Cross-Correlation Analysis of Cryptographically Useful Boolean Functions and S-Boxes*

P. Sarkar[1] and S. Maitra[2]

[1]Applied Statistics Unit, Indian Statistical Institute,
203 B.T. Road, Calcutta 700 035, India
palash@isical.ac.in

[2]Computer and Statistical Service Centre, Indian Statistical Institute,
203 B.T. Road, Calcutta 700 035, India
subho@isical.ac.in

Abstract. We use the cross-correlation function as a fundamental tool to study cryptographic properties of Boolean functions. This provides a unified treatment of a large section of Boolean function literature. In the process we generalize old results and obtain new characterizations of cryptographic properties. In particular, new characterizations of bent functions and functions satisfying propagation characteristics are obtained in terms of the cross-correlation and auto-correlation properties of subfunctions. The exact relationship between the algebraic structure of the non-zeros of the spectrum and the auto-correlation values is obtained for a cryptographically important class of functions. Finally we study the suitability of S-boxes in stream ciphers and conclude that currently known constructions for S-boxes may not be adequate for such applications.

1. Introduction

In his seminal paper on cryptography, Shannon [14] outlined the basic design principles of secret key cryptosystems. These principles were called *confusion* and *diffusion*. The principle of confusion underlines the importance of hiding the overall structure of the cryptosystem, while diffusion suggests that uncertainty is spread out evenly over the whole system.

---

* This work was done while Palash Sarkar was at the Centre for Applied Cryptographic Research, University of Waterloo.

In most secret key cryptosystems, the basic components are Boolean functions, which are maps from n-bit strings to $\{0, 1\}$. Attempts have been made to translate Shannon's notions of confusion and diffusion to properties of Boolean functions [1]. From a more practical standpoint, research in cryptanalysis of secret key systems have shown the necessity for Boolean functions to possess certain cryptographic properties.

Here we approach the design problem for Boolean functions from Shannon's standpoints of confusion and diffusion. We try to explain these concepts in terms of correlation between two Boolean functions. If two functions are highly correlated, then they are "close" to each other in a precise statistical sense. On the other hand a correlation of zero between two functions means that statistically the functions are far apart. The notion of confusion can be interpreted as meaning that the constituent functions of a secret key system should have small correlation to each other. This results in the constituent functions being "very different" from each other. Diffusion on the other hand can be interpreted as meaning that the constituent Boolean functions should have certain "uniformity" properties, leading to an overall "uniformity" of the cryptosystem.

Most works on Boolean function design have been motivated by properties which resist known attacks. While this is useful for current practice, a fundamental understanding is required in the long run. The main theoretical requirement is to understand the relationship between Shannon's informal concepts of confusion and diffusion and cryptographic properties of Boolean functions motivated by practical considerations. In this article we attempt such an investigation.

The basic tool in our study is correlation between two Boolean functions. Special forms of this correlation have already been studied. For example, the correlations of a Boolean function to linear functions constitute the spectrum of the Boolean function and have been used quite extensively in Boolean function literature. Another kind of correlation is the correlation of a function with its dyadic shifts. The values of this kind of correlation is given by the auto-correlation function.

We study the more general notion of correlation between two arbitrary functions. This is called the cross-correlation between the functions. Here we treat the cross-correlation function as a fundamental tool and present a unified view of a large section of Boolean function theory. The relationship between cross-correlation and spectra of functions is characterized. The concept of cross-correlation allows us to generalize many of the results on cryptographic properties of Boolean functions that have previously appeared in the literature. Further, we obtain new characterization of bent functions and functions satisfying propagation characteristics in terms of the cross-correlation and auto-correlation of subfunctions.

The relationship between the algebraic structure of the non-zeros of the spectrum and the auto-correlation values is characterized for functions whose non-zero spectral values have the same magnitude. This class of functions encompass several cryptographically important classes of functions. The use of S-boxes in stream ciphers have been proposed to speed up the system further. We carefully examine this proposition and conclude that the currently known constructions may not be adequate for such applications.

2. Preliminaries

An n-variable Boolean function is a map $f\colon \{0, 1\}^n \to \{0, 1\}$. In Section 7 we consider S-boxes (or vectorial functions) which are maps $f\colon \{0, 1\}^n \to \{0, 1\}^m$. Let $F_2 = GF(2)$.

We consider the domain of a Boolean function to be the vector space $(F_2^n, \oplus)$ over F_2, where $\oplus$ is used to denote the addition operator over both F_2 and the vector space F_2^n. The inner product of two vectors $u, v \in F_2^n$ will be denoted by $\langle u, v \rangle$. The weight of an n-bit vector u is the number of ones in u and will be denoted by $\mathrm{wt}(u)$.

The fundamental tool that we use in this paper is the correlation between two arbitrary Boolean functions which is called the cross-correlation. The cross-correlation between two functions f and g is an integer-valued function $C_{f,g}\colon \{0,1\}^n \to [-2^n, 2^n]$ defined by

$$C_{f,g}(u) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus g(x \oplus u)}. \tag{1}$$

Note that the quantity $C_{f,g}(0)$ denotes the correlation between the functions f and g. The following simple result states some of the basic properties of the cross-correlation function. The proof is just routine verification from the definition.

Lemma 2.1. *Let $f(x)$, $g(x)$ be n-variable functions and define $h(x) = f(x) \oplus g(x \oplus a)$ for some $a \in F_2^n$. Then* (a) $\mathrm{wt}(h(x)) = \mathrm{wt}(h(x \oplus a))$, (b) $C_{f,g}(a) = 2^n - 2 \times \mathrm{wt}(h(x))$ *and* (c) $C_{f,g}(a) = C_{g,f}(a)$.

We say that two n-variable functions f and g are *perfectly uncorrelated* if $C_{f,g}(u) = 0$ for all $u \in F_2^n$. Weaker forms of this notion are obtained by restricting the set of u for which $C_{f,g}(u) = 0$. We say that two functions are *uncorrelated of degree k* if $C_{f,g}(u) = 0$ for all $u \in F_2^n$ such that $0 \le \mathrm{wt}(u) \le k$.

We interpret Shannon's notion of confusion in the sense of heterogeneity. If the component functions of a secret key system are pairwise perfectly uncorrelated, then the statistical distance between any two functions is the maximum possible and we say that the system has the best possible confusion. However, this may be too restrictive in practice. Thus it may be desirable to enforce pairwise uncorrelatedness of degree k. Another approach could be to ensure that for each u, the values of $|C_{f,g}(u)|$ is bounded above by a "small" constant. This will ensure that the cross-correlation between the functions is uniformly small.

The Fourier Transform is the most widely used tool in the analysis of Boolean functions. In most cases it is convenient to apply the Fourier Transform to $(-1)^{f(x)}$ instead of $f(x)$. The resulting transform is called the Walsh Transform of $f(x)$. More precisely, the Walsh Transform of $f(x)$ is an integer-valued function $W_f\colon \{0,1\}^n \to [-2^n, 2^n]$ defined by (see [6])

$$W_f(u) = \sum_{w \in F_2^n} (-1)^{f(w) \oplus \langle u, w \rangle}.$$

The Walsh Transform is called the spectrum of f. Note that the spectrum measures the cross-correlations between a function and the set of linear functions. Another way of looking at the spectrum is via Hadamard matrices. Let H_n be the Hadamard matrix of order 2^n defined recursively as (see [9])

$$H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$H_n = H_1 \otimes H_{n-1} \qquad \text{for} \quad n > 1,$$

where $\otimes$ denotes the Kronecker product of two matrices. Considering the rows and columns of H_n to be indexed by the elements of F_2^n, we obtain $[H_n]_{(u,v)} = (-1)^{\langle u,v\rangle}$. Using this fact the Walsh Transform can be written as

$$[(-1)^{f(0)}, \ldots, (-1)^{f(2^n-1)}]H_n = [W_f(0), \ldots, W_f(2^n-1)].$$

Since $H_n H_n = 2^n I_{2^n}$, post-multiplying both sides by H_n, we get the inverse Walsh Transform:

$$(-1)^{f(u)} = \frac{1}{2^n} \sum_{w \in F_2^n} W_f(w)(-1)^{\langle u,w\rangle}.$$

A parameter of fundamental importance in cryptography is the non-linearity of a function (see [9]). This is defined to be the distance from the set of all affine functions. It is more convenient to define it in terms of the spectrum of a Boolean function. The non-linearity $\mathrm{nl}(f)$ of an n-variable Boolean function f, is defined as

$$\mathrm{nl}(f) = 2^{n-1} - \tfrac{1}{2} \max_{u \in F_2^n} |W_f(u)|.$$

Another commonly used tool is the auto-correlation function which provides the cross-correlation values of a function with its dyadic shifts. The auto-correlation function is an integer-valued map C_f: $\{0,1\}^n \to [-2^n, 2^n]$ defined by (see [9] for a related concept called the directional derivative)

$$C_f(u) = \sum_{w \in F_2^n} (-1)^{f(w) \oplus f(u \oplus w)}.$$

It is clear that $C_f(0) = 2^n$. The auto-correlation is not a transform in the sense that it does not uniquely determine the function.

Several important classes of Boolean functions can be described in terms of the spectrum and the auto-correlation function:

1. For even n, an n-variable function f is called *bent* if $W_f(u) = \pm 2^{n/2}$, for all $u \in F_2^n$ (see [12]). This class of functions are important in both cryptography and coding theory.
2. An n-variable function is called *correlation immune* of order m (m-CI) if $W_f(u) = 0$ for all $1 \le \mathrm{wt}(u) \le m$ (see [15] and [17]). Further, if the function is balanced, then $W_f(0) = 0$ and the function is called *m-resilient*.
3. An n-variable function is said to satisfy *propagation characteristics* of order k (PC(k)) if $C_f(u) = 0$ for all $1 \le \mathrm{wt}(u) \le k$ (see [11]).

If f is a bent function, then $C_f(u) = 0$ for all non-zero u [9]. Hence bent functions satisfy PC(n).

3. Cross-Correlation Theorem

In this section we present the Cross-Correlation Theorem and its consequences.

Theorem 3.1 (Cross-Correlation Theorem). *Let f and g be n-variable functions. Then*

$$[C_{f,g}(0), \ldots, C_{f,g}(2^n-1)]H_n = [W_f(0)W_g(0), \ldots, W_f(2^n-1)W_g(2^n-1)]. \quad (2)$$

Proof. It is sufficient to show that for each $w \in F_2^n$, $\sum_{u\in F_2^n} C_{f,g}(u)(-1)^{\langle u,w\rangle} = W_f(w)W_g(w)$. We proceed to do this as follows:

$$\begin{aligned}
\sum_{u\in F_2^n} C_{f,g}(u)(-1)^{\langle u,w\rangle} &= \sum_{u\in F_2^n}\sum_{x\in F_2^n}(-1)^{f(x)\oplus g(x\oplus u)}(-1)^{\langle u,w\rangle}\\
&= \sum_{x\in F_2^n}(-1)^{f(x)}\sum_{u\in F_2^n}(-1)^{g(x\oplus u)\oplus\langle u,w\rangle}\\
&= \sum_{x\in F_2^n}(-1)^{f(x)}\sum_{u\in F_2^n}(-1)^{g(u)\oplus\langle w,x\oplus u\rangle}\\
&= \sum_{x\in F_2^n}(-1)^{f(x)}\sum_{u\in F_2^n}(-1)^{g(u)\oplus\langle w,x\rangle\oplus\langle w,u\rangle}\\
&= \sum_{x\in F_2^n}(-1)^{f(x)\oplus\langle w,x\rangle}\sum_{u\in F_2^n}(-1)^{g(u)\oplus\langle w,u\rangle}\\
&= W_f(w)W_g(w). \qquad \square
\end{aligned}$$

A special case of the Cross-Correlation Theorem is when $f = g$ and gives us the following:

Corollary 3.1. *Let f be an n-variable function. Then*

$$[C_f(0),\ldots,C_f(2^n-1)]H_n = [W_f^2(0),\ldots,W_f^2(2^n-1)].$$

This result is called the Wiener–Khintchine Theorem in continuous analysis and has also been obtained for Boolean functions [2], [20], [11]. Applying the inverse transform to the cross-correlation vector gives the following:

Corollary 3.2. *Let f and g be n-variable functions. Then*

$$2^n[C_{f,g}(0),\ldots,C_{f,g}(2^n-1)] = [W_f(0)W_g(0),\ldots,W_f(2^n-1)W_g(2^n-1)]H_n. \quad (3)$$

Applying the inverse transform with $g = f$, gives $\sum_{u\in F_2^n} W_f^2(u) = 2^n C_f(0) = 2^{2n}$. This is a conservation law for the spectral values of f and is known as Parseval's theorem (see [6]).

Let $h(x) = f(x)\oplus g(x)$, $g_1(x) = g(x)\oplus\langle u,x\rangle$. Then $W_{g_1}(w) = W_g(u\oplus w)$ for all $w\in F_2^n$ and $W_h(u) = C_{f,g_1}(0)$. Using Corollary 3.2, this gives

$$W_h(u) = \frac{1}{2^n}\sum_{w\in F_2^n} W_f(w)W_{g_1}(w) = \frac{1}{2^n}\sum_{w\in F_2^n} W_f(w)W_g(u\oplus w),$$

which is the so-called Convolution Theorem. We summarize this as

Corollary 3.3. *Let $h(x) = f(x)\oplus g(x)$, where both f and g are n-variable functions. Then*

$$W_h(u) = \frac{1}{2^n}\sum_{w\in F_2^n} W_f(w)W_g(u\oplus w). \quad (4)$$

We say that two functions f and g have *non-intersecting spectra* if $W_f(u)W_g(u) = 0$ for all u. Using Theorem 3.1 and Corollary 3.2 we get the following characterization of perfect uncorrelatedness in terms of the spectra of f and g.

Corollary 3.4. *Let f and g be two n-variable functions. Then f and g have non-intersecting spectra if and only if they are perfectly uncorrelated.*

Remarks. 1. Let f and g be n-variable functions. Then f and g are perfectly uncorrelated if and only if $X_{n+1} \oplus f$ and $X_{n+1} \oplus g$ are perfectly uncorrelated. Further, if f and g are perfectly uncorrelated, then using $W_f(u)W_g(u) = 0$ for all $u \in F_2^n$, it is possible to show (see [13]) that the $(n+1)$-variable function h defined by $h(X_1, X_2, \ldots, X_n, X_{n+1}) = (1 \oplus X_{n+1})f(X_1, \ldots, X_n) \oplus X_{n+1}g(X_1, \ldots, X_n)$ has nonlinearity $2^{n-1} + \min(\mathrm{nl}(f), \mathrm{nl}(g))$.

2. The Walsh Transform of an n-variable Boolean function can be computed in time $O(n2^n)$ using the fast Walsh Transform [9]. Using this algorithm and Corollary 3.2 we obtain an $O(n2^n)$ algorithm to compute the cross-correlation between a pair of Boolean functions. Similarly, using the fast Walsh Transform and Corollary 3.1 we obtain an $O(n2^n)$ algorithm to compute the auto-correlation of a Boolean function.

3.1. *Algebraic Properties*

Here we study algebraic properties of cross-correlations. Using the Cross-Correlation Theorem we are able to generalize many previous results concerning cryptographic properties of Boolean functions. We present three such cases.

Proposition 3.1. *Let f and g be n-variable functions. Then $\sum_{v \in F_2^n} C_{f,g}^2(v) \leq 2^{3n}$.*

Proof. Let $W = (W_f(0)W_g(0), \ldots, W_f(0)W_g(0))$ and $C = (C_{f,g}(0), \ldots, C_{f,g}(0))$. Then

$$\langle W, W \rangle = \langle CH_n, CH_n \rangle = CH_n H_n^T C = 2^n \langle C, C \rangle.$$

Hence

$$2^n \sum_{u \in F_2^n} C_{f,g}^2(u) = \sum_{u \in F_2^n} W_f^2(u) W_g^2(u)$$

$$\leq \left(\sum_{u \in F_2^n} W_f^2(u) \right) \left(\sum_{u \in F_2^n} W_g^2(u) \right) = 2^{2n} 2^{2n} = 2^{4n}.$$

From this the result follows. □

The above generalizes the bounds on sum of squares of the auto-correlation coefficients obtained in Theorem 2 of [20].

Theorem 3.2. *Let f and g be n-variable functions and let E be a subspace of F_2^n. Then*

$$\sum_{w\in E} W_f(w)W_g(w) = |E| \sum_{u\in E^\perp} C_{f,g}(u).$$

Proof. Using Theorem 3.1, we can write

$$\begin{aligned}\sum_{w\in E} W_f(w)W_g(w) &= \sum_{w\in E}\sum_{u\in F_2^n} C_{f,g}(u)(-1)^{\langle u,w\rangle} \\ &= \sum_{u\in F_2^n}\sum_{w\in E} C_{f,g}(u)(-1)^{\langle u,w\rangle}.\end{aligned}$$

If $u \in E^\perp$, then $\langle u, w\rangle = 0$ for all $w \in E$. If $u \notin E^\perp$, then $\langle u, w\rangle = 0$ for half of the vectors $w \in E$ and $\langle u, w\rangle = 1$ for the other half of the vectors $w \in E$. Thus we get

$$\sum_{w\in E} W_f(w)W_g(w) = |E| \sum_{u\in E^\perp} C_{f,g}(u). \qquad \square$$

For the special case of $f = g$, this result has been obtained in Proposition 5 of [1].

Let N_r be the number of zeros of the auto-correlation function $C_f()$ and let N_w be the number of zeros of the spectrum $W_f()$. In Theorem 2.1 of [2] it was proved that $(2^n - N_r)(2^n - N_w) \geq 2^n$ and the condition when equality holds was precisely characterized. Here we obtain a similar relation between the zeros of the cross-correlation function of f and g and the pointwise product of the spectra of f and g.

Theorem 3.3. *Let f and g be n-variable functions. Then*

$$(2^n - N_c)(2^n - N_s) \geq \max_{u\in F_2^n} |C_{f,g}(u)|, \tag{5}$$

where $N_c = |\{u \in F_2^n\colon\ C_{f,g}(u) = 0\}|$ and $N_s = |\{u \in F_2^n\colon\ W_f(u)W_g(u) = 0\}|$.

Proof. First note that if $C_{f,g}(u) = 0$ for all $u \in F_2^n$, then $N_c = 2^n$ and the result holds. So suppose there exists some u such that $C_{f,g}(u) \neq 0$. Using Theorem 3.1, this implies that $W_f(u)W_g(u)$ cannot be zero for all u. We prove two separate lower bounds on the quantitites $2^n - N_c$ and $2^n - N_s$. Multiplying the bounds will provide the desired result.

For a pair of Boolean functions h_1 and h_2, define $n_c(h_1, h_2) = |\{u \in F_2^n\colon\ C_{h_1,h_2}(u) = 0\}|$ and $n_s(h_1, h_2) = |\{u \in F_2^n\colon\ W_{h_1}(u)W_{h_2}(u) = 0\}|$. Then $N_c = n_c(f, g)$ and $N_s = n_s(f, g)$.

We first obtain a lower bound on $2^n - N_c$. Let $w \in F_2^n$ be such that

$$|W_f(w)W_g(w)| = \max_{u\in F_2^n} |W_f(u)W_g(u)|.$$

Define a function g_1 in the following manner. If $W_f(w)W_g(w) < 0$, then $g_1 = 1 \oplus g$, else $g_1 = g$. Thus we have $W_f(w)W_{g_1}(w) = |W_f(w)W_g(w)| > 0$ and $n_c(f, g) = n_c(f, g_1)$.

Now define $h_1(x) = f(x) + \langle w, x\rangle$ and $h_2(x) = g_1(x) + \langle w, x\rangle$. This implies $W_{h_1}(0) = W_f(w)$ and $W_{h_2}(0) = W_{g_1}(w)$ and so $W_{h_1}(0)W_{h_2}(0) = \max_{u\in F_2^n} |W_f(u)W_g(u)|$. Also $n_c(h_1, h_2) = n_c(f, g_1) = n_c(f, g) = N_c$. Since the values of $C_{h_1,h_2}()$ are all at most 2^n, we obtain

$$(2^n - N_c) = (2^n - n_c(h_1, h_2)) \geq 2^{-n} \sum_{u\in F_2^n} C_{h_1,h_2}(u). \tag{6}$$

Using the facts that $\sum_{u\in F_2^n} C_{h_1,h_2}(u) = W_{h_1}(0)W_{h_2}(0)$ and $W_{h_1}(0)W_{h_2}(0) = \max_{u\in F_2^n} |W_f(u)W_g(u)|$, we obtain

$$(2^n - N_c) \geq 2^{-n} \max_{u\in F_2^n} |W_f(u)W_g(u)|. \tag{7}$$

Now we obtain a lower bound on $(2^n - N_s)$. Let $v \in F_2^n$ be such that $|C_{f,g}(v)| = \max_{u\in F_2^n} |C_{f,g}(v)|$. Define g_1 in the following manner. If $C_{f,g}(v) < 0$, then $g_1 = 1 \oplus g$, else $g_1 = g$. Then $C_{f,g_1}(v) = \max_{u\in F_2^n} |C_{f,g}(v)|$ and $n_s(f, g_1) = n_s(f, g)$. We now write

$$\begin{aligned}\sum_{u\in F_2^n} |W_f(u)W_{g_1}(u)| &\geq \sum_{u\in F_2^n} W_f(u)W_{g_1}(u)(-1)^{\langle u,v\rangle} \\ &= 2^n C_{f,g_1}(v) = 2^n \max_{u\in F_2^n} |C_{f,g}(u)|.\end{aligned} \tag{8}$$

Also we have

$$(2^n - N_s) = (2^n - n_s(f, g_1)) \geq \frac{\sum_{u\in F_2^n} |W_f(u)W_{g_1}(u)|}{\max_{u\in F_2^n} |W_f(u)W_{g_1}(u)|}. \tag{9}$$

Using inequality (8) we obtain

$$(2^n - N_s) \geq \frac{2^n \max_{u\in F_2^n} |C_{f,g}(v)|}{\max_{u\in F_2^n} |W_f(u)W_g(u)|}. \tag{10}$$

Multiplying inequalities (7) and (10), we obtain the desired inequality. □

Equality holds in (5) if and only if equality holds in (6), (8) and (9). However, there does not seem to be any simple characterization of these conditions.

4. Characterization of Bent Functions

In this section we present a new characterization of bent functions in terms of the auto-correlation and cross-correlation properties of its subfunctions. This can be considered to be a refinement of the characterization of bent functions presented in [1].

Let f be an n-variable Boolean function. Let $v \in \{0, 1\}^r$ with $1 \leq r \leq n$ and $v = v_r \cdots v_1$, where each $v_i \in \{0, 1\}$. By f_v we denote the function $f(X_n = v_r, \ldots, X_{n-r+1} = v_1, X_{n-r}, \ldots, X_1)$. Given $u \in \{0, 1\}^r$ and $w \in \{0, 1\}^{n-r}$, we use the notation uw to denote the n-bit string formed by concatenating u and w.

Theorem 4.1. *Let $u \in \{0,1\}^r$, $w \in \{0,1\}^{n-r}$ and f be an n-variable Boolean function. Then*

$$C_f(uw) = \sum_{v \in F_2^r} C_{f_v, f_{v \oplus a}}(w).$$

Proof. By definition,

$$C_f(uw) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus f(x \oplus uw)} = \sum_{v \in F_2^r} \sum_{z \in F_2^{n-r}} (-1)^{f(vz) \oplus f(vz \oplus uw)},$$

where the n-bit vector x is written as the concatenation of an r-bit string v and an $(n-r)$-bit string z. For a fixed v we have $f(vz) = f_v(z)$ and $f(vz \oplus uw) = f_{v \oplus u}(z \oplus w)$. This gives

$$C_f(uw) = \sum_{v \in F_2^r} \sum_{z \in F_2^{n-r}} (-1)^{f_v(z) \oplus f_{v \oplus a}(z \oplus w)} = \sum_{v \in F_2^r} C_{f_v, f_{v \oplus a}}(w). \qquad \square$$

Corollary 4.1. *Let f be an n-variable function and let f_0 and f_1 be obtained from f by restricting the variable X_n to 0 and 1, respectively. Then we have:*

1. $C_f(0w) = C_{f_0}(w) + C_{f_1}(w)$.
2. $C_f(1w) = C_{f_0, f_1}(w) + C_{f_1, f_0}(w) = 2C_{f_0, f_1}(w)$.

An immediate consequence of this result is to obtain a new characterization of bent functions based on the auto-correlation properties of its subfunctions. We say that two functions f and g have *complementary auto-correlation* if $C_f(u) + C_g(u) = 0$ for all non-zero u.

Theorem 4.2. *Let n be an odd integer and let h be an $(n+1)$-variable function and we write*

$$h(X_{n+1}, X_n, \ldots, X_1) = (1 \oplus X_{n+1}) f(X_n, \ldots, X_1) \oplus X_{n+1} g(X_n, \ldots, X_1).$$

Then the following are equivalent:

1. *h is bent.*
2. *f and g have complementary autocorrelation.*
3. *f and g are perfectly uncorrelated and* $\mathrm{nl}(f) = \mathrm{nl}(g) = 2^{n-1} - 2^{(n-1)/2}$.

Proof. (1) $\Rightarrow$ (2) If h is bent, then $C_h(w) = 0$ for all non-zero $w \in F_2^{n+1}$. Let u be a non-zero vector in F_2^n. Using Corollary 4.1, we get $C_h(0u) = C_f(u) + C_g(u)$. Since $u \neq 0$ we have $C_h(0u) = 0$. This gives $C_f(u) = -C_g(u)$.

(2) $\Rightarrow$ (3) Suppose $C_f(v) = -C_g(v)$ for all non-zero $v \in F_2^n$. Using Corollary 3.1, we have for each $u \in F_2^n$,

$$W_f^2(u) = \sum_{v \in F_2^n} C_f(v)(-1)^{\langle u,v \rangle} = 2^n - \sum_{v \neq 0, v \in F_2^n} C_g(v)(-1)^{\langle u,v \rangle} = 2^{n+1} - W_g^2(u).$$

This gives $W_f^2(u) + W_g^2(u) = 2^{n+1}$.

We now use Jacobi's lemma (see Chapter VI of [5]), which states that for odd m, the only integer solutions to the equation $x^2 + y^2 = 2^{m+1}$ are $x = 0$, $y = \pm 2^{(m+1)/2}$ and $x = \pm 2^{(m+1)/2}$, $y = 0$.

Thus we get that either $W_f^2(u) = 2^{n+1}$ and $W_g^2(u) = 0$ or $W_f^2(u) = 0$ and $W_g^2(u) = 2^{n+1}$. In either case we have $W_f(u)W_g(u) = 0$ and $\mathrm{nl}(f) = \mathrm{nl}(g) = 2^{n-1} - 2^{(n-1)/2}$. Since this holds for each $u \in F_2^n$, the spectra of f and g are non-intersecting. Using Corollary 3.4 it follows that the functions f and g are perfectly uncorrelated, i.e. $C_{f,g}(u) = 0$ for each $u \in F_2^n$.

(3) $\Rightarrow$ (1) Since the non-linearity of both f and g is $2^{n-1} - 2^{(n-1)/2}$, it follows that for each $u \in F_2^n$, we must have $|W_f(u)|, |W_g(u)| \leq 2^{(n+1)/2}$. Let the number of non-zero points of $W_f()$ and $W_g()$ be k_1 and k_2, respectively. Using Parseval's theorem and the bound on $|W_f(u)|, |W_g(u)|$ we have $2^{2n} \leq k_1 2^{n+1}$ and $2^{2n} \leq k_2 2^{n+1}$. This gives $k_1, k_2 \geq 2^{n-1}$. Since f and g are perfectly uncorrelated, their spectra are non-intersecting, i.e. $W_f(u)W_g(u) = 0$ for all $u \in F_2^n$. Thus the number of points at which $W_f()$ is zero is at least as large as the number of points where $W_g()$ is non-zero. Hence $2^n - k_1 \geq k_2$. This combined with $k_1, k_2 \geq 2^{n-1}$ shows that $k_1 = k_2 = 2^{n-1}$ and hence the spectra of f and g can take only the values $0, \pm 2^{(n+1)/2}$. Also for each $u \in F_2^n$, exactly one of $W_f(u)$ and $W_g(u)$ is non-zero and takes the value $\pm 2^{(n+1)/2}$.

Let $w \in F_2^{n+1}$. Then we can write $w = 0u$ or $w = 1u$ for some $u \in F_2^n$. It is easy to verify that $W_h(0u) = W_f(u) + W_g(u)$ and $W_h(1u) = W_f(u) - W_g(u)$. Since exactly one of $W_f(u)$ and $W_g(u)$ is non-zero and equal to $\pm 2^{(n+1)/2}$, it follows that $W_h(w) = \pm 2^{(n+1)/2}$ for all $w \in F_2^{n+1}$. Hence h is bent. □

Remark. The subfunctions f and g have non-intersecting three valued spectra and both their non-linearities are $2^{n-1} - 2^{(n-1)/2}$. These facts are also stated in Theorems 4(ii) and 5(iv) of [1]. However, the complementariness of the auto-correlation of f and g and their perfect uncorrelatedness have not been considered in [1].

5. Propagation Characteristics

The concept of propagation characteristics was introduced by Preneel [11]. Later investigations can be found in [3], [4] and [8]. Here we study the cross-correlation between the subfunctions of a function satisfying propagation characteristics. We characterize propagation characteristics in terms of the uncorrelatedness of its subfunctions. By $f_{X_i=0}$ and $f_{X_i=1}$ we denote the $(n-1)$-variable subfunctions obtained from f by setting X_i to 0 and 1, respectively.

Theorem 5.1. *Let f be an $(n+1)$-variable function. Then f satisfies* PC$(l+1)$ *if and only if for each $1 \le i \le n+1$, the pair of functions $f_{X_i=0}$ and $f_{X_i=1}$ are uncorrelated of degree l.*

Proof. Suppose f satisfies PC$(l+1)$. Let $g = f_{X_i=0}$ and $h = f_{X_i=1}$ and let $u \in F_2^n$ be of weight l. Let π be a permutation of the variables which interchanges X_i and X_{n+1}. Let f' be the new function formed from f. Clearly, f' also satisfies PC$(l+1)$. Since $0 \le \mathrm{wt}(u) \le l$, the vector $1u \in F_2^{n+1}$ is non-zero and has weight at most $l+1$. Thus $C_{f'}(1u) = 0$. Using Corollary 4.1, we have $C_{f'}(1u) = 2C_{g,h}(u)$. Hence $C_{g,h}(u) = 0$.

We now prove the converse. Let $w \in F_2^{n+1}$ be non-zero and have weight at most $l+1$. Since $w \neq 0$, there is an i, such that $w_i = 1$. Let $g = f_{X_i=0}$ and $h = f_{X_i=1}$. Then from the given condition $C_{g,h}(v) = 0$ for all $0 \le \mathrm{wt}(v) \le l$. Again let π be a permutation that interchanges X_{n+1} and X_i. Let the corresponding changes on f and w be denoted by f' and w'. Then w' is of the form $1u$ for some $u \in F_2^n$ and $0 \le \mathrm{wt}(u) \le l$. Then $C_f(w) = C_{f'}(w') = C_{f'}(1u) = 2C_{g,h}(u) = 0$. □

Let f be any function defined on the domain F_2^n. By a *dyadic shift* of $f(x)$ by u we mean the function $f(x \oplus u)$. When f is a Boolean function the sum (over F_2) of f and its dyadic shift by u is called the derivative of f at u. Propagation characteristics assures that the derivative is balanced at all u of bounded Hamming weight. A dyadic shift of the spectrum $W_f()$ of f by u is the function $W_f^u()$ defined by $W_f^u(v) = W_f(u \oplus v)$. We next explore the relationship between the spectra of the derivatives of a Boolean function and the dyadic shifts in its spectrum.

Let $h_a(x) = f(x) \oplus f(x \oplus a)$. We now define two matrices as follows. Let D_f be a $2^n \times 2^n$ matrix whose rows and columns are indexed by the elements of F_2^n. The (u, v)th entry of D_f is $W_{h_v}(u)$. Let T_f be another $2^n \times 2^n$ matrix whose rows and columns are indexed by the elements of F_2^n, where the (u, v)th entry of T_f is $W_f(u)W_f(u \oplus v)$. The entries of D_f are the spectral values of the derivatives of f. On the other hand, the entries of T_f are products of the spectral values of f with its dyadic shifts. The following result relates these two matrices and provides the relationship between the spectra of the derivatives of f and the dyadic shifts of the spectra of f.

Theorem 5.2. *For any n-variable Boolean function $H_n T_f = 2^n D_f$, where H_n is the Hadamard matrix of order 2^n.*

Proof. Let $g_a(x) = f(x \oplus a)$. It is easy to verify that $W_{g_a}(u) = (-1)^{\langle a,u\rangle} W_f(u)$. By Corollary 3.3, we have

$$W_{h_a}(u) = \frac{1}{2^n} \sum_{w \in F_2^n} W_f(w) W_{g_a}(u \oplus w) = \frac{1}{2^n} \sum_{w \in F_2^n} W_{g_a}(w) W_f(u \oplus w)$$

$$= \frac{1}{2^n} \sum_{w \in F_2^n} (-1)^{\langle a,w\rangle} W_f(w) W_f(u \oplus w).$$

The last expression is the inner product of the ath row of H_n and the uth column of T_f. Hence the result follows. □

A consequence of the above is the following known result [6], which states that the dyadic shifts of the spectrum of f are orthogonal to each other.

Corollary 5.1. *Let f be any Boolean function. Then*

$$\sum_{w \in F_2^n} W_f(w) W_f(u \oplus w) = 2^{2n} \quad \text{if} \quad u = 0,$$
$$= 0 \quad \text{if} \quad u \neq 0.$$

6. Non-Linear Combining Functions

Boolean functions are used as non-linear combining functions in LFSR-based stream ciphers. The outputs of several independent LFSRs are combined using a Boolean function to produce the keystream. Research in stream cipher cryptanalysis have shown that such a function must be balanced, have high non-linearity, high resiliency and high algebraic degree. Here we study the correlation properties of this class of Boolean functions.

In [18] the concept of maximum correlation analysis was introduced. This considers the correlation of an n-variable function to all n-variable function which are non-degenerate on at most m variables. For the usual notion of correlation immunity, correlation to only the linear functions are considered. The next result assures us that if a function is m-resilient then it is uncorrelated to *any* subfunction on at most m variables.

An n-variable function $f(X_1, \ldots, X_n)$ is said to be degenerate on variable X_i if the functions

$$f(X_1, \ldots, X_{i-1}, X_i = 0, X_{i+1}, \ldots, X_n)$$

and

$$f(X_1, \ldots, X_{i-1}, X_i = 1, X_{i+1}, \ldots, X_n)$$

are identical. Otherwise f is said to be non-degenerate on the variable X_i.

Theorem 6.1. *Let f be an m-*CI *(respectively m-resilient) function. Then $C_{f,g}(0) = (1/2^n) W_f(0) W_g(0)$ (respectively $C_{f,g}(0) = 0$) for any n-variable function g which is non-degenerate on at most m variables.*

Proof. Let $w \in F_2^n$ be a vector of weight at most w such that $w_i = 1$ if and only if g is non-degenerate on variable X_i. Then for any vector $u \in F_2^n$, such that $u \not\leq w$, we have $g(x) \oplus \langle u, x \rangle$ to be a balanced function and hence $W_g(u) = 0$. Using Corollary 3.2, we have $C_{f,g}(0) = (1/2^n) \sum_{u \in F_2^n} W_f(u) W_g(u)$. Since f is m-CI, we have $W_f(u) = 0$ for all $u \in F_2^n$ with $1 \leq \mathrm{wt}(u) \leq m$. If $\mathrm{wt}(u) > m$, then $u \not\leq w$ and hence $W_g(u) = 0$. Thus we get $C_{f,g}(0) = (1/2^n) W_f(0) W_g(0)$. If further f is balanced we have $W_f(0) = 0$ and hence $C_{f,g}(0) = 0$. □

The Walsh Transform of a function f determines the correlation of the function to the linear and affine functions. However, f may be correlated to non-affine functions also. Any function g with which f has a non-zero correlation is called a correlator of f. Suppose f is m-resilient. This implies that the correlation of f to any affine function non-degenerate on at most m variables is zero. However, there is the possibility that there exists non-affine functions non-degenerate on at most m variables to which f is correlated. Theorem 6.1 assures us that this does not happen.

Remarks. 1. In Theorem 6.1 it is easy to see that if f is not balanced, then the function g (non-degenerate on at most m variables) to which f is maximally correlated is the all zero function.

2. Let g be non-degenerate on $m+1$ variables and let w be defined from g as in the proof of Theorem 6.1. Suppose that f is m-resilient. Then using the argument of Theorem 6.1, we have $C_{f,g}(0) = (1/2^n)W_f(w)W_g(w)$. Clearly, $C_{f,g}(0)$ is maximum when $g(x) = b \oplus \langle w, x\rangle$, for $b \in \{0,1\}$. Thus the maximum correlators of an m-resilient function with respect to any $(m+1)$ variables are the two non-degenerate affine functions on these $m+1$ variables. In fact, this is the result obtained in Theorem 3 of [18].

3. If we consider more than $m+1$ variables, then the maximum correlator of an m-resilient function need not be an affine function. As an example, let $f(X_1, X_2, X_3, X_4, X_5) = (1 \oplus X_5)(1 \oplus X_4)(X_2 \oplus X_1) \oplus (1 \oplus X_5)X_4(X_3 \oplus X_1) \oplus X_5(1 \oplus X_4)(X_3 \oplus X_2) \oplus X_5X_4(X_3 \oplus X_2 \oplus X_1)$. The function f is 1-resilient and $W_f(u) = 0, \pm 8$, for all $u \in F_2^5$ and hence the maximum correlation to affine functions is 8. However, if we choose $g_1(X_1, X_2, X_3, X_4, X_5) = X_2 \oplus X_1X_2 \oplus X_2X_3 \oplus X_1X_3 \oplus X_2X_4 \oplus X_1X_4 \oplus X_3X_4 \oplus X_1X_3X_4$, then $C_{f,g}(0) = 16$. Again if we choose $g(X_1, X_2, X_3, X_4, X_5) = X_1 \oplus X_2 \oplus X_3 \oplus X_1X_2X_3$, then $C_{f,g}(0) = 12$. These are the (non-affine) maximum correlators for four and three variables, respectively.

We now concentrate on functions for which the magnitude of the non-zero spectrum values are all equal. Such functions can have at most three valued spectra. Functions of these type are important from the cryptographic point of view. We give three examples:

1. Bent functions of n variables have two valued spectra $\pm 2^{n/2}$.
2. Subfunctions of n variables obtained from $(n+1)$-variable bent functions by restricting any one variable to zero or one have three valued spectra: $0, \pm 2^{(n+1)/2}$. Such functions have been studied in [1].
3. Resilient functions of order m with maximum possible non-linearity have three valued spectra [13].

We analyse the relation between spectrum and auto-correlation values for the above type of functions. Given a Boolean function f, we define $\mathrm{NZ}(f)$ to be a matrix whose rows are $u \in F_2^n$ such that $W_f(u) \neq 0$. In other words, $\mathrm{NZ}(f)$ is a matrix whose rows are the vectors at which the spectrum of f is non-zero. Suppose $\mathrm{NZ}(f)$ is an $r \times n$ matrix, i.e. r is the number of places where $W_f()$ is non-zero. Let the magnitudes of all the non-zero spectrum values be M. Using Parseval's theorem we have $rM^2 = 2^{2n}$, where f is an n-variable function. This gives $r = 2^{2n}/M^2$. It is clear that M has to be a power of two,

say $M = 2^k$. Thus $r = 2^{2n-2k}$. Using Corollary 3.1 we can write

$$\begin{aligned} C_f(u) &= \frac{1}{2^n}\sum_{v\in F_2^n} W_f^2(v)(-1)^{\langle u,v\rangle} = 2^{2k-n}\sum_{\{v:\ W_f(v)\neq 0\}}(-1)^{\langle u,v\rangle} \\ &= 2^{2k-n}\sum_{v\in \mathrm{NZ}(f)}(-1)^{\langle u,v\rangle} = 2^{2k-n}(2^{2n-2k} - 2\,\mathrm{wt}(\mathrm{NZ}(f)u^T)) \\ &= 2^n - 2^{2k+1-n}\,\mathrm{wt}(\mathrm{NZ}(f)u^T), \end{aligned}$$

where $\mathrm{NZ}(f)u^T$ is the product of the matrix $\mathrm{NZ}(f)$ and the vector u^T. We summarize the above description as

Theorem 6.2. *Let f be an n-variable function for which the magnitude of the non-zero spectral values are all equal to 2^k. Then $C_f(u) = 2^n - 2^{2k+1-n}\,\mathrm{wt}(\mathrm{NZ}(f)u^T)$ for all $u \in F_2^n$.*

Remark. If $u = 0$, then we have $C_f(0) = 2^n$ as expected. For bent functions, $k = n/2$ and $\mathrm{NZ}(f) = F_2^n$. Hence for any non-zero u, we have $\mathrm{wt}(\mathrm{NZ}(f)u^T) = 2^{n-1}$ and so $C_f(u) = 0$.

An elegant recursive construction for resilient functions has been provided in [16]. A modified version of this construction has been used in [10] to construct functions with the best possible tradeoff among the parameters non-linearity, resiliency and algebraic degree. We study the auto-correlation values of the functions constructed by the method of [10]. To do that we briefly describe the construction of [16] as modified in [10].

The initial function to the recursive construction in [10] is a t-variable, resiliency p function, which is formed by the concatenation of two $(t-1)$-variable, resiliency p functions f and g having non-intersecting spectra and hence perfectly uncorrelated. The spectra of f and g are three valued: $0, \pm 2^{p+2}$. (In [10] the initial function used is a 7-variable, resiliency 2 function that was obtained by computer search.) The method of [10] constructs functions h_i of $t + 3i$ variables for $i \geq 0$. The function h_i is the concatenation of two functions f_i, g_i of $((t-1)+3i)$ variables. For the base case, $f_0 = f$ and $g_0 = g$ and h_0 is the concatenation of f_0 and g_0. The recursive construction of f_{i+1}, g_{i+1} from f_i, g_i is the following. Let $h_i^2 = X_{t+3i} \oplus f_i$ and $h_i^3 = X_{t+3i} \oplus g_i$. Define $f_{i+1} = X_{t+2+3i} \oplus X_{t+1+3i} \oplus h_i$ and $g_{i+1} = X_{t+2+3i} \oplus (1 \oplus X_{t+2+3i} \oplus X_{t+1+3i})h_i^2 \oplus (X_{t+2+3i} \oplus X_{t+1+3i})h_i^3$. Then h_{i+1} is the concatenation of f_{i+1} and g_{i+1}. We have the following result on the maximum auto-correlation value of h_{i+1}.

Theorem 6.3. *Let h_{i+1} be the $(n = t+3(i+1))$-variable $(i \geq 0)$ function constructed by the above described method. Then* $\max_{u\in F_2^n-\{0\}} |C_{h_{i+1}}(u)| = 2^{(t-1)+3(i+1)} = 2^{n-1}$.

Proof. The non-zeros of the spectra of f and g are the rows of the matrices $\mathrm{NZ}(f)$ and $\mathrm{NZ}(g)$. The matrix $\mathrm{NZ}(h_i)$ is formed from $\mathrm{NZ}(f)$ and $\mathrm{NZ}(g)$. In fact, we can provide a recursive description of $\mathrm{NZ}(h_i)$ for all $i \geq 0$. For this we need to introduce some notation. Let $u \in F_2^r$ and let M be an $s \times t$ matrix of bits. Then $u||M$ is the $s \times (r+t)$

matrix whose rows are of the form uv, where v is a row of M. We number the columns of M from the right, i.e. the rightmost is numbered 1 and the leftmost column gets the highest number.

The structures of $\mathrm{NZ}(f_{i+1})$, $\mathrm{NZ}(g_{i+1})$ and $\mathrm{NZ}(h_{i+1})$ are as follows:

$$\mathrm{NZ}(f_{i+1}) = \begin{bmatrix} 110||\,\mathrm{NZ}(f_i) \\ 111||\,\mathrm{NZ}(f_i) \\ 110||\,\mathrm{NZ}(g_i) \\ 111||\,\mathrm{NZ}(g_i) \end{bmatrix},$$

$$\mathrm{NZ}(g_{i+1}) = \begin{bmatrix} 011||\,\mathrm{NZ}(f_i) \\ 101||\,\mathrm{NZ}(f_i) \\ 011||\,\mathrm{NZ}(g_i) \\ 101||\,\mathrm{NZ}(g_i) \end{bmatrix},$$

$$\mathrm{NZ}(h_{i+1}) = \begin{bmatrix} 0||\,\mathrm{NZ}(f_{i+1}) \\ 1||\,\mathrm{NZ}(f_{i+1}) \\ 0||\,\mathrm{NZ}(g_{i+1}) \\ 1||\,\mathrm{NZ}(g_{i+1}) \end{bmatrix} = \begin{bmatrix} 0110||\,\mathrm{NZ}(f_i) \\ 0111||\,\mathrm{NZ}(f_i) \\ 0110||\,\mathrm{NZ}(g_i) \\ 0111||\,\mathrm{NZ}(g_i) \\ 1110||\,\mathrm{NZ}(f_i) \\ 1111||\,\mathrm{NZ}(f_i) \\ 1110||\,\mathrm{NZ}(g_i) \\ 1111||\,\mathrm{NZ}(g_i) \\ 0011||\,\mathrm{NZ}(f_i) \\ 0101||\,\mathrm{NZ}(f_i) \\ 0011||\,\mathrm{NZ}(g_i) \\ 0101||\,\mathrm{NZ}(g_i) \\ 1011||\,\mathrm{NZ}(f_i) \\ 1101||\,\mathrm{NZ}(f_i) \\ 1011||\,\mathrm{NZ}(g_i) \\ 1101||\,\mathrm{NZ}(g_i) \end{bmatrix}.$$

Note that $\mathrm{NZ}(f_{i+1}) \cap \mathrm{NZ}(g_{i+1}) = \emptyset$, hence f_{i+1}, g_{i+1} have non-intersecting spectra and consequently are perfectly uncorrelated.

The function h_{i+1} is a function of $n = t + 3(i+1)$ variables and is $(p + 2(i+1))$-resilient. From this it follows that the spectrum of h_{i+1} takes only the values 2^k where $k = p + 2 + 2(i+1)$ (see [10] and [13]). Then the number of non-zeros of the spectrum of h_{i+1} is $r = 2^{2n-2k}$. Let u be such that $u_{n-1} = 1$ and $u_j = 0$ for $j \neq n-1$. Then it is easy to see that $\mathrm{wt}(\mathrm{NZ}(h_{i+1})u^T) = r/2 + r/4$. Using Theorem 6.2 we get $C_{h_{i+1}}(u) = 2^n - 2^{2k+1-n}(r/2 + r/4) = -2^{n-1}$. Also a careful examination of the linear

combinations of the columns of $\mathrm{NZ}(h_{i+1})$ shows that there is no combination which provides an absolute auto-correlation of more than 2^{n-1}. □

7. S-Boxes for Stream Ciphers

Here we consider functions with more than one output, i.e. maps from F_2^n to F_2^m. Such functions are called S-boxes and are mostly used in block ciphers. However, the use of S-boxes in stream ciphers can speed up encryption/decryption in the following way. A non-linear combining function extracts only one key bit per n bits. Use of an S-box will mean that $m > 1$ bits can be extracted per n bits. Thus the use of S-boxes for stream ciphers is an attractive proposition and has been suggested in recent papers [19], [7]. Here we carefully examine this idea and show that there are several difficulties in such an approach.

Note that a trivial way to extract more than one bit per clock cycle is to increase the number of LFSRs. For example, if n LFSRs are used to obtain one bit per cycle, then we can repeat this arrangement (with different combining functions) k times to obtain k bits per cycle. However, increasing the number of LFSRs will escalate the cost of implementation. Hence the idea is to obtain more than one bit per clock cycle without increasing the number of LFSRs. This means that the security parameters remain constant, but we will still be able to increase the speed of encryption. It is this approach that we investigate here.

Let $f\colon \{0,1\}^n \to \{0,1\}^m$ be an S-box used to extract m bits from each n-bit input provided by n LFSRs at each clock. An m-length decimation of the output key stream will provide the sequence of bits generated by a component Boolean function of the output of the S-box. An obvious extension of the correlation attack would be to look for correlations between some combination of the output bits and (some linear combination of) the input bits.

Thus we would like the cross-correlation between an arbitrary combination of the output and any linear combination of the input to be zero. Of course this is not possible since it would violate Parseval's theorem. Instead we require that any arbitrary non-trivial combination of the output is uncorrelated to any linear combination of input involving not more than t variables. Hence using Theorem 6.1, it is also uncorrelated to any arbitrary combination of the input involving not more than t variables.

A class of S-boxes called resilient functions have been studied in the literature. An S-box $f\colon \{0,1\}^n \to \{0,1\}^m$ is said to be t-resilient if any subfunction of f obtained by fixing at most t input bits to constant is balanced. Here, by balanced we mean that every vector in F_2^m occurs in the output of the subfunction the same number 2^{n-m-t} times. It is known that an S-box is t-resilient if and only if every non-zero linear combination of the component function of the output is t-resilient. However, this does not assure that an arbitrary combination of the output is correlated to a linear combination of the input. First we prove this for $m = 2$. Let $f\colon \{0,1\}^n \to \{0,1\}^m$ be an S-box and let $g\colon \{0,1\}^m \to \{0,1\}$ be the m-variable Boolean function. Then $g \circ f$ is an n-variable Boolean function defined by $(g \circ f)(x) = g(f(x))$.

Theorem 7.1. *Let $f\colon \{0,1\}^n \to \{0,1\}^2$ be a t-resilient function. Let g be any two-variable Boolean function. Then $g \circ f$ is t-CI.*

Proof. Let the component functions of f be f_1, f_2. Then f_1, f_2, $f_1 \oplus f_2$ are n-variable, t-resilient Boolean functions. The function $g(X_2, X_1) = a \oplus bX_1 \oplus cX_2 \oplus dX_1X_2$, where $a, b, c, d \in \{0, 1\}$. Without loss of generality we can take $a = 0$. If $d = 0$, then clearly $g \circ f$ is t-resilient for any combinations of b and c. Thus let $d = 1$. If $b = c = 0$, then the function g is the logical AND of X_1, X_2. It is not difficult to verify that $(-1)^{(g\circ f)(x)} = (-1)^{f_1(x)f_2(x)} = \frac{1}{2}(1 + (-1)^{f_1(x)} + (-1)^{f_2(x)} - (-1)^{f_1(x)\oplus f_2(x)})$.

Hence $W_{g\circ f}(u) = \frac{1}{2}(2^n\delta(u) + W_{f_1}(u) + W_{f_2}(u) - W_{f_1\oplus f_2}(u))$, where $\delta(u) = 1$ if $u = 0$, else it is 0. From this it follows that $g \circ f$ is t-CI. If $b = c = 1$, then g is the logical OR of X_1 and X_2. In this case $(g \circ f)(x) = f_1(x) \vee f_2(x) = 1 \oplus (1 \oplus f_1(x))(1 \oplus f_2(x))$.

Hence for each $u \in F_2^n$, $W_{g\circ f}(u) = -\frac{1}{2}(2^n\delta(u) - W_{f_1}(u) - W_{f_2}(u) - W_{f_1\oplus f_2}(u))$. Again we have that $g \circ f$ is t-CI.

The only cases that remain to be considered are when exactly one of b or c is zero. Without loss of generality let $b = 0, c = 1$. Then $g(X_2, X_1) = X_2(1 \oplus X_1)$ and $(g \circ f)(x) = f_2(x)(1 \oplus f_1(x))$. Using an argument similar to the logical AND case we have $g \circ f$ to be t-CI. □

Remark. It is not clear how this result can be extended when g is a function of three or more variables. Thus it may be possible that for $m > 2$, some Boolean combination of the output is correlated to a linear combination of the input. Further, the next result shows that the non-linearity of non-affine output combinations can be very low.

Theorem 7.2. *Let f: $\{0, 1\}^n \to \{0, 1\}^m$ be a t-resilient S-box where $m \geq 2$ and $f_1, \ldots, f_m$ are the component n-variable Boolean functions. Then* $\mathrm{nl}(f_i \wedge f_j), \mathrm{nl}(f_i \vee f_j) \leq 2^{n-1} - 2^{n-2}$, *for all* $1 \leq i, j \leq n$.

Proof. From the proof of Theorem 7.1, $W_{f_1\wedge f_2}(u) = \frac{1}{2}(2^n\delta(u) + W_{f_1}(u) + W_{f_2}(u) - W_{f_1\oplus f_2}(u))$. Since f is t-resilient, we have f_1, f_2, $f_1 \oplus f_2$ to be t-resilient and so $W_{f_1}(0) = W_{f_2}(0) = W_{f_1\oplus f_2}(0) = 0$. Hence $W_{f_1\wedge f_2}(0) = 2^{n-1}$ and consequently $\mathrm{nl}(f_1 \wedge f_2) \leq 2^{n-1} - 2^{n-2}$. Similarly for $f_1 \vee f_2$. □

This shows that it is possible to obtain good affine approximations of certain non-affine output combinations and could also prove to be a potential weakness. Similar analysis is possible for the algebraic degree and the order of resiliency of Boolean combinations of the output. Our conclusion from these results is that though extracting more than one bit at each clock cycle is an attractive proposition, the concept needs to be examined more closely before it can be considered secure. A suitable model for extracting multiple bits from the n LFSR bits is a future research question.

8. Conclusion

In this paper we have studied several classes of cryptographically useful Boolean functions and S-boxes. Our main tool has been the Cross-Correlation Theorem. This has

allowed us to obtain new characterizations and explore relationships between the spectrum and correlation properties of a Boolean function. We have studied the possibility of using S-boxes in LFSR-based stream ciphers. Our conclusion is that currently known constructions of S-boxes are not suitable for such applications.

Acknowledgment

The authors are grateful to the reviewers for their careful reading of the paper and critical comments which helped to improve the paper substantially.

References

[1] A. Canteaut, C. Carlet, P. Charpin and C. Fontaine. Propagation characteristics and correlation-immunity of highly non-linear Boolean functions. In *Advances in Cryptology - Eurocrypt* 2000, pages 507–522. Number 1807 in Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2000.

[2] C. Carlet. Partially-bent functions. In *Advances in Cryptology - CRYPTO* '92, pages 280–291. Number 740 in Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1992.

[3] T. W. Cusick. Boolean functions satisfying a higher order strict avalanche criteria. *Advances in Cryptology - Eurocrypt* '93, pages 102–117.

[4] T. W. Cusick. Bounds on the number of functions satisfying the strict avalanche criteria. Information Processing Letter, 57(5):261–263 (1996).

[5] L. E. Dickson. *History of the Theory of Numbers*, volume II. Chelsea, New York, 1919.

[6] C. Ding, G. Xiao and W. Shan. *The Stability Theory of Stream Ciphers*. Number 561 in Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1991.

[7] T. Johansson and E. Pasalic. A construction of resilient functions with high nonlinearity. *International Symposium on Information Theory, ISIT* 2000.

[8] K. Kurosawa and T. Satoh. Design of $SAC/PC(l)$ of order k Boolean functions and three other cryptographic criteria. In *Advances in Cryptology - Eurocrypt* '97, pages 434–449. Number 1233 in Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1997.

[9] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error Correcting Codes*. North-Holland, Amsterdam, 1977.

[10] E. Pasalic, S. Maitra, T. Johansson and P. Sarkar. New constructions of resilent and correlation immune Boolean functions achieving upper bounds on nonlinearity. In *Proceedings of the Workshop on Cryptography and Coding Theory*, Paris, 2001. Electronic Notes in Discrete Mathematics, Volume 6, Elsevier, Amsterdam, 2000.

[11] B. Preneel. Analysis and design of cryptographic hash functions. Doctoral dissertation, K.U. Leuven, 1993.

[12] O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, 20:300–305, 1976.

[13] P. Sarkar and S. Maitra. Nonlinearity bounds and constructions of resilient Boolean functions. In *Advances in Cryptology - CRYPTO* 2000, pages 515–532. Number 1880 in Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2000.

[14] C. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.

[15] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776–780, September 1984.

[16] Y. V. Tarannikov. On resilient Boolean functions with maximum possible nonlinearity. *Proceedings of INDOCRYPT*, pages 19–30. Number 1977 in Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2000.

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

[18] M. Zhang. Maximum correlation analysis of nonlinear combining functions in stream ciphers. *Journal of Cryptology*, 13:301–313, 2000.

[19] M. Zhang and A. Chan. Maximum correlation analysis of nonlinear S-boxes in stream ciphers. In *Advances in Cryptology - CRYPTO* 2000, pages 501–514. Number 1880 in Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2000.

[20] X.-M. Zhang and Y. Zheng, GAC—the criterion for global avalanche characteristics of cryptographic functions. *Journal for Universal Computer Science*, 1(5):316–333, 1995.