, y) = \alpha \cdot \pi(y + \beta) + x \cdot (\pi(y + \beta) + \pi(y)) + D_\beta g(y) \ .$$

Our choice for permutation π implies that the degree of $D_{(\alpha,\beta)} f$ is at least 2 when $(\alpha, \beta) \neq (0, 0)$ (see e.g. [19]). It follows that g has no linear structure; it can therefore be transformed into a 1-resilient almost optimal function. Since there is no restriction on h, h can be chosen of any degree less than or equal to $(n + 1)/2$. Thus g can take any degree d, $4 \leq d \leq (n + 1)/2$. Note that such almost optimal functions of degree 2 and 3 can easily be constructed from the functions with 5 variables given in [1]. □

Note that Sarkar and Maitra [24] provide a construction method for 1-resilient functions with n variables having nonlinearity $2^{n-1} - 2^{(n-1)/2}$ and degree $(n-2)$, for any odd $n \geq 5$.

References

1. E.R. Berlekamp and L.R. Welch. Weight distributions of the cosets of the (32,6) Reed-Muller code. *IEEE Trans. Inform. Theory*, 18(1):203–207, 1972.
2. E. Biham, A. Biryukov, and A. Shamir. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In *Advances in Cryptology - EUROCRYPT'99*, number 1592 in Lecture Notes in Computer Science, pages 12–23. Springer-Verlag, 1999.
3. E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, 1991.
4. A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine. On cryptographic properties of the cosets of $R(1, m)$. Submitted.
5. C. Carlet. Partially-bent functions. In *Advances in Cryptology - CRYPTO'92*, number 740 in Lecture Notes in Computer Science, pages 280–291. Springer-Verlag, 1992.
6. C. Carlet. Two new classes of bent functions. In *Advances in Cryptology - EUROCRYPT'93*, number 765 in Lecture Notes in Computer Science, pages 77–101. Springer-Verlag, 1994.
7. C. Carlet. On the propagation criterion of degree ℓ and order k. In *Advances in Cryptology - EUROCRYPT'98*, number 1403 in Lecture Notes in Computer Science, pages 462–474. Springer-Verlag, 1998.
8. L. E. Dickson. *History of the Theory of Numbers*, volume II. Chelsea Publishing Compagny, 1919.
9. J.F. Dillon. *Elementary Hadamard Difference sets.* PhD thesis, University of Maryland, 1974.
10. E. Filiol and C. Fontaine. Highly nonlinear balanced Boolean functions with a good correlation-immunity. In *Advances in Cryptology - EUROCRYPT'98*, number 1403 in Lecture Notes in Computer Science, pages 475–488. Springer-Verlag, 1998.
11. C. Fontaine. On some cosets of the First-Order Reed-Muller code with high minimum weight. *IEEE Trans. Inform. Theory*, 45(4):1237–1243, 1999.
12. T. Johansson and F. Jönsson. Fast correlation attacks based on turbo code techniques. In *Advances in Cryptology - CRYPTO'99*, number 1666 in Lecture Notes in Computer Science, pages 181–197. Springer-Verlag, 1999.
13. T. Johansson and F. Jönsson. Improved fast correlation attack on stream ciphers via convolutional codes. In *Advances in Cryptology - EUROCRYPT'99*, number 1592 in Lecture Notes in Computer Science, pages 347–362. Springer-Verlag, 1999.
14. F.J. MacWilliams and N.J.A. Sloane. *The theory of error-correcting codes.* North-Holland, 1977.
15. M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology - EUROCRYPT'93*, number 765 in Lecture Notes in Computer Science. Springer-Verlag, 1994.
16. R.J. McEliece. Weight congruence for p-ary cyclic codes. *Discrete Mathematics*, 3:177–192, 1972.
17. W. Meier and O. Staffelbach. Fast correlation attack on certain stream ciphers. *Jounal of Cryptology*, pages 159–176, 1989.
18. W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology - EUROCRYPT'89*, number 434 in Lecture Notes in Computer Science, pages 549–562. Springer-Verlag, 1990.
19. K. Nyberg. Differentially uniform mappings for cryptography. In *Advances in Cryptology - EUROCRYPT'93*, number 765 in Lecture Notes in Computer Science, pages 55–64. Springer-Verlag, 1993.

20. N.J. Patterson and D.H. Wiedemann. The covering radius of the $[2^{15}, 16]$ Reed-Muller code is at least 16276. *IEEE Trans. Inform. Theory*, IT-36(2):443, 1983.
21. N.J. Patterson and D.H. Wiedemann. Correction to [20]. *IEEE Trans. Inform. Theory*, IT-36(2):443, 1990.
22. B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of Boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, number 437 in Lecture Notes in Computer Science, pages 155–165, Springer-Verlag, 1990. Springer-Verlag.
23. O.S. Rothaus. On bent functions. *J. Combin. Theory Ser. A*, 20:300–305, 1976.
24. P. Sarkar and S. Maitra. Construction of nonlinear boolean functions with important cryptographic properties. In *Advances in Cryptology - EUROCRYPT 2000*, number 1807 in Lecture Notes in Computer Science, pages 491–512, Springer-Verlag, 2000 (this volume).
25. C.E. Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28:656–715, 1949.
26. T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. Inform. Theory*, IT-30(5):776–780, 1984.
27. T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Trans. Computers*, C-34(1):81–84, 1985.
28. A.F. Webster and S.E. Tavares. On the design of S-boxes. In *Advances in Cryptology - CRYPTO'85*, number 219 in Lecture Notes in Computer Science, pages 523–534. Springer-Verlag, 1985.
29. G. Xiao and J.L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Trans. Inform. Theory*, IT-34(3):569–571, 1988.
30. X.-M. Zhang and Y. Zheng. GAC - the criterion for global avalanche characterics of cryptographic functions. *Journal of Universal Computer Science*, 1(5):320–337, 1995.
31. X.-M. Zhang and Y. Zheng. Characterizing the structures of cryptographic functions satisfying the propagation criterion for almost all vectors. *Designs, Codes and Cryptography*, 7(1):11–134, 1996.
32. Y. Zheng and X.-M. Zhang. Plateaued functions. In *Information and Communication Security, ICICS'99*, number 1726 in Lecture Notes in Computer Science, pages 284–300. Springer-Verlag, 1999.