Maximum Correlation Analysis of Nonlinear S-boxes in Stream Ciphers

Muxiang Zhang[1] and Agnes Chan[2]

[1] GTE Laboratories Inc., 40 Sylvan Road LA0MS59, Waltham, MA 02451
mzhang@gte.com
[2] College of Computer Science, Northeastern University, Boston, MA 02115
ahchan@ccs.neu.edu

Abstract. This paper investigates the design of S-boxes used for combining linear feedback shift register (LFSR) sequences in combination generators. Such combination generators have higher throughput than those using Boolean functions as the combining functions. However, S-boxes tend to leak more information about the LFSR sequences than Boolean functions. To study 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. Using Walsh transform, a spectral characterization of the maximum correlation coefficients, together with their upper and lower bounds, are established. For the perfect nonlinear S-boxes designed for block ciphers, 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. 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. A combination generator consists of several linear feedback shift registers 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 output 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 some

M. Bellare (Ed.): CRYPTO 2000, LNCS 1880, pp. 501–514, 2000.

linear functions of its input, in fact, 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 function 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 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 extensively studied [1,3,4,10,16]. In this paper, we investigate the design of S-boxes for stream ciphers. Compared with a combination generator using 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 bit of the S-box leaks 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. It is shown that the mutual information between the output of an S-box and linear functions of the input is bounded by the maximum correlation coefficients. In terms of the Walsh transform, a spectral characterization of the maximum correlation coefficients is developed. Based on the spectral characterization bounds on the maximum correlation coefficients are developed, as well as the relationship between maximum correlation and nonlinearity [11] of S-boxes. For the perfect nonlinear S-boxes [10] designed for block ciphers to defend against differential cryptanalysis, an upper bound on the maximum correlation coefficient is presented.

2 Maximum Correlation of S-boxes

An S-box of n-bit input and m-bit output can be described by a function F from $GF(2)^n$ 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., $z = F(x)$. Then F can be represented 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. In addition, the m binary sequences can also be combined together to perform correlation attacks. In this case, larger correlation to the LFSR-sequences may 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 has small correlation to linear functions of the input. It is clear that the second design rule is a generalization of the first one. To investigate the correlation properties of S-boxes, let's first review the notion of correlation coefficient of Boolean functions.

Definition 1. Let $f, g : GF(2)^n \to GF(2)$ be Boolean functions and X be a uniformly distributed random variable over $GF(2)^n$. Then $Z = f(X)$ and $Z' = g(X)$ are random variables over $GF(2)$. The correlation coefficient of f and g, denoted by $c(f, g)$, is defined as follows:

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

The correlation with linear functions is of special interest in the analysis and design of stream ciphers. A linear function of n variables can be expressed as an inner product, $w \cdot x = w_1x_1 \oplus w_2x_2 \oplus \ldots \oplus w_nx_n$. Such a linear function is often denoted by $l_w(x)$. The correlation coefficient $c(f, l_w)$ describes the statistical dependency between f and l_w, and is interpreted as the nonlinearity of f with respect to l_w.

Definition 2. Let F be a function from $GF(2)^n$ to $GF(2)^m$ and let $\mathcal{G}$ denote the set of all Boolean functions defined on $GF(2)^m$. 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 $g \in \mathcal{G}$ and $c(g \circ F, l_w)$ is maximum, then g is called the maximum correlator of F to l_w.

Nyberg [11] has investigated a special case where the set $\mathcal{G}$ contains only linear and affine functions. Based on Hamming distance, Nyberg defined the nonlinearity of S-boxes. The Hamming distance between two Boolean functions $f, g : GF(2)^n \to GF(2)$ is defined by

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

It is easy to prove [15] that the Hamming distance $d(f, g)$ is related to the correlation coefficient $c(f, g)$ by

$$c(f, g) = 1 - 2^{-n+1}d(f, g). \tag{2}$$

Definition 3. Let F be a function from $GF(2)^n$ to $GF(2)^m$. The nonlinearity of F is defined as

$$\mathcal{N}_F = \min_{\substack{v \in GF(2)^m \\ v \neq 0}} \min_{\substack{w \in GF(2)^n \\ a \in GF(2)}} d(l_v \circ F, a \oplus l_w). \tag{3}$$

Assume that $\mathcal{N}_F = d(l_v \circ F, a \oplus l_w)$ for some nonzero $v \in GF(2)^m$ and some affine function $a \oplus l_w$. It is clear that $\mathcal{N}_F$ is also equal to $d(a \oplus l_v \circ F, l_w)$. By (2) and (3), $c(a \oplus l_v \circ F, l_w)$ is the maximum correlation between linear and affine functions of the output and linear functions of the input of F. By Definition 2, it is obvious that $c(a \oplus l_v \circ F, l_w) \leq \mathcal{C}_F(w)$, with strict inequality if the maximum correlator of F to l_w is not linear. Hence, the nonlinearity of F does not necessarily imply maximum correlation between the output and linear functions of the input.

In general, it is difficult to figure out the maximum correlation coefficients since there are 2^{2^m} functions in $\mathcal{G}$. The following theorem provides a method to compute the maximum correlation coefficients.

Theorem 1. Let F be a function from $GF(2)^n$ to $GF(2)^m$ and X be a uniformly distributed random variable over $GF(2)^n$, $Z = F(X)$. For $w \in GF(2)^n$ and $z \in GF(2)^m$, let $e_w(z)$ denote the conditional probability difference between $w \cdot X = 1$ and $w \cdot X = 0$ under the condition $Z = z$, namely,

$$e_w(z) = P(w \cdot X = 1 | Z = z) - P(w \cdot X = 0 | Z = z). \tag{4}$$

Then

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

Moreover, the function $g(z) = sgn(e_w(z))$ 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 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 $P(w \cdot X = g(Z)) + P(w \cdot X \neq g(Z)) = 1$, $c(g \circ F, l_w)$ can be represented as follows

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

Therefore,

$$\max_{g \in \mathcal{G}} c(g \circ F, l_w) = \max_{g \in \mathcal{G}} \sum_{z \in GF(2)^n} (2P(w \cdot X = g(z)|_{Z=z}) - 1) P(Z = z). \tag{5}$$

Note that maximizing the sum in (5) is equivalent to maximizing every term in the sum, i.e.,

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

As $g(z)\in GF(2)$ and $P(w\cdot X=1|Z=z)+P(w\cdot X=0|Z=z)=1$, 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,

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

while

$$2P(w\cdot X=0|Z=z)-1 = P(w\cdot X=0|Z=z)-P(w\cdot X=1|Z=z).$$

Hence,

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

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 $g(z)=sgn(e_w(z))$ is the maximum correlator of F to l_w.

Based on Theorem 1, the maximum correlation of F to l_w can be computed when the conditional probability difference $e_w(z)$ is known for every $z\in GF(2)^m$. The conditional probability difference can be calculated from the algebraic expression or from the truth table of F, with a complexity 2^{m+n}, which is far below $2^n 2^{2^m}$ as required by exhaustive search. Furthermore, if $Z=F(X)$ is uniformly distributed over $GF(2)^m$, Theorem 1 implies the following bounds for $\mathcal{C}_F(w)$,

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

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 some 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. Using maximum correlation, we can approximate the random variable $w\cdot X$ by a Boolean function of Z. 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

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

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.,

$$h(x) = -x\log_2 x - (1-x)\log_2(1-x), \quad 0 \le x \le 1. \tag{6}$$

Then, for $-0.5 \le x \le 0.5$, $1 - 2|x| \le h(0.5+x) \le 1 - 2(\log_2 e)x^2$.

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, $\varphi(x) \ge \varphi(0) = 0$.

Definition 4. Let F be a function from $GF(2)^n$ to $GF(2)^m$ and X be a uniformly distributed random variable over $GF(2)^n$. If $Z = F(X)$ is uniformly distributed over $GF(2)^m$, then F is called a balanced function.

Theorem 2. Let F be a balanced function from $GF(2)^n$ to $GF(2)^m$ and X be a uniformly distributed random variable over $GF(2)^n$, $Z = F(X)$. 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 any 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

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

Using the binary entropy function $h()$ defined in (6), the mutual information $I(w\cdot X; Z)$ can be expressed as

$$I(w\cdot X; Z) = 1 - \frac{1}{2^m}\sum_{z\in GF(2)^m} h(P(w\cdot x = 1|Z=z)). \tag{7}$$

By (4), $P(w\cdot X = 1|Z=z)$ can be replaced by $0.5 + e_w(z)/2$. Thus,

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

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,

$$\frac{1}{2^m} \sum_{z \in GF(2)^m} \frac{\log_2 e}{2} (e_w(z))^2 \le I(w \cdot X; Z) \le \frac{1}{2^m} \sum_{z \in GF(2)^m} |e_w(z)|. \quad (8)$$

By Theorem 1, it is clear that $I(w \cdot X; Z) \le \mathcal{C}_F(w)$.

Next, by Cauchy's 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 (8), it follows that

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

Again, 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 flexibility for the analysis and design of S-boxes. Conceptually, mutual information provides us a tool to analyze the information leakage from the output bits while maximum correlation explicitly describes 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 balanced function F with $\mathcal{C}_F(w) < \delta$.

3 A Spectral Characterization of Maximum Correlation Coefficients

In the analysis and design of Boolean functions, Walsh transform [6] has played an important role. The merit of Walsh transform lies in that it provides illustrative description of Boolean functions having certain cryptographic properties [12,18]. The Walsh transform of a real-valued function f on $GF(2)^n$ is defined as follows:

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

The function $f(x)$ can be recovered from the inverse Walsh transform,

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

When f is a Boolean function, we often turn it into a function $\hat{f}(x) = (-1)^{f(x)}$ and define the Walsh transform of f as that of $\hat{f}$.

Let F be a function from $GF(2)^n$ to $GF(2)^m$. For any $v \in GF(2)^m$, $l_v \circ F$ defines a Boolean function on $GF(2)^n$. 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 given by

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

Theorem 3. Let F be a function from $GF(2)^n$ 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 uniformly distributed random variable over $GF(2)^n$ and $Z = F(X)$. For any $w \in GF(2)^n$ and $v \in GF(2)^m$,

$$P(w \cdot X = v \cdot Z) = P(w \cdot X = 0, v \cdot Z = 0) + P(w \cdot X = 1, v \cdot Z = 1). \quad (9)$$

Since $P(v \cdot Z = 0) = P(w \cdot X = 0, v \cdot Z = 0) + P(w \cdot X = 1, v \cdot Z = 0)$, we have

$$P(v \cdot Z = 0) - P(w \cdot X = v \cdot Z) = P(w \cdot X = 1, v \cdot Z = 0) - P(w \cdot X = 1, v \cdot Z = 1). \quad (10)$$

Note that the right-hand side of (10) is equal to the sum,

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

which implies that $P(v \cdot Z = 0) - P(w \cdot X = v \cdot Z)$ is the Walsh transform of $2^m P(w \cdot X = 1, Z = z)$. Taking the inverse Walsh transform,

$$P(w \cdot X = 1, Z = z) = \frac{1}{2^m} \sum_{v \in GF(2)^m} (P(v \cdot Z = 0) - P(w \cdot X = v \cdot Z))(-1)^{v \cdot z}. \quad (11)$$

Next, the probability $P(v \cdot Z = 0)$ can also be expressed by the following sum,

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

Thus,

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

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

$$P(Z = z) = \frac{1}{2^m} \sum_{v \in GF(2)^m} (2P(v \cdot Z = 0) - 1)(-1)^{v \cdot z}. \quad (12)$$

From (11) and (12), it follows that

$$2P(w \cdot X = 1, Z = z) - P(Z = z) = \frac{1}{2^m} \sum_{v \in GF(2)^m} (1 - 2P(w \cdot X = v \cdot Z))(-1)^{v \cdot z}. \tag{13}$$

By Theorem 1,

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

Hence, by (13),

$$\mathcal{C}_F(w) = \frac{1}{2^m} \sum_{z \in GF(2)^m} | \sum_{v \in GF2^m} (1 - 2P(w \cdot X = v \cdot Z))(-1)^{v \cdot z}|. \tag{14}$$

Since X is uniformly distributed over $GF(2)^n$, $P(w \cdot X = v \cdot Z) - P(w \cdot X \neq v \cdot Z)$ equals 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 can be represented as

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

Therefore,

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

As a consequence,

$$2P(w \cdot X = v \cdot Z) - 1 = P(w \cdot X = v \cdot Z) - P(w \cdot X \neq v \cdot Z) = S_F(v, w). \tag{15}$$

Substituting (15) into (14),

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

Theorem 3 relates the maximum correlation coefficient to the Walsh transforms of a set of Boolean functions. Since Boolean functions have been extensively studied with respect to various cryptographic properties. Using 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 from $GF(2)^n$ to $GF(2)^m$. For any $w \in GF(2)^n$,

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

Moreover,

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

Proof. By definition 2, it is obvious that $\mathcal{C}_F(0) = 1$. Hence,

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

By Theorem 3, the maximum correlation coefficient $\mathcal{C}_F(w)$ can be expressed as

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

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 described by

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

According to the orthogonal property of Walsh function [7],

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

Hence,

$$\sum_{z \in GF(2)^m} b_z^2(w) = 2^m \sum_{v \in GF(2)^m} S_F^2(v, w). \tag{16}$$

By Cauchy inequality,

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

By (16), it follows that

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

Hence,

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

and

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

By Parsevals's Theorem [7],

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

Therefore,

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

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. It has been shown [9] that 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 weak combining functions.

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

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

where $\mathcal{N}_F$ is the nonlinearity of F defined by (3).

Proof. As has been shown in [9], the nonlinearity $\mathcal{N}_F$ can be expressed in terms of the Walsh transform of F,

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

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,

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

Theorem 5 demonstrates that the maximum correlation coefficients are small if the nonlinearity is large. Based on Theorem 5, we can control the maximum correlation coefficients by controlling the nonlinearity of S-boxes.

4 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 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 5. A function F from $GF(2)^n$ to $GF(2)^m$ is called a perfect nonlinear S-box if for every fixed $w \in GF(2)^n$, the difference $F(x+w) - F(x)$ takes on 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 proved that perfect nonlinear Boolean functions are actually a class of previously known bent functions introduced by Rothaus [13] in combinatorial theory.

Definition 6. 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 function of the output variables is a bent functions.

Lemma 2. A function F from $GF(2)^n$ 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 from $GF(2)^n$ 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

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

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 function of the input bits is $2^{-n/2}$, which is very small when n is large. Lemma 2 implies that linear functions of the output bits do not help increasing the correlation coefficients. However, Theorem 6 demonstrates that the correlation coefficients may 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 should 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.

5 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 is introduced. It is a generalization 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 is 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 is shown that the maximum correlation coefficients are upper bounded by $2^{(m-n)/2}$.

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, Advances 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, Advances 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, Advances 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, Advances 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.