Maximum Correlation Analysis of Nonlinear S-boxes in Stream Ciphers

Muxiang Zhang
GTE Laboratories Incorporated
40 Sylvan Road MS 59
Waltham, MA 02451
zhangmx@ccs.neu.edu

Agnes H. Chan
College of Computer Science
Northeastern University
Boston, MA 02115
ahchan@ccs.neu.edu

Abstract This paper investigates the design of S-boxes for stream ciphers. When used to combine several LFSR sequences in a combination generator, S-boxes leak more information about the LFSR sequences than Boolean functions. To mitigate the information leakage, the notion of maximum correlation is introduced, which is based on the correlation between linear functions of the input and all the Boolean functions (linear and nonlinear) of the output of an S-box. In terms of Walsh transform, a spectral characterization of the maximum correlation coefficients is developed, which is used to derive upper and lower bounds on the maximum correlation coefficients, as well as the relationship between maximum correlation and nonlinearity of S-boxes. For the perfect nonlinear S-boxes designed for block ciphers to defend against differential cryptanalysis, an upper bound on the maximum correlation coefficients is presented.

1 Introduction

Stream ciphers have a long history and still play an important role in secure communications. Typically, a stream cipher consists of a keystream generator whose output sequence is added modulo-2 to the plaintext sequence. A major goal in stream cipher design is to efficiently produce random-looking sequences, that is, sequences that as closely as possible resemble coin-tossing sequences. So far, many kinds of keystream generators have been proposed, among which combination generators [15] and filter generators [14] are two of the most widely used keystream generators. These keystream generators are based on linear feedback shift register (LFSR), a structure that has a mature mathematical theory [6] and is easy to implement in VLSI circuitry. A combination generator consists of several LFSRs whose output sequences are combined by a nonlinear Boolean function (also called a nonlinear combining function or combiner) . A filter generator consists of a single LFSR and uses a nonlinear Boolean function to filter the content of the shift register. It is clear that a filter generator is a special case of the combination generator, where all the combined sequences are produced by the same LFSR. The security of these keystream generators relies heavily on the nonlinear combining functions. In [17] Siegenthaler has shown that if the nonlinear combining function of a combination generator leaks information about the individual LFSR sequences into the keystream sequence, the LFSR sequences can be analyzed from a known segment of the keystream sequence. This kind of attacks are referred to as correlation attacks. To prevent correlation attacks, the nonlinear combining function should not leak information about its input. However, it has been shown in [9] that the output of a Boolean function is always correlated to certain linear functions of its input, and actually the sum of the squares of the correlation coefficients is always 1. Thus, zero correlation to some linear functions of the input necessarily implies higher correlation to other linear functions of the input. The best one can do is to make the correlation between the output and every linear functions of the input uniformly small.

In hardware, combination generators and filter generators have fast speed and simple VLSI circuitry. With respect to software implementation, however, there are two major problems for the LFSR-base keystream generators. First, the speed of a software implemented LFSR is much slower than that of a hardware implemented one. Keystream generators consisting of several LFSRs make the speed of the software implementation even slower. Second, combination generators and filter generators only output one bit at every clock, which again makes the software implementation inefficient. To increase the throughput, a direct approach is to use nonlinear combining functions that output several bits at a time. Nonlinear functions with multiple-bit input and multiple-bit output are referred to as S-boxes in block ciphers and have been intensively studied [1,3,4,10,16] in the analysis and design of block ciphers. In this paper, we investigate the design of S-boxes for stream ciphers. Compared with a combination generator with a Boolean function as the combiner, a combination generator utilizing an S-box as the combiner might be much easier to attack since every output bits of the S-box leak information about the input. How to control the information leakage is a crucial problem for the design of keystream generators that produce several bits at a time. To mitigate the information leakage, we investigate the maximum correlation between linear functions of the input and all Boolean functions, linear and nonlinear, of the output of an S-box and introduce the notion of maximum correlation coefficient. In terms of the Walsh transform, a spectral characterization of the maximum correlation coefficients of S-boxes is developed, which is used to investigate bounds on the maximum correlation coefficients.

The paper is organized as follows. Section 2 reviews the correlation properties of Boolean functions. Section 3 introduces the notion of maximum correlation and investigates the relationship between maximum correlation and mutual information of an S-box. Section 4 presents the spectral characterization of the maximum correlation of S-boxes. For the perfect nonlinear S-boxes introduced by Nyberg [10], an upper bound on the maximum correlation coefficients is given in Section 5.

2 Correlation Properties of Boolean Functions

Let $f, g : GF(2)^n \to GF(2)$ be Boolean functions and let X be a random variable that takes on values $x \in GF(2)^n$ with uniform probability 2^{-n}. Then $Z = f(X)$ and $Z' = g(X)$ are random variables over $GF(2)$. The correlation coefficient, $c(f, g)$, of f and g is defined as follows:

$$c(f,g) = P(Z = Z') - P(Z \neq Z'), \tag{1}$$

the probability that f and g coincide in their truth tables is given by

$$P(Z = Z') = \frac{1}{2} + \frac{c(f,g)}{2}.$$

The correlation coefficients between a nonlinear Boolean function and every linear functions are of special interest in the analysis and design of stream ciphers. A linear function of n

input variables can be expressed as the form, $w \cdot x = w_1x_1 \oplus w_2x_2 \oplus \ldots \oplus w_nx_n$, where $w \cdot x$ denotes the inner product of $w = (w_1, w_2, \ldots, w_n)$ and $x = (x_1, x_2, \ldots, x_n)$. Such a linear function is simply denoted by $l_w(x)$. The correlation coefficient $c(f, l_w)$ describes the statistical dependency between f and l_w, and is usually interpreted as the nonlinearity of f with respect to l_w.

In the analysis and design of Boolean functions, Walsh transform [6] is a very convenient tool. The Walsh transform of $f : GF(2)^n \to GF(2)$ is defined as follows:

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

The function $(-1)^{f(x)}$ can be recovered from the inverse Walsh transform,

$$(-1)^{f(x)} = \sum_{w \in GF(2)^n} S_f(w)(-1)^{w \cdot x}.$$

From (1) and (2), the correlation coefficient $c(f, l_w)$ can be expressed in terms of the Walsh spectral coefficients,

$$c(f, l_w) = 2^{-n} \sum_{x \in GF(2)^n} (-1)^{f(x) \oplus w \cdot x} = S_f(w).$$

Based on the spectral representation, it can be concluded that $Z = f(X)$ and $Z' = l_w(X)$ are statistically independent if and only if $c(f, L_w) = 0$, or equivalently, if and only if $c_f(w) = 0$.

In addition to the correlation coefficient, an alternative approach to describe the nonlinearity of Boolean functions is the Hamming distance to the set of linear or affine functions. The distance between two Boolean fictions f and g is defined by

$$d(f, g) = |\{x \in GF(2)^n : f(x) \neq g(x)\}|.$$

The distance of f to a linear function l_w is related to the correlation coefficient $c(f, l_w)$ by

$$d(f, L_w) = 2^{n-1}(1 - c(f, l_w)), \tag{3}$$

and may equivalently be expressed in terms of the Walsh transform $S_f(w)$

$$d(f, l_w) = 2^{n-1}(1 - S_f(w)).$$

Let the distance $d(f, \mathcal{G})$ of f to a set of Boolean functions $\mathcal{G}$ be defined as

$$d(f, \mathcal{G}) = \min_{g \in \mathcal{G}} d(f, g),$$

that is, the distance between f and the nearest neighbor of f in $\mathcal{G}$. As a consequence, the distance of f to the set $\mathcal{A}$ of linear and affine functions is given by

$$d(f, \mathcal{A}) = 2^{n-1}(1 - \max_{w \in GF2^n} |S_f(w)|). \tag{4}$$

The distance $d(f, \mathcal{A})$ is defined as the nonlinearity of f in [11]. By Parseval's theorem [6],

$$\sum_{w \in GF(2)^n} S_f^2(w) = 1,$$

which means that there exists $w \in GF(2)^n$ for which $S_f^2(w) \geq 2^{-n}$. Hence, for any Boolean function f, its nonlinearity is upper-bounded by

$$d(f, \mathcal{A}) \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

The upper bound is reached if for any $w \in GF(2)^n$, $|S_f(w)| = 2^{\frac{n}{2}}$, this type of Boolean functions are called bent functions [13].

3 Maximum Correlation of S-boxes

An S-box of n-bit input and m-bit output can be described by a function F of $GF(2)^n$ to $GF(2)^m$. Let $x = (x_0, x_1, \ldots, x_{n-1}) \in GF(2)^n$ and $z = (z_0, z_1, \ldots, z_{m-1}) \in GF(2)^m$ denote the input and output of the S-box, i.e., $z = F(x)$. The S-box can also be specified by a vector, $(f_0, f_1, \ldots, f_{m-1})$, of m Boolean functions, where $z_i = f_i(x)$. Each Boolean function is called a component function of F. When F is used to combine n LFSR-sequences, we have a keystream generator that outputs m binary sequences simultaneously. The individual binary sequence is produced by a combination generator in which a component function of F is used as the combiner. Obviously, each binary sequence can be used to perform correlation attacks. As a consequence, the first design rule for the S-box is that every component function of F has small correlation to linear functions. The m binary sequences may also be combined together to perform correlation attacks. In this case, larger correlation to the LFSR-sequences might be exploited. To defend against this kind of attacks, the second design rule for the S-box is that every combination (linear and nonlinear) of the output have small correlation to linear functions of the input. It is clear that the second design rule is a generalization of the first one. To measure the quality of S-boxes under the second design rule, we introduce the following definition.

Definition 1 Let F be a function of $GF(2)^n$ to $GF(2)^m$ and let $\mathcal{G}$ denote the set of all Boolean functions of $GF(2)^m$ to $GF(2)$. For any $w \in GF(2)^n$, the maximum correlation coefficient between F and the linear function l_w is defined by

$$\mathcal{C}_F(w) = \max_{g \in \mathcal{G}} c(g \circ F, l_w),$$

where $g \circ F$ is the composition of g and F, that is, $g \circ F(x) = g(F(x))$. If $\hat{g} \in \mathcal{G}$ and $\mathcal{C}_F(w) = c(\hat{g} \circ F, l_w)$, then $\hat{g}$ is called the maximum correlator of F to l_w.

Nyberg [11] has investigated a special case where the set $\mathcal{G}$ only contains linear or affine functions. Based on Hamming distance, Nyberg defined the nonlinearity for S-boxes.

Definition 2 Let F be a function of $GF(2)^n$ to $GF(2)^m$ and let $\mathcal{A}$ denote the set of linear or affine functions of $GF(2)^m$ to $GF(2)$. The nonlinearity of F is defined as

$$\mathcal{N}_F = \min_{0 \neq v \in GF(2)^m} d(l_v \circ F, \mathcal{A}). \tag{5}$$

Assume that $\mathcal{N}_F = d(l_v \circ F, a \oplus l_w), v \in GF(2)^m, v \neq 0, w \in GF(2)^n, a \in GF(2)$. By (3) and (5), $c(l_v \circ F, a \oplus l_w)$ is the maximum correlation between nonzero linear functions of the output and linear or affine functions of the input of F. By Definition 1, it is always true that $c(l_v \circ F, a \oplus l_w) \leq c_F(w)$, with strict inequality if the maximum correlator of F to l_w is not linear. Generally it is difficult to compute the maximum correlation coefficients since there are 2^{2^m} functions in $\mathcal{G}$.

Theorem 1 Let F be a function of $GF(2)^n$ to $GF(2)^m$. Assume that X is a random variable that takes on values $x \in GF(2)^n$ with uniform probability 2^{-n}, $Z = f(X)$. For $w \in GF(2)^n$ and $z \in GF(2)^m$, let

$$e_w(z) = 2P(w \cdot X = 1 | Z = z) - 1. \tag{6}$$

Then

$$\mathcal{C}_F(w) = \sum_{z \in GF(2)^m} |e_w(z)| P(Z = z).$$

Moreover, the function $\hat{g}(z) = sgn(e_w(z))$ is the maximum correlator of F to l_w, where

$$sgn(x) = \begin{cases} 1, & x > 0, \\ 0 \text{ or } 1, & x = 0, \\ 0, & x < 0. \end{cases}$$

Proof. For any $w \in GF(2)^n$, and $g \in \mathcal{G}$, where $\mathcal{G}$ denotes the set of all Boolean functions defined on $GF(2)^m$, by (1),

$$c(g \circ F, l_w) = P(w \cdot X = g(Z)) - P(w \cdot X \neq g(Z)).$$

Since

$$P(w \cdot X = g(Z)) + P(w \cdot X \neq g(Z)) = 1,$$

it follows that

$$\begin{aligned} c(g \circ F, l_w) &= 2P(w \cdot x = g(Z)) - 1 \\ &= \sum_{z \in GF(2)^m} 2P(w \cdot X = g(Z)|_{Z=z}) P(Z = z) - 1 \\ &= \sum_{z \in GF(2)^m} (2P(w \cdot X = g(z)|_{Z=z}) - 1) P(Z = z). \end{aligned}$$

Therefore,

$$\max_{g \in \mathcal{G}} c(g \circ F, l_w) = \max_{g \in \mathcal{G}} \sum_{z \in GF(2)^n} (2P(w \cdot X = g(z)|_{Z=z}) - 1) P(Z = z). \tag{7}$$

Note that maximizing the sum in (7) is equivalent to maximizing every terms in the sum, i.e.,

$$\max_{g \in \mathcal{G}} c(g \circ F, l_w) = \sum_{z \in GF(2)^n} \max_{g(z) \in GF(2)} (2P(w \cdot X = g(z)|_{Z=z}) - 1) P(Z = z).$$

Since $g(z) \in GF(2)$, and

$$P(w \cdot X = 1|_{Z=z}) + P(w \cdot X = 0|_{Z=z}) = 1,$$

by (6), it can be concluded that

$$\max_{g(z) \in GF(2)} (2P(w \cdot X = g(z)|_{Z=z}) - 1) = \begin{cases} 2P(w \cdot X = 1|_{Z=z}) - 1, & \text{if } e_w(z) \geq 0, \\ 2P(w \cdot X = 0|_{Z=z}) - 1, & \text{if } e_w(z) < 0. \end{cases}$$

On the other hand,

$$e_w(z) = 2P(w \cdot X = 1|_{Z=z}) - 1 = -(2P(w \cdot X = 0|_{Z=z}) - 1),$$

it is clear that

$$\max_{g(z)\in GF(2)}(2P(w\cdot X=g(z)|_{Z=z})-1)=|2P(w\cdot X=1|_{Z=z})-1|,$$

the maximum value is reached if $g(z)=sgn(e_w(z))$. Therefore,

$$\mathcal{C}_F(w)=\max_{g\in\mathcal{G}}c(g\circ F,l_w)=\sum_{z\in GF(2)^m}|e_w(z)|P(Z=z),$$

and $\hat{g}(z)=sgn(e_w(z))$ is the maximum correlator of F to l_w. $\square$

Based on Theorem 1, the maximum correlation of F to l_w can be computed when the conditional probabilities $P(w\cdot X=1|_{Z=z})$ are known for every $z\in GF(2)^m$. These conditional probabilities can be calculated from the algebraic expression or from the truth table of F, with a complexity about 2^{m+n}, which is far below $2^n 2^{2^m}$ as required by exhaustive search. When $Z=F(X)$ is uniformly distributed on $GF(2)^m$, it is easy to derive the following bounds for $\mathcal{C}_F(w)$,

$$\min_{z\in GF(2)^m}|e_w(z)|\le\mathcal{C}_F(w)\le\max_{z\in GF(2)^m}|e_w(z)|.$$

Theoretically, the correlation between $Z=F(X)$ and $w\cdot X$ is measured by the mutual information $I(w\cdot X;Z)$. If $I(w\cdot X;Z)$ is small, we can not get much information about $w\cdot X$ from Z. In contrast, if $I(w\cdot X;Z)$ is large, we should be able to get much information about $w\cdot X$. However, the mutual information $I(w\cdot X;Z)$ does not tell us how to get information about $w\cdot X$ from Z. With the idea of maximum correlation, we can use a Boolean function of Z to approximate the random variable $w\cdot X$. The successful rate of the approximation is measured by the maximum correlation coefficient. According to the Data Processing Inequality [5] of information theory, we have

$$I(w\cdot X;g(Z))\le I(w\cdot X;Z).$$

So we actually lose information about $w\cdot X$ when we perform maximum correlation. In the following, we investigate the relationship between mutual information and maximum correlation.

Lemma 1 Let $h(x)$ denote the binary entropy function, i.e.,

$$h(x)=-x\log_2 x-(1-x)\log_2(1-x),\quad 0\le x\le 1 \tag{8}$$

Then, for $-0.5\le x\le 0.5$,

$$h(0.5+x)\ge 1-2|x|.$$

Moreover,

$$1-4(\log_2 e)x^2\le h(0.5+x)\le 1-2(\log_2 e)x^2.$$

Proof. Let $\psi(x)=h(0.5+x)-(1-2|x|)$. Since $h(0.5+x)$ is a convex function, $\psi(x)$ is convex in both intervals $(-0.5,0)$ and $(0,0.5)$. Also, since $\psi(-0.5)=\psi(0)=\psi(0.5)=0$, it can be concluded that $\psi(x)\ge 0$, for $-0.5\le x\le 0.5$, i.e. , $h(0.5+x)\ge 1-2|x|$.

Next, let $\varphi(x)=1-2(\log_2 e)x^2-h(0.5+x)$. Then

$$\varphi'(x)=-4x\log_2 e+(\ln(0.5+x)-\ln(0.5-x))\log_2 e$$

and

$$\varphi''(x) = -4\log_2 e + \frac{4\log_2 e}{1-(2x)^2}.$$

Since $0 \le 1-(2x)^2 \le 1$, $\varphi''(x) \ge 0$. Hence, $\varphi(x)$ is a convex function. Moreover, $\varphi'(0) = 0$, which implies that $x = 0$ is the stationary point of $\varphi(x)$. Thus, $\varphi(x) \ge \varphi(0) = 0$.

From the convexity of $-\log_2(x)$, we have

$$\begin{aligned} h(0.5+x) &= -(0.5+x)\log_2(0.5+x) - (0.5-x)\log_2(0.5-x) \\ &\ge -\log_2((0.5+x)^2 + (0.5-x)^2) \\ &= 1 - \log_2(1+(2x)^2). \end{aligned}$$

Since $\log_2(1+(2x)^2) \le (2x)^2 \log_2 e$, it follows that $h(0.5+x) \ge 1 - 4(\log_2 e)x^2$. □

Definition 3 Let F be a function of $GF(2)^n$ to $GF(2)^m$ and let X be a random variable that takes on values $x \in GF(2)^n$ with uniform probability 2^{-n}. If $Z = F(X)$ is uniformly distributed on $GF(2)^m$, i.e., $P(Z = z) = 2^{-m}$ for every $z \in GF(2)^m$, then F is called a balanced function.

Theorem 2 Let F be a balanced function of $GF(2)^n$ to $GF(2)^m$. Assume that X is a random variable that takes on values $x \in GF(2)^n$ with uniform probability 2^{-n}, $Z = f(X)$. Then for any nonzero $w \in GF(2)^n$,

$$I(w \cdot X; Z) \le \mathcal{C}_F(w) \le \sqrt{2(\ln 2) I(w \cdot X; Z)}.$$

Proof. For every nonzero w, it is easy to prove that the random variable $w \cdot X$ is uniformly distributed over $GF(2)$. Thus, $H(w \cdot X) = 1$, and

$$\begin{aligned} I(w \cdot X; Z) &= H(w \cdot X) - H(w \cdot X|Z) \\ &= 1 + \sum_{\substack{y \in GF(2) \\ z \in GF(2)^n}} P(w \cdot X = y, Z = z) \log_2 P(w \cdot X = y|_{Z=z}) \\ &= 1 + \frac{1}{2^m} \sum_{\substack{y \in GF(2) \\ z \in GF(2)^n}} P(w \cdot X = y|_{Z=z}) \log_2 P(w \cdot X = y|_{Z=z}). \end{aligned}$$

With the binary entropy function $h()$ as defined in (8), The mutual information $I(w \cdot X; Z)$ is represented by

$$I(w \cdot X; Z) = 1 - \frac{1}{2^m} \sum_{z \in GF(2)^m} h(P(w \cdot x = 1|_{Z=z})). \tag{9}$$

By (6), we have

$$P(w \cdot X = 1|_{Z=z}) = 0.5 + e_w(z)/2. \tag{10}$$

Substituting (10) into (9),

$$I(w \cdot X; Z) = 1 - \frac{1}{2^m} \sum_{z \in GF(2)^m} h(0.5 + e_w(z)/2).$$

By Lemma 1,

$$1 - |e_w(z)| \le h(0.5 + e_w(z)/2) \le 1 - \frac{1}{2}(e_w(z))^2 \log_2 e.$$

Therefore,

$$\frac{1}{2^m}\sum_{z\in GF(2)^m}\frac{\log_2 e}{2}(e_w(z))^2 \le I(w\cdot X;Z)\le \frac{1}{2^m}\sum_{z\in GF(2)^m}|e_w(z)|. \tag{11}$$

By Theorem 1,

$$\mathcal{C}_F(w)=\frac{1}{2^m}\sum_{z\in GF(2)^m}|e_w(z)|\ge I(w\cdot X;Z).$$

On the other hand, by Cauchy inequality,

$$\sum_{z\in GF(2)^m}(e_w(z))^2\ge \frac{1}{2^m}(\sum_{z\in GF(2)^m}|e_w(z)|)^2.$$

From (11), it follows that

$$(\frac{1}{2^m}\sum_{z\in GF(2)^m}|e_w(z)|)^2\le 2(\log_2 e)I(w\cdot X;Z).$$

By Theorem 1, $\mathcal{C}_F(w)\le\sqrt{2(\ln 2)I(w\cdot X;Z)}$. □

Theorem 2 establishes a connection between the mutual information and the maximum correlation. This connection provides us great flexibility for the analysis and design of S-boxes. Since mutual information is an abstract concept while maximum correlation has explicit physical meaning, it is convenient to use maximum correlation to describe the correlation properties of S-boxes. For example, to design a balanced function with $I(w\cdot X;Z)\le\delta$, we only need to design a function F with $c_F(w)<\delta$.

4 A Spectral Characterization of Maximum Correlation Coefficients

Walsh transform is a useful tool in the analysis and design of Boolean functions. The merit with Walsh transform is that it provides illustrative description of Boolean functions satisfying certain cryptographic conditions. As shown by (4), the distance of a Boolean function to the set of linear or affine functions has a very elegant description in terms of the Walsh transform. In the design highly nonlinear Boolean functions, we may concentrate on the Walsh spectral coefficients and construct Boolean functions whose spectral coefficients are uniformly small. In addition to nonlinearity, Walsh transform has also played an important role in the study of other cryptographic properties, such as correlation-immunity [18] and avalanche property [12].

With slight modification of (2), we can define Walsh transform for S-boxes. Let F be a function of $GF(2)^n$ to $GF(2)^m$. For any $v\in GF(2)^m$, $l_v\circ F$ defines a Boolean function of $GF(2)^n$ to $GF(2)$. For $x\in GF(2)^n$, $l_v\circ F(x)$ can be expressed by the inner product $v\cdot F(x)$. The Walsh transform of $l_v\circ F$, denoted by $S_F(v,w)$, is called the Walsh transform of F and is described as follows:

$$S_F(v,w)=\frac{1}{2^n}\sum_{x\in GF(2)^n}(-1)^{v\cdot F(x)+w\cdot x}.$$

The function $(-1)^{v\cdot F(x)}$ can be recovered from the inverse Walsh transform,

$$(-1)^{v\cdot F(x)} = \sum_{w\in GF(2)^n} S_F(v,w)(-1)^{w\cdot x}.$$

By Parseval's theorem, we also have

$$\sum_{w\in GF(2)^m} S_F^2(v,w) = 1.$$

Theorem 3 Let F be a function of $GF(2)^n$ to $GF(2)^m$. For any $w \in GF(2)^n$,

$$\mathcal{C}_F(w) = \frac{1}{2^m} \sum_{z\in GF(2)^m} |\sum_{v\in GF(2)^m} S_F(v,w)(-1)^{v\cdot z}|.$$

Proof. Let X be a random variable that takes on values $x \in GF(2)^n$ with uniform probability 2^{-n}, $Z = F(X)$. Then Z is a random variable defined on $GF(2)^m$. For any $w \in GF(2)^n$ and $v \in GF(2)^m$,

$$P(w\cdot X = v\cdot Z) = P(w\cdot X = 0, v\cdot Z = 0) + P(w\cdot X = 1, v\cdot Z = 1). \tag{12}$$

Since

$$P(v\cdot Z = 0) = P(w\cdot X = 0, v\cdot Z = 0) + P(w\cdot X = 1, v\cdot Z = 0), \tag{13}$$

Subtracting (13) by (12),

$$P(v\cdot Z = 0) - P(w\cdot X = v\cdot Z) = P(w\cdot X = 1, v\cdot Z = 0) - P(w\cdot X = 1, v\cdot Z = 1). \tag{14}$$

Furthermore, the right-hand side of (14) can be described by the following sum,

$$\sum_{z\in GF(2)^m} P(w\cdot X = 1, Z = z)(-1)^{v\cdot z},$$

which means that $P(w\cdot X = 1, v\cdot Z = 0) - P(w\cdot X = 1, v\cdot Z = 1)$ is the Walsh transform of $P(w\cdot X = 1, Z = z)$. Taking the inverse Walsh transform,

$$P(w\cdot X = 1, Z = z) = \frac{1}{2^m} \sum_{v\in GF(2)^m} (P(w\cdot X = 1, v\cdot Z = 0) - P(w\cdot X = 1, v\cdot Z = 1)(-1)^{v\cdot z}.$$

From (14), it follows that

$$P(w\cdot X = 1, Z = z) = \frac{1}{2^m} \sum_{v\in GF(2)^m} (P(v\cdot Z = 0) - P(w\cdot X = v\cdot Z))(-1)^{v\cdot z}. \tag{15}$$

Similarly, the probability $P(v\cdot Z = 0)$ can be represented by the following sum,

$$\begin{aligned} P(v\cdot Z = 0) &= \sum_{z\in GF(2)^m} P(Z = z, v\cdot z = 0) \\ &= \sum_{z\in GF(2)^m} P(Z = z)(1 + (-1)^{v\cdot z})/2. \end{aligned}$$

With a slight modification of the above equation, we have

$$2P(v \cdot Z = 0) - 1 = \sum_{z \in GF(2)^m} P(Z = z)(-1)^{v \cdot z},$$

which implies that $2^{-m}(2P(v \cdot Z = 0) - 1)$ is the Walsh transform of $P(Z = z)$. Therefore,

$$P(Z = z) = \frac{1}{2^m} \sum_{v \in GF(2)^m} (2P(v \cdot Z = 0) - 1)(-1)^{v \cdot z}. \tag{16}$$

From (15) and (16), it can be derived that

$$2P(w \cdot X = 1, Z = z) - P(Z = z) = \frac{1}{2^m} \sum_{v \in GF(2)^m} (1 - 2P(w \cdot X = v \cdot Z))(-1)^{v \cdot z}. \tag{17}$$

By Theorem 1,

$$\begin{aligned} \mathcal{C}_F(w) &= \sum_{z \in GF(2)^m} |2P(w \cdot X = 1|_{Z=z}) - 1| P(Z = z) \\ &= \sum_{z \in GF(2)^m} |2P(w \cdot X = 1, Z = z) - P(Z = z)|. \end{aligned}$$

By (17), we have

$$\mathcal{C}_F(w) = \frac{1}{2^m} \sum_{z \in GF(2)^m} | \sum_{v \in GF2^m} (1 - 2P(w \cdot X = v \cdot Z))(-1)^{v \cdot z}|. \tag{18}$$

Since X is uniformly distributed on $GF(2)^n$, $P(w \cdot X = v \cdot Z) - P(w \cdot X \neq v \cdot Z)$ is equal to

$$2^{-n}(|x \in GF(2)^n : w \cdot x = v \cdot F(x)| - |x \in GF(2)^n : w \cdot x \neq v \cdot F(x)|),$$

which is also equal to the following sum,

$$\frac{1}{2^n} \sum_{x \in GF(2)^n} (-1)^{v \cdot F(x) + w \cdot x}.$$

Therefore,

$$P(w \cdot X = v \cdot Z) - P(w \cdot X \neq v \cdot Z) = S_F(v, w).$$

Consequently,

$$2P(w \cdot X = v \cdot Z) - 1 = P(w \cdot X = v \cdot Z) - P(w \cdot X \neq v \cdot Z) = S_F(v, w). \tag{19}$$

Substituting (19) into (18),

$$\mathcal{C}_F(w) = \frac{1}{2^m} \sum_{z \in GF(2)^m} | \sum_{v \in GF(2)^m} S_F(v, w)(-1)^{v \cdot z}|,$$

which proves the theorem. □

Theorem 3 relates the maximum correlation coefficient to the Walsh transforms of a set of Boolean functions. This relationship provides flexibility for the analysis and design of S-boxes. Boolean functions of various cryptographic properties have been intensively investigated and there are a wealth of research results available . Based on Theorem 3, we can make use of the known results about Boolean functions to study the correlation properties of S-boxes.

Theorem 4 Let F be a function of $GF(2)^n$ to $GF(2)^m$. For any $w \in GF(2)^n$,

$$\mathcal{C}_F(w) \leq 2^{\frac{m}{2}} \max_{v \in GF(2)^m} |S_f(v,w)|.$$

Moreover,

$$1 \leq \sum_{w \in GF(2)^n} \mathcal{C}_F^2(w) \leq 2^m.$$

Proof. When $w = 0$, $\mathcal{C}_F(w) = 1$, and the maximum correlator of F to l_0 is 0. Obviously,

$$\sum_{w \in GF(2)^n} \mathcal{C}_F^2(w) \geq 1.$$

By Theorem 2, the maximum correlation coefficient $\mathcal{C}_F(w)$ can be expressed as follows,

$$\mathcal{C}_F(w) = \frac{1}{2^m} \sum_{z \in GF(2)^m} |b_z(w)|,$$

where

$$b_z(w) = \sum_{v \in GF(2)^m} S_F(v,w)(-1)^{v \cdot z}.$$

The sum of the squares of $b_z(w)$ over $z \in GF(2)^m$ is given by

$$\begin{aligned} \sum_{z \in GF(2)^m} b_z^2(w) &= \sum_{z \in GF(2)^m} \sum_{u \in GF(2)^m} S_F(u,w)(-1)^{u \cdot z} \sum_{v \in GF(2)^m} S_F(v,w)(-1)^{v \cdot z} \\ &= \sum_{\substack{u \in GF(2)^m \\ v \in GF(2)^m}} S_F(u,w) S_F(v,w) \sum_{z \in GF(2)^m} (-1)^{(u \oplus v) \cdot z}. \end{aligned}$$

Since

$$\sum_{z \in GF(2)^m} (-1)^{(u \oplus v) \cdot z} = \begin{cases} 2^m, & \text{if} \quad u = v, \\ 0, & \text{otherwise}, \end{cases}$$

we have

$$\sum_{z \in GF(2)^m} b_z^2(w) = 2^m \sum_{v \in GF(2)^m} S_F^2(v,w). \tag{20}$$

By Cauchy inequality,

$$\begin{aligned} \mathcal{C}_F^2(w) &= \frac{1}{2^{2m}} \Big(\sum_{z \in GF(2)^m} |b_z(w)| \Big)^2 \\ &\leq \frac{1}{2^m} \sum_{z \in GF(2)^m} b_z^2(w). \end{aligned}$$

By (20), it follows that

$$\mathcal{C}_F^2(w) \leq \sum_{v \in GF(2)^m} S_F^2(v,w).$$

Hence,

$$\mathcal{C}_F(w) \leq 2^{\frac{m}{2}} \max_{v \in GF(2)^m} |S_f(v,w)|,$$

and

$$\sum_{w\in GF(2)^n} \mathcal{C}_F^2(w) \le \sum_{v\in GF(2)^m} \sum_{w\in GF(2)^n} S_F^2(v,w) = 2^m,$$

which proves the theorem. □

For Booleans functions, it is well known [9] that the sum of the squares of the correlation coefficients is always 1. For S-boxes, however, the sum of the squares of the maximum correlation coefficients might be greater than 1. To defend against correlation attacks, the maximum correlation coefficients should be uniformly small for all nonzero w. Theorem 4 indicates that the maximum correlation coefficients can be controlled through the Walsh spectral coefficients. For any nonzero w, the maximum value of $|S_F(v,w)|$ is at least $2^{-n/2}$. As a consequence, the tightest upper bound deduced from Theorem 4 is $2^{(m-n)/2}$, which means that the number of output bits m can not be too large compared with the number of input bits n. Obviously, increasing the value of m will introduce extra source that leaks information about the input. In the extreme case when $m = n$ and F is a one-to-one function, $\mathcal{C}_F(w) = 1$. Hence, nonlinear permutations are not good combining functions.

Theorem 5 Let F be a function of $GF(2)^n$ to $GF(2)^m$. For any $w \in GF(2)^n, w \neq 0$,

$$\mathcal{C}_F(w) \le 2^{m/2}(1 - 2^{-n+1}\mathcal{N}_f),$$

where $\mathcal{N}_f$ is the nonlinearity of F as defined by (5).

Proof. From (4) and (5), the nonlinearity $\mathcal{N}_f$ can be expressed in terms of the Walsh transform of F,

$$\begin{aligned}\mathcal{N}_F &= \min_{0\neq v\in GF(2)^m} d(l_v \circ F, \mathcal{A}) \\ &= \min_{0\neq v\in GF(2)^m} 2^{n-1}(1 - \max_{w\in GF(2)^n} |S_f(v,w)|).\end{aligned}$$

Thus,

$$\max_{w\in GF(2)^n} \max_{0\neq v\in GF(2)^m} |S_f(v,w)| = 1 - 2^{-n+1}\mathcal{N}_f.$$

For any nonzero $w \in GF(2)^n$, $S_F(0,w) = 0$. Hence,

$$\max_{v\in GF(2)^m} |S_f(v,w)| = \max_{0\neq v\in GF(2)^m} |S_f(v,w)|.$$

By Theorem 4,

$$\begin{aligned}\mathcal{C}_F(w) &\le 2^{\frac{m}{2}} \max_{0\neq v\in GF(2)^m} |S_F(v,w)| \\ &\le 2^{\frac{m}{2}} \max_{w\in GF(2)^n} \max_{0\neq v\in GF(2)^m} |S_F(v,w)| \\ &= 2^{\frac{m}{2}}(1 - 2^{-n+1}\mathcal{N}_f),\end{aligned}$$

which proves the theorem. □

Theorem 5 demonstrates that the maximum correlation coefficients are small if the nonlinearity is large. Hence, nonlinearity does reflect the suitability of S-boxes as nonlinear combining functions in certain extent. Based on Theorem 5, we can control the maximum correlation coefficients by controlling the nonlinearity of S-boxes.

5 Maximum Correlation Analysis of Perfect Nonlinear S-boxes

Originally S-boxes were used in the American Data Encryption Standard (DES). The security analysis of DES has resulted in a series of design criteria [1,3] for S-boxes. These design criteria reflect the capability of DES-like block ciphers to defend against the known attacks. So far, the most successful attacks on DES-like block ciphers are differential cryptanalysis developed by Biham and Shamir [2] and linear cryptanalysis developed by Matsui [8]. Differential cryptanalysis makes uses of the property that with certain changes in the input of an S-box the change in the output is known with a high probability. To immune against differential cryptanalysis, S-boxes should have evenly distributed output changes corresponding to any input changes. Nyberg [10] defines this type of S-boxes as perfect nonlinear S-boxes.

Definition 4 A function F of $GF(2)^n$ to $GF(2)^m$ is called a perfect nonlinear S-box if for every fixed $w \in GF(2)^n$, the difference

$$F(x+w) - F(x)$$

obtains each value $z \in GF(2)^n$ for 2^{n-m} values of x.

When $m = 1$, the perfect nonlinear S-box F is also called a perfect nonlinear Boolean function. In [9] Meier and Staffelbach has proved that perfect nonlinear Boolean functions are actually a class of previously known bent functions introduced by Rothaus [13] in combinatorial theory.

Definition 5 A Boolean function f defined on $GF(2)^n$ is called a bent function if for every $w \in GF(2)^n$, $|S_f(w)| = 2^{-n/2}$.

Nyberg [10] has shown that an S-box is perfect nonlinear if and only if every nonzero linear functions of the output variables are bent functions.

Lemma 2 A function F of $GF(2)^n$ to $GF(2)^m$ is perfect nonlinear if and only if for every nonzero $v \in GF(2)^m$ the function $l_v \circ F$ is a perfect nonlinear Boolean function or bent function.

Based on Lemma 2, two construction methods of perfect nonlinear S-boxes were given by Nyberg. In the following we will study the maximum correlation properties of these S-boxes.

Theorem 6 Let F be a perfect nonlinear S-box of $GF(2)^n$ to $GF(2)^m$. Then for any non-zero $w \in GF(2)^n$,

$$\mathcal{C}_F(w) \leq 2^{(m-n)/2}.$$

Proof. By Lemma 2, $v \cdot F(x)$ is a bent function for every nonzero $v \in GF(2)^m$, thus, for every $w \in GF(2)^n$,

$$|S_F(v,w)| = 2^{-n/2}.$$

When $v = 0$, $S_F(v,w) = 0$ for nonzero w. Hence, for every nonzero $w \in GF(2)^n$,

$$\max_{v \in GF(2)^m} |S_F(v,w)| = \max_{0 \neq v \in GF(2)^m} |S_F(v,w)| = 2^{-n/2}.$$

By Theorem 4, it is clear that

$$\mathcal{C}_F(w) \leq 2^{m/2} \max_{v \in GF(2)^m} |S_F(v,w)| = 2^{(m-n)/2},$$

which proves the theorem. □

For a perfect nonlinear S-box of n-bit input and m-bit output, it is known [9] that the correlation coefficient between each output bit and every nonzero linear functions of the input bits is $2^{-n/2}$, which is very small when n is large. Lemma2 implies that linear functions of the output bits do not help increasing the correlation coefficients. However, Theorem 6 demonstrates that the correlation coefficients might be increased by a factor as large as $2^{m/2}$ if nonlinear functions of the output bits are used. Hence, when used in stream ciphers, we need to consider the number of bits a perfect nonlinear S-box can output. Nyberg [10] has shown that perfect nonlinear S-boxes only exist if $m \leq n/2$. With respect to correlation attacks, we also want to make sure that $2^{(m-n)/2}$ is a very small number. On the other hand, large value of m means large throughput of the data streams generated by keystream generators. Hence, there is a trade-off between the capability to defend against correlation attacks and the throughput of the keystream sequences. In the design of stream ciphers, we choose n and m according to the expected security strength and the throughput requirement.

6 Conclusion

This paper is devoted to the design of S-boxes for stream ciphers. When used to combine several LFSR sequences in a combination generator, S-boxes leak more information about the LFSR sequences than Boolean functions. To control the information leakage, the notion of maximum correlation was introduced. It is a generation of Nyberg's nonlinearity of S-boxes. The merit with maximum correlation is that more information about linear functions of the input may be obtained when all Boolean functions, instead of just linear functions, of the output of the S-box are exploited. In terms of Walsh transform, a spectral characterization of the maximum correlation coefficients was presented, which can be used to investigate upper and lower bounds on the maximum correlation coefficients as well as the relationship between maximum correlation and nonlinearity. For a perfect nonlinear S-box with n-bit input and m-bit output, it was shown that the maximum correlation coefficients are upper bounded by $2^{(m-n)/2}$. Hence, there is a trade-off between the capability to defend against correlation attacks and the throughput of the keystream sequences when perfect nonlinear S-boxes are used in Stream ciphers.

References

[1] C.M. Adams and S.E. Tavares. The structured design of cryptographically good S-boxes. *Journal of Cryptology*, vol. 3, pp. 27-41, 1990.

[2] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, vol. 4, no. 1, pp. 3-72, 1991.

[3] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis. In *Lectures in Computer Science, Advance in Cryptology-EUROCRYPT'94*, vol. 950, pp. 356-365, Springer-Verlag, 1995.

[4] J.H. Cheon, S. Chee, and C. Park. S-boxes with controllable nonlinearity. In *Lecture Notes in Computer Science, Advance in Cryptology-EUROCRYPT'99*, vol. 1592, pp. 286-294, Springer-Verlag, 1999.

[5] T.M. Cover and J.A. Thomas. *Elements of Information Theory.* John Wiley & Sons Inc., 1991.

[6] S.W. Golomb. *Shift Register Sequences.* Holden-Day, San Francisco, 1976. Reprinted by Aegean Park Press, 1982.

[7] M.G. Karpovsky. *Finite Orthogonal Series in the Design of Digital Devices.* New York and Jerudalem: Wiley and TUP, 1976.

[8] M. Matsui. Linear cryptanalysis method for DES ciphers. In *Lecture Notes in Computer Science, Advance in Cryptology-EUROCRYPT'93*, vol. 765, pp. 386-397, Springer-Verlag, 1994.

[9] W. Meier and O. Staffelbach. Nonlinear criteria for cryptographic functions. In *Lecture Notes of Computer Science, Advance in Cryptology: Proceedings of EUROCRYPT'89*, vol. 434, pp. 549–562, Springer–Verlag, 1990.

[10] K. Nyberg. Perfect nonlinear S-boxes. In *Lecture Notes in Computer Science, Advance in Cryptology-EUROCRYPT'91*, vol. 547, pp. 378-385, Springer-Verlag, 1991.

[11] K. Nyberg. On the construction of highly nonlinear permutations. In *Lecture Notes in Computer Science, Advance in Cryptology-EUROCRYPT'92*, vol. 658, pp. 92-98, Springer-Verlag, 1993.

[12] B. Preneel, W.V. Leekwijck, L.V. Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of Boolean functions. In *Lecture Notes in Computer Science, Advance in Cryptology-EUROCRYPT'90*, vol. 473, pp. 161-173, Springer-Verlag, 1991.

[13] O. S. Rothaus. On bent functions. *J. Combinatorial Theory*, Series A, vol. 20, pp. 300–305, 1976.

[14] R. Rueppel. *Analysis and Design of Stream Ciphers.* Springer-Verlag, Berlin, 1986.

[15] R. A. Rueppel. Stream ciphers. In *Contemporary Cryptology: The Science of Information Integrity*, G. Simmons ed., New York: IEEE Press, pp. 65–134, 1991.

[16] J. Seberry, X.M. Zhang, and Y. ZHeng. Systematic generation of cryptographically robust S-boxes. In *Proceedings of the first ACM Conference on Computer and Communications Security*, pp. 172-182, 1993.

[17] T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Trans. Computer*, vol. C-34, no. 1, pp. 81–85, 1985.

[18] Guozhen Xiao and J. L. Massey. A spectral characterization of correlation–immune combining functions. *IEEE Trans. on Information Theory*, vol. IT–34, no. 3, pp. 564–571, 1988.