J. Cryptology (2000) 13: 301–313
DOI: 10.1007/s001450010007

Journal of
CRYPTOLOGY

© 2000 International Association for Cryptologic Research

Maximum Correlation Analysis of Nonlinear Combining Functions in Stream Ciphers*

Muxiang Zhang
College of Computer Science, Northeastern University,
Boston, MA 02115, U.S.A.
zhangmx@ccs.neu.edu

Communicated by James Massey

Received 14 February 1996 and revised 15 January 2000
Online publication 9 May 2000

Abstract. The maximum correlation of a Boolean function to all Boolean functions of a subset of its input variables is investigated. A relationship is derived between the maximum correlation and the mutual information between the output of a balanced Boolean function and a subset of its random input variables. For bent functions (which are never balanced), both the mutual information and the maximum correlation are bounded and shown to be small in a strong sense.

Key words. Stream cipher, Keystream generator, Correlation attack, Boolean function, Mutual information.

1. Introduction

In stream ciphers a common form of keystream generator is the combination generator which consists of several linear feedback shift registers (LFSRs) whose output sequences are combined by a nonlinear Boolean function. A major goal of the keystream generator is to produce random-looking sequences, that is, sequences that as closely as possible resemble coin-tossing sequences. If the keystream sequence is correlated with an LFSR sequence, Siegenthaler [13] has shown that the subkey residing in the LFSR can be analyzed independently of subkeys residing in other LFSRs. Siegenthaler's method that independently solves for the subkey residing in each LFSR is referred to as a divide-and-conquer correlation attack. Further extensions and refinements of Siegenthaler's correlation attack can be found in [6], [15], [4], and [8]. In subsequent work [12] Siegenthaler has also noticed that correlation attacks in which more than one subkeys are analyzed can still be made even if there is no correlation between the keystream sequence and any single LFSR sequence. For this reason, Siegenthaler introduced the notion of correlation-immunity.

* This work was partially done while the author was on leave from the Department of Applied Mathematics, Xidian University, Xian, Shaanxi 710071, People's Republic of China.

A Boolean function f of n input variables is called mth-order correlation-immune if the output of f is statistically independent of every subset of m random input variables. It has been shown in [14] and [1] that f is mth-order correlation-immune if and only if f is not correlated to linear functions of any subset of m input variables. Consequently, the keystream sequence is independent of linear combinations of m LFSR sequences when f is used as the combiner. However, Meier and Staffelbach [7] have proved that the sum of the squares of the correlation coefficients of f to all linear functions is always one. Thus, zero correlation to some linear functions implies a stronger correlation to other linear functions. The best one can do is to make the correlation to every linear functions uniformly small. Meier and Staffelbach [7] have also shown that the previously known bent functions introduced by Rothaus [10] in combinatorial theory have such a nice property. With bent functions, it is easy to design combination generators whose keystream sequences have small correlation to linear functions of the LFSR sequences. However, bent functions only guarantee small correlation to linear functions. If a bent function has a large correlation to nonlinear functions of a few of the input variables, one can still perform correlation attacks when the bent function is used as a nonlinear combiner. This motivates us to investigate the maximum correlation of a Boolean function to all Boolean functions (linear and nonlinear) of a subset of its input variables.

In this paper the mutual information is used to measure the correlation between the output of a Boolean function and a subset of its random input variables. For balanced Boolean functions a relationship between the mutual information and the maximum correlation is derived. It is shown that the larger the mutual information, the stronger the maximum correlation, and vice versa. For bent functions (which are never balanced), both the mutual information and the maximum correlation are bounded and shown to be small in a strong sense.

2. Maximum Correlation and Mutual Information

Let $z = f(x_1, x_2, \ldots, x_n)$ be a Boolean function. We assume from hereon that the n input variables $x_1, x_2, \ldots, x_n$ are independent and uniformly distributed binary random variables. If z is also uniformly distributed, f is called a balanced Boolean function. For a subset $\mathbf{x}' = (x_{i_1}, x_{i_2}, \ldots, x_{i_m})$ of m input variables, the correlation or statistical dependency between z and $\mathbf{x}'$ is measured by the mutual information $I(z; \mathbf{x}')$,

$$I(z; \mathbf{x}') = \sum_{k \in GF(2)} -P(z = k) \log_2 P(z = k) + \sum_{\substack{k \in GF(2) \\ \mathbf{y} \in GF(2)^m}} P(z = k, \mathbf{x}' = \mathbf{y}) \log_2 P(z = k|_{\mathbf{x}' = \mathbf{y}}).$$

Since $x_{i_1}, x_{i_2}, \ldots, x_{i_m}$ are independent and uniformly distributed random variables, $P(\mathbf{x}' = \mathbf{y}) = 2^{-m}$. Let $h(x)$ denote the binary entropy function, that is,

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

Then the mutual information $I(z; \mathbf{x}')$ can be represented as follows:

$$I(z; \mathbf{x}') = h(P(z = 1)) - \frac{1}{2^m} \sum_{\mathbf{y} \in GF(2)^m} h(P(z = 1|_{\mathbf{x}'=\mathbf{y}})). \tag{2}$$

Since $0 \le h(x) \le 1$, it is clear that $0 \le I(z; \mathbf{x}') \le 1$. If $I(z; \mathbf{x}') = 1$, z is completely determined by $\mathbf{x}'$, that is, there exists a Boolean function g such that $z = g(\mathbf{x}')$. If, for every subset $\mathbf{x}'$ of m variables, $I(z; \mathbf{x}') = 0$, then f is mth-order correlation-immune [12].

Definition 1. Let $z = f(x_1, x_2, \ldots, x_n)$ and $z' = g(x_1, x_1, \ldots, x_n)$ be Boolean functions. The correlation coefficient of f and g, denoted by $C(f, g)$, is defined as follows:

$$C(f, g) = P(z = z') - P(z \ne z').$$

Since $P(z = z') + P(z \ne z') = 1$, the probability $P(z = z')$ is related to $C(f, g)$ by the following equation:

$$P(z = z') = \frac{1}{2} + \frac{C(f, g)}{2}. \tag{3}$$

Definition 2. Let $z = f(x_1, x_2, \ldots, x_n)$ be a Boolean function. For a subset $\mathbf{x}'$ of m variables $x_{i_1}, x_{i_2}, \ldots, x_{i_m}$, let G denote the set of all Boolean functions of $\mathbf{x}'$. The maximum correlation of f to G, denoted by $C_f(\mathbf{x}')$, is defined as follows:

$$C_f(\mathbf{x}') = \max_{g \in G} C(f, g). \tag{4}$$

For simplicity, $C_f(\mathbf{x}')$ is referred to as the maximum correlation of f with respect to $\mathbf{x}'$. If $g \in G$ and $C(f, g) = C_f(\mathbf{x}')$, then g is called a maximum correlator of f with respect to $\mathbf{x}'$.

Since there are 2^{2^m} Boolean functions of $\mathbf{x}'$, it is difficult to compute $C_f(\mathbf{x}')$ through exhaustive search. If f is balanced, then the following theorem demonstrates that the computation complexity can be greatly reduced.

Theorem 1. *Let $z = f(x_1, x_2, \ldots, x_n)$ be a balanced Boolean function, i.e., $P(z = 1) = 0.5$. For a subset $\mathbf{x}' = (x_{i_1}, x_{i_2}, \ldots, x_{i_m})$ of m variables, let*

$$e_{\mathbf{x}'}(\mathbf{y}) = P(z = 1|_{\mathbf{x}'=\mathbf{y}}) - P(z = 1). \tag{5}$$

Then

$$C_f(\mathbf{x}') = \frac{2}{2^m} \sum_{\mathbf{y} \in GF(2)^m} |e_{\mathbf{x}'}(\mathbf{y})|,$$

and $\hat{g}$ is a maximum correlator of f with respect to $\mathbf{x}'$ if and only if, for any $\mathbf{y} \in GF(2)^m$, $\hat{g}(\mathbf{y}) = \operatorname{sgn}(e_{\mathbf{x}'}(\mathbf{y}))$, where

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

Proof. Let g be a Boolean function of $\mathbf{x}'$ and $z' = g(\mathbf{x}')$. By Definition 1,

$$C(f,g) = P(z = z') - P(z \neq z').$$

Since $x_1, x_2, \ldots, x_n$ are independent and uniformly distributed binary random variables, the correlation coefficient $C(f,g)$ can be represented as follows:

$$\begin{aligned} C(f,g) &= \frac{1}{2^n} \sum_{\mathbf{x} \in GF(2)^n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x})} \\ &= \frac{1}{2^n} \sum_{\mathbf{x} \in GF(2)^n} (1 - 2f(\mathbf{x}))(1 - 2g(\mathbf{x})) \\ &= 1 - 2P(z = 1) - 2P(z' = 1) + \frac{4}{2^n} \sum_{\mathbf{x} \in GF(2)^n} f(\mathbf{x}) g(\mathbf{x}). \end{aligned}$$

Let $\mathbf{x}'' = (x_{i_{m+1}}, x_{i_{m+2}}, \ldots, x_{i_n})$ denote the $n - m$ variables of $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ that are not in $\mathbf{x}'$. Since $x_{i_{m+1}}, x_{i_{m+2}}, \ldots, x_{i_n}$ are not input variables of g, it is clear that

$$\begin{aligned} \frac{4}{2^n} \sum_{\mathbf{x} \in GF(2)^n} f(\mathbf{x}) g(\mathbf{x}) &= \frac{4}{2^n} \sum_{\mathbf{x}' \in GF(2)^m} g(\mathbf{x}') \sum_{\mathbf{x}'' \in GF(2)^{n-m}} f(\mathbf{x}) \\ &= \frac{4}{2^m} \sum_{\mathbf{y} \in GF(2)^m} g(\mathbf{y}) P(z = 1|_{\mathbf{x}' = \mathbf{y}}). \end{aligned}$$

Hence, it follows that

$$C(f,g) = 1 - 2P(z = 1) - 2P(z' = 1) + \frac{4}{2^m} \sum_{\mathbf{y} \in GF(2)^m} g(\mathbf{y}) P(z = 1|_{\mathbf{x}' = \mathbf{y}}). \tag{6}$$

By (5),

$$P(z = 1|_{\mathbf{x}' = \mathbf{y}}) = e_{\mathbf{x}'}(\mathbf{y}) + P(z = 1). \tag{7}$$

Since f is balanced, $P(z = 1) = 0.5$. Substituting (7) into (6), $C(f,g)$ can be represented as the following form:

$$C(f,g) = \frac{4}{2^m} \sum_{\mathbf{y} \in GF(2)^m} g(\mathbf{y}) e_{\mathbf{x}'}(\mathbf{y}).$$

As $g(\mathbf{y}) \in \{0, 1\}$ and

$$\sum_{\mathbf{y} \in GF(2)^m} e_{\mathbf{x}'}(\mathbf{y}) = 0,$$

it can be concluded that

$$\sum_{\mathbf{y} \in GF(2)^m} g(\mathbf{y}) e_{\mathbf{x}'}(\mathbf{y}) \leq \frac{1}{2} \sum_{\mathbf{y} \in GF(2)^m} |e_{\mathbf{x}'}(\mathbf{y})|, \tag{8}$$

with equality if and only if $g(\mathbf{y}) = sgn(e_{\mathbf{x}'}(\mathbf{y}))$, which completes the proof of the theorem. □

Table 1. Maximum correlation of $f(\mathbf{x}) = x_1 \oplus x_2x_3 \oplus x_2x_5 \oplus x_4x_5$.

$\mathbf{x}'$	$C_f(\mathbf{x}')$	Maximum correlator
x_1	0.25	x_1
x_1x_2	0.25	$x_1 \oplus x_2$
x_1x_3	0.25	$x_1 \oplus x_3$
x_1x_4	0.25	$x_1 \oplus x_4$
x_1x_5	0.25	$x_1 \oplus x_5$
$x_1x_2x_3$	0.5	$x_1 \oplus x_2x_3$
$x_1x_2x_4$	0.25	$x_1 \oplus x_2x_4$
$x_1x_2x_5$	0.25	$x_1 \oplus x_2x_5$
$x_1x_3x_4$	0.5	$x_1 \oplus x_3x_4$
$x_1x_3x_5$	0.25	$x_1 \oplus x_3x_5$
$x_1x_4x_5$	0.5	$x_1 \oplus x_4x_5$
$x_1x_2x_3x_4$	0.5	$x_1 \oplus x_2x_3x_4$
$x_1x_2x_3x_5$	0.5	$x_1 \oplus x_2x_3 \oplus x_2x_3x_5$
$x_1x_2x_4x_5$	0.5	$x_1 \oplus x_4x_5 \oplus x_2x_4x_5$
$x_1x_3x_4x_5$	0.5	$x_1 \oplus x_3x_4x_5$
$x_1x_2x_3x_4x_5$	1.0	$x_1 \oplus x_2x_3 \oplus x_2x_5 \oplus x_4x_5$

From Theorem 1, it is clear that the maximum correlator of a balanced Boolean function may not be unique. Knowing the probability differences as described by (5), one can determine all the maximum correlators of f. The probability differences can be calculated from the logical expression or directly from the truth table of f, with a computational complexity of $O(2^n)$. As an example, the maximum correlation of $f(x_1, x_2, x_3, x_4, x_5) = x_1 \oplus x_2x_3 \oplus x_2x_5 \oplus x_4x_5$ with respect to every subset $\mathbf{x}'$ of its variables has been computed based on Theorem 1. The results are outlined in Table 1. For those $\mathbf{x}'$ not appearing in the table, $C_f(\mathbf{x}') = 0$.

Lemma 1. *Let $h(x)$ denote the binary entropy function as defined in* (1). *For* $-0.5 \leq x \leq 0.5$,

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

Moreover,

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

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 $\psi(x) \geq 0$, for $-0.5 \leq x \leq 0.5$, i.e., $h(0.5 + x) \geq 1 - 2|x|$.

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 $-\log_2(x)$, it is clear that

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

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

Theorem 2. *Let $z = f(x_1, x_2, \ldots, x_n)$ be a Boolean function. Then for any subset $\mathbf{x}'$ of m variables $x_{i_1}, x_{i_2}, \ldots, x_{i_m}$,*

$$I(z;\mathbf{x}') \le C_f(\mathbf{x}') \le \sqrt{(2\ln 2) I(z;\mathbf{x}')}.$$

Proof. Since f is balanced, $P(z=1) = 0.5$, and consequently $h(P(z=1)) = 1$. By (2), the mutual information $I(z;\mathbf{x}')$ is expressed by

$$I(z;\mathbf{x}') = 1 - \frac{1}{2^m} \sum_{\mathbf{y} \in GF(2)^m} h(0.5 + e_{\mathbf{x}'}(\mathbf{y})).$$

By Lemma 1,

$$1 - 2|e_{\mathbf{x}'}(\mathbf{y})| \le h(0.5 + e_{\mathbf{x}'}(\mathbf{y})) \le 1 - \tfrac{1}{2}(2e_{\mathbf{x}'}(\mathbf{y}))^2 \log_2 e.$$

Hence,

$$\frac{1}{2^m} \sum_{\mathbf{y} \in GF(2)^m} \frac{\log_2 e}{2} (2e_{\mathbf{x}'}(\mathbf{y}))^2 \le I(z;\mathbf{x}') \le \frac{1}{2^m} \sum_{\mathbf{y} \in GF(2)^m} 2|e_{\mathbf{x}'}(\mathbf{y})|.$$

By Theorem 1, $C_f(\mathbf{x}') \ge I(z;\mathbf{x}')$.

Next, by the Cauchy inequality,

$$\sum_{\mathbf{y} \in GF(2)^m} (2e_{\mathbf{x}'}(\mathbf{y}))^2 \ge \frac{1}{2^m} \left(\sum_{\mathbf{y} \in GF(2)^m} 2|e_{\mathbf{x}'}(\mathbf{y})| \right)^2.$$

Thus,

$$I(z;\mathbf{x}') \ge \frac{\log_2 e}{2} \left(\frac{2}{2^m} \sum_{\mathbf{y} \in GF(2)^m} |e_{\mathbf{x}'}(\mathbf{y})| \right)^2.$$

Again, by Theorem 1, $C_f(\mathbf{x}') \le \sqrt{(2\ln 2) I(z;\mathbf{x}')}$. □

Recall that the mutual information $I(z;\mathbf{x}')$ is a measure of the statistical dependency between z and $\mathbf{x}'$. For balanced Boolean functions, Theorem 2 establishes a relationship

between the mutual information and the maximum correlation coefficients. To defend against correlation attacks using linear or nonlinear combinations of a few LFSR sequences, the correlation between the keystream sequence and every small subset of LFSR sequences should be as small as possible, which coincides with the idea of correlation-immunity.

Let m be the maximum correlation-immunity order of a Boolean function $f(x_1, x_2, \ldots, x_n)$. It has been shown in [14] that f is correlated to at least one linear function of $m+1$ variables. Furthermore, it has been shown in [16] that the maximum correlation of f to all linear functions of $m+1$ variables is greater than or equal to $1/2^{n-m-1}$. In [5] it has been expected that nonlinear Boolean functions of $m+1$ variables might further increase the correlation. However, the following theorem demonstrates that Boolean functions of $m+1$ variables that are maximally correlated to a balanced mth-order correlation-immune function must be linear or affine.

In the analysis and design of Boolean functions, Walsh transform is a very useful tool. The Walsh transform of a Boolean function $f(x_1, x_2, \ldots, x_n)$ is defined as follows:

$$\hat{F}(\omega) = \frac{1}{2^n} \sum_{\mathbf{x} \in GF(2)^n} (-1)^{f(\mathbf{x}) \oplus \omega \cdot \mathbf{x}},$$

where $\omega \cdot \mathbf{x} = \omega_1 x_1 \oplus \omega_2 x_2 \oplus \cdots \oplus \omega_n x_n$, $\omega \in GF(2)^n$. The function $\hat{f}(\mathbf{x}) = (-1)^{f(\mathbf{x})}$ can be recovered from the inverse Walsh transform

$$\hat{f}(\mathbf{x}) = \sum_{\omega \in GF(2)^n} \hat{F}(\omega)(-1)^{\omega \cdot \mathbf{x}}.$$

Theorem 3. *Let $z = f(x_1, x_2, \ldots, x_n)$ be a balanced mth-order correlation-immune Boolean function. For a subset $\mathbf{x}' = (x_{i_1}, x_{i_2}, \ldots, x_{i_{m+1}})$ of $m+1$ variables, assume that $I(z; \mathbf{x}') \neq 0$. Then the maximum correlator of f with respect to $\mathbf{x}'$ is either $x_{i_1} \oplus x_{i_2} \oplus \cdots \oplus x_{i_{m+1}}$ or $1 \oplus x_{i_1} \oplus x_{i_2} \oplus \cdots \oplus x_{i_{m+1}}$.*

Proof. Let g be a Boolean function of $\mathbf{x}'$ and $z' = g(\mathbf{x}')$. By Definition 1,

$$\begin{aligned} C(f, g) &= P(z = z') - P(z \neq z') \\ &= \frac{1}{2^n} \sum_{\mathbf{x} \in GF(2)^n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x})} \\ &= \frac{1}{2^n} \sum_{\mathbf{x} \in GF(2)^n} \hat{f}(\mathbf{x}) \hat{g}(\mathbf{x}). \end{aligned}$$

By Parseval's theorem [11],

$$\frac{1}{2^n} \sum_{\mathbf{x} \in GF(2)^n} \hat{f}(\mathbf{x}) \hat{g}(\mathbf{x}) = \sum_{\omega \in GF(2)^n} \hat{F}(\omega) \hat{G}(\omega).$$

Hence,

$$C(f, g) = \sum_{\omega \in GF(2)^n} \hat{F}(\omega) \hat{G}(\omega). \tag{9}$$

Let $\mathbf{x}'' = (x_{i_{m+2}}, x_{i_{m+3}}, \ldots, x_{i_n})$ denote the variables of $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ that are not in $\mathbf{x}'$. Correspondingly, for any $\omega = (\omega_1, \omega_2, \ldots, \omega_n) \in GF(2)^n$, let $\omega' = (\omega_{i_1}, \omega_{i_2}, \ldots, \omega_{i_{m+1}})$ and $\omega'' = (\omega_{i_{m+2}}, \omega_{i_{m+3}}, \ldots, \omega_{i_n})$. Since $g(\mathbf{x}) = g(\mathbf{x}')$, $\hat{G}(\omega)$ can be described as follows:

$$\begin{aligned}\hat{G}(\omega) &= \frac{1}{2^n} \sum_{\mathbf{x} \in GF(2)^n} \hat{g}(\mathbf{x})(-1)^{\omega \cdot \mathbf{x}} \\ &= \frac{1}{2^n} \sum_{\mathbf{x}' \in GF(2)^{m+1}} \hat{g}(\mathbf{x}')(-1)^{\omega' \cdot \mathbf{x}'} \sum_{\mathbf{x}'' \in GF(2)^{n-m-1}} (-1)^{\omega'' \cdot \mathbf{x}''}.\end{aligned}$$

According to the orthogonal property of Walsh function, for all nonzero ω'', $(-1)^{\omega'' \cdot \mathbf{x}''} = 0$. Consequently, (9) can be rewritten as follows:

$$C(f, g) = \sum_{\substack{\omega' \in GF(2)^{m+1} \\ \omega'' = \mathbf{0}}} \hat{F}(\omega)\hat{G}(\omega).$$

Since f is a balanced mth-order correlation-immune Boolean function [14], $\hat{F}(\omega) = 0$ for all ω with $W(\omega) \leq m$, where $W(\omega)$ denotes the Hamming weight of ω. Therefore,

$$C(f, g) = \hat{F}(\theta)\hat{G}(\theta), \tag{10}$$

where $\theta \in GF(2)^n$, and $\theta_{i_1} = \theta_{i_2} = \cdots = \theta_{i_{m+1}} = 1$, $\theta_{i_{m+2}} = \theta_{i_{m+3}} = \cdots = \theta_{i_n} = 0$.

Since $I(z; \mathbf{x}') \neq 0$, by Theorem 2, $C_f(\mathbf{x}') \neq 0$. So, $\hat{F}(\theta) \neq 0$. By (10), g is the maximum correlator if and only if $\hat{G}(\theta) = \mathrm{sgn}(\hat{F}(\theta))$, which is the Walsh transform of $a \oplus x_{i_1} \oplus x_{i_2} \oplus \cdots \oplus x_{i_{m+1}}$, $a \in GF(2)$. Thus, the maximum correlator of f with respect to $\mathbf{x}'$ is either $x_{i_1} \oplus x_{i_2} \oplus \cdots \oplus x_{i_{m+1}}$ or $1 \oplus x_{i_1} \oplus x_{i_2} \oplus \cdots \oplus x_{i_{m+1}}$. □

3. Correlation Analysis of Bent Functions

The notion of bent function was originally introduced in combinatorial theory [10]. In [7] it has been shown that the absolute values of the correlation coefficients of a bent function to every linear or affine function are equal, thus giving a solution to the linear correlation problem when bent functions are used as nonlinear combiners. The construction of bent functions has been studied in [7], [9], [11], [2], and [3].

Definition 3. A Boolean function $f(x_1, x_2 \ldots, x_n)$ is called a bent function if $|\hat{F}(\omega)| = 2^{-n/2}$ for all $\omega \in GF(2)^n$.

Let $z = f(x_1, x_2, \ldots, x_n)$ be a bent function. It is clear that f is not correlation-immune. Moreover, z is correlated to every subset $\mathbf{x}' = (x_{i_1}, x_{i_2}, \ldots, x_{i_m})$ of m variables, $1 \leq m \leq n$. An important problem relating to correlation attacks is how large the correlation would be. Since bent functions are not balanced, we cannot use Theorem 1 to calculate the maximum correlation $C_f(\mathbf{x}')$, nor can we use Theorem 2 to obtain upper and lower bounds for $C_f(\mathbf{x}')$. In what follows, we derive upper and lower bounds for $C_f(\mathbf{x}')$ and $I(z; \mathbf{x}')$, respectively.

Lemma 2. *Let $z = f(x_1, x_2, \ldots, x_n)$ be a bent function. For any subset $\mathbf{x}'$ of m variables $x_{i_1}, x_{i_2}, \ldots, x_{i_m}$,*

$$\sum_{\mathbf{y} \in GF(2)^n} (e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0))^2 = 2^{2m-n-2}.$$

Proof. Let $V(i_1, i_2, \ldots, i_m) = \{\omega\colon \omega \in GF(2)^n, \omega_{i_{m+1}} = \omega_{i_{m+2}} = \cdots = \omega_{i_n} = 0\}$. Then $V(i_1, i_2, \ldots, i_m)$ is an m-dimensional subspace of $GF(2)^n$. For any ω in the subspace, let $o(\omega) = (\omega_{i_1}, \omega_{i_2}, \ldots, \omega_{i_m})$, then

$$\begin{aligned}
\hat{F}(\omega) &= \frac{1}{2^n} \sum_{\mathbf{x} \in GF(2)^n} (-1)^{f(\mathbf{x})} (-1)^{\omega \cdot \mathbf{x}} \\
&= \frac{1}{2^n} \sum_{\mathbf{x} \in GF(2)^n} (1 - 2f(\mathbf{x}))(-1)^{o(\omega) \cdot \mathbf{x}'} \\
&= \frac{1}{2^m} \sum_{\mathbf{y} \in GF(2)^m} (1 - 2P(z = 1|_{\mathbf{x}'=\mathbf{y}}))(-1)^{o(\omega) \cdot \mathbf{y}}.
\end{aligned}$$

By the inverse Walsh transform,

$$1 - 2P(z = 1|_{\mathbf{x}'=\mathbf{y}}) = \sum_{\omega \in V(i_1, i_2, \ldots, i_m)} \hat{F}(\omega)(-1)^{o(\omega) \cdot \mathbf{y}}.$$

Thus,

$$P(z = 1|_{\mathbf{x}'=\mathbf{y}}) = \tfrac{1}{2} - \tfrac{1}{2} \sum_{\omega \in V(i_1, i_1, \ldots, i_m)} \hat{F}(\omega)(-1)^{o(\omega) \cdot \mathbf{y}}.$$

From the expression for $\hat{F}(0)$,

$$\hat{F}(0) = \frac{1}{2^n} \sum_{\mathbf{x} \in GF(2)^n} (-1)^{f(\mathbf{x})} = 1 - 2P(z = 1),$$

it follows that

$$P(z = 1) = \tfrac{1}{2} - \tfrac{1}{2}\hat{F}(0). \tag{11}$$

Therefore,

$$\begin{aligned}
e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0) &= P(z = 1|_{\mathbf{x}'=\mathbf{y}}) - P(z = 1) - \tfrac{1}{2}\hat{F}(0) \\
&= -\tfrac{1}{2} \sum_{\omega \in V(i_1, i_2, \ldots, i_m)} \hat{F}(\omega)(-1)^{o(\omega) \cdot \mathbf{y}}.
\end{aligned}$$

By Parseval's theorem,

$$\sum_{\mathbf{y} \in GF(2)^m} (e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0))^2 = \frac{2^m}{4} \sum_{\omega \in V(i_1, i_2, \ldots, i_m)} \hat{F}^2(\omega) = 2^{2m-n-2},$$

which completes the proof of the lemma. □

Theorem 4. *Let $z = f(x_1, x_2, \ldots, x_n)$ be a bent function. Then for any subset $\mathbf{x}'$ of m variables $x_{i_1}, x_{i_2}, \ldots, x_{i_m}$, the mutual information $I(z; \mathbf{x}')$ is bounded by*

$$(2^{m-n-1} - 2^{-n}) \log_2 e \le I(z; \mathbf{x}') \le (2^{m-n} - 2^{-n-1}) \log_2 e. \tag{12}$$

Proof. By (2), (7), and (11), the mutual information $I(z; \mathbf{x}')$ can be described as follows:

$$I(z; \mathbf{x}') = h(\tfrac{1}{2} - \tfrac{1}{2}\hat{F}(0)) - \frac{1}{2^m} \sum_{\mathbf{y} \in GF(2)^m} h(\tfrac{1}{2} + e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0)).$$

By Lemma 1,

$$1 - (\hat{F}(0))^2 \log_2 e \le h(\tfrac{1}{2} - \tfrac{1}{2}\hat{F}(0)) \le 1 - \tfrac{1}{2}(\hat{F}(0))^2 \log_2 e$$

and

$$1 - 4(e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0))^2 \log_2 e \le h(\tfrac{1}{2} + e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0)) \le 1 - 2(e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0))^2 \log_2 e.$$

From the two inequalities derived above, it follows that

$$\begin{aligned} I(z; \mathbf{x}') &\ge 1 - (\hat{F}(0))^2 \log_2 e - \frac{1}{2^m} \sum_{\mathbf{y} \in GF(2)^m} (1 - 2(e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0))^2 \log_2 e) \\ &= \frac{2 \log_2 e}{2^m} \sum_{\mathbf{y} \in GF(2)^m} (e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0))^2 - (\hat{F}(0))^2 \log_2 e \end{aligned}$$

and

$$I(z; \mathbf{x}') \le \frac{4 \log_2 e}{2^m} \sum_{\mathbf{y} \in GF(2)^m} (e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0))^2 - \tfrac{1}{2}(\hat{F}(0))^2 \log_2 e.$$

By Lemma 2,

$$(2^{m-n-1} - 2^{-n}) \log_2 e \le I(z; \mathbf{x}') \le (2^{m-n} - 2^{-n-1}) \log_2 e,$$

which completes the proof of the theorem. □

Theorem 4 shows that the mutual information between z and every subset of m variables is small if n is large and m is small. For example, if $n = 10$ and $m = 4$, then $0.01 \le I(z; \mathbf{x}') \le 0.02$. Based on Theorem 4, we can determine how many LFSRs should be combined such that the resultant combination generator can defend against certain types of correlation attacks.

Theorem 5. *Let $z = f(x_1, x_2, \ldots, x_n)$ be a bent function. Then for any subset $\mathbf{x}'$ of m variables $x_{i_1}, x_{i_2}, \ldots, x_{i_m}$, the maximum correlation coefficient $C_f(\mathbf{x}')$ is bounded by*

$$2^{m-n} - 2^{-n/2+2} \le C_f(\mathbf{x}') \le 2^{(m-n)/2} + 2^{-n/2+2}.$$

Proof. Let g be a Boolean function of $\mathbf{x}'$ and $z' = g(\mathbf{x}')$. By (11), (7), and (6), we have

$$C(f,g) = \hat{F}(0) + \frac{4}{2^m} \sum_{\mathbf{y} \in GF(2)^m} g(\mathbf{y})(e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0)). \tag{13}$$

Since $g(\mathbf{y}) \in GF(2)$,

$$\begin{aligned} C(f,g) &\le |\hat{F}(0)| + \frac{2}{2^m} \sum_{\mathbf{y} \in GF(2)^m} |g(\mathbf{y})\hat{F}(0)| + \frac{4}{2^m} \left| \sum_{\mathbf{y} \in GF(2)^m} g(\mathbf{y}) e_{\mathbf{x}'}(\mathbf{y}) \right| \\ &\le 3|\hat{F}(0)| + \frac{4}{2^m} \left| \sum_{\mathbf{y} \in GF(2)^m} g(\mathbf{y}) e_{\mathbf{x}'}(\mathbf{y}) \right|. \end{aligned}$$

By (8), it follows that

$$\begin{aligned} C(f,g) &\le 3|\hat{F}(0)| + \frac{2}{2^m} \sum_{\mathbf{y} \in GF(2)^m} |e_{\mathbf{x}'}(\mathbf{y})| \\ &\le 4|\hat{F}(0)| + \frac{2}{2^m} \sum_{\mathbf{y} \in GF(2)^m} |e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0)|. \end{aligned}$$

On the other hand,

$$\sum_{\mathbf{y} \in GF(2)^m} |e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0)| \le \left(2^m \sum_{\mathbf{y} \in GF(2)^m} (e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0))^2 \right)^{1/2}.$$

Hence,

$$C(f,g) \le 4\hat{F}(0) + \frac{2}{2^m} \left(2^m \sum_{\mathbf{y} \in GF(2)^m} (e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0))^2 \right)^{1/2}.$$

By Lemma 2, $C(f,g) \le 2^{(m-n)/2} + 2^{-n/2+2}$, which implies that $C_f(\mathbf{x}') \le 2^{(m-n)/2} + 2^{-n/2+2}$.

Next, let $\hat{g}(\mathbf{y}) = \mathrm{sgn}(e_{\mathbf{x}'}(\mathbf{y}))$. Then, by (8) and (13),

$$\begin{aligned} C(f,\hat{g}) &= \hat{F}(0) + \frac{2}{2^m} \sum_{\mathbf{y} \in GF(2)^m} |e_{\mathbf{x}'}(\mathbf{y})| - \frac{2\hat{F}(0)}{2^m} \sum_{\mathbf{y} \in GF(2)^m} \hat{g}(\mathbf{y}) \\ &\ge \frac{2}{2^m} \sum_{\mathbf{y} \in GF(2)^m} |e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0)| - 4|\hat{F}(0)| \\ &\ge \frac{4}{2^m} \sum_{\mathbf{y} \in GF(2)^m} |e_{\mathbf{x}'}(\mathbf{y}) - \tfrac{1}{2}\hat{F}(0)|^2 - 4\hat{F}(0). \end{aligned}$$

By Lemma 2, $C(f,\hat{g}) \ge 2^{m-n} - 2^{-n/2+2}$. Hence, $C_f(\mathbf{x}') \ge 2^{m-n} - 2^{-n/2+2}$. □

4. Conclusion

In this paper the maximum correlation of a Boolean function to all Boolean functions of a subset of its variables was investigated. It was shown that the correlation of a balanced Boolean function to Boolean functions of a subset of the input variables is large if the output of the balanced Boolean function is highly correlated to the subset of input variables. Hence, the correlation between the output and every small subset of input variables should be small in order to defend against correlation attacks, which coincides with the idea of Siegenthaler's correlation-immunity. For a bent function of n variables, it has been shown that the mutual information between the output and every subset of m random input variables is small if n is large and m is small, and the same is also true for the maximum correlation. Therefore, bent functions are a class of good nonlinear combining functions with respect to correlations to both linear and nonlinear Boolean functions.

Acknowledgments

The author is grateful to Joan Feigenbaum for her support. The author would like to thank the anonymous referees for their suggestions which were helpful for improving the paper. The author would also like to thank Yuguang Fang of Boston University for his valuable discussions and suggestions.

References

[1] L. Brynielsson, A short proof of the Xiao–Massey lemma, *IEEE Transactions on Information Theory*, vol. IT-35, no. 6 (1989), p. 1344.

[2] C. Carlet, Partially bent functions, *Designs, Codes, and Cryptography*, vol. 3 (1993), pp. 135–145.

[3] C. Carlet, Two new classes of bent functions, *Advance in Cryptology—EUROCRYPT* '93 *Proceedings*, Lecture Notes in Computer Science, vol. 765, Springer-Verlag, Berlin, 1994, pp. 77–101.

[4] V. Chepyzhov and B. Smeets, On a fast correlation attack on stream ciphers, *Advance in Cryptology—EUROCRYPT* '91 *Proceedings*, Lecture Notes in Computer Science, vol. 547, Springer-Verlag, Berlin, 1991, pp. 176–185.

[5] J. Dj. Golic, On the security of shift register based keystream generators, *Fast Software Encryption, Proceedings of Cambridge Security Workshop*, Lecture Notes in Computer Science, vol. 809, Springer-Verlag, Berlin, 1994, pp. 90–100.

[6] W. Meier and O. Staffelbach, Fast correlation attacks on certain stream ciphers, *Journal of Cryptology*, vol. 1, no. 3 (1989), pp. 159–176.

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

[8] M. J. Mihaljevic and J. Dj. Golic, Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence, *Advance in Cryptology—EUROCRYPT* '92 *Proceedings*, Lecture Notes in Computer Science, vol. 658, Springer-Verlag, Berlin, 1993, pp. 124–137.

[9] K. Nyberg, Constructions of bent functions and difference sets, *Advance in Cryptology—EUROCRYPT* '90 *Proceedings*, Lecture Notes in Computer Science, vol. 473, Springer-Verlag, Berlin, 1991, pp. 151–160.

[10] O. S. Rothaus, On bent functions, *Journal of Combinatorial Theory, Series A*, vol. 20 (1976), pp. 300–305.

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

[12] T. Siegenthaler, Correlation-immunity for nonlinear combining functions for cryptographic applications, *IEEE Transactions on Information Theory*, vol. IT-30, no. 5 (1984), pp. 776–780.
[13] T. Siegenthaler, Decrypting a class of stream ciphers using cipher text only, *IEEE Transactions on Computers*, vol. C-34, no. 1 (1985), pp. 81–85.
[14] G. Xiao and J. L. Massey, A spectral characterization of correlation-immune combining functions, *IEEE Transactions on Information Theory*, vol. IT-34, no. 3 (1988), pp. 564–571.
[15] K. C. Zeng, C. H. Yang, and T. R. N. Rao, An improved linear syndrome algorithm in cryptanalysis with applications, *Advance in Cryptology—CRYPTO* '90 *Proceedings*, Lecture Notes in Commputer Science, vol. 537, Springer-Verlag, Berlin, 1991, pp. 34–47.
[16] M. Zhang and G. Xiao, Nonlinearity and correlation-immunity of memoryless combining functions, *Acta Electronica Sinica*, vol. 22, no. 7 (1994), pp. 41–47.