3

Cryptographic Criteria on Vector Boolean Functions

José Antonio Álvarez-Cubero and Pedro J. Zufiria
Universidad Politécnica de Madrid (UPM)
Spain

1. Introduction

Most modern block and stream ciphers can be expressed as certain arrangement of Vector Boolean Functions. Thus, in the context of block and stream ciphers' design (mainly in S-boxes and combining functions respectively), it is essential to define criteria which measure the cryptographic strength of Boolean Functions and Vector Boolean Functions. Ideally, some of the following requirements must be fulfilled by this criteria:

1. The principles of confusion and diffusion must be enforced by the criterion Shannon (1949). *Confusion* obscures the relationship between the plaintext and the ciphertext Schneier (1995). *Difussion* dissipates the redundancy of the plaintext by spreading it over the ciphertext. Both techniques make more difficult for a cryptanalyst to find out redundancy and statistical patterns in the ciphertext.
2. The criterion must be expressed in terms of a distance to an appropriate set S of cryptographically weak functions Meier & Staffelbach (1990). Functions that exhibit properties common to cryptographically weak functions are also considered to be cryptographically weak.
3. The criterion should remain invariant under a certain group of transformations Meier & Staffelbach (1990). This symmetry group should contain the group of affine transformations.

A function is considered to be cryptographically weak if it is easily breakable or it can be turned into a weak function by means of simple (e.g. linear or affine) transformations. This definition is congruent with the notion of similar secrecy introduced by Shannon in Shannon (1949), so that two functions R and S are said to be "similar" if there exists a fixed transformation A, with an inverse A^{-1}, such that $R = AS$. Hereunder are described the best known cryptographically weak functions.

- *Linear and affine functions.* These functions are easily breakable because the simultaneous complementation of a subset of the input variables causes the value of a linear or an affine function to always change (from the original value before complementation) or to never change.
- *Functions with non-zero linear structures.* The cryptanalytic value of linear structures lies in their potential to map a nonlinear function to a degenerate function via a linear transformation, which may reduce the size of the keyspace.

- *Functions not balanced*. The output of these kind of functions are not uniformly distributed, avoiding statistical dependence between the input and the output (which can be used in attacks).
- *Functions with low algebraic degree* can be approximated by low complex functions easing their attack.
- *m-th order correlation-immune functions* are those whose output distribution probability are unaltered when any m (or, equivalently, at most m) of the inputs are kept constant.
- *Functions with low degree of Propagation Criterion* has little diffusion property and their output distribution probability are altered when some coordinates of the input are complemented.

The main objective of this chapter is to characterize the more relevant cryptographic criteria (nonlinearity, linear distance, balancedness, algebraic degree, correlation immunity, resiliency and propagation criterion) for constructions of Vector Boolean Functions such as composition, addition of coordinate functions, direct sum and bricklayering, from the knowledge of their components. The study of these functions are relevant in cryptology due to the strong connection between cryptographic attacks on the one hand and cryptographic properties of these building blocks on the other hand. In most cases, the security against a particular class of attack can be expressed by the existence of a certain property of the Vector Boolean function, which results in a measure of security against that class of attacks:

- *Linear cryptanalysis* is based on the idea of finding high probable linear or affine relations between the inputs and outputs of S-boxes present in the cipher, that is, finding S-boxes with low nonlinearity Matsui (1994).
- *Differential cryptanalysis* is a chosen-plaintext attack based on the idea of finding high probable differentials pairs between the inputs and outputs of S-boxes present in the cipher, that is, finding S-boxes with low linearity distance. Differential cryptanalysis Biham & Shamir (1991) can be seen as an extension of the ideas of attacks based on the presence of linear structures Nyberg (1991).
- *Distinguishing attacks* are able to distinguish the pseudorandom sequence from a random sequence by observing that the distribution of the sequences is not uniform for not balanced functions.
- Jakobsen and Knudsen identified *interpolation attacks* on block ciphers with S-boxes having small algebraic degree Jakobsen & Knudsen (1997). Later Canteaut and Videau provided *Higher order differential attacks* which exploit the fact that the algebraic degree of the S-box is low. In the case of combining functions, the sequence produced by n combined LSFRs can be obtained by a single LSFR.
- For the pseudo-random generators, the best known cryptanalytic technique is the *correlation attack*, which is based on the idea of finding correlation between the outputs and the inputs, that is, finding S-boxes with low resiliency.
- Propagation Characteristic (PC) is an important cryptographic property for S-boxes to resist differential cryptanalysis. To get uniform output distribution, S-boxes in block ciphers should have $PC(l)$ of higher order for $l \geq 1$.

2. Preliminaries

2.1 Definitions

Let $< \mathrm{GF}(2), +, \cdot >$ be the finite field of order 2, where $\mathrm{GF}(2) = Z_2 = \{0,1\}$, '+' the 'integer addition modulo 2' and '$\cdot$' the 'integer multiplication modulo 2'. $\mathrm{V_n}$ is the vector space of n-tuples of elements from GF(2). The *direct sum* of $\mathbf{x} \in \mathrm{V_{n_1}}$ and $\mathbf{y} \in \mathrm{V_{n_2}}$ is defined as $\mathbf{x} \oplus \mathbf{y} = (x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}) \in \mathrm{V_{n_1+n_2}}$. The *inner product* of $\mathbf{x}, \mathbf{y} \in \mathrm{V_n}$ is denoted by $\mathbf{x} \cdot \mathbf{y}$, and of real vectors $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ is denoted by $\langle \mathbf{x}, \mathbf{y} \rangle$. Let $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, the pointwise product is defined as $\mathbf{x} \centerdot \mathbf{y} = (x_1 \cdot y_1, \ldots, x_n \cdot y_n)$.

$f : \mathrm{V_n} \to \mathrm{GF}(2)$ is called a *Boolean function* and $\mathcal{F}_n$ is the set of all Boolean functions on $\mathrm{V_n}$. $\mathcal{L}_n$ is the set of all linear Boolean functions on $\mathrm{V_n}$: $\mathcal{L}_n = \{l_\mathbf{u} \; \forall \, \mathbf{u} \in \mathrm{V_n} \mid l_\mathbf{u}(\mathbf{x}) = \mathbf{u} \cdot \mathbf{x}\}$ and $\mathcal{A}_n$ is the set of all affine Boolean functions on $\mathrm{V_n}$. The *directional derivative* of $f \in \mathcal{F}_n$ in the direction of $\mathbf{u} \in \mathrm{V_n}$ is defined by $\Delta_\mathbf{u} f(\mathbf{x}) = f(\mathbf{x} + \mathbf{u}) + f(\mathbf{x})$, $\mathbf{x} \in \mathrm{V_n}$. If the following equality is satisfied: $\Delta_\mathbf{u} f(\mathbf{x}) = c$, $c \in \mathrm{GF}(2) \; \forall \, \mathbf{x} \in \mathrm{V_n}$ then $\mathbf{u} \in \mathrm{V_n}$ is called a linear structure of f.

The real-valued mapping $\chi_\mathbf{u}(\mathbf{x}) = (-1)^{\sum_{i=1}^{i=n} u_i x_i} = (-1)^{\mathbf{u} \cdot \mathbf{x}}$ for $\mathbf{x}, \mathbf{u} \in \mathrm{V_n}$ is called a *character*. The character form of $f \in \mathcal{F}_n$ is defined as $\chi_f(\mathbf{x}) = (-1)^{f(\mathbf{x})}$. The truth table of χ_f is called as the $(1,-1)$-*sequence vector* or *sequence vector* of f and is denoted by $\xi_f \in \mathbb{R}^{2^n}$. In other words: $\xi_f = \mathbf{T}_{\mathbf{\emptyset_f}} = ((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})})$.

Let two real functions $\varphi, \psi : \mathrm{V_n} \to \mathbb{R}$, the *circular convolution* or *cross-correlation* $(\varphi * \psi) : \mathrm{V_n} \to \mathbb{R}$ is defined by: $(\varphi * \psi)(\mathbf{x}) = \sum_{\mathbf{u} \in \mathrm{V_n}} \varphi(\mathbf{u}) \psi(\mathbf{x} + \mathbf{u})$.

$F : \mathrm{V_n} \to \mathrm{V_m}$, $F(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}))$ is called a *Vector Boolean function* and $\mathcal{F}_{n,m}$ is the set of all Vector Boolean functions $F : \mathrm{V_n} \to \mathrm{V_m}$. Each $f_i : \mathrm{V_n} \to \mathrm{GF}(2) \; \forall \, i \in \{1, \ldots, m\}$ is a coordinate function of F. The *indicator function* of $F \in \mathcal{F}_{n,m}$, denoted by $\theta_F : \mathrm{V_n} \times \mathrm{V_m} \to \mathbb{R}$, is defined in Chabaud & Vaudenay (1994) as $\theta_F(\mathbf{x}, \mathbf{y}) = 1$ if $\mathbf{y} = F(\mathbf{x})$ and $\theta_F(\mathbf{x}, \mathbf{y}) = 0$ if $\mathbf{y} \neq F(\mathbf{x})$. The character form of $(\mathbf{u}, \mathbf{v}) \in \mathrm{V_n} \times \mathrm{V_m}$ can be defined as follows: $\chi_{(\mathbf{u},\mathbf{v})}(\mathbf{x}, \mathbf{y}) = (-1)^{\mathbf{u} \cdot \mathbf{x} + \mathbf{v} \cdot \mathbf{y}}$.

Let $F \in \mathcal{F}_{n,m}$ and $\mathbf{u} \in \mathrm{V_n}$, then the *difference Vector Boolean function* of F in the direction of $\mathbf{u} \in \mathrm{V_n}$, denoted by $\Delta_\mathbf{u} F \in \mathcal{F}_{n,m}$ is defined as follows: $\Delta_\mathbf{u} F(\mathbf{x}) = F(\mathbf{x} + \mathbf{u}) + F(\mathbf{x})$, $\mathbf{x} \in \mathrm{V_n}$. If the following equality is satisfied: $\Delta_\mathbf{u} F(\mathbf{x}) = \mathbf{c}$, $\mathbf{c} \in \mathrm{V_n} \; \forall \, \mathbf{x} \in \mathrm{V_n}$ then $\mathbf{u} \in \mathrm{V_n}$ is called a linear structure of F.

We define the simplifying notation for the maximum of the absolute values of a set of real numbers $\{a_\mathbf{uv}\}_{\mathbf{u},\mathbf{v}}$, characterized by vectors $\mathbf{u}$ and $\mathbf{v}$, as: $\max\,(a_\mathbf{uv}) = \max_{(\mathbf{u},\mathbf{v})} \{|a_\mathbf{uv}|\}$. Using the same simplifying notation, we define the $\overset{*}{\max}\,(\cdot)$ operator on a set of real numbers $\{a_\mathbf{uv}\}_{\mathbf{u},\mathbf{v}}$, as: $\overset{*}{\max}\,(a_\mathbf{uv}) = \max_{(\mathbf{u},\mathbf{v}) \neq (\mathbf{0},\mathbf{0})} \{|a_\mathbf{uv}|\}$.

2.2 Constructions of Vector Boolean Functions

In this chapter, some secondary contructions are studied, which build (n, m) variable Vector Boolean Functions from (n', m') variable ones (with $n' \leq n, m' \leq m$). The direct sum construction has been used to construct resilient and bent Boolean functions Carlet (2004), Maitra & Pasalic (2002), Pasalic et al. (2001), Sarkar & Maitra (2000a), Sarkar & Maitra (2000b). Adding coordinate functions and bricklayering are operations used to build modern ciphers such as CAST Adams & Tavares (1993), DES Des (1977) and AES Daemen & Rijmen (2002).

2.2.1 Direct sum

Definition 1. *Let $n = n_1 + n_2, n_1, n_2 \geq 1, m \geq 1$, $F_1 \in \mathcal{F}_{n_1,m}$ and $F_2 \in \mathcal{F}_{n_2,m}$. The direct sum of F_1 and F_2 is the function:*

$$\begin{array}{l}(F_1 \oplus F_2) : \mathrm{V_{n_1}} \times \mathrm{V_{n_2}} \rightarrow \mathrm{V_m} \\ (\mathbf{x}, \mathbf{y}) \rightarrow (F_1 \oplus F_2)(\mathbf{x}, \mathbf{y}) = F_1(\mathbf{x}) + F_2(\mathbf{y})\end{array} \tag{1}$$

This is a generalization for Vector Boolean functions of the construction of Boolean functions first introduced in Rothaus (1976).

2.2.2 Adding coordinate functions

Definition 2. *Let $n \geq 1, m = m_1 + m_2, m_1, m_2 \geq 1$ and $F \in \mathcal{F}_{n,m_1}$ and $G \in \mathcal{F}_{n,m_2}$. The result of adding coordinate functions of F and G is the function:*

$$\begin{array}{l}(F, G) : \mathrm{V_n} \rightarrow \mathrm{V_{m_1}} \times \mathrm{V_{m_2}} \\ \qquad \mathbf{x} \rightarrow (F, G)(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_{m_1}(\mathbf{x}), g_1(\mathbf{x}), \ldots, g_{m_2}(\mathbf{x}))\end{array} \tag{2}$$

This is a generalization for Vector Boolean functions of the method used in the CAST algorithm and studied in Nyberg (1995) by adding more than one coordinate function at the same time.

2.2.3 Bricklayer

Definition 3. *Let $n = n_1 + n_2, n_1, n_2 \geq 1, m = m_1 + m_2, m_1, m_2 \geq 1$, $F \in \mathcal{F}_{n_1,m_1}$ and $G \in \mathcal{F}_{n_2,m_2}$. The Bricklayer of F and G is the function $F|G \in \mathcal{F}_{n,m}$:*

$$\begin{array}{l}F|G : \mathrm{V_{n_1}} \times \mathrm{V_{n_2}} \rightarrow \mathrm{V_{m_1}} \times \mathrm{V_{m_2}} \\ \qquad (\mathbf{x}, \mathbf{y}) \rightarrow F|G(\mathbf{x}, \mathbf{y}) = (f_1(\mathbf{x}), \ldots, f_{m_1}(\mathbf{x}), g_1(\mathbf{y}), \ldots, g_{m_2}(\mathbf{y}))\end{array} \tag{3}$$

This construction corresponds to the bricklayer function Daemen & Rijmen (2002) as a parallel application of a number of Vector Boolean functions operating on smaller inputs.

Another interesting operation is the restriction o projection of a Vector Boolean Function, which can be found in ciphers such as MacGuffin Blaze & Schneier (1995).

2.2.4 Projection

Definition 4. *Let $F \in \mathcal{F}_{n,m}$ and ordered set $\mathsf{A} = \{i_1, \ldots, i_p\} \subseteq \{1, \ldots, m\}$. The result of projecting F onto A is the function:*

$$\begin{array}{l}F|_{\mathsf{A}} : \mathrm{V_n} \rightarrow \mathrm{V_p} \\ \qquad \mathbf{x} \rightarrow F|_{\mathsf{A}}(\mathbf{x}) = (f_{i_1}(\mathbf{x}), \ldots, f_{i_p}(\mathbf{x}))\end{array} \tag{4}$$

2.3 Walsh spectrum, autocorrelation spectrum and differential profile

The Walsh and Autocorrelation Spectrum together with the Differential Profile of the Vector Boolean Functions conforming a cipher play an important role. The cryptograhic criteria nonlinearity, resiliency, balancedness, linearity distance and propagation criteria can be obtained from these three matrices.

Definition 5. *Let a Boolean function $f \in \mathcal{F}_n$, the Walsh Transform of f at $\mathbf{u} \in \mathrm{V_n}$ is the n-dimensional Discrete Fourier Transform and can be calculated as follows:*

$$\mathcal{W}_f(\mathbf{u}) = \hat{\chi}_f(\mathbf{u}) = \left\langle \xi_f, \xi_{l_\mathbf{u}} \right\rangle = \sum_{\mathbf{x}\in \mathrm{V_n}} \chi_f(\mathbf{x})\chi_\mathbf{u}(\mathbf{x}) = \sum_{\mathbf{x}\in \mathrm{V_n}} (-1)^{f(\mathbf{x})+\mathbf{ux}} \tag{5}$$

The *Walsh Spectrum* of f can be represented by a matrix whose rows are characteristiced by $\mathbf{u} \in \mathrm{V_n}$ in lexicographic order, denoted by $\mathsf{WS}(f) \in \mathsf{M}_{2^n\times 1}(\mathbb{R})$ and defined as $\mathsf{WS}(f) = \left(\hat{\chi}_f(\mathbf{ff_0}) \ldots \hat{\chi}_f(\mathbf{u}) \ldots \hat{\chi}_f(\mathbf{ff_{2^n-1}})\right)^T$ where $\hat{\chi}_f(\mathbf{u}) = \mathsf{WS}(f)(\mathbf{u})$ and satisfying that $-2^n \leq \hat{\chi}_f(\mathbf{u}) \leq 2^n$.

The following fundamental result can be seen as an extension of the usual Fourier Transform properties:

Theorem 1. *$\forall\, f, g \in \mathcal{F}_n$ it holds that:*

$$\xi_f \centerdot \xi_g \overset{W}{\longleftrightarrow} \tfrac{1}{2^n}\mathsf{WS}(f) * \mathsf{WS}(g) \tag{6}$$

Proof.

$$\begin{aligned}
&\mathcal{W}\{\xi_f \centerdot \xi_g\}(\mathbf{u}) = \textstyle\sum_{\mathbf{x}\in \mathrm{V_n}}(\xi_f \centerdot \xi_g)(\mathbf{x})\chi_\mathbf{u}(\mathbf{x}) = \sum_{\mathbf{x}\in \mathrm{V_n}} \chi_f(\mathbf{x})\chi_g(\mathbf{x})\chi_\mathbf{u}(\mathbf{x}) \\
&= \textstyle\sum_{\mathbf{x}\in \mathrm{V_n}} \left(\frac{1}{2^n}\sum_{\mathbf{v}\in \mathrm{V_n}} \hat{\chi}_f(\mathbf{v})\chi_\mathbf{v}(\mathbf{x})\right)\chi_g(\mathbf{x})\chi_\mathbf{u}(\mathbf{x}) \\
&= \tfrac{1}{2^n}\textstyle\sum_{\mathbf{v}\in \mathrm{V_n}} \hat{\chi}_f(\mathbf{v}) \sum_{\mathbf{x}\in \mathrm{V_n}} \chi_\mathbf{v}(\mathbf{x})\chi_g(\mathbf{x})\chi_\mathbf{u}(\mathbf{x}) \\
&= \tfrac{1}{2^n}\textstyle\sum_{\mathbf{v}\in \mathrm{V_n}} \hat{\chi}_f(\mathbf{v}) \sum_{\mathbf{x}\in \mathrm{V_n}} \chi_g(\mathbf{x})\chi_{\mathbf{u}+\mathbf{v}}(\mathbf{x}) \\
&= \tfrac{1}{2^n}\textstyle\sum_{\mathbf{v}\in \mathrm{V_n}} \hat{\chi}_f(\mathbf{v})\hat{\chi}_g(\mathbf{u}+\mathbf{v}) = \frac{1}{2^n}(\mathsf{WS}(f) * \mathsf{WS}(g))(\mathbf{u})
\end{aligned}$$

□

Theorem 2. *Let $\mathbf{u} \in \mathrm{V_n}, \mathbf{u_1} \in \mathrm{V_{n_1}}, \mathbf{u_2} \in \mathrm{V_{n_2}}, n = n_1 + n_2$ so that $\mathbf{u} = \mathbf{u_1} \oplus \mathbf{u_2}$. Let $f_1 \in \mathcal{F}_{n_1}$ and $f_2 \in \mathcal{F}_{n_2}$, their direct sum $f_1 \oplus f_2 \in \mathcal{F}_n$, and it satisfies: $\hat{\chi}_{f_1\oplus f_2}(\mathbf{u}) = \hat{\chi}_{f_1}(\mathbf{u_1}) \cdot \hat{\chi}_{f_2}(\mathbf{u_2})$ Sarkar & Maitra (2000a).*

Definition 6. *Let the Vector Boolean function $F \in \mathcal{F}_{n,m}$, its Walsh Transform is the two-dimensional Walsh Transform defined by:*

$$\mathcal{W}_F(\mathbf{u},\mathbf{v}) = \hat{\theta}_F(\mathbf{u},\mathbf{v}) = \sum_{\mathbf{x}\in \mathrm{V_n}}\sum_{\mathbf{y}\in \mathrm{V_m}} \theta_F(\mathbf{x},\mathbf{y})\chi_{(\mathbf{u},\mathbf{v})}(\mathbf{x},\mathbf{y}) = \sum_{\mathbf{x}\in \mathrm{V_n}} (-1)^{\mathbf{ux}+\mathbf{v}F(\mathbf{x})} \tag{7}$$

Corollary 1. *The value of the Walsh transform of Vector Boolean function $F \in \mathcal{F}_{n,m}$ at $(\mathbf{u},\mathbf{v})$ coincides with the value of the Walsh transform of the Boolean function $\mathbf{v}\cdot F$ at $\mathbf{u}$: $\hat{\theta}_F(\mathbf{u},\mathbf{v}) = \hat{\chi}_{\mathbf{v}\cdot F}(\mathbf{u})\ \ \forall\,(\mathbf{u},\mathbf{v}) \in \mathrm{V_n}\times\mathrm{V_m}$.*

The *Walsh Spectrum* of F can be represented by a matrix whose rows are characteristiced by $\mathbf{u} \in \mathrm{V_n}$ and whose columns are characteristiced by $\mathbf{v} \in \mathrm{V_m}$ in lexicographic order, denoted by $\mathsf{WS}(F) \in \mathsf{M}_{2^n\times 2^m}(\mathbb{R})$. It holds that $\hat{\theta}_F(\mathbf{u},\mathbf{v}) = \mathsf{WS}(F)(\mathbf{u},\mathbf{v})$, $\mathsf{WS}(F)_\mathbf{u}$ is the row of the Walsh Spectrum characteristiced by $\mathbf{u}$ and $\mathsf{WS}(F)^\mathbf{v}$ is the column of the Walsh Sprectrum characteristiced by $\mathbf{v}$.

Theorem 3. *Let $L_{\mathsf{A},\mathbf{b}} \in \mathcal{F}_{n,m}$ an affine Vector Boolean function where $L_{\mathsf{A},\mathbf{b}}(\mathbf{x}) = \mathsf{A}\mathbf{x} + \mathbf{b}$ with $\mathsf{A} \in \mathsf{M}_{n\times m}(\mathrm{GF}(2))$ and $\mathbf{b} \in \mathrm{V_m}$, its spectrum holds that Pommerening (2005):*

$$\hat{\theta}_{L_{\mathsf{A},\mathbf{b}}}(\mathbf{u},\mathbf{v}) = \begin{cases} 2^n & \text{if } \mathbf{v}^T\mathsf{A} = \mathbf{u}^T,\ \mathbf{v}^T\mathbf{b} = 0 \\ -2^n & \text{if } \mathbf{v}^T\mathsf{A} = \mathbf{u}^T,\ \mathbf{v}^T\mathbf{b} = 1 \\ 0 & \text{if } \mathbf{v}^T\mathsf{A} \neq \mathbf{u}^T \end{cases}$$

Theorem 4. *If $F \in \mathcal{F}_{n,n}$ is bijective then it holds that: $\hat{\theta}_F(\mathbf{u},\mathbf{v}) = \hat{\theta}_{F^{-1}}(\mathbf{v},\mathbf{u})$.*

Definition 7. *The autocorrelation of $f \in \mathcal{F}_n$ with respect to the shift $\mathbf{u} \in \mathrm{V_n}$ is the cross-correlation of f with itself, denoted by $r_f(\mathbf{u}) : \mathrm{V_n} \to \mathbb{R}$ and defined by:*

$$r_f(\mathbf{u}) = \frac{1}{2^n}\sum_{\mathbf{x}\in\mathrm{V_n}} \chi_f(\mathbf{x})\chi_f(\mathbf{x}+\mathbf{u}) = \frac{1}{2^n}\sum_{\mathbf{x}\in\mathrm{V_n}} (-1)^{f(\mathbf{x})+f(\mathbf{u}+\mathbf{x})} \tag{8}$$

Definition 8. *The autocorrelation of $F \in \mathcal{F}_{n,m}$ with respect to the shift $(\mathbf{u},\mathbf{v}) \in \mathrm{V_n}\times\mathrm{V_m}$ is the cross-correlation of F with itself, denoted by $r_F(\mathbf{u},\mathbf{v}) : \mathrm{V_n}\times\mathrm{V_m} \to R$, so that Nyberg (1995):*

$$r_F(\mathbf{u},\mathbf{v}) = \tfrac{1}{2^n}\textstyle\sum_{\mathbf{x}\in\mathrm{V_n}} \chi_{\mathbf{v}F}(\mathbf{x}+\mathbf{u})\chi_{\mathbf{v}F}(\mathbf{x}) = \tfrac{1}{2^n}\sum_{\mathbf{x}\in\mathrm{V_n}}(-1)^{\mathbf{v}F(\mathbf{x}+\mathbf{u})+\mathbf{v}F(\mathbf{x})} \tag{9}$$

Let $F \in \mathcal{F}_{n,m}$, if we denote by $D_F(\mathbf{u},\mathbf{v})$ the set of vectors where the difference Vector Boolean function of F in the direction of $\mathbf{u} \in \mathrm{V_n}$ coincides with $\mathbf{v} \in \mathrm{V_m}$ by: $D_F(\mathbf{u},\mathbf{v}) = \{\mathbf{x} \in \mathrm{V_n} \mid \Delta_{\mathbf{u}}F(\mathbf{x}) = \mathbf{v}\}$.

Let $F \in \mathcal{F}_{n,m}$ where $n \geq m$. The matrix containing all posible values of $\#D_F(\mathbf{u},\mathbf{v})$ is referred to as its *XOR or Differential Distribution Table*. Let $DU(F)$ be the largest value in differential distribution table of F (not counting the first element in the first row), namely,

$$DU(F) = \max_{(\mathbf{u},\mathbf{v})\neq(\mathbf{0},\mathbf{0})} \#D_F(\mathbf{u},\mathbf{v}) = \max_{(\mathbf{u},\mathbf{v})\neq(\mathbf{0},\mathbf{0})} \#\{\mathbf{x} \in \mathrm{V_n} \mid \Delta_{\mathbf{u}}F(\mathbf{x}) = \mathbf{v}\} \tag{10}$$

Then F is said to be differentially $DU(F)$-uniform, and accordingly, $DU(F)$ is called the *differential uniformity* of F J. Seberry & Zheng (1994). By normalizing the elements of the differential distribution table we obtain the Differential profile:

Definition 9. *Let the function $\delta_F : \mathrm{V_n}\times\mathrm{V_m} \to Q$ $\delta_F(\mathbf{u},\mathbf{v}) = \frac{1}{2^n}\#D_F(\mathbf{u},\mathbf{v})$, then the Differential Profile of F can be represented by a matrix whose rows are characterized by $\mathbf{u} \in \mathrm{V_n}$ and whose columns are characterized by $\mathbf{v} \in \mathrm{V_m}$ in lexicographic order, denoted by $\mathsf{DP}(F) \in \mathsf{M}_{2^n\times 2^m}(\mathbb{R})$ where $\delta_F(\mathbf{ff_i},\mathbf{ff_j})$ with $i \in \{1,\ldots,2^n-1\}$ and $j \in \{1,\ldots,2^m-1\}$.*

Definition 10. *The maximum value of $\delta_F(\mathbf{u},\mathbf{v})$ is called the differential potential of F: $dp(F) = \max\{\delta_F(\mathbf{u},\mathbf{v}) \mid \forall\,\mathbf{u} \in \mathrm{V_n}, \mathbf{v} \in \mathrm{V_m}, (\mathbf{u},\mathbf{v}) \neq (\mathbf{0},\mathbf{0})\}$.*

Let $F \in \mathcal{F}_{n,m}$ then $\frac{1}{2^m} \leq dp(F) \leq 1$ and the lower bound holds if and only if F is bent and the upper bound is reached when F is linear or affine. The differential uniformity of $F \in \mathcal{F}_{n,m}$ and its differential potential are related as follows: $dp(F) = \frac{1}{2^n}DU(F)$. The differential profile at $(\mathbf{u},\mathbf{v})$ is related with the autocorrelation in the same point in the following way Nyberg (1995): $\delta_F(\mathbf{u},\mathbf{v}) = \frac{1}{2^{n+m}}\sum_{\mathbf{w}\in\mathrm{V_m}} r_F(\mathbf{u},\mathbf{w})\chi_{\mathbf{v}}(\mathbf{w})$.

3. Characteristics

The resistance of the cryptosystems to the known attacks can be quantified through some fundamental characteristics of the Vector Boolean functions used in them. In this chapter, we consider the characteristics most commonly employed for the design of cryptographic functions present in modern block and stream ciphers.

3.1 Nonlinearity

Definition 11. *The nonlinearity of the Boolean function $f \in \mathcal{F}_n$ is a characteristic defined as the distance to the nearest affine function as follows:* $\mathcal{NL}(f) = \min_{a_{\mathbf{u}} \in \mathcal{A}_n} d(f, a_{\mathbf{u}}) = 2^{n-1} - \frac{1}{2} \max_{\mathbf{u} \in \mathrm{V_n}} |\hat{\chi}_f(\mathbf{u})|$ *Meier & Staffelbach (1990).*

Definition 12. *The nonlinearity of a Vector Boolean function $F \in \mathcal{F}_{n,m}$ is defined as the minimum among the nonlinearities of all nonzero linear combinations of the coordinate functions of F Nyberg (1993):*

$$\mathcal{NL}(F) = \min_{\mathbf{v} \neq \mathbf{0} \in \mathrm{V_m}} \mathcal{NL}(\mathbf{v} \cdot F) = 2^{n-1} - \frac{1}{2} \overset{*}{\max} \left(\mathsf{WS}(F)(\mathbf{u}, \mathbf{v})\right) \tag{11}$$

Alternatively, and also associated with the cardinality of the sets of values for which $F \in \mathcal{F}_{n,m}$ satisfies any given linear relation parametrized by $(\mathbf{u}, \mathbf{v})$ we can define the *linear potential* of $F \in \mathcal{F}_{n,m}$ as $lp(F) = \frac{1}{2^{2n}} \cdot \overset{*}{\max} \left(\mathsf{WS}(F)(\mathbf{u}, \mathbf{v})^2\right)$ which is also exploited as a measure of linearity in linear cryptanalysis, and satisfies Chabaud & Vaudenay (1994) $\frac{1}{2^n} \leq lp(F) \leq 1$ so that the lower bound holds if and only if F has maximum nonlinearity (F is bent) and the upper bound is reached when F is linear or affine.

3.2 Linearity distance

Definition 13. *The linearity distance of the Vector Boolean function $F \in \mathcal{F}_{n,m}$ is defined as the minimum among the linearity distances of all nonzero linear combinations of the coordinate functions of F:*

$$\mathcal{LD}(F) = \min_{\mathbf{v} \neq \mathbf{0} \in \mathrm{V_m}} \mathcal{LD}(\mathbf{v} \cdot F) = 2^{n-1} \cdot \min_{\mathbf{u} \neq \mathbf{0} \in \mathrm{V_n}, \mathbf{v} \neq \mathbf{0} \in \mathrm{V_m}} \{\delta_F(\mathbf{u}, \mathbf{v})\} \tag{12}$$

Definition 14. *The linearity distance can be expressed in terms of the differential potential as follows:* $\mathcal{LD}(F) = 2^{n-1} \cdot (1 - dp(F)) = 2^{n-1} \cdot \left(1 - \overset{*}{\max} \left(\mathsf{DP}(F)\right)\right)$ *Pommerening (2005).*

3.3 Balancedness

Definition 15. *$f \in \mathcal{F}_n$ is balanced if its output is uniformly distributed over* $\mathrm{GF}(2)$ *satisfying* $\hat{\chi}_f(\mathbf{0}) = 0$.

Definition 16. *$F \in \mathcal{F}_{n,m}$ is balanced (or to have balanced output) if each possible output m-tuple occurs with equal probability $\frac{1}{2^m}$, that is, its output is uniformly distributed in* $\mathrm{V_m}$. *This is equivalent to say that for every* $\mathbf{y} \in \mathrm{V_m}$:

$$\#\{\mathbf{x} \in \mathrm{V_n} \mid F(\mathbf{x}) = \mathbf{y}\} = 2^{n-m} \longleftrightarrow \hat{\theta}_F(\mathbf{0}, \mathbf{v}) = 0, \ \forall\, \mathbf{v} \neq \mathbf{0} \in \mathrm{V_m} \tag{13}$$

3.4 Correlation immunity

Definition 17. *$f \in \mathcal{F}_n$ is called correlation-immune of order t (t-CI) if for every subset $\{i_1, i_2, \ldots, i_t\} \subseteq \{1, 2, \ldots, n\}$, f is statistically independent of $(x_{i_1}, x_{i_2}, \ldots, x_{i_t})$, satisfying Xiao & Massey (1988): $\hat{\chi}_f(\mathbf{u}) = 0$, $\forall\, \mathbf{u} \in \mathrm{V_n}$, $1 \leq wt(\mathbf{u}) \leq t$. f can also be denoted as $(n, 1, t)$-CI function.*

Definition 18. *$F \in \mathcal{F}_{n,m}$ is an (n, m, t)-CI function if and only if every nonzero linear combination $f(\mathbf{x}) = \sum_{i=1}^{m} v_i f_i(\mathbf{x})$ of coordinate functions of F is an $(n, 1, t)$-CI function, where $\mathbf{x} \in \mathrm{V_n}$, $v_i \in \mathrm{GF}(2)$ $i = 1, \ldots, m$ and not all zeroes. This is equivalent to say Chen et al. (2004):*

$$\hat{\theta}_F(\mathbf{u}, \mathbf{v}) = 0,\ \forall\, \mathbf{u} \in \mathrm{V_n},\ 1 \leq wt(\mathbf{u}) \leq t,\ \forall\, \mathbf{v} \neq \mathbf{0} \in \mathrm{V_m} \tag{14}$$

3.5 Resiliency

Definition 19. *$f \in \mathcal{F}_n$ is a t-resilient function if if it is balanced and t-CI, satisfying: $\hat{\chi}_f(\mathbf{u}) = 0$, $\forall\, \mathbf{u} \in \mathrm{V_n}$, $0 \leq wt(\mathbf{u}) \leq t$. A balanced Boolean function f can be considered as a 0-resilient function.*

Definition 20. *$F \in \mathcal{F}_{n,m}$ is said to be t-resilient if it is balanced and t-CI, satisfying:*

$$\hat{\theta}_F(\mathbf{u}, \mathbf{v}) = 0,\ \forall\, \mathbf{u} \in \mathrm{V_n},\ 0 \leq wt(\mathbf{u}) \leq t,\ \forall\, \mathbf{v} \neq \mathbf{0} \in \mathrm{V_m} \tag{15}$$

F can also be denoted as an (n, m, t)-resilient. A balanced Vector Boolean function F can be considered as a 0-resilient function.

3.6 Propagation

Definition 21. *Let $f \in \mathcal{F}_n$, then f satisfies the propagation criterion of degree $l, PC(l) (1 \leq l \leq n)$, if $f(\mathbf{x})$ changes with a probability of $1/2$ whenever $i (1 \leq i \leq t)$ bits of $\mathbf{x}$ are complemented Preneel et al. (2006).*

Definition 22. *$F \in \mathcal{F}_{n,m}$ satisfies the $PC(l)$ if any nonzero linear combination of the component boolean functions satisfies the $PC(l)$:*

$$r_F(\mathbf{u}, \mathbf{v}) = 0,\ \forall\, \mathbf{u} \in \mathrm{V_n},\ 1 \leq wt(\mathbf{u}) \leq l,\ \forall\, \mathbf{v} \neq \mathbf{0} \in \mathrm{V_m} \tag{16}$$

4. Criteria for constructions with Vector Boolean functions

In this Section, we address the behavior of Walsh Spectra, Differential Profiles, Autocorrelation Spectra and the cited characteristics under several operations of Vector Boolean functions. We present the known properties without a proof and the new to the best of our knowledge results appear with their respective proofs.

4.1 Composition of Vector Boolean functions

Let $F \in \mathcal{F}_{n,p}$, $G \in \mathcal{F}_{p,m}$ and the composition function $G \circ F \in \mathcal{F}_{n,m}$.

Theorem 5. *The Walsh Spectrum for the composition of two Vector Boolean function can be calculated from the product of their respective Walsh Spectra in the following way Pommerening (2005):*

$$\mathsf{WS}(G \circ F) = \frac{1}{2^p} \mathsf{WS}(F) \cdot \mathsf{WS}(G) \tag{17}$$

Theorem 6. *Let $F \in \mathcal{F}_{n,m}$ and let $L_{\mathsf{A},\mathbf{b}} \in \mathcal{F}_{n,n}$ an affine bijection. The Differential Profile for their composition can be calculated from the product of their respective Differential Profiles in the following way:*

$$\mathsf{DP}(F \circ L_{\mathsf{A},\mathbf{b}}) = \frac{1}{2^n}\mathsf{DP}(L_{\mathsf{A},\mathbf{b}}) \cdot \mathsf{DP}(F) \tag{18}$$

Proof. Taking into account the equality $r_{F\circ L_{\mathsf{A},\mathbf{b}}}(\mathbf{u},\mathbf{v}) = r_F(\mathsf{A}\mathbf{u},\mathbf{v})$ described in Millan (1998), it holds that:

$$\begin{array}{l}\delta_{F\circ L_{\mathsf{A},\mathbf{b}}}(\mathbf{u},\mathbf{w}) = \frac{1}{2^{n+m}}\sum_{\mathbf{w}\in \mathrm{V_m}} r_{F\circ L_{\mathsf{A},\mathbf{b}}}(\mathbf{u},\mathbf{w})\chi_{\mathbf{v}}(\mathbf{w}) \\ = \frac{1}{2^{n+m}}\sum_{\mathbf{w}\in \mathrm{V_m}} r_F(\mathsf{A}\mathbf{u},\mathbf{w})\chi_{\mathbf{v}}(\mathbf{w}) = \delta_F(\mathsf{A}\mathbf{u},\mathbf{w})\end{array}$$

□

Theorem 7. *If F is a t-resilient function and G is balanced, then $G \circ F$ is also a t-resilient function.*

Corollary 2. *If F is a balanced function, then $G \circ F$ is also a balanced function.*

4.2 Affine bijections of Vector Boolean functions

Let $F \in \mathcal{F}_{n,m}$ and let $L_{\mathsf{A},\mathbf{b}} \in \mathcal{F}_{m,m}$ and $L_{\mathsf{C},\mathbf{d}} \in \mathcal{F}_{n,n}$ be linear (or affine) bijections.

Lemma 1. *From Theorem 5 and Theorem 3 we can conclude that the effect of applying an invertible linear function before (or after) a function is only a permutation of its columns (or rows). In case it is an affine bijection, the sign of all the elements of some of its columns (or rows) are changed.*

Corollary 3. *As a corollary of Lemma 1, we get the following:*

$$\begin{array}{l}\overset{*}{\max}\,(\mathsf{WS}(L_{\mathsf{A},\mathbf{b}} \circ F \circ L_{\mathsf{C},\mathbf{d}})) = \overset{*}{\max}\,(\mathsf{WS}(F)) \\ \overset{*}{\max}\,(\mathsf{DP}(L_{\mathsf{A},\mathbf{b}} \circ F \circ L_{\mathsf{C},\mathbf{d}})) = \overset{*}{\max}\,(\mathsf{DP}(F))\end{array}$$

Corollary 4. *The nonlinearity and the linearity distance are invariant under linear (or affine) bijections of the input space and of the output space, so that Nyberg (1995):*

$$\mathcal{NL}(L_{\mathsf{A},\mathbf{b}} \circ F \circ L_{\mathsf{C},\mathbf{d}}) = \mathcal{NL}(F) \;\; \mathcal{LD}(L_{\mathsf{A},\mathbf{b}} \circ F \circ L_{\mathsf{C},\mathbf{d}}) = \mathcal{LD}(F)$$

Here we give alternative proofs as those given by Nyberg in Nyberg (1995) by using corollary 3:

Proof.

$$\begin{array}{l}\mathcal{NL}(L_{\mathsf{A},\mathbf{b}} \circ F \circ L_{\mathsf{C},\mathbf{d}}) = 2^{n-1} - \frac{1}{2}\overset{*}{\max}\,(\mathsf{WS}(L_{\mathsf{A},\mathbf{b}} \circ F \circ L_{\mathsf{C},\mathbf{d}})) \\ = 2^{n-1} - \frac{1}{2}\overset{*}{\max}\,(\mathsf{WS}(F)) = \mathcal{NL}(F)\end{array}$$

$$\begin{array}{l}\mathcal{LD}(L_{\mathsf{A},\mathbf{b}} \circ F \circ L_{\mathsf{C},\mathbf{d}}) = 2^{n-1} \cdot \left(1 - \overset{*}{\max}\,(\mathsf{DP}(L_{\mathsf{A},\mathbf{b}} \circ F \circ L_{\mathsf{C},\mathbf{d}}))\right) \\ = 2^{n-1} \cdot \left(1 - \overset{*}{\max}\,(\mathsf{DP}(F))\right) = \mathcal{LD}(F)\end{array}$$

□

Theorem 8. *Let $F \in \mathcal{F}_{n,m}$ and let $L_{\mathbf{A},\mathbf{b}} \in \mathcal{F}_{n,n}$ an affine bijection, then $F \circ L_{\mathbf{A},\mathbf{b}}$ satisfies the $PC(l)$ if and only if F satisfies the $PC(l)$.*

Proof. If we use the equality $r_{F\circ L_{\mathrm{A,b}}}(\mathbf{u},\mathbf{v}) = r_F(\mathsf{A}\mathbf{u},\mathbf{v})$ described in Millan (1998), we can obtain the following:

$$
\begin{aligned}
& F \circ L_{\mathbf{A},\mathbf{b}} \text{ satisfies the } PC(l) \\
& \longleftrightarrow r_{F\circ L_{\mathrm{A,b}}} = 0,\ \forall\, \mathbf{u} \in \mathrm{V_n},\ 1 \leq wt(\mathbf{u}) \leq l,\ \forall\, \mathbf{v} \in \mathrm{V_m} \\
& \longleftrightarrow r_F(\mathsf{A}\mathbf{u},\mathbf{v}) = 0,\ \forall\, \mathbf{u} \in \mathrm{V_n},\ 1 \leq wt(\mathbf{u}) \leq l,\ \forall\, \mathbf{v} \in \mathrm{V_m} \\
& \longleftrightarrow r_F(\mathbf{u},\mathbf{v}) = 0,\ \forall\, \mathbf{u} \in \mathrm{V_n},\ 1 \leq wt(\mathbf{u}) \leq l,\ \forall\, \mathbf{v} \in \mathrm{V_m}
\end{aligned}
$$

□

4.3 Adding coordinate functions

Let $F = (f_1,\ldots,f_{m_1}) \in \mathcal{F}_{n,m_1}$, $G = (g_1,\ldots,g_{m_2}) \in \mathcal{F}_{n,m_2}$ and the function conformed by adding the coordinate functions $(F,G) = (f_1,\ldots,f_{m_1},g_1,\ldots,g_{m_2}) \in \mathcal{F}_{n,m_1+m_2}$. Let $\mathbf{v} \in \mathrm{V_{m_1+m_2}}$,$\mathbf{v_F} \in \mathrm{V_{m_1}}$ and $\mathbf{v_G} \in \mathrm{V_{m_2}}$ so that $\mathbf{v} = \mathbf{v_F} \oplus \mathbf{v_G}$.

Theorem 9. *The columns of the Walsh Spectrum of the Vector Boolean function constructed by adding the coordinate functions of two Vector Boolean functions are calculated by the correlation of their respective columns in the following way:*

$$\mathsf{WS}((F,G))^{\mathbf{v}} = \frac{1}{2^n}\mathsf{WS}(F)^{\mathbf{v_F}} * \mathsf{WS}(G)^{\mathbf{v_G}}$$

where $\mathsf{WS}((F,G))^{\mathbf{v}}$ is the column of the Walsh Spectrum characteristiced by $\mathbf{v}$.

Proof.

$$
\begin{aligned}
& \hat{\theta}_{(F,G)}(\mathbf{u},\mathbf{v}) = \hat{\chi}_{\mathbf{v_F}\oplus\mathbf{v_G}\cdot(F,G)}(\mathbf{u}) = \mathcal{W}\{\xi_{\mathbf{v_F}\cdot F} \centerdot \xi_{\mathbf{v_G}\cdot G}\}(\mathbf{u}) \\
& = \tfrac{1}{2^n}\textstyle\sum_{\mathbf{x}\in \mathrm{V_n}} \hat{\chi}_{\mathbf{v_F}\cdot F}(\mathbf{u}+\mathbf{x})\hat{\chi}_{\mathbf{v_G}\cdot G}(\mathbf{x})
\end{aligned}
$$

□

Corollary 5. *The exact value of the nonlinearity of (F,G) cannot be easily obtained from the knowledge of the nonlinearities of F and G.*

Corollary 6. *The columns of both $\mathsf{WS}(F)$ and $\mathsf{WS}(G)$ are contained in the matrix $\mathsf{WS}((F,G))$.*

Corollary 7. *From corollary 6 it can be deduced that:*

$$\mathcal{NL}((F,G)) \leq \min\{\mathcal{NL}(F),\ \mathcal{NL}(G)\} \tag{19}$$

The corollary 7 is a generalization of the Theorem 16 in Nyberg (1995). It can be useful, for instance, to find upper bounds of nonlinearity in S-boxes whose number of output bits is high by calculating the nonlinearities of shorter S-boxes (see Example 2).

Example 1. *The F-function of the MacGuffin block cipher algorithm consists of the* 8 *S-boxes of the DES, but the two middle output bits of each S-box are neglected so that* $S_i(MacG) \in \mathcal{F}_{6,2}$. *Let define the* 4*-th S-box of DES as* $S_4(DES) = (f_1, f_2, f_3, f_4)$, *then it holds that* $S_4(MacG) = (f_1, f_4)$. *If we denote MacDES the S-box which uses the second and third component functions of DES, then* $S_4(MacDES) = (f_2, f_3)$. *The S-box* $S_4(DES)$ *can be obtained by adding the coordinate functions which constitute MacDES and aplying a permutation to reorder the coordinate functions. If we want to obtain the last column of the Walsh Spectrum of* $S_4(DES)$ *from the last columns of the Walsh Spectra of* $S_4(MacG)$ *and* $S_4(MacDES)$, *then the effect of the permutation can be omitted and the results are the following:*

$$\mathsf{WS}\left(S_4(DES)\right)^{(\mathbf{1111})} = \tfrac{1}{2^6}\mathsf{WS}\left(S_4(MacG)\right)^{(\mathbf{11})} * \mathsf{WS}\left(S_4(MacDES)\right)^{(\mathbf{11})} \tag{20}$$

Example 2. *The first substitution function of the CAST algorithm Adams & Tavares (1993) , Adams (1994) denoted by* $S_1 \in \mathcal{F}_{8,32}$ *has a nonlinearity of* 74 *Youssef et al. (1997). If we decompose this Vector Boolean function into two, taking the first* 16 *output bits* ($S_{1a} \in \mathcal{F}_{8,16}$) *and the second* 16 *output bits* ($S_{1b} \in \mathcal{F}_{8,16}$) *respectively, we can see that the corollary 7 is satisfied:*

$$74 = \mathcal{NL}(S_1) \leq \min\{\mathcal{NL}(S_{1a}),\ \mathcal{NL}(S_{1b})\} = \min\{86,\ 82\} \tag{21}$$

Theorem 10. *If* $F, G \in \mathcal{F}_{n,n}$ *are bijective,* F^{-1} *is a* t_1*-resilient function and* G^{-1} *is a* t_2*-resilient function, then the inverse of the Vector Boolean function obtained by adding the coordinates functions of F and G, denoted by* $(F, G)^{-1} \in \mathcal{F}_{2n,n}$ *is a* $2 \cdot \min\{t_1, t_2\}$*-resilient function.*

Proof.

$$\begin{aligned}
&F^{-1} \text{ is a } t_1\text{-resilient function } \wedge\ G^{-1} \text{ is a } t_2\text{-resilient function}\\
&\leftrightarrow \hat{\theta}_F(\mathbf{v}, \mathbf{u_F}) = 0,\ \forall\, \mathbf{v} \neq \mathbf{0} \in \mathrm{V_n},\ \forall\, \mathbf{u_F} \in \mathrm{V_n},\ 0 \leq wt(\mathbf{u_F}) \leq t_1\\
&\wedge\ \hat{\theta}_G(\mathbf{v}, \mathbf{u_G}) = 0,\ \forall\, \mathbf{v} \neq \mathbf{0} \in \mathrm{V_n},\ \forall\, \mathbf{u_G} \in \mathrm{V_n},\ 0 \leq wt(\mathbf{u_G}) \leq t_2\\
&\leftrightarrow \hat{\theta}_{(F,G)^{-1}}(\mathbf{u}, \mathbf{v}) = 0\ \forall\, \mathbf{u} \in \mathrm{V_{2n}},\ 0 \leq wt(\mathbf{u}) \leq 2 \cdot \min\{t_1, t_2\},\ \forall\, \mathbf{v} \neq \mathbf{0} \in \mathrm{V_n}
\end{aligned}$$

where $\mathbf{u} = \mathbf{u_F} \oplus \mathbf{u_G}$ □

Corollary 8. *If* $F, G \in \mathcal{F}_{n,n}$ *are bijective,* F^{-1} *is a balanced Vector Boolean function and* G^{-1} *is a balanced Vector Boolean function, then the inverse of the Vector Boolean function resulting of adding the coordinates functions of F and G, denoted by* $(F, G)^{-1}$ *is a balanced Vector Boolean function.*

Theorem 11. *The autocorrelation of the Vector Boolean function resulting by adding the coordinate functions of two Vector Boolean functions can be expressed in terms of their respective directional derivatives as follows:*

$$r_{(F,G)}(\mathbf{u}, \mathbf{v}) = \tfrac{1}{2^n} \textstyle\sum_{\mathbf{x} \in \mathrm{V_n}} (-1)^{\Delta_{\mathbf{u}} \mathbf{v_F} F(\mathbf{x})} \cdot (-1)^{\Delta_{\mathbf{u}} \mathbf{v_G} G(\mathbf{x})}$$

Proof.

$$\begin{aligned}
&r_{(F,G)}(\mathbf{u}, \mathbf{v}) = \tfrac{1}{2^n} \textstyle\sum_{\mathbf{x} \in \mathrm{V_n}} (-1)^{\mathbf{v_F} \oplus \mathbf{v_G}(F,G)(\mathbf{x}+\mathbf{u}) + \mathbf{v_F} \oplus \mathbf{v_G}(F,G)(\mathbf{x})}\\
&= \tfrac{1}{2^n} \textstyle\sum_{\mathbf{x} \in \mathrm{V_n}} (-1)^{\mathbf{v_F} F(\mathbf{x}+\mathbf{u}) \oplus \mathbf{v_G} G(\mathbf{x}+\mathbf{u}) + \mathbf{v_F} F(\mathbf{x}) \oplus \mathbf{v_G} G(\mathbf{x})}\\
&= \tfrac{1}{2^n} \textstyle\sum_{\mathbf{x} \in \mathrm{V_n}} (-1)^{\mathbf{v_F} F(\mathbf{x}+\mathbf{u}) + \mathbf{v_F} F(\mathbf{x})} \cdot (-1)^{\mathbf{v_G} G(\mathbf{x}+\mathbf{u}) + \mathbf{v_G} G(\mathbf{x})}
\end{aligned}$$

□

Corollary 9. *If* $\mathbf{u}$ *is a linear structure of* G*, then the autocorrelation of* (F, G) *is proportional to the autocorrelation of* F*:*

$$r_{(F,G)}(\mathbf{u}, \mathbf{v}) = (-1)^{c_{\mathbf{v_G}G}} \cdot r_F(\mathbf{u}, \mathbf{v_F})$$

where $\Delta_{\mathbf{u}}\mathbf{v_G}G(\mathbf{x}) = c_{\mathbf{v_G}G}\ \forall\, \mathbf{x} \in \mathrm{V_n}, \forall\, \mathbf{v_G} \in \mathrm{V_{m_2}}$.

Corollary 10. *Let* $F \in \mathcal{F}_{n,m_1}$ *satisfy the* $PC(l)$ *and let all the vectors in* $\mathrm{V_n}$ *with weight at most* l *be linear structures of* $G \in \mathcal{F}_{n,m_2}$*, then* $(F, G) \in \mathcal{F}_{n,m_1+m_2}$ *satisfies* $PC(l)$*.*

Proof. By applying corollary 10:

$$r_F(\mathbf{u}, \mathbf{v_F}) = 0,\ \forall\, \mathbf{u} \in \mathrm{V_n},\ 1 \leq wt(\mathbf{u}) \leq l,\ \forall\, \mathbf{v_F} \neq \mathbf{0} \in \mathrm{V_{m_1}}$$
$$r_{(F,G)}(\mathbf{u}, \mathbf{v}) = 0,\ \forall\, \mathbf{u} \in \mathrm{V_n},\ 1 \leq wt(\mathbf{u}) \leq l,\ \forall\, \mathbf{v} \neq \mathbf{0} \in \mathrm{V_m}$$

□

Corollary 11. *If we add coordinates of a Vector Boolean function which satisfies the* $PC(l)$ *and a Linear (or Affine) Vector Boolean function then the resulting Vector Boolean function satisfies the* $PC(l)$*.*

Corollary 12. *If* $\mathbf{u}$ *is a linear structure of* G*, then the coefficients of the Differential Profile of* (F, G) *is proportional to the coefficients of the Differential Profile of* F*:*

$$\delta_{(F,G)}(\mathbf{u}, \mathbf{v}) = (-1)^{c_{\mathbf{v_G}G}} \cdot \delta_F(\mathbf{u}, \mathbf{v_F})$$

Proof.

$$\begin{aligned}
&\delta_{(F,G)}(\mathbf{u}, \mathbf{v}) = \tfrac{1}{2^{n+m}} \textstyle\sum_{\mathbf{w} \in \mathrm{V_m}} r_{(F,G)}(\mathbf{u}, \mathbf{w}) \chi_{\mathbf{v}}(\mathbf{w}) \\
&= \tfrac{1}{2^{n+m_1+m_2}} \textstyle\sum_{\mathbf{w_F} \in \mathrm{V_{m_1}}} \sum_{\mathbf{w_G} \in \mathrm{V_{m_2}}} (-1)^{c_{\mathbf{v_G}G}} r_F(\mathbf{u}, \mathbf{w_F}) \chi_{\mathbf{v_F}}(\mathbf{w_F}) \chi_{\mathbf{v_G}}(\mathbf{w_G}) \\
&= \tfrac{(-1)^{c_{\mathbf{v_G}G}}}{2^{n+m_1+m_2}} \textstyle\sum_{\mathbf{w_G} \in \mathrm{V_{m_2}}} \chi_{\mathbf{v_G}}(\mathbf{w_G}) \sum_{\mathbf{w_F} \in \mathrm{V_{m_1}}} r_F(\mathbf{u}, \mathbf{w_F}) \chi_{\mathbf{v_F}}(\mathbf{w_F}) \\
&= \tfrac{(-1)^{c_{\mathbf{v_G}G}}}{2^{n+m_1}} \textstyle\sum_{\mathbf{w_F} \in \mathrm{V_{m_1}}} r_F(\mathbf{u}, \mathbf{w_F}) \chi_{\mathbf{v_F}}(\mathbf{w_F})
\end{aligned}$$

□

4.4 Projection of a Vector Boolean function

Let $F = (f_1, \ldots, f_m) \in \mathcal{F}_{n,m}$, $\mathsf{A} = \{i_1, \ldots, i_{m_1}\} \subseteq \{1, \ldots, m\}$, $\mathsf{B} = \{j_1, \ldots, j_{m_2}\} \subseteq \{1, \ldots, m\}, \mathsf{A} \cap \mathsf{B} = \emptyset$ so that $m = m_1 + m_2$ then $F|_{\mathsf{A}} = (f_{i_1}, \ldots, f_{i_{m_1}}) \in \mathcal{F}_{n,m_1}$ and $F|_{\mathsf{B}} = (f_{j_1}, \ldots, f_{j_{m_2}}) \in \mathcal{F}_{n,m_2}$.

Corollary 13. *By Theorem 9, it can be demonstrated that the Walsh spectrum of the projection* $F|_{\mathsf{A}}$ *is obtained by extracting the columns of* $\mathsf{WS}(F)$ *characteristiced by* $\mathbf{v} = (v_1, \ldots, v_m)$ *so that if* $i \in \mathsf{A}$ *then* $v_i = 1$ *and if* $i \notin \mathsf{A}$ *then* $v_i = 0$*.*

Theorem 12. *The set of vectors where the difference Vector Boolean function of* F *in the direction of* $\mathbf{u} \in \mathrm{V_n}$ *coincides with* $\mathbf{v} \in \mathrm{V_m}$ *is a subset of the respective set of vectors of* $F|_{\mathsf{A}}$*.*

Proof. Let $\mathbf{v} = \mathbf{v}|_{\mathsf{A}} \oplus \mathbf{v}|_{\mathsf{B}}$:

$$D_F(\mathbf{u},\mathbf{v}) = \{\mathbf{x} \in \mathrm{V_n} \mid F(\mathbf{x}+\mathbf{u}) + F(\mathbf{x}) = \mathbf{v}\} = \{\mathbf{x} \in \mathrm{V_n} \mid F|_{\mathsf{A}}(\mathbf{x}+\mathbf{u}) + F|_{\mathsf{A}}(\mathbf{x}) = \mathbf{v}|_{\mathsf{A}}\}$$
$$\cap \{\mathbf{x} \in \mathrm{V_n} \mid F|_{\mathsf{B}}(\mathbf{x}+\mathbf{u}) + F|_{\mathsf{B}}(\mathbf{x}) = \mathbf{v}|_{\mathsf{B}}\} \subseteq D_{F|_{\mathsf{A}}}(\mathbf{u},\mathbf{v})$$

□

Corollary 14. $\overset{*}{\max}\,(\mathsf{WS}(F|_{\mathsf{A}}) \leq \overset{*}{\max}\,(\mathsf{WS}(F))$, $\overset{*}{\max}\,(\mathsf{DP}(F|_{\mathsf{A}}) \geq \overset{*}{\max}\,(\mathsf{DP}(F))$.

Corollary 15. $\mathcal{NL}(F|_{\mathsf{A}}) \geq \mathcal{NL}(F)$, $\mathcal{LD}(F|_{\mathsf{A}}) \leq \mathcal{LD}(F)$.

Example 3. *The F-function of the DES block cipher algorithm consists of 8 S-boxes $S_i(DES) \in \mathcal{F}_{6,4}$ whose respective nonlinearities and linearity distances are the following:*

i	1	2	3	4	5	6	7	8
$\mathcal{NL}(S_i(DES))$	14	16	16	16	16	18	14	16
$\overset{*}{\max}\,(\mathsf{WS}(S_i(DES)))$	36	32	32	32	32	28	36	32

$$\mathcal{LD}(S_i(DES)) = 24, dp(S_i(DES)) = \tfrac{1}{4}\ \forall\, i = 1,\ldots,8$$

MacGuffin's S-boxes result from restriction of DES S-Boxes, and its characteristics satisfy Corollary 15:

i	1	2	3	4	5	6	7	8
$\mathcal{NL}(S_i(MG))$	18	18	18	16	20	20	18	20
$\overset{*}{\max}\,(\mathsf{WS}(S_i(MG)))$	28	28	28	32	24	24	28	24

and

$$\begin{aligned}
&\mathcal{LD}(S_1(MG)) = 15,\ \ dp(S_1(MG)) = 0.53125\\
&\mathcal{LD}(S_2(MG)) = 14,\ \ dp(S_2(MG)) = 0.5625\\
&\mathcal{LD}(S_3(MG)) = 15,\ \ dp(S_3(MG)) = 0.53125\\
&\mathcal{LD}(S_4(MG)) = 16,\ \ dp(S_4(MG)) = 0.5\\
&\mathcal{LD}(S_5(MG)) = 16,\ \ dp(S_5(MG)) = 0.5\\
&\mathcal{LD}(S_6(MG)) = 18,\ \ dp(S_6(MG)) = 0.4375\\
&\mathcal{LD}(S_7(MG)) = 15,\ \ dp(S_7(MG)) = 0.53125\\
&\mathcal{LD}(S_8(MG)) = 16,\ \ dp(S_8(MG)) = 0.5
\end{aligned}$$

Corollary 16. *By Theorem 9, it can be demonstrated that if F is t-resilient, then $F|_{\mathsf{A}}$ is at least t-resilient.*

4.5 Direct sum of Vector Boolean functions

Let $n_1, n_2 \geq 1$, $F_1 \in \mathcal{F}_{n_1,m}, F_2 \in \mathcal{F}_{n_2,m}$ and their direct sum $F_1 \oplus F_2 \in \mathcal{F}_{n_1+n_2,m}$. Let $\mathbf{u_1} \in \mathrm{V_{n_1}}$, $\mathbf{u_2} \in \mathrm{V_{n_2}}$, $\mathbf{v} \in \mathrm{V_m}$ and $\mathbf{u} = \mathbf{u_1} \oplus \mathbf{u_2}$.

Theorem 13. *The elements which conform a row in the Walsh Spectrum of the direct sum of two Vector Boolean functions are equal to the product of the respective components of the rows in both Walsh Spectra . The rows of the Differential Profile of the direct sum of two Vector Boolean functions are obtained by the correlation of the rows of the Differential Profiles of each Vector Boolean function.*

$$\hat{\theta}_{F_1 \oplus F_2}(\mathbf{u},\mathbf{v}) = \hat{\theta}_{F_1}(\mathbf{u_1},\mathbf{v}) \cdot \hat{\theta}_{F_2}(\mathbf{u_2},\mathbf{v})$$

$$\mathsf{DP}(F_1 \oplus F_2)_{\mathbf{u}} = \frac{1}{2^m}\mathsf{DP}(F_1)_{\mathbf{u_1}} * \mathsf{DP}(F_2)_{\mathbf{u_2}}$$

The first result was already known for Boolean functions Sarkar & Maitra (2000a), here we give a proof for Vector Boolean functions.

Proof.

$$\hat{\theta}_{F_1 \oplus F_2}(\mathbf{u}, \mathbf{v}) = \hat{\chi}_{\mathbf{v} \cdot (F_1 \oplus F_2)}(\mathbf{u_1} \oplus \mathbf{u_2}) = \hat{\chi}_{\mathbf{v} \cdot F_1 \oplus \mathbf{v} \cdot F_2}(\mathbf{u_1} \oplus \mathbf{u_2}) = \hat{\chi}_{\mathbf{v} \cdot F_1}(\mathbf{u_1}) \cdot \hat{\chi}_{\mathbf{v} \cdot F_2}(\mathbf{u_2})$$

□

The second result is new and the proof is given below:

Proof.

$$\begin{aligned}
&(\mathsf{DP}(F_1)_{\mathbf{u_1}} * \mathsf{DP}(F_2)_{\mathbf{u_2}})(\mathbf{v}) = \textstyle\sum_{\mathbf{w} \in \mathrm{V_m}} \delta_{F_1}(\mathbf{u_1}, \mathbf{w} + \mathbf{v}) \cdot \delta_{F_2}(\mathbf{u_2}, \mathbf{w}) \\
&= \textstyle\sum_{\mathbf{w} \in \mathrm{V_m}} \frac{1}{2^{n_1+m}} \sum_{\mathbf{s} \in \mathrm{V_m}} r_{F_1}(\mathbf{u_1}, \mathbf{s}) \chi_{\mathbf{w}+\mathbf{v}}(\mathbf{s}) \frac{1}{2^{n_2+m}} \sum_{\mathbf{t} \in \mathrm{V_m}} r_{F_2}(\mathbf{u_2}, \mathbf{t}) \chi_{\mathbf{w}}(\mathbf{t}) \\
&= \textstyle\frac{1}{2^{n_1+n_2+2m}} \sum_{\mathbf{z} \in \mathrm{V_m}} r_{F_1}(\mathbf{u_1}, \mathbf{z}) r_{F_2}(\mathbf{u_2}, \mathbf{z}) \chi_{\mathbf{v}}(\mathbf{z}) \\
&= \textstyle\frac{1}{2^{n+2m}} \sum_{\mathbf{z} \in \mathrm{V_m}} r_{F_1 \oplus F_2}(\mathbf{u}, \mathbf{z}) \chi_{\mathbf{v}}(\mathbf{z}) = \frac{1}{2^m} \mathsf{DP}(F_1 \oplus F_2)_{\mathbf{u}}(\mathbf{v})
\end{aligned}$$

□

Corollary 17.

$$\overset{*}{\max}\,(\mathsf{WS}(F_1 \oplus F_2)) = \max_{\mathbf{v} \in \mathrm{V_m}} \{\overset{*}{\max}\,(\mathsf{WS}(\mathbf{v} \cdot F_1)) \cdot \overset{*}{\max}\,(\mathsf{WS}(\mathbf{v} \cdot F_2)\} \tag{22}$$

Corollary 18.

$$\mathcal{NL}(F_1 \oplus F_2) = 2^{n_1+n_2-1} - \tfrac{1}{2} \max_{\mathbf{v} \in \mathrm{V_m}} \{(2^{n_1} - 2\mathcal{NL}(\mathbf{v} \cdot F_1))\,(2^{n_2} - 2\mathcal{NL}(\mathbf{v} \cdot F_2))\}$$

Proof.

$$\begin{aligned}
&\mathcal{NL}(F_1 \oplus F_2) = 2^{n-1} - \tfrac{1}{2} \overset{*}{\max}\,(\hat{\theta}_{F_1 \oplus F_2}(\mathbf{u}, \mathbf{v})) \\
&= 2^{n-1} - \tfrac{1}{2} \max_{\mathbf{v} \in \mathrm{V_m}} \{\overset{*}{\max}\,(\hat{\theta}_{F_1}(\mathbf{u_1}, \mathbf{v})) \cdot \overset{*}{\max}\,(\hat{\theta}_{F_2}(\mathbf{u_2}, \mathbf{v}))\} \\
&= 2^{n_1+n_2-1} - \tfrac{1}{2} \max_{\mathbf{v} \in \mathrm{V_m}} \{(2^{n_1} - 2\mathcal{NL}(\mathbf{v} \cdot F_1))\,(2^{n_2} - 2\mathcal{NL}(\mathbf{v} \cdot F_2))\}
\end{aligned}$$

□

This result is a generalization of what is obtained for Boolean functions. Let $f \in \mathcal{F}_{n_1}, g \in \mathcal{F}_{n_2}$ then $f \oplus g \in \mathcal{F}_{n_1+n_2}$ holds that:

$$\mathcal{NL}(f \oplus g) = 2^{n_1+n_2-1} - \tfrac{1}{2}\,(2^{n_1} - 2\mathcal{NL}(f))\,(2^{n_2} - 2\mathcal{NL}(g))$$

Corollary 19. *Let* $F_1 \oplus \cdots \oplus F_i \in \mathcal{F}_{n_i,m}$

$$\begin{aligned}
&\mathcal{NL}(F_1 \oplus \cdots \oplus F_i) = \\
&= 2^{n-1} - \tfrac{1}{2} \max_{\mathbf{v} \in \mathrm{V_m}} \{\overset{*}{\max}\,(\mathsf{WS}(\mathbf{v} \cdot F_1)) \cdots \overset{*}{\max}\,(\mathsf{WS}(\mathbf{v} \cdot F_i))\}
\end{aligned} \tag{23}$$

Example 4. *The full substitution function of the CAST algorithm $S(CAST) \in \mathcal{F}_{32,32}$ is constructed by forming the direct sum of 4 S-boxes $S_i(CAST) \in \mathcal{F}_{8,32}$ satisfying:*

$$\begin{array}{l} \max_{\mathbf{v}\in V_{32}}\{\overset{*}{\max}\,(\mathsf{WS}\,(\mathbf{v}\cdot S_1(CAST)))\cdot \overset{*}{\max}\,(\mathsf{WS}\,(\mathbf{v}\cdot S_2(CAST)))\cdot \\ \overset{*}{\max}\,(\mathsf{WS}\,(\mathbf{v}\cdot S_3(CAST)))\cdot \overset{*}{\max}\,(\mathsf{WS}\,(\mathbf{v}\cdot S_4(CAST)))\} = 29417472 \end{array} \tag{24}$$

For the exact calculation of the $S(CAST)$ nonlinearity we need to find out the maximum value from all the elements of a $2^{32}\times 2^{32}$ matrix representing its Walsh Spectrum, or alternatively, to determine the Walsh Spectra of the 2^{32} linear combinations of its coordinate functions which are $2^{32}\times 1$ matrices. Nevertheless, by 19, the nonlinearity is obtained by calculating the maximum value of the product of the maxima values of four Walsh Spectra ($2^8\times 1$ matrices) for each of the 2^{32} linear combinations of its coordinate functions.

$$\begin{array}{l} \mathcal{NL}\,(S(CAST)) = 2^{32-1} - \frac{1}{2}29417472 = 2132774912 \\ lp\,(S(CAST)) = 4.69127\cdot 10^{-5} \end{array}$$

This result coincides with the estimation of nonlinearity done in Youssef et al. (1997).

Theorem 14. *Let F_1 be an (n_1, m, t_1) resilient function and F_2 be an (n_2, m, t_2)-resilient function, then $F_1 \oplus F_2$ is an (n_1+n_2, m, t_1+t_2+1)-resilient function.*

Here we give alternative proof as those given in Zhang & Zheng (1997):

Proof. For all $\mathbf{u}\in V_{n_1+n_2}$ satisfying $wt(\mathbf{u}) = t_1+t_2+1$, exists either $\mathbf{u_1}\in V_{n_1}$ with $wt(\mathbf{u_1}) = t_1+1$ and $\mathbf{u_2}\in V_{n_2}$ with $wt(\mathbf{u_2}) = t_2$ so that $\mathbf{u} = \mathbf{u_1}\oplus\mathbf{u_2}$ or $\mathbf{u_1}\in V_{n_1}$ with $wt(\mathbf{u_1}) = t_1$ and $\mathbf{u_2}\in V_{n_2}$ with $wt(\mathbf{u_2}) = t_2+1$ so that $\mathbf{u} = \mathbf{u_1}\oplus\mathbf{u_2}$. In both scenarios, it holds that:

$$\begin{array}{l} \hat{\theta}_{F_1}(\mathbf{u_1},\mathbf{v})\cdot\hat{\theta}_{F_2}(\mathbf{u_2},\mathbf{v}) = 0,\ \forall\,\mathbf{u}\in V_{n_1+n_2},\ 0\le wt(\mathbf{u})\le t_1+t_2+1,\ \forall\,\mathbf{v}\neq\mathbf{0}\in V_m \\ \longrightarrow \hat{\theta}_{F_1\oplus F_2}(\mathbf{u},\mathbf{v}) = 0,\ \forall\,\mathbf{u}\in V_{n_1+n_2},\ 0\le wt(\mathbf{u})\le t_1+t_2+1,\ \forall\,\mathbf{v}\neq\mathbf{0}\in V_m \end{array}$$

□

Corollary 20. *Let F_1 anf F_2 balanced functions, then $F_1\oplus F_2$ is an $(n_1+n_2, m, 1)$-resilient function. This result is an extension of what was obtained in Seberry & Zhang (1993) for Boolean functions.*

Theorem 15. *The elements which conform a row in the Autocorrelation Spectrum of the direct sum of two Boolean functions are obtained by the product of the respective components of the rows in both Autocorrelation Spectra. Let $f_1\in\mathcal{F}_{n_1}, f_2\in\mathcal{F}_{n_2}$, then:*

$$r_{f_1\oplus f_2}(\mathbf{u}) = r_{f_1}(\mathbf{u_1})\cdot r_{f_2}(\mathbf{u_2})$$

Proof.

$$\begin{array}{l} r_{f_1\oplus f_2}(\mathbf{u}) = \frac{1}{2^n}\sum_{\mathbf{x}\in V_n}\chi_{f_1\oplus f_2}(\mathbf{x}+\mathbf{u})\chi_{f_1\oplus f_2}(\mathbf{x}) \\ = \frac{1}{2^{n_1+n_2}}\sum_{\mathbf{x_1}\in V_{n_1}}\sum_{\mathbf{x_2}\in V_{n_2}}\chi_{f_1}(\mathbf{x_1})\chi_{f_2}(\mathbf{x_2})\chi_{f_1}(\mathbf{x_1}+\mathbf{u_1})\chi_{f_2}(\mathbf{x_2}+\mathbf{u_2}) \\ = \left(\frac{1}{2^{n_1}}\sum_{\mathbf{x_1}\in V_{n_1}}\chi_{f_1}(\mathbf{x_1}+\mathbf{u_1})\chi_{f_1}(\mathbf{x_1})\right)\left(\frac{1}{2^{n_2}}\sum_{\mathbf{x_2}\in V_{n_2}}\chi_{f_2}(\mathbf{x_2}+\mathbf{u_2})\chi_{f_2}(\mathbf{x_2})\right) \\ = r_{f_1}(\mathbf{u_1})\cdot r_{f_2}(\mathbf{u_2}) \end{array}$$

□

Theorem 16. *Let f_1 satisfies the $PC(l_1)$ and f_2 satisfies the $PC(l_2)$, then $f_1 \oplus f_2$ satisfies the $PC(l)$ with $l = \min\{l_1, l_2\}$. Moreover, it holds that $r_{f_1 \oplus f_2}(\mathbf{u}) = 0$ for all $\mathbf{u} = \mathbf{u_1} \oplus \mathbf{u_2}$ with $wt(\mathbf{u}) = l_1 + l_2 + 1$ except those which satisfies $\mathbf{u_1} = \mathbf{0}$ or $\mathbf{u_2} = \mathbf{0}$.*

Proof. By Theorem 15 we can show:

$$
\begin{aligned}
&f_1 \text{ satisfies the } PC(l_1) \text{ and } f_2 \text{ satisfies the } PC(l_2)\\
&r_{f_1}(\mathbf{u_1}) = 0,\ \forall\, \mathbf{u_1} \in \mathrm{V}_{\mathrm{n}_1},\ 1 \le wt(\mathbf{u_1}) \le l_1 \text{ and}\\
&r_{f_2}(\mathbf{u_2}) = 0,\ \forall\, \mathbf{u_2} \in \mathrm{V}_{\mathrm{n}_2},\ 1 \le wt(\mathbf{u_2}) \le l_2\\
&r_{f_1}(\mathbf{u_1}) \cdot r_{f_2}(\mathbf{u_2}) = 0,\ \forall\, \mathbf{u} = \mathbf{u_1} \oplus \mathbf{u_2} \in \mathrm{V}_{\mathrm{n}_1+\mathrm{n}_2},\ 1 \le wt(\mathbf{u}) \le \min\{l_1, l_2\}\\
&\longrightarrow r_{f_1 \oplus f_2}(\mathbf{u}) = 0,\ \forall\, \mathbf{u} \in \mathrm{V}_{\mathrm{n}_1+\mathrm{n}_2},\ 1 \le wt(\mathbf{u}) \le \min\{l_1, l_2\}
\end{aligned}
$$

Besides, for all $\mathbf{u} \in \mathrm{V}_{\mathrm{n}_1+\mathrm{n}_2}$ satisfying $wt(\mathbf{u}) = l_1 + l_2 + 1$, exists either $\mathbf{u_1} \in \mathrm{V}_{\mathrm{n}_1}$ with $wt(\mathbf{u_1}) = l_1 + 1$ and $\mathbf{u_2} \in \mathrm{V}_{\mathrm{n}_2}$ with $wt(\mathbf{u_2}) = l_2$ so that $\mathbf{u} = \mathbf{u_1} \oplus \mathbf{u_2}$ or $\mathbf{u_1} \in \mathrm{V}_{\mathrm{n}_1}$ with $wt(\mathbf{u_1}) = l_1$ and $\mathbf{u_2} \in \mathrm{V}_{\mathrm{n}_2}$ with $wt(\mathbf{u_2}) = l_2 + 1$ so that $\mathbf{u} = \mathbf{u_1} \oplus \mathbf{u_2}$. In both scenarios, it holds that:

$$r_{f_1}(\mathbf{u_1}) \cdot r_{f_2}(\mathbf{u_2}) = 0,\ \forall\, \mathbf{u} = \mathbf{u_1} \oplus \mathbf{u_2} \in \mathrm{V}_{\mathrm{n}_1+\mathrm{n}_2},\ 1 \le wt(\mathbf{u}) \le l_1 + l_2 + 1$$

except those where $\mathbf{u_1} = \mathbf{0}$ because $r_{f_1}(\mathbf{0}) = 1$ and $r_{f_2}(\mathbf{u_2})$ could be non-zero or where $\mathbf{u_2} = \mathbf{0}$ because $r_{f_2}(\mathbf{0}) = 1$ and $r_{f_1}(\mathbf{u_1})$ could be non-zero. □

Example 5. *Let $f_1, f_2 \in \mathcal{F}_5$ which both satisfy $PC(2)$ where $f_1(\mathbf{x}) = x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5 + x_2x_3x_4x_5 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_5 + x_3x_4$ and $f_2(\mathbf{x}) = x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5 + x_2x_3x_4x_5 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_5 + x_3x_4 + x_1 + x_2 + x_3 + x_4 + x_5$. By Theorem 16 then $f_1 \oplus f_2$ satisfies $PC(2)$.*

4.6 Bricklayer of Vector Boolean functions

Let $n_1, n_2, m_1, m_2 \ge 1$ and $F_1 \in \mathcal{F}_{n_1,m_1}$, $F_2 \in \mathcal{F}_{n_2,m_2}$ and the Bricklayer function $F_1|F_2 \in \mathcal{F}_{n_1+n_2,m_1+m_2}$. Let $\mathbf{u_1} \in \mathrm{V}_{\mathrm{n}_1}$, $\mathbf{u_2} \in \mathrm{V}_{\mathrm{n}_2}$ and $\mathbf{u} = \mathbf{u_1} \oplus \mathbf{u_2}$, $\mathbf{v_1} \in \mathrm{V}_{\mathrm{m}_1}$, $\mathbf{v_2} \in \mathrm{V}_{\mathrm{m}_2}$ and $\mathbf{v} = \mathbf{v_1} \oplus \mathbf{v_2}$.

Theorem 17. *The elements which conform the Walsh Spectrum (respect. Differential Profile) of the Bricklayer of two Vector Boolean functions are obtained by the product of the respective components in both Walsh Spectra (respect. Differential Profiles).*

$$
\begin{aligned}
\hat{\theta}_{F_1|F_2}(\mathbf{u}, \mathbf{v}) &= \hat{\theta}_{F_1}(\mathbf{u_1}, \mathbf{v_1}) \cdot \hat{\theta}_{F_2}(\mathbf{u_2}, \mathbf{v_2})\\
\delta_{F_1|F_2}(\mathbf{u}, \mathbf{v}) &= \delta_{F_1}(\mathbf{u_1}, \mathbf{v_1}) \cdot \delta_{F_2}(\mathbf{u_2}, \mathbf{v_2})
\end{aligned}
$$

Proof.

$$\hat{\theta}_{F_1|F_2}(\mathbf{u}, \mathbf{v}) = \hat{\chi}_{(\mathbf{v_1}, \mathbf{v_2}) \cdot (F_1|F_2)}((\mathbf{u_1}, \mathbf{u_2})) = \hat{\chi}_{\mathbf{v_1} \cdot F_1}(\mathbf{u_1}) \cdot \hat{\chi}_{\mathbf{v_2} \cdot F_2}(\mathbf{u_2})$$

□

Proof.

$$
\begin{aligned}
&\delta_{F_1|F_2}(\mathbf{u}, \mathbf{v}) = \tfrac{1}{2^{n+m}} \textstyle\sum_{\mathbf{w} \in \mathrm{V}_{\mathrm{m}}} r_{F_1|F_2}(\mathbf{u}, \mathbf{w}) \chi_{\mathbf{v}}(\mathbf{w})\\
&= \tfrac{1}{2^{n+m}} \textstyle\sum_{\mathbf{w} \in \mathrm{V}_{\mathrm{m}}} r_{F_1|F_2}(\mathbf{u_1}, \mathbf{w}) r_{F_1|F_2}(\mathbf{u_2}, \mathbf{w}) \chi_{\mathbf{v_1}}(\mathbf{w}) \chi_{\mathbf{v_2}}(\mathbf{w})\\
&= \left(\tfrac{1}{2^{n_1+m_1}} \textstyle\sum_{\mathbf{w} \in \mathrm{V}_{\mathrm{m}}} r_{F_1|F_2}(\mathbf{u_1}, \mathbf{w}) \chi_{\mathbf{v_1}}(\mathbf{w}) \right) \left(\tfrac{1}{2^{n_2+m_2}} \textstyle\sum_{\mathbf{w} \in \mathrm{V}_{\mathrm{m}}} r_{F_1|F_2}(\mathbf{u_2}, \mathbf{w}) \chi_{\mathbf{v_2}}(\mathbf{w}) \right)\\
&= \delta_{F_1}(\mathbf{u_1}, \mathbf{v_1}) \cdot \delta_{F_2}(\mathbf{u_2}, \mathbf{v_2})
\end{aligned}
$$

□

Corollary 21. *The Walsh Spectrum (respectively Differential Profile) of the Bricklayer of i Vector Boolean functions $F_1|\cdots|F_i$ is equal to the Kronecker products of their Walsh Spectra (respectively Differential Profiles):*

$$\begin{aligned}\mathsf{WS}(F_1|\cdots|F_i) &= \mathsf{WS}(F_1)\otimes\cdots\otimes\mathsf{WS}(F_i)\\ \mathsf{DP}(F_1|\cdots|F_i) &= \mathsf{DP}(F_1)\otimes\cdots\otimes\mathsf{DP}(F_i)\end{aligned} \tag{25}$$

Corollary 22.

$$\begin{aligned}\mathcal{NL}(F_1|F_2) &= 2^{n_1+n_2-1} - \tfrac{1}{2}\max\{2^{n_1}(2^{n_2}-2\mathcal{NL}(F_2)), 2^{n_2}(2^{n_1}-2\mathcal{NL}(F_1))\}\\ \mathcal{LD}(F_1|F_2) &= 2^{n_1+n_2-1}\cdot(1-\max\{1-\tfrac{\mathcal{LD}(F_1)}{2^{n_1-1}}, 1-\tfrac{\mathcal{LD}(F_2)}{2^{n_2-1}}\})\end{aligned}$$

Proof. On one hand

$$\begin{aligned}&\mathcal{NL}(F_1|F_2) = 2^{n-1} - \tfrac{1}{2}\overset{*}{\max}(\hat{\theta}_{F_1|F_2}(\mathbf{u},\mathbf{v}))\\ &= 2^{n-1} - \tfrac{1}{2}\max\{\hat{\theta}_{F_1}(\mathbf{u_1},\mathbf{v_1})\cdot\max(\hat{\theta}_{F_2}(\mathbf{u_2},\mathbf{v_2})\} \text{ where } ((\mathbf{u_1},\mathbf{u_2})\neq\mathbf{0})\wedge((\mathbf{v_1},\mathbf{v_2})\neq\mathbf{0})\\ &= 2^{n-1} - \tfrac{1}{2}\max\{2^{n_1}\cdot\overset{*}{\max}(\hat{\theta}_{F_2}(\mathbf{u_2},\mathbf{v_2})), 2^{n_2}\cdot\overset{*}{\max}(\hat{\theta}_{F_1}(\mathbf{u_1},\mathbf{v_1}))\}\\ &= 2^{n_1+n_2-1} - \tfrac{1}{2}\max\{2^{n_1}\cdot(2^{n_2}-2\mathcal{NL}(F_2)), 2^{n_2}\cdot(2^{n_1}-2\mathcal{NL}(F_1))\}\end{aligned}$$

On the other hand

$$\begin{aligned}&\mathcal{LD}(F_1|F_2) = 2^{n-1}\cdot\left(1-\overset{*}{\max}(\delta_{F_1|F_2}(\mathbf{u},\mathbf{v}))\right)\\ &= 2^{n-1}\cdot(1-\max\{\delta_{F_1}(\mathbf{u_1},\mathbf{v_1})\cdot\delta_{F_2}(\mathbf{u_2},\mathbf{v_2})\}) \text{ where } ((\mathbf{u_1},\mathbf{u_2})\neq\mathbf{0})\wedge((\mathbf{v_1},\mathbf{v_2})\neq\mathbf{0})\\ &= 2^{n-1}\cdot(1-\max\{\overset{*}{\max}(\delta_{F_1}(\mathbf{u_1},\mathbf{v_1})), \overset{*}{\max}(\delta_{F_2}(\mathbf{u_2},\mathbf{v_2}))\})\\ &= 2^{n_1+n_2-1}\cdot\left(1-\max\left\{1-\tfrac{\mathcal{LD}(F_1)}{2^{n_1-1}}, 1-\tfrac{\mathcal{LD}(F_2)}{2^{n_2-1}}\right\}\right)\end{aligned}$$

□

Corollary 23. *Let $F_1|\cdots|F_i \in \mathcal{F}_{n,m}$*

$$dp(F_1|\cdots|F_i) = \max\{dp(F_1),\ldots,dp(F_i)\} \tag{26}$$

The following theorem and corollary are presented without proofs as they are very similar to the analogous in the previous subsection.

Theorem 18. *Let F_1 be an (n_1,m_1,t_1)-resilient function and F_2 be an (n_2,m_2,t_2)-resilient function, then $F_1|F_2$ is an $(n_1+n_2, m_1+m_2, t_1+t_2)$-resilient function.*

Corollary 24. *$F_1|F_2$ is an $(n_1+n_2, m, 1)$-resilient function if and only if F_1 or F_2 are balanced functions.*

Example 6. *Let denote S the result of bricklayering all DES S-boxes $S_i \in \mathcal{F}_{6,4}\ \forall\, i = 1,\ldots,8$, so that $S = S_1|\cdots|S_8$. Thanks to the corollary 22, it is possible to calculate the nonlinearity and linearity distance of S by calculating the maximum values of the Walsh Spectra and Differential Profiles of the 8 S-boxes. This algorithm deals with eight $2^6\times 2^4$ matrices instead of one $2^{48}\times 2^{32}$ matrix.*

$$\begin{aligned}&\mathcal{NL}(S) = 2^{48-1} - \tfrac{1}{2}36\cdot 2^{42} = 61572651155456\\ &lp(S) = 0.31640625\ dp(S) = \tfrac{1}{4}\\ &\mathcal{LD}(S) = 2^{48-1}\cdot\left(1-\tfrac{1}{4}\right) = 3\cdot 2^{45}\end{aligned}$$

As all $S_i \in \mathcal{F}_{6,4}\ \forall\, i = 1,\ldots,8$ are balanced S-boxes, then by Theorem 18 it holds that S is an $(48,32,7)$- resilient function.

5. Conclusions

In this chapter, several characteristics have been obtained for Vector Boolean Functions which are constructed using simpler functions combined in different ways. Precisely, the Walsh Spectrum of the overall function is obtained from the spectra of the functions when they are combined via composition, addition of coordinate functions, direct sum or bricklayer construction. In addition, when affine bijections or projection are employed, the maximum value of the overall Walsh Spectrum is obtained from the maximum values of the involved elements spectra. These results allow for the computation of nonlinearity, balancedness and resiliency of the mentioned constructions.

Alternatively, the Differential Profile of the system resulting from the composition with an affine function, direct sum, or bricklayer is also derived from the Differential Profiles of the involved elements. Moreover, when affine bijections or projections are employed, bounds on the maximum value of the Differential Profile for the resulting Function are also obtained. Therefore, the linearity distance for the cited constructions is computed.

Finally, the Autocorrelation Spectrum of a Vector Boolean Function constructed via affine bijections of Vector Boolean Functions and direct sum of Boolean functions is provided from the knowledge of the respective elements Autocorrelation Spectra. Moreover, the autocorrelation coefficients resulting from adding coordinate functions with linear structures are obtained. As a consequence, the propagation criterion resulting from the cited constructions is also provided.

5.1 Acknowledgements

This work has been partially supported by project MTM2010-15102 of Ministerio de Ciencia e Innovación, Spain, and by projects Q09 0930-182 and Q10 0930-144 of the Universidad Politécnica de Madrid (UPM), Spain.

6. References

Adams, C. (1994). Simple and effective key scheduling for symmetric ciphers, *Workshop on Selected Areas in Cryptography*, pp. 129–133.

Adams, C. M. & Tavares, S. E. (1993). Designing s-boxes for ciphers resistant to differential cryptanalysis (extended abstract), *Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography*, pp. 181–190.

Biham, E. & Shamir, A. (1991). Differential cryptanalysis of des-like cryptosystems, *Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '90, Springer-Verlag, London, UK, UK, pp. 2–21.

Blaze, M. & Schneier, B. (1995). The macguffin block cipher algorithm, *Fast Software Encryption, volume 1008 of Lecture*, Springer-Verlag, pp. 97–110.

Carlet, C. (2004). On the secondary constructions of resilient and bent functions, *Progress in Computer Science and Applied Logic* 23: 3–28.

Chabaud, F. & Vaudenay, S. (1994). Links between differential and linear cryptanalysis, *Advances in Cryptology- Eurorypt 1994*, pp. 356–365.

Chen, L., Fu, F.-W. & Wei, V. K.-W. (2004). On the constructions and nonlinearity of binary vector-output correlation-immune functions, *J. Complex.* 20: 266–283.

Daemen, J. & Rijmen, V. (2002). *The Design of Rijndael*, Springer-Verlag New York, Inc., Secaucus, NJ, USA.

Des (1977). Data encryption standard, *In FIPS PUB 46, Federal Information Processing Standards Publication*, pp. 46–2.

J. Seberry, X. Z. & Zheng, Y. (1994). Nonlinearity characteristics of quadratic substitution boxes, *Proceedings of the Workshop on SAC'94*.

Jakobsen, T. & Knudsen, L. R. (1997). The interpolation attack on block ciphers, *Proceedings of the 4th International Workshop on Fast Software Encryption*, FSE '97, Springer-Verlag, London, UK, pp. 28–40.

Maitra, S. & Pasalic, E. (2002). Further constructions of resilient boolean functions with very high nonlinearity, *IEEE Transactions on Information Theory* 48(7): 1825 –1834.

Matsui, M. (1994). Linear cryptanalysis method for des cipher, *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, EUROCRYPT '93, Springer-Verlag New York, Inc., Secaucus, NJ, USA, pp. 386–397.

Meier, W. & Staffelbach, O. (1990). Nonlinearity criteria for cryptographic functions, *Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology*, Springer-Verlag New York, Inc., New York, NY, USA, pp. 549–562.

Millan, W. L. (1998). *Analysis and Design of Boolean. Functions for Cryptographic Applications*, PhD thesis, Queensland University of Technology, Faculty of Information Technology.

Nyberg, K. (1991). Perfect nonlinear s-boxes, *Proceedings of the 10th annual international conference on Theory and application of cryptographic techniques*, EUROCRYPT'91, Springer-Verlag, Berlin, Heidelberg, pp. 378–386.

Nyberg, K. (1993). On the construction of highly nonlinear permutations, *Proceedings of the 11th annual international conference on Theory and application of cryptographic techniques*, EUROCRYPT'92, Springer-Verlag, Berlin, Heidelberg, pp. 92–98.

Nyberg, K. (1995). S-boxes and round functions with controllable linearity and differential uniformity, *in* B. Preneel (ed.), *Fast Software Encryption*, Vol. 1008 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, pp. 111–130.

Pasalic, E., Maitra, S., Johansson, T. & Sarkar, P. (2001). New constructions of resilient and correlation immune boolean functions achieving upper bound on nonlinearity, *Electronic Notes in Discrete Mathematics* 6(0): 158 – 167. WCC2001, International Workshop on Coding and Cryptography.

Pommerening, K. (2005). LinearitatsmaSSe fur boolesche abbildungen, *Technical report*, Fachbereich Mathematik der Johannes-Gutenberg-Universitaet.

Preneel, B., Van Leekwijck, W., Van Linden, L., Govaerts, R. & Vandewalle, J. (2006). Propagation characteristics of boolean functions, *in* I. DamgÃěrd (ed.), *Advances in Cryptology EUROCRYPT'90*, Vol. 473 of *Lecture Notes in Computer Science*, Springer Berlin / Heidelberg, pp. 161–173.

Rothaus, O. S. (1976). On "bent" functions., *J. Comb. Theory, Ser. A* 20(3): 300–305.

Sarkar, P. & Maitra, S. (2000a). Construction of nonlinear boolean functions with important cryptographic properties, *Proceedings of the 19th international conference on Theory and application of cryptographic techniques*, EUROCRYPT'00, Springer-Verlag, Berlin, Heidelberg, pp. 485–506.

Sarkar, P. & Maitra, S. (2000b). Nonlinearity bounds and constructions of resilient boolean functions, *Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '00, Springer-Verlag, London, UK, pp. 515–532.

Schneier, B. (1995). *Applied cryptography (2nd ed.): protocols, algorithms, and source code in C*, John Wiley & Sons, Inc., New York, NY, USA.

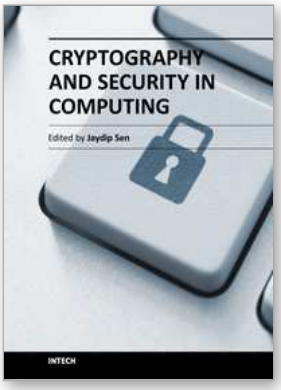
Seberry, J. & Zhang, X.-M. (1993). Highly nonlinear 0-1 balanced boolean functions satisfying strict avalanche criterion, *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology*, ASIACRYPT '92, Springer-Verlag, London, UK, pp. 145–155.

Shannon, C. E. (1949). Communication theory of secrecy systems, *Bell System Technical Journal* 28(4): 657–715.

Xiao, G.-Z. & Massey, J. (1988). A spectral characterization of correlation-immune combining functions, *IEEE Transactions on Information Theory* 34(3): 569 –571.

Youssef, A., Chen, Z. & Tavares, S. (1997). Construction of highly nonlinear injective s-boxes with application to cast-like encryption algorithms, *IEEE 1997 Canadian Conference on Electrical and Computer Engineering, 1997*, Vol. 1, pp. 330 –333 vol.1.

Zhang, X.-M. & Zheng, Y. (1997). Cryptographically resilient functions, *IEEE Transactions on Information Theory* 43(5): 1740 –1747.



Cryptography and Security in Computing

Edited by Dr. Jaydip Sen

ISBN 978-953-51-0179-6
Hard cover, 242 pages
Publisher InTech
Published online 07, March, 2012
Published in print edition March, 2012

The purpose of this book is to present some of the critical security challenges in today's computing world and to discuss mechanisms for defending against those attacks by using classical and modern approaches of cryptography and other defence mechanisms. It contains eleven chapters which are divided into two parts. The chapters in Part 1 of the book mostly deal with theoretical and fundamental aspects of cryptography. The chapters in Part 2, on the other hand, discuss various applications of cryptographic protocols and techniques in designing computing and network security solutions. The book will be useful for researchers, engineers, graduate and doctoral students working in cryptography and security related areas. It will also be useful for faculty members of graduate schools and universities.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821